Információs Társadalom

Biztonság és magánélet

2017. XVII. évfolyam 1. szám

Információs Társadalom

TÁRSADALOMTUDOMÁNYI FOLYÓIRAT
Alapítva 2001-ben

Megbízott főszerkesztő: Csótó Mihály

Lapterv: Szépkilátás Stúdió
Kiadványszerkesztés: VEGA^{2000} Bt.

Kiadja
Az INFONIA (Információs Társadalomért, Információs Kultúráért) Alapítvány és a Gondolat Kiadó

A folyóirat kiadásában közreműködik az Óbudai Egyetem Digitális Kultúra és Humán Technológia Tudásközpontja

Szerkesztőség: 1032 Budapest, Kiscelli utca 78. 214-es szoba
e-mail: titkarsag@infonia.hu
Gondolat Kiadó: tel: 486-1527, www.gondolatkiado.hu

Készült a Rolling Site Nyomdában
ISSN 1587-8694
A folyóirat 2008/1. számától kezdve megtalálható a Thomson Reuters indexeiben (Social Scientes Citation Index®, Social Scisearch®, Journal Citation Reports/Social/Sciences Edirion)

Biztonság és magánélet. Egy témakör két folyóiratban

A „biztonság” és a „magánélet” *(privacy)* olyan fogalmak, amelyeket kiterjedten használunk a köznyelvben, de egyúttal számos tudomány- és szakterület – köztük a filozófia, a szociológia, a jog, a közgazdaságtan, a kriminológia és nem utolsósorban a megfigyeléstudomány *(Surveillance Studies)* – kiemelt kutatási tárgya. Közismert fogalmakról van tehát szó, amelyek jelentését az utca embere magától értetődőnek tartja, és amelyekről különböző nézőpontokból már eddig is könyvtárnyi tudományos és szakirodalmi publikáció született, de amelyeket többdimenziós voltuk és komplexitásuk miatt mégis nehéz egzakt módon definiálni. Viszonyuk is ellentmondásos: van, aki a személyes magánszféráját és biztonságát mintegy iker-követelménynek tekinti, mások a biztonságot közösségi értéknek, a magánélet érvényesíthetőségét egyéni értéknek ítélik. A médiafogyasztó állampolgár pedig a „szekuritizáció” korában, és főleg az információs és kommunikációs technológiák által támogatott és inspiráltmegfigyelési eszközök és rendszerek közegében látszólag elkerülhetetlen alkuhelyzettel szembesül: amennyivel fontosabb számára az egyik érték, annyival többről kell lemondania a másik érvényesítésében. Az alkuszemléletet erősíti az is, hogy aki az egyik fogalommal kapcsolatos valamely szakterületen jártas, a másikhoz nem, vagy csak felületesen ért, és szemléletében is azonosul a sugallt alku két fő elemének valamelyikével. A magyar nyelvű szakirodalomban eleve kevés tudományos igényű publikáció született a két fogalom bármelyikének vizsgálatára, viszonyuk, összefüggéseik sokoldalúságának elemzésével pedig adósak magyarul publikáló kutatóink, szerzőink.

Olvasóink már értesültek róla, hogy a Replika és az Információs Társadalom szerkesztősége a közelmúltban elhatározta: a jövőben együttműködik egymás folyóiratszámainak, cikkeinek népszerűsítésében és egyes, mindkét periodika szakterületébe tartozó témák közös gondozásában. Kölcsönös recenziókkal, tartalomjegyzékek közlésével már találkozhattak az olvasók, jelen számunkban pedig az első közös tematikus összeállítás tanulmányait olvashatják, amelyek a két folyóiratban egyszerre jelennek meg, nyomtatott és elektronikus formában egyaránt. A közös téma a biztonság és a magánélet (privacy) viszonyrendszere. Azok a tanulmányok, amelyek elsősorban társadalomelméleti vagy szociológiai szempontból elemzik a kérdéskört vagy annak egy részterületét, a Replika hasábjain jelennek meg, az új információs technológiák alkalmazását és hatását involváló írások pedig az Információs Társadalom rovataiban.

Együttműködésünk egyúttal műfaji újdonságot is eredményez: tudomásunk szerint a magyar sajtótörténetben még nem fordult elő, hogy egy kétrészes tanulmány első része az egyik folyóiratban, második része pedig a vele egy időben publikált másik független folyóiratban jelenjen meg. Esetünkben a kétrészes, háromszerzős felvezető tanulmány első részét a Replika közli, második részét pedig az Információs Társadalom – aki tehát érdeklődik a tanulmány folytatása iránt (vagy kíváncsi az előzményére), lapozza fel a másik periodikát, vagy kattintson át a másik honlapra.

Az Információs Társadalom jelen számában *Székely Iván, Somody Bernadette és Szabó Máté Dániel* közös tanulmányuk második részében a biztonság-magánélet alku-modell érvényesülését egy sajátos területen, az Emberi Jogok Európai Bírósága esetjogában vizsgálják olyan ügyekben, ahol a megfigyelés a személyes magánszféra érvényesülésének korlátjaként szerepel a bírói döntésekben. Következtetéseikben javaslatot tesznek a szükségességi-arányossági teszt tényadatokon alapuló fázisainak erősítésére, hogy így a morális mérlegelésen alapuló utolsó fázis (a voltaképpeni alku-modell) kisebb súllyal szerepeljen a döntésekben, ezt követően pedig transzponálják a teszt logikáját a döntéstámogatás területére, ahol egyénekre irányuló megfigyelőrendszerek telepítésének példáján mutatják be a döntés meghozatalához szükséges, sok elágazásos döntési folyamatot, amelyet részletes folyamatábrán is ábrázolnak. *Pásztor Emese* a nagy nemzetközi figyelmet keltő Szabó és Vissy kontra Magyarország ügy kapcsán vizsgálja a jogi kontrollmechanizmusok szerepét a nemzetbiztonsági célú titkos megfigyelések hatókörének korlátozásában (a strasbourgi bíróságon nyertes beadványozók a Terrorelhárítási Központ bírói engedélyt nem igénylő lehallgatási jogosítványait kifogásolták). A szerző azt elemzi, hogy intézményi, hatásköri, illetve eljárási szempontból hogyan rajzolható fel egy olyan, a strasbourgi mércének és a magyar alkotmányos hagyománynak megfelelő rendszer, amely valóban alkalmas is a titkos megfigyelések hatékony külső kontrolljának megvalósítására. *Szabó Endre Győző* és *Révész Balázs* tanulmányukban a magánszféra és biztonság kérdéskörének komplexitását érzékeltetik, s a két terület közös pontjaként az adatbiztonság, és ezzel összefüggésben a tudatos, felelős felhasználói attitűd jelentőségét hangsúlyozzák. Kitérnek az új egységes európai adatvédelmi rendelet (GDPR) magánszférát és biztonságot egyaránt szolgáló leendő jogintézményeinek bemutatására is. *Kiss Attila* és *Krasznay Csaba* a felhasználói viselkedéselemzés kiberbiztonsági hasznosságát és egyúttal adatvédelmileg vitatható természetét elemzi. A szerzők megítélése szerint a kiberbiztonság védelmi oldalán állók lemaradásba kerültek a támadó oldallal szemben, és ennek ledolgozására az egyik ígéretes módszer a felhasználók viselkedésének prediktív elemzése. E módszer nyilvánvaló társadalmi kockázatainak kezelésére elvi szinten a traszparencia biztosítását, az adatalanyi kontroll érvényesíthetőségét, a hozzáférési jogok egyértelmű tisztázását és az elszámoltathatóság és ellenőrzés megvalósítását tartják alkalmasnak. *Gulyás Gábor György* a legfrissebb kutatási eredményeket foglalja össze tanulmányában a privátszféra-barát, bizalmas kommunikációt lehetővé tevő anonimizálási módszerek gépi tanulás alkalmazásával történő visszafejtése területén. Ezek a deanonimizációs eljárások tovább fokozhatják az üzleti, politikai vagy biztonsági célú megfigyelés hatékonyságát, egyúttal tovább szűkítik az adatalanyok információs önrendelkezésének lehetőségét. Konferenciabeszámoló rovatunkban *Székely Iván* a tízéves jubileumához érkezett Computers, Privacy and Data Protection (CPDP) konferenciáról, a magánélet és az adatvédelem kapcsolatának talán legnagyobb és legjelentősebb nemzetközi rendezvényéről ír, felvázolva a konferencia történetét és azt a kontextust is, amely a CPDP-t kiemeli a hasonló tárgyú szakmai rendezvények sorából.

A szerkesztők

Székely Iván – Somody Bernadette – Szabó Máté Dániel

Biztonság és magánélet: az alku-modell megkérdőjelezése és meghaladása II. rész

Jogi és döntéstámogatási megközelítések

Bevezetés a II. részhez

Ez a tanulmány a biztonság és a magánélet sokrétegű, sokszempontú viszonyát elemzi, közelebbről a közöttük fennálló feltételezett alku-helyzet érvényességét és meghaladási lehetőségeit. A tanulmány két nagy egységre tagolódik, és két részben jelenik meg, két együttműködő tudományos folyóirat egy időben megjelenő, tematikusan összehangolt lapszámaiban.[1] Az első rész a Replika 103. lapszámában olvasható, a második rész pedig az Információs Társadalom jelen számában, mindkét esetben nyomtatott és elektronikus formában egyaránt.

A tanulmány első része azt igazolta az empirikus szociológia és a matematikai statisztika módszereivel, hogy a biztonság kontra magánélet alku-modell nem tükröződik az emberek gondolkodásában, a két érték egymástól független, az emberek többsége mind a kettőt fontosnak tartja. Az elemzés ugyanakkor azt nem zárta ki, hogy az alku-modellt implikáló döntési szituációban ugyanezek az emberek hajlamosak önként alkut kötni a magánélet és a biztonság között. A tanulmány második része már kifejezetten a magánélet kontra biztonság döntési szituációkra koncentrál. A hasonló értékkonfliktusokat megítélő emberi jogi bíróságok által követett módszer alapul vételével az alku-modell meghaladását segítő módszertani javaslatokat fogalmaz meg azokra a helyzetekre, amelyekben a biztonság fokozása érdekében a magánszférába beavatkozó intézkedésekről döntenek.

Az arányossági teszt anatómiája

Első lépésként röviden bemutatjuk, hogy a demokratikus jogrendszerek miképpen kezelik az alapvető jogok és legitim érdekek konfliktusát, és azt, hogy a joggyakorlat hogyan erősíti annak illúzióját, hogy közöttük az alku elkerülhetetlen. A jogok és érdekek kollíziójának feloldására a demokratikus jogállamok felsőbíróságai többféle módszert alakítottak ki[2], amelyek közül a magyar gondolkodás számára is az európai joggyakorlatot uraló, az aláb-

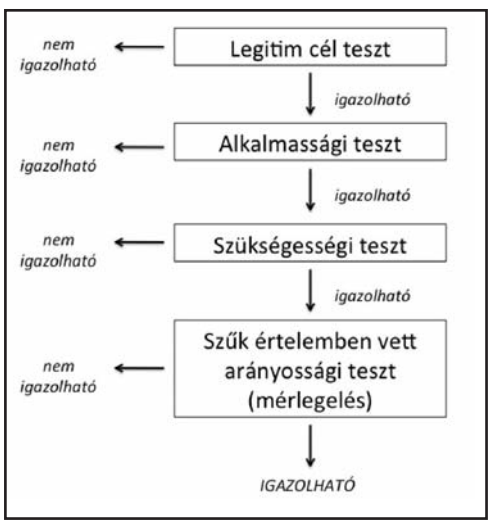
[1]A kétrészes tanulmány alapjául szolgáló multidiszciplináris kutatást a három szerző közösen végezte, a kutatás eredményeit rögzítő egyes tanulmányrészek megírásában szakmai kompetenciáiknak megfelelően működtek közre.

[2] Az Amerikai Egyesült Államokban a jogok konfliktusát a „balancing" módszerével ítélik meg, míg az európai megközelítésben ugyanerre az arányossági teszt szolgál. Végső soron azonban mindkettő hasonló funkciót lát el és hasonló eredményre is vezet; az arányossági teszt utolsó altesztje, a szűk értelemben vett arányossági teszt lényegében az amerikai „balancing" megfelelője. A két módszertan közötti fő különbség abban áll, hogy az európai teszt a végső mérlegelés fázisa előtt az amerikainál jóval analitikusabb szerkezetet követ. Bővebben lásd Cohen-Eliya és Porat (2010).

biakban elemzett arányossági teszt az irányadó. Célunk rámutatni arra, hogy a kellő módszertani fegyelem a teszt alkalmazása során segíthet az alku-modell meghaladásában.

Az arányosság koncepciója a Német Szövetségi Alkotmánybíróságtól ered, de hatása messze túlmutatott Németországon: az arányosság a második világháború utáni emberi jogvédelem paradigmájává vált. Ezt a koncepciót tette magáévá a strasbourgi Emberi Jogok Európai Bírósága (EJEB) is, amely az Európai Emberi Jogi Egyezmény (EEJE) 8-11. cikkeiben foglalt korlátozási klauzulákat az arányosság elve alapján értelmezte. A "strasbourgi módszer" a jogkorlátozás legitim céljának azonosítását, és – a "szükséges egy demokratikus társadalomban" fordulat körében – a korlátozás szükségességének és arányosságának vizsgálatát foglalja magában.

Annak megítélése, hogy egy alapvető jog adott korlátozása megengedhető-e, módszertani kihívást is jelent. Legyen szó akár alkotmányos, akár az Egyezményben biztosított jogról, a bíróság (alkotmánybíróság vagy az EJEB) ítéletét azzal igazolhatja, azzal növelheti annak meggyőző erejét és biztosíthatja autoritását, ha szorosan követi a jogkorlátozási teszt lépéseit, amelyek közül csupán az utolsó jelent morális érveket is felhasználó tényleges mérlegelést az egymással ütköző jogok és érdekek között. Mindezt megelőzően a bíróságoknak, és így az EJEB-nek is először arról kell döntenie, hogy az alkotmány vagy az EEJE által védett jog érintett-e az ügyben, másodszor pedig arról, hogy a jogkorlátozó jogszabály megfelel-e a minőségi követelményeknek. Ezt követheti tehát az arányossági teszt alkalmazása.



3. ábra: Az arányossági teszt szerkezete

Az arányossági teszt nem egyetlen teszt: négy alteszt alkotja: a legitim cél teszt, az alkalmassági teszt, a szükségességi teszt és végül a szűk értelemben vett arányossági teszt (3. ábra).

Az első alteszt szerint egy alapjog korlátozását kizárólag olyan cél igazolhatja, amely a társadalom valamely alapértékét fejezi ki. Alkotmányos demokráciákban általánosságban szólva az alapvető emberi jogok védelme és bizonyos mértékben a közérdek szolgálata vehető számításba a jogkorlátozás legitim céljaként. Az EEJE speciális jogkorlátozási klauzulákat tartalmaz, amelyek felsorolják az adott jog korlátozását igazoló legitim célokat. Megjegyzendő, hogy a jogi értékelés szempontjából a biztonsághoz fűződő közérdek, mint a legitim célok egyike nem igényel további igazolást azokban az esetekben, amikor a biztonságot vagy annak valamely aspektusát az alkalmazandó korlátozási klauzula kifejezetten nevesíti.

A második alteszt körében az az eldöntendő kérdés, hogy a jogkorlátozás – feltéve, hogy volt legitim célja – megfelel-e a kitűzött cél elérésére. Annak megítélése, hogy van-e észszerű kapcsolat a korlátozás célja és a korlátozás eszköze között, más tudományágak kutatási eredményeinek bevonását is igényelheti. Egyebek mellett a szociológia vagy a

kriminológia tudományos eredményei teszik a jogkorlátozó intézkedés alkalmasságának kérdését ténykérdéssé. Így például kriminológiai kutatások bizonyították, hogy több megfigyelő kamera használata nem szükségszerűen javítja a biztonságot.[3]

A harmadik altesztben, a cél legitimitásának és a korlátozás alkalmasságának megállapítását követően, a korlátozás szükségességét kell megvizsgálni, vagyis azt, hogy a lehető legkevésbé korlátozó eszközt alkalmazzák-e a cél elérésére. Így például a magánszférába való beavatkozást jelentő intézkedések szükségességének igazolásakor olyan eszközöket is számításba kell venni, amelyek kevésbé, vagy egyáltalán nem járnak a jogok korlátozásával. A tapasztalatok azt mutatják, hogy ugyanazon biztonsági célok elérhetők magánszféra-barát technológiákkal, akár megfigyelés nélkül is.

Az utolsó alteszt a szűk értelemben vett arányossági teszt, a bírói mérlegelés valódi terepe, amely két érték összemérését teszi szükségessé: egyrészről a korlátozás céljában kifejeződő értékét, másrészről pedig a korlátozott alapvető jogot. Valamely alapvető jog korlátozása akkor tekinthető igazoltnak, ha a jogkorlátozási cél megvalósításával elért előnyök megfelelő arányban állnak az alapjogba való beavatkozás mértékével.

Amint láthattuk, a jogkorlátozás megengedhetőségének megítéléséhez a bemutatott négy altesztben alapuló módszertani lépéssorozatot kell követni. Még ha az arányossági teszt szerkezeti elemei nem is feltétlenül egyértelműen azonosíthatók minden egyes bírósági döntésben, a módszertan szigorú alkalmazása megköveteli, hogy a soron következő altesztet csak akkor lehet elvégezni, ha a megelőző próbát a jogkorlátozás sikeresen kiállta.[4]

A magánélet/biztonság konfliktus kezelése az EJEB gyakorlatában

Bár az EEJE kifejezetten nem rögzíti az arányossági tesztet, az EJEB az Egyezmény 8–11. cikkeihez fűzött korlátozási klauzulákat az arányosság koncepciójával összhangban értelmezi, és alkalmazza a teszt módszertani lépéseit.

A strasbourgi székhelyű EJEB minden kétséget kizáróan a legjelentősebb emberi jogvédő fórum Európában, amely meghatározza az európai államok számára az alapjogvédelem minimumsztenderdjeit, és amelynek esetjoga meghatározó az Európai Unió és az Alapjogi Chartát értelmező Európai Bíróság számára is.[5] Az arányossági teszt strasbourgi alkalmazását a jogirodalom széleskörűen feldolgozta. E tanulmány megközelítésének sajátosságát az a módszertani fegyelem jelenti, amellyel az arányossági teszt egyes lépéseit követjük és elemezzük. Ebből a szempontból számos ügyet megvizsgáltunk, hogy végül javaslatot tehessünk egy olyan jogi megoldásra, amellyel az uralkodó alku-modell meghaladható.

A következőkben a strasbourgi bíróság magánszférát, azon belül is az információs magánszférát érintő esetjogára koncentrálunk, amely a személyes adatok kezelésével össze-

[3] A biztonsági célú megfigyelő rendszerek számos tanulmány szerint nem hatékonyak. Lásd: http://www.no-cctv.org.uk/caseagainst/reports.asp

[4] A frissebb joggyakorlatról lásd Barak (2012).

[5] Megjegyezzük, hogy az Európai Bíróság egy a magánszféra és a biztonság konfliktusát érintő, néhány évvel ezelőtti döntésében az arányossági tesztet rendkívül részletes, dogmatikailag rigorózus módon alkalmazta. Lásd a C-293/12. és C-594/12. számú egyesített ügyekben (Digital Rights Ireland and Seitlinger and Others) 2014. április 8-án született ítéletet az adatmegőrzési irányelv érvénytelenségéről.

függésben biztosítja az emberi személyiség védelmét. E védelmet elsősorban az EEJE 8. cikke nyújtja, amely a magán- és családi élet tiszteletben tartásához fűződő jogról szól. A 8. cikk tekintetében az arányossági teszt lényege abban áll, hogy a magánszférába való, biztonsági célú beavatkozás akkor igazolható, ha e két érték (magánszféra és biztonság) egyensúlyban áll egymással. Ez az értelmezés, úgy tűnik, hogy az alku-modellnek kedvez, amely szerint a magánszféra és a biztonság közötti konfliktus zéró összegű játszma, és az emberek kénytelenek választani közülük.[6] Az arányossági teszt szerint a bíróságoknak az összeütköző jogok és érdekek között választaniuk kell, a magánszféra és a biztonság között egyensúlyt kell kialakítaniuk, hiszen – ahogyan az arányossági teszt sugallja – a konfliktus éppen abból ered, hogy egyidejűleg mindkettő nem garantálható. Ugyanakkor, amint fentebb említettük, a gyakorlati tapasztalatok és az empirikus kutatások egyaránt azt mutatják, hogy léteznek olyan eszközök és módszerek, amelyek alkalmazásával egyszerre erősíthető meg a biztonság és a magánszféra is. Ráadásul az emberek a biztonságot és a magánszférát önálló értékeknek tekintik, és mindkettőre igényt tartanak. Ezért, miután elemezzük az arányossági teszt alkalmazását az EJEB gyakorlatában, arra a kérdésre próbálunk választ találni, hogy a magánszféra és a biztonság közötti alkukeresés meghaladható-e az arányossági teszt keretei között.

Információs magánszféra, adatvédelem és az EJEB gyakorlata

A magánszférához való jog az emberi személyiség számos különböző aspektusának védelmet nyújtó, kiemelkedő jelentőségű emberi jog. A döntési privacy biztosítja annak szabadságát, hogy dönthessünk testünkről és családi kapcsolatainkról. Ennek kontinentális megfelelője, az önrendelkezési jog alapozza meg például a terhességmegszakítást, a művi meddővétételt, az életfenntartó kezelések visszautasítását, a drogfogyasztást és a szexuális önrendelkezést is. A hagyományos magánszféra-ügyek egy része egyáltalán nem veti fel a biztonsági érdekekkel való összemérés kérdését. A biztonsági célú megfigyelés kifejezetten az információs magánszférát érinti, a magánszférához való jognak azt a speciális vetületét, amely a polgárok személyes adatainak gyűjtésével, felhasználásával és hozzáférhetővé tételével szemben biztosít védelmet.[7] A biztonság szintjének emelését célzó megfigyelés azáltal érinti a polgárokat, hogy eszközei és módszerei személyes adatok gyűjtésével, tárolásával, használatával és hozzáférhetővé tételével járnak, kizárják a saját személyes adatokhoz való hozzáférést, vagy korlátozzák a személyes információk feletti kontrollt. A magánélet/biztonság konfliktus elemzése érdekében ebben az írásban azokat az eseteket vizsgáljuk, amelyekben a polgárok magánéletébe történő beavatkozás a rájuk vonatkozó információk kezelésében testesül meg.

[6] Robert Alexy a jogok és érdekek konfliktusát a közgazdaságtanban használatos közömbösségi görbével illusztrálta (Alexy 2010: 102-105).

[7] Az információs magánszféra lényegének megragadására számos jól ismert definíció és tipológia született: a rólunk szóló tudás feletti ellenőrzés gyakorlásának lehetősége (Fried 1968: 475), egyének az iránti igénye, hogy meghatározhassák, a rájuk vonatkozó információk mikor, hogyan és milyen mértékben juthatnak mások tudomására (Westin 1967: 7), vagy egy újabb műben a privacy hét típusa (Finn et al. 2013) szintén tartalmaz információs magánszférával kapcsolatos elemeket, úgy mint a kommunikációs magánszféra, az adatok és a képmás védelme. A magánszféra különböző vetületeinek megkülönböztetéséről és az információs magánszféra meghatározásáról lásd Solove et al. (2006).

Amellett érvelünk, hogy az EJEB gyakorlatában az információs magánszféra védelme az egyezmény 8. cikkén alapul, amely biztosítja mindenki jogát magán- és családi életének, lakásának és levelezésének tiszteletben tartásához – annak ellenére, hogy ez a cikk nem használja a személyes információ vagy a személyes adat kategóriáját. Az EJEB nem tisztázta a magánszférához való jog és az adatvédelem elméleti kapcsolatát. Viszonyuk továbbra is nyitott kérdés, hiszen az az európai jogrendszereket – ideértve az EJEB ítélkezési gyakorlatát is – vizsgálva többféle logikai kapcsolatként is leírható.[8] Azon ítéletek alapján, amelyek kapcsolatot teremtenek e jogok között, érvelhetünk úgy, hogy e jogoknak van egymással átfedésben lévő közös szegmense, bár a magánszféra-védelem és az adatvédelem által kínált védelem jellege eltérő, továbbá az adatvédelem hatóköre olyan személyes információkra is kiterjed, amelyek távoli vagy közvetett kapcsolatban állnak a magánszférával.

Mindazonáltal megállapíthatjuk, hogy az EJEB ítélkezési gyakorlatában számos olyan élethelyzetet vizsgált, amelyben adatvédelmi szempontok merültek fel, és ezek mindegyikét az EEJE 8. cikke alapján bírálta el. A személyes adatok védelmének sérelme, ideértve a lehallgatási ügyeket[9], különböző megfigyelési ügyeket[10] és a hatóságok általi személyesadat-tárolással kapcsolatos ügyeket[11], a 8. cikkben biztosított jogok megsértésére hivatkozással vihető a strasbourgi bíróság elé. A megfigyelés és a személyes adatok rögzítése, tárolása szoros kapcsolatban áll a magánélet védelmével. Néhány esetben, amelyekben az EJEB-nek arról kellett állást foglalnia, hogy történt-e beavatkozás a kérelmezők magánszféra-jogaiba – vagyis amikor a 8. cikk alkalmazhatóságát vizsgálta – következetesen széles értelemben használta a magánélet fogalmát, amelynek adható kimerítő meghatározás[12], de vitathatatlanul magában foglalja az adatvédelem körébe tartozó kérdéseket is. Az EJEB szerint a nemi identitás, a név, a szexuális orientáció és a szexuális élet a 8. cikk által védett magánszféra fontos elemei.[13] A 8. cikk ugyancsak védi az identitáshoz és a személyiség kibontakozásához való jogot, valamint a másokkal és a külvilággal való kapcsolattartáshoz fűződő jogot.[14]

[8] A magánszféra-védelemnek és az adatvédelemnek a napjaink európai jogában kirajzolódó kapcsolatáról lásd Kokott és Sobotta (2013), vagy Fuster (2014), valamint Fuster és Gutwirth (2017).

[9] Például *Malone v. the United Kingdom*, no. 8691/79, 2 August 1984, *Copland v. the United Kingdom*, no. 62617/00, 3 April 2007.

[10] Például *Klass and Others v. Germany*, no. 5029/71, 6 September 1978, *Uzun v. Germany*, no. 35623/05, 2 September 2010.

[11] Például *Leander v. Sweden* no. 9248/81, 26 March 1987, *S and Marper v. the United Kingdom*, no. 30562/04, 4 December 2008.

[12] Lásd például *Glor v. Switzerland*, no. 13444/04, § 52, ECHR 2009; *Tysiąc v. Poland*, no.5410/03, § 107, ECHR 2007-I; *Hadri-Vionnet v. Switzerland*, no. 55525/00, 14 February 2008, § 51; *Pretty v. the United Kingdom*, no. 2346/02, § 61, ECHR 2002-III; és *S. and Marper v. the United Kingdom*, nos. 30562/04 and 30566/04, § 66, ECHR 2008.

[13] Lásd például *B. v. France*, 25 March 1992, Series A no. 232-C, § 63; *Burghartz v. Switzerland*, 22 February 1994, Series A no. 280-B, § 24; *Dudgeon v. the United Kingdom*, 22 October 1981, Series A no. 45, § 41; és *Laskey, Jaggard and Brown v. the United Kingdom*, 19 February 1997, *Reports* 1997-1, § 36.

[14] Lásd például *Burgartz v. Switzerland*, no. 16213/90, Opinion of the Commission, p. 37, § 47, és *Friedl v. Austria*, 31 January 1995, Series A no. 305-B, Opinion of the Commission, § 45.

A Bíróság szerint a másokkal való kapcsolatnak még a nyilvánosságban is van olyan területe, amely a magánélet körébe tartozik.[15] Magánéleti megfontolások olyan esetekben is felmerülhetnek, amelyekben szisztematikus vagy állandó nyilvántartásokat a nyilvánosságban hozzáférhető adatokból hoznak létre. Ebből következik, hogy a titkosszolgálatok által egy meghatározott személyről gyűjtött adatok a 8. cikk hatókörébe tartoznak még akkor is, ha az információkat nem beavatkozó vagy fedett módszerekkel gyűjtötték.[16] A Bíróság számos alkalommal döntött úgy, hogy a titkos telefonlehallgatás a 8. cikk hatókörébe tartozik. Bár általában a felvételeket azért készítik, hogy a beszélgetések tartalmát használják fel valamilyen módon, a Bíróság megállapította, hogy a hangminta céljára rögzített felvételek nem tekinthetők úgy, mint amelyek kívül esnek a 8. cikk által biztosított védelem körén. A hangmintát az érintett hangjából állítják elő, és kifejezetten abból a célból elemzik, hogy a személyét további személyes adatai tekintetében is azonosítsák. A kérelmező hangjának rögzítése és elemzése, amire gyanúsítotti kihallgatása során került sor, az érintett személyes adatai kezelésének tekintendő.[17]

A biztonságot mint a magánszférába való beavatkozás célját értelmező esetjog számos különféle élethelyzetet érint (például olyanokat, amelyekben fogvatartás, tartózkodási engedély megtagadása vagy másik országba történő kiutasítás miatt megakadályozták a kérelmezőket abban, hogy közeli hozzátartozóikkal kommunikáljanak). Mivel azonban mi a magánszférához való jogot korlátozó biztonsági célú megfigyelésekkel foglalkozunk, elemzésünk körét kifejezetten azokra az ügyekre szűkítettük, amelyekben a megfigyelési intézkedések az információs magánszférával kerültek összeütközésbe. Ezek az ügyek a biztonság és az információs magánszféra/adatvédelem közötti tipikus konfliktusokat vetik fel: magánközlések lehallgatása, személyek titkos megfigyelése, polgárok adatainak rögzítése lusztrációs célú adatbázisokban, bűncselekmények felderítése stb.

A biztonság mint legitim cél

A magánélet tiszteletben tartásához fűződő jogról szóló EEJE cikkhez kapcsolódó korlátozási klauzula kimerítően felsorolja azokat az okokat, amelyeket a jogkorlátozás legitim céljaként számításba lehet venni. A 8. cikk (2) bekezdése szerint a joggyakorlásba való beavatkozás a következő célokat szolgálhatja: a nemzetbiztonság, a közbiztonság vagy az ország gazdasági jóléte, zavargás vagy bűncselekmény megelőzése, a közegészség vagy az erkölcsök védelme, vagy mások jogainak és szabadságainak védelme.

Egyrészről megállapíthatjuk, hogy a biztonság a jogkorlátozás legitim céljának minősül. Másrészt viszont meg kell jegyezni, hogy a biztonságnak csak azok a vetületei elfogadhatók, amelyeket az idézett rendelkezés *kifejezetten nevesít*. A 8. cikk szövege alapján az EJEB a biztonságot kizárólag a nemzetbiztonság, a közbiztonság, illetve a zavargás vagy bűncselekmény megelőzése körében veheti számításba. A strasbourgi bíróság gyakorlatában a biztonság az említett kategóriák valamelyikeként jelenik meg.

A legitim cél azonosítása, és az arról hozott döntés, hogy a magánszférához való jog korlátozása szolgálja-e ezt a célt, tények és azok közötti logikai összefüggések kérdése. A teszt

[15] Lásd *von Hannover v. Germany (No. 2)*, nos. 40660/08 and 60641/08, § 95.
[16] Lásd *Rotaru v. Romania*, no. 28341/95, §§ 43-44, ECHR 2000-V, *P.G. and J.H. v. the United Kingdom* no. 44787/98, 25 September 2001, § 59.
[17] *P.G. and J.H. v. the United Kingdom*, § 59.

e lépései – legalábbis elméletileg – nem hagynak teret mérlegelésre, amely csak a teszt utolsó fázisában, a szűk értelemben vett arányossági vizsgálatban jelenik meg. Az a kérdés, hogy adott élethelyzetben a biztonság (illetve annak valamely nevesített aspektusa) áll-e konfliktusban a magánszférához való joggal, igennel vagy nemmel megválaszolható, eldöntendő kérdés.

A biztonsághoz fűződő közérdek mint jogkorlátozási cél kifejezetten megjelenik az Egyezmény szövegében, fennállta pedig ténykérdés. Ezek alapján valamely konkrét ügyben annak eldöntése, hogy a magánszférába való beavatkozás valóban a biztonságot szolgálja-e, az arányossági teszt szigorúan alkalmazandó részkövetelménye lehetne. A gyakorlatban azonban a legitim cél vizsgálata e módszertan leggyengébb összetevőjének bizonyul.

Az EJEB magánszférával és biztonsággal kapcsolatos gyakorlatában a magánszférához fűződő jog számos komponense azonosítható, ám a biztonsággal összefüggő jogkorlátozási célok tekintetében ez nem jellemző. A 8. cikkben felsorolt releváns jogkorlátozási célok (nemzetbiztonság stb.) tartalmát a bíróság ilyen precizitással nem bontja ki. A döntésekben nem találunk absztrakt definíciókat vagy olyan magyarázatokat, amelyekből a biztonság egyes aspektusainak vagy általában magának a biztonságnak a fogalma rekonstruálható lenne. E kategóriák jól meghatározott kontúrjainak hiányát mutatja az is, hogy a Bíróság rendszerint a korlátozásnak nem egyetlen célját jelöli meg, amely az adott ügyben a biztonság releváns aspektusaként kiválasztható lenne. Az EJEB gyakran a 8. cikk (2) bekezdésében felsoroltak közül két vagy három biztonsággal összefüggő célt is megnevez, anélkül, hogy rámutatna a különféle célok adott esettel kapcsolatos jelentőségére.

A Bíróság leggyakrabban alkalmazott formulájában egyszerűen *egyetlen mondatban felsorolja* a szóba jöhető célokat, így például „*a nemzetbiztonságot vagy az ország gazdasági jólétét, vagy ezzel egyenértékűen, a zavargás vagy bűncselekmény megelőzését*".[18] Más esetekben az ítélet a legitim célt *még csak nem is specifikálja*, a bíróság pusztán deklarálja, hogy „*a korlátozások a 8. cikk (2) bekezdésében felsorolt egy vagy több legitim célt szolgáltak*."[19] A felhívott legitim célok esetlegességét leginkább az mutatja, amikor az ítélet szövegezése *példálózó jellegű*, például a Bíróság kimondja: „*A Bíróság szerint kétségtelen, hogy a kérelmező levelezésének megfigyelése a 8. cikk (2) bekezdésében megjelölt legitim célokat szolgálta*, többek között, *a 'nemzetbiztonság' védelmét és/vagy a 'zavargás vagy bűncselekmény' megelőzését.*"[20]

Azokban az ügyekben, amelyekben a jogkorlátozást biztonsággal összefüggő célok igazolták, alig néhány mondatot találhatunk a releváns legitim célokról, és ezekben az EJEB megelégszik a cél puszta megjelölésével. A Bíróság általában meg sem kísérli, hogy meghatározza a felhívott legitim cél mibenlétét, és nem kínál semmiféle indokolást arra, hogy hogyan és miért szolgálja az állami beavatkozás az adott legitim célt.

Az érvelés hiányát jól szemléltetik az ítéleteknek a legitim célok fennálltának vizsgálatáról szóló bekezdéseiben használt olyan megfogalmazások, mint például „*A Bíróság megalapozottnak találja*"[21] vagy „*[a] Bíróság kész elfogadni*"[22], amire a Kormány hivatkozik,

[18] A példa forrása: *Mubilanzila Mayeka and Kaniki Mitunga v. Belgium*, no. 13178/03, 12 October 2006, § 79.
[19] Lásd például: *Nada v. Switzerland*, no. 10593/08, 12 September 2012, § 174.
[20] *Erdem v. Germany*, no. 38321/9, 5 July 2001, § 60.
[21] *Nada v. Switzerland*, § 174.
[22] *Liu v. Russia (No. 2)*, no. 29157/09, 26 July 2011, § 80.

vagy „*a Bíróság szerint kétségtelen*”[23] a cél fennállása. Ugyanez a helyzet, amikor „*a Bíróság elfogadja a Kormány állítását*” a célról.[24] Amennyiben a kérelmező nem állítja az ellenkezőjét, már az is elegendő lehet ahhoz, hogy az EJEB megalapozottnak ítélje a legitim célt: *“a kérelmező nem tagadta, hogy a kifogásolt korlátozások legitim célokat szolgáltak”*.[25] Amikor pedig a felek nem állítják vagy tagadják valamely legitim cél fennállását, az EJEB maga siet a segítségükre: *“Míg a kérelmező vitatta a legitim cél létezését, a Kormány az ügyben nem hivatkozott egyetlen legitim célra sem. A Bíróság a maga részéről kész elfogadni, hogy a kifogásolt intézkedés a nemzetbiztonságnak és a zavargások megelőzésének legitim céljait szolgálta.”* [26]

Valamely legitim cél fennálltának valószínűsége vagy lehetősége is elegendő lehet a Bíróság számára: így például a beavatkozás a releváns célok „*érdekében történhetett*” vagy „*a Bíróság ezért úgy döntött, hogy a beavatkozás releváns célt szolgált…*”.[27]

Mindezek alapján arra a következtetésre juthatunk, hogy a Bíróság álláspontja szerint a magánszférába való beavatkozás biztonsággal összefüggő legitim céljainak felhívása alapvetően a kormányok hatáskörébe tartozik, amelyet az EEJE nem érint, és az EJEB sem vizsgálhat felül. Mindez pedig ahhoz vezet, hogy a strasbourgi fórumok csak igen ritkán állapítják meg az Egyezményben biztosított jogok sérelmét a legitim cél követelményének megsértése miatt.[28]

A magánszférába való beavatkozás szükségessége és arányossága

Amint ezt fentebb bemutattuk, az EJEB kevéssé hajlandó felülvizsgálni a kormányok hivatkozásait a különféle biztonsági érdekekre, ebből következően pedig a hangsúly átkerül az arányossági teszt későbbi lépéseire. Ezekben a fázisokban ugyanakkor a bírósági érvelés általános iránya hasonlóságot mutat: a vizsgálat középpontjában a „*szükséges egy demokratikus társadalomban*” sztenderdet helyezi (van Dijk et al. 2006: 335). Ez egyúttal azt is jelenti, hogy a magánszférába való beavatkozás igazolása elsősorban mérlegelési kérdéssé válik. A magánélet védelme az állami érdekekkel szemben tehát a bírósági mérlegelés függvénye, amely a biztonsági érdek és a magánszféra súlyának összemérésében ölt testet.

Az arányossági teszt módszertanát, egyebek mellett, ki kell egészítenünk az EJEB gyakorlatában kimunkált tagállami mérlegelési mozgástér (*margin of appreciation*) fogalmával.

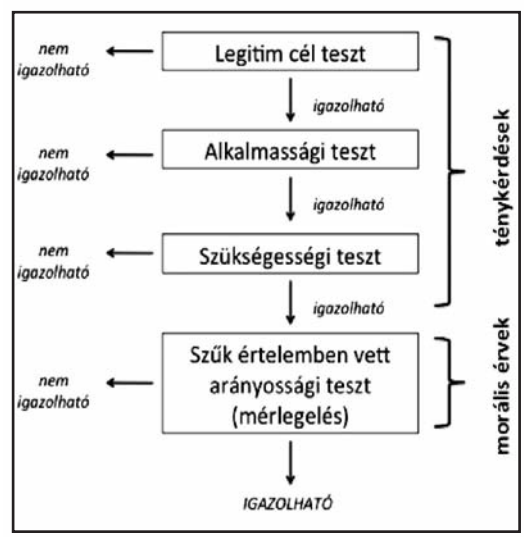
[23] *Erdem v. Germany*, § 60.
[24] *Drakšas v. Lithuania*, no. 36662/04, 31 July 2012, § 58.
[25] *Nada v. Switzerland*, § 174.
[26] A példa forrása: *Ciubotaru v. Moldova*, no. 27138/04, 27 April 2010, § 55.
[27] A példa forrása: *Mubilanzila Mayeka and Kaniki Mitunga v. Belgium*, § 79.
[28] Ugyanez igaz általában, a biztonsággal összefüggőeken kívüli legitim célokra is (van Dijk et al. 2006: 340). Érdemes megjegyezni, hogy az állami (tömeges) megfigyeléssel összefüggő magánszféra-sértésekkel kapcsolatban a Bíróság elnagyoltan ragadja meg az egyéni jogok és érdekek sérelmét is. Néhány esetben a Bíróság hajlik arra, hogy megalapozottnak találjon nem tényleges, bekövetkezett, hanem hipotetikus sérelmeket, vagy azok valószínű voltát (például *Malone v. the United Kingdom* ügyben). Más esetekben a Bíróság elismeri a még be sem következett, de várható sérelmet, vagy az intézkedés dermesztő hatását (*chilling effect*) az igény alapjául (lásd például *Marckx v. Belgium*). Bizonyos esetekben a Bíróság az absztrakt sérelmet is elfogadja, annak ellenére, hogy jogszabályok és kormányzati politikák jogellenességére alapozott sérelmeket állító kérelmeket általában nem szokott befogadni (például *Liberty and others v. the United Kingdom*). – Lásd: van der Sloot (2016).

E doktrína európai egyetértés hiányában bizonyos fokú szabadságot enged a nemzeti kormányoknak, amit a strasbourgi bíróság figyelembe vesz a korlátozás igazoltságának és arányosságának megítélésekor. A magánszférába való biztonsági célú beavatkozás tekintetében ennek különös jelentősége van, mivel ezekben az ügyekben az EJEB a tagállamok széles mérlegelési mozgásterét ismeri el.

Az egyik legtöbbet hivatkozott, a biztonsági célú megfigyelés igazoltságával foglalkozó ítéletében az EJEB a következőképpen foglalta össze a jogi értékelés releváns módszertani lépéseit, nevezetesen a szükségesség, az arányosság és a tagállami mérlegelési mozgástér megítélését: „*A szükségesség fogalma magában foglalja, hogy a beavatkozás kényszerítő társadalmi igénynek felel meg, és azt is, hogy arányos a kitűzött jogszerű céllal [...]. Ugyanakkor a Bíróság elismeri, hogy a nemzeti hatóságok mérlegelési joggal bírnak, amelynek terjedelme nem csupán a beavatkozás céljától, hanem annak pontos jellegétől is függ. Jelen ügyben a kérelmezett állam nemzetbiztonság-védelmi érdekét a kérelmező magánéletének tiszteletben tartásához fűződő jogába való beavatkozás súlyosságával együtt kell mérlegre tenni.*”[29]

Az alku-modell meghaladása a teszt keretében

Bár az arányossági teszt lépései és szerkezete a jogirodalomban és a bírósági gyakorlatban egyaránt jól ismert, csak kevesen elemezték annak a lehetőségét, hogy a teszt egyes fázisait aszerint osztályozzák, hogy az adott alteszt inkább ténybeli vagy morális megfontolásokon alapul. Ha összevetjük a teszt szerkezeti felépítését a fentebb elemzett ügyekkel, illetve az EJEB gyakorlatával általában, azt találjuk, hogy az első három alteszt ténykérdéseken alapul, és csupán az utolsó lépés igényel morális megfontolásokat, vagyis a tulajdonképpeni mérlegelést, amely az alku-megközelítésen alapulhat (4. ábra).



4. ábra: Tényleges és morális érvek az arányossági tesztben

Az a bírósági gyakorlat, amelyben az altesztek keverednek vagy legalábbis nincsenek kellőképpen elválasztva, illetve amelyben az első három altesztet összevonják, könnyen vezethet arra az eredményre, hogy az eljárás egésze morális mérlegeléssé válik. Ez a módszertani oka annak, hogy az alku elkerülhetetlennek tűnik. A tanulmány első tézise ezért azt állítja, hogy az arányossági teszt ténybeli és morális fázisainak jobb elválasztása, valamint az, ha a ténybeli és a morális elemek súlyát az előbbiek javára megváltoztatjuk,

[29] *Leander v. Sweden*, no. 9248/81, 26 March 1987, §§ 58-59.

módszertani fegyelemmel párosulva, megalapozottabb bírói döntésekre vezethet a magánszféra/biztonság konfliktusokban, továbbá csökkentheti az alku-modell alkalmazási terét.

Mindemellett a strasbourgi esetjogban számos más elv és tényező is azonosítható, amelyeket szintén számításba kell venni az arányossági teszt keretei között a magánszféra/biztonság konfliktusok értékelésekor. Megfogalmazhatunk néhány kiegészítő tételt, amelyek tovább pontosítják a teszt lépéseit és támogatják a nemzeti bíróságokat és más hatóságokat az arányossági teszt használatában a megfigyelés és az információs magánszféra közötti konfliktusokban. Ilyen kiegészítő tétel, miszerint a 8. cikk (2) bekezdését megszorítóan kell értelmezni. Mivel a magánélet tiszteletben tartásához fűződő jog alóli kivételeket jelentenek, a megengedhető korlátozásokat, mint amilyen a megfigyelés, szigorú vizsgálatnak kell alávetni. Ezt az általános elvet az EJEB is elismeri: "*[A] titkos megfigyelési jogosítványok, amelyek a rendőrállamokat jellemzik, az Egyezmény alapján csak akkor elfogadhatóak, ha a demokratikus intézmények védelméhez elengedhetetlenül szükségesek.*"[30]

Napjainkban a megfigyelés elsősorban különféle megfigyelési technológiák alkalmazásával valósul meg.[31] Ebből következik a második kiegészítő tétel, miszerint a teszt alkalmazása során az adott ügyben alkalmazott megfigyelési technológia sajátosságait is figyelembe kell venni. Ez magától értetődőnek tűnhet, azonban a technológiai sajátosságok strukturált vizsgálata egyaránt lényeges a beavatkozás szükségességének és arányosságának megítélésekor is. Egy beavatkozó megfigyelési technológia használata csak akkor tekinthető szükségesnek, ha valamely kevésbé beavatkozó megfigyelési módszer nem vezet eredményre. Ami pedig a szűkebb értelemben vett arányosságot illeti, a biztonsági érdek és a magánszférához fűződő jog közötti egyensúlyt szintén érinthetik a technológiai eszközöknek vagy azok használatának a jellemzői. Számos kérdés lehet e körben releváns, mint például az alkalmazott technológia összekapcsolása más technológiákkal, az adatokhoz való hozzáférés vagy éppen a megfigyelési technológia alkalmazásának ideje és időtartama.[32]

Harmadrészt hangsúlyoznunk kell, hogy a biztonsági indokok jelentősége függhet a történelmi körülményektől is. Az EJEB több esetben megállapította, hogy napjaink demokratikus társadalmait a kémkedés és a terrorizmus igen modern és kidolgozott formái fenyegetik, amiből a Bíróság szerint is az következik, hogy az államoknak a fenyegetések hatékony elhárítása érdekében képesnek kell lenniük a területükön tevékenykedő felforgató és romboló elemeket titokban megfigyelni. A Bíróság ezért elfogadja, hogy kivételes feltételek mellett bizonyos megfigyelési intézkedések szükségesek egy demokratikus társadalomban a nemzetbiztonság és/vagy a zavargások és bűncselekmények megelőzése érdekében.[33] A terrorveszély intenzitása az évek során folyamatosan változik, és a Bíróság erre tekintettel is van: elfogadja az aktuális terrorcselekmények kontextusában értékelt

[30] *Klass and Others v. Germany,* § 42.

[31] Ezeket megfigyelés-orientált biztonsági technológiáknak, *surveillance-oriented security technologies*nak (SOST) is nevezik. Természetesen számos olyan biztonsági célú technológia létezik, amelyek nem megfigyelés-orientáltak.

[32] *Uzun v. Germany,* §§ *78-80.*

[33] *Klass and Others v. Germany*. A legújabb gyakorlatból pedig: *Roman Zakharov v. Russia*, no. 47143/06, 4 December 2015.

terrorveszélyt, mint ami a törvényhozás beavatkozó intézkedéseit indokolja, de arra is figyelmeztet, hogy az ilyen intézkedések fenntartása vagy megerősítése hosszabb ideig nem lehet indokolt.[34] Az időmúlás ugyancsak csökkentheti az összegyűjtött személyes adatok jelentőségét és ezért gyengítheti a kapcsolatot a személyesadat-megőrzés és annak legitim célja, a biztonság között. A további megőrzést már nem feltétlenül támasztják alá az eredeti indokok, amelyek hosszabb idő elteltével irrelevánssá és elégtelenné válhatnak.[35]

Végül meg kell jegyeznünk, hogy a megfigyelési intézkedések által szolgált biztonság és az információs magánszféra közötti egyensúly megállapításához tekintetbe kell venni bizonyos eljárási garanciákat is. Ezeknek a biztosítékoknak a körébe tartoznak a hatékony nemzeti bírósági eljárások; az EJEB vizsgálja, hogy a nemzeti eljárásokat megfelelő eljárási garanciák övezték-e. A Bíróság hangsúlyozza, hogy még abban az esetben is, ha a nemzetbiztonság forog kockán, a törvényesség és a jogállamiság egy demokratikus társadalomban megköveteli, hogy az alapvető emberi jogokat érintő intézkedések a döntés indokainak és a releváns bizonyítékoknak a felülvizsgálatára jogosult független szerv előtt megmérettessenek, amennyiben szükséges, a minősített adatok megfelelő védelme mellett. Az egyéneknek jogosultaknak kell lenniük arra, hogy vitassák a hatóságok állítását a nemzetbiztonság veszélyeztetettségéről. E biztosítékok hiányában a hatóságok önkényesen avatkozhatnának be az EEJE által védett jogok gyakorlásába.[36]

A teszt alkalmazása a döntéstámogatásban

A magánszféra/biztonság alku bevett megközelítés a bírói gyakorlatban, de ugyancsak népszerű azokban a döntéshozatali helyzetekben, amelyekben magánszféra-korlátozó intézkedéseket vezetnek be a nagyobb biztonság érdekében. Ez a megközelítés nem csak azon kommunikációs és reklámszakemberek számára természetes, akik feladata, hogy „eladják" és társadalmilag elfogadottá tegyék az üzleti, politikai vagy más érdekekből következő biztonsági intézkedéseket, hanem azok körében is, akiknek a bevezetendő intézkedések megengedhetőségéről kell döntést hozniuk.

A fenti elemzés és az abból következő megállapítások megmutatják, hogy a kellő módszertani szigor megtartásával elmozdulhatunk az alku-modelltől még a jog területén is. A tanulmány következő részében azt vizsgáljuk meg, hogy az arányossági teszt módszertana átvihető-e a döntéstámogatás területére, pontosabban a magánszféra-sérelem lehetőségével járó megfigyelési intézkedések bevezetésével kapcsolatos döntési helyzetekre.

Természetesen jelentős különbségek vannak a két alkalmazási terület között: a tesztet eredendően az állam és a polgárok közötti vertikális viszonyokra fejlesztették ki, a döntéshozatali környezetben viszont a teszt a döntéshozót szolgálja egyfajta döntéstámogatási eszközként, a döntés hatósági ellenőrzésekor jut szerephez, vagy a döntés védelmét segíti a politikai és társadalmi viták során. További eltérés, hogy a bíróságoknak nem feladatuk,

[34] *Nada v. Switzerland*, § 186. Az ítélet a 2001. évi terrortámadások utáni félelem éveire utal.
[35] *Segerstedt-Wiberg and Others v. Sweden*, no. 62332/00, 6 June 2006, § 90.
[36] *Liu v. Russia (No. 2)*. A *Klass and Others v. Germany* és a *Leander v. Sweden* ügyekben az eljárási garanciák voltak a döntésekben a legmeghatározóbbak.

hogy olyan megoldási javaslatokat tegyenek, amelyek elfogadhatóbbá teszik a magánszférába beavatkozó megfigyelési intézkedéseket, sem pedig az, hogy felhívják a döntéshozó figyelmét a mindenki számára előnyös megoldási lehetőségekre, habár a döntéshozókat kifejezetten ösztönözni kellene ezek alkalmazására.

E különbségek miatt a teszt egyes lépéseit, sorrendjüket és jelentőségüket szükségszerűen át kell alakítani, az egyes fázisok részletezést is igényelnek, mialatt meg kell őrizni a teszt alapvető elemeit, valamint a ténybeli és a morális érvek elkülönítését.

Az alábbi felsorolás azokat a kérdéseket veszi sorra, amelyeket a döntéshozónak a magánszférát érintő megfigyelési intézkedések bevezetéséről (fenntartásáról, kiterjesztéséről) szóló döntés meghozatala előtt meg kell válaszolnia. Meg kell jegyeznünk, hogy ezen a területen léteznek az utóbbi években kifejlesztett döntéstámogató eszközök, amelyek ugyancsak kérdéssorokat ajánlanak.[37] Az ilyen jellegű eszközök *támogathatják* a döntéshozatali eljárást, de a döntéshozók belátására bízzák, hogy mely kérdéseket teszik fel és milyen jelentőséget tulajdonítanak az arra adott válasznak. Ezzel ellentétben az általunk javasolt módszer megköveteli az alkalmazójától, hogy a kérdéseket lépésről lépésre végigkövesse, és csak akkor lépjen tovább a következő kérdésre, ha a megelőzőt sikeresen megválaszolta (hasonlóan az arányossági teszt logikájához), máskülönben a döntés nem lesz igazolt.

A kérdések listája

A döntéstámogató rendszer felhasználójának az alábbi kérdéseket egyenként a legjobb tudása szerint kell megválaszolnia. Amennyiben nem áll rendelkezésére a szükséges információ egy-egy kérdés megfelelő megválaszolásához, azt be kell szereznie, mielőtt végez az adott kérdéssel és a következőre lép. A válasz tartalmától függően a következő kérdésre térhet át, vagy valamilyen változtatást kell eszközölnie a tervezett megfigyelésen, vagy – ha a változtatás nem kivihető – el kell állnia a tervezett megfigyelés megvalósításától. A folyamat egészét az 5. ábra foglalja össze.

1.1 A tervezett megfigyelés érinti-e az egyének magánszféráját?
Bármely megfigyelési technológia alkalmazása érintheti az egyének magánszféráját, de kétségtelen, hogy e főszabály alól vannak kivételek. Kérdés, hogy az adott megfigyelés e kivételek körébe tartozik-e.

1.2 Ha a megfigyelés jelenleg nem érinti a magánszférát, feltételezhető, hogy a jövőben érinteni fogja?
Elképzelhető, hogy a járművek forgalmát megfigyelő, alacsony felbontást használó kamerarendszer jelenleg nem teszi lehetővé a kamera látóterébe kerülő személyek azonosítását, de ha újabb, nagyobb felbontású képet készítő kamerákkal helyettesítik a régieket, a gyalogosok és az autóvezetők közvetlenül azonosíthatóvá válnak.

2.1 A kérdéses megfigyelésnek van jogalapja? Azonosítsa a megfigyelés jogalapját!
A jogszabályok általában nem tartalmaznak kifejezett felhatalmazást vagy tiltást valamely konkrét megfigyelőrendszer felállítására. Ehelyett egy általánosabb jogalap, mint például az érintettek informált beleegyezése, lehet szükséges.

2.2 Szigorúan értelmezte a jogalapot? A jogalap a szigorú értelmezés szerint is megfelelő alapot szolgáltat?

[37] Lásd például IRISS Consortium (2014).

Például a tájékozott hozzájárulás sem tekinthető megfelelő jogalapnak, ha megadása nem önkéntes (például egy munkavállaló hozzájárulása zártláncú kamerarendszer kialakításához a munkahelyén). Kifejezett felhatalmazás esetén annak hatályát megszorítóan kell értelmezni (például a kifejezetten a munkavállalók megfigyeléséről szóló jogalap nem alkalmazható tanulókra).

2.3 A kérdéses megfigyelés ütközik-e kifejezett tilalomba?
Kifejezett jogi előírások tilthatják bizonyos élethelyzetekben a megfigyelést, amelyekben az az emberi méltóságot sértheti (például öltözőkben).

3 Meg tudja határozni a kérdéses megfigyelés célját olyan pontosan, amennyire csak lehetséges?
Önmagában a megfigyelő rendszerek elterjedt volta, és az, hogy különböző célok elérésére hatékonynak tűnnek, e körben nem kielégítő válasz. A célnak a lehető legpontosabban meghatározottnak kell lennie (például a lopások rögzítése és az elkövetők azonosítása).

4.1 Meg tudja határozni azt a biztonsági kockázatot, amelyre a megfigyelés reagál?
A megfigyelés céljára vonatkozó kérdéshez hasonlóan a konkrét biztonsági kockázatot is a lehető legpontosabban kell meghatározni (például vandalizmus, rablás, munkavállalók tétlensége).

4.2 A kérdéses megfigyelés alkalmas a biztonsági kockázat csökkentésére?
Szociológiai, kriminológiai, pszichológiai stb. módszerekkel bizonyítani kell, hogy a megfigyelőrendszer az előzőekben meghatározott kockázatok csökkentésének megfelelő eszköze.

5.1 A megfigyelés által szolgált cél (amelyet a 3. kérdésben azonosított) elérhető megfigyelés nélkül is?
A döntéshozónak meg kell fontolnia a megfigyelés alternatíváit. A magánszférát nem érintő megoldásokat (például a tulajdon fizikai védelme) előnyben kell részesíteni.

5.2 Ha a cél elérhető megfigyelés nélkül is, az alternatív módszer érint-e a magánszférán kívül más jogokat vagy érdekeket?
Az alternatív megoldások számbavételekor azoknak más jogokra és legitim érdekekre ható következményeire is tekintettel kell lenni (például a tulajdon fizikai védelme a tulajdon tárgyában károkat okozhat). Más joggal vagy legitim érdekkel való konfliktus hasonló kérdéslista megválaszolását teheti szükségessé.

5.3 Hogyan határozhatóak meg az alkalmazni tervezett megfigyelési technológia jellemzői?
Például milyen személyes vagy különleges adatok gyűjtésére kerül sor? Ki fér majd hozzá ezekhez az adatokhoz? Hol, mikor és mennyi ideig alkalmazzák majd a megfigyelést?

5.4 Az 5.3. kérdésnél azonosított jellemzők egyenkénti figyelembevételével, a megfigyelés (3. kérdésnél azonosított) célja elérhető-e olyan megfigyeléssel, amely kisebb mértékű beavatkozást jelent a magánszférába?
Például a távoli megfigyelés nem igényli, hogy a zártláncú kamerarendszer megőrizze a felvételeket.

6.1 A kérdéses megfigyelés által érintett egyéneknek van lehetőségük ellenőrzést gyakorolni a megfigyelésük felett?
Az egyének az őket érintő megfigyelések befolyásolására jogokkal rendelkezhetnek, így jogosultak lehetnek tájékoztatást kapni a velük kapcsolatba hozható adatokról vagy azok helyesbítését kérni. Az egyének számára praktikus védelmet biztosít, ha lehetőségük van az adataikat töröltetni, helyesbíttetni, illetve kiegészíttetni.

6.2 Meg tudná határozni az egyének ilyen lehetőségeit?
Például proaktív módon tájékoztatták őket? Kaptak a részletekről további információkat? Lehetőségük volt tiltakozni a megfigyelés vagy annak bizonyos részei ellen stb.?

6.3 Ezek a lehetőségek minden törvényben előírt követelményt kielégítenek?
Például lehetőséget kell biztosítani arra, hogy az adatalanyok személyesen megtekinthessék a személyes adataikról készült és tárolt felvételeket az adatkezelő hivatali helyiségében, és tájékoztatni kell őket jogérvényesítési lehetőségeikről. A zártláncú kamerarendszer üzemeltetőjének ezeket a szabályokat be kell tartania.

6.4 A fentebb említett intézkedéseket (6.1-6.2 kérdések) – a jogi követelmények teljesítésén túl – magánszféra-barát módon hajtják végre?
A jogszabályi rendelkezések általában hagynak mozgásteret a kötelezettségek teljesítésének konkrét módját illetően.

7 Ez a végső mérlegelés a 3. kérdésben azonosított cél és a magánszféra-jogok között.

A döntéstámogatási folyamat összefoglalása

A következő részletes folyamatábra a fenti kérdéssor logikáját követi, elágazásokkal, feladatokkal, visszacsatolásokkal és befejezési pontokkal kiegészítve (*5. ábra*).

Összefoglalás

Láthattuk, hogy az arányossági teszt használata nem pusztán elméleti jogi kérdés, hanem az ítélkezési gyakorlatban is nagy jelentőséggel bír. Első tézisünk szerint, ha nagyobb hangsúlyt fektetünk a teszt első három fázisára, vagyis a ténykérdéseket jelentő altesztekre, továbbá ha kellő módszertani szigort alkalmazunk, akkor a mérlegelés köre jelentősen szűkül, és így az alku-megközelítés is meghaladható. Ezek a hatások még inkább érvényesülhetnek, ha figyelembe vesszük a kiegészítő javaslatainkat.

Megmutattuk azt is, hogy e módszertan, amelyet eredetileg az állam és a polgárok közötti kapcsolatokra dolgoztak ki, sikeresen alkalmazható ettől eltérő környezetben is, nevezetesen olyan döntéstámogatási eljárásokban, amelyek az emberek magánszféráját potenciálisan sértő megfigyelési intézkedések bevezetéséről szólnak. Ez az új környezet megkívánta, hogy módosítsuk a teszt lépéseinek sorrendjét és egymáshoz viszonyított súlyát, továbbá részletesebb kérdéseket kellett megfogalmaznunk a tervezett megfigyelési intézkedések jellemzőivel és a magánszférát érintő következményeikkel kapcsolatban. Mindazonáltal megőriztük az arányossági teszt alapvető összetevőit, és a ténybeli és morális érvek különválasztását is. Ezeket a módszertani lépéseket olyan kérdések formájában fogalmaztuk meg, amelyeket maga a döntéshozó tehet fel. A teljes eljárást részletes folyamatábrával illusztráltuk.

Javaslataink, ha alkalmazzák őket, lehetővé tehetik a biztonság és a magánszféra közötti alku-modelltől való elmozdulást a joggyakorlatban éppúgy, mint a döntéshozatali környezetben.

Irodalom

Alexy, Robert, *A Theory of Constitutional Rights*, Oxford University Press, New York, 2010.

Barak, Aharon, *Proportionality: Constitutional Rights and their Limitations*, Cambridge University Press, New York, 2012.

Cohen-Eliya, Moshe and Iddo Porat "American balancing and German proportionality: The historical origins", *International Journal of Constitutional Law*, Vol. 8. (2010) No. 2., pp. 263-286. https://doi.org/10.1093/icon/moq004

van Dijk, Pieter, Fried van Hoof, Arjen van Rijn and Leo Zwaak (eds.), *Theory and Practice of the European Convention on Human Rights*, Intersentia, Antwerpen – Oxford, 2006.

Finn, Rachel L., David Wright and Michael Friedewald, "Seven Types of Privacy", in Serge Gutwirth, Ronald Leenes, Paul de Hert and Yves Poullet (eds.), *European data protection: Coming of age,* Springer, Cham, Switzerland, 2013, pp. 3–32. https://dx.doi.org/10.1007/978-94-007-5170-5_1

Fried, Charles, "Privacy", *Yale Law Journal*, Vol. 77. (1968) No. 3., pp. 475-493. https://dx.doi.org/10.2307/794941

González Fuster, Gloria, *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, Springer International Publishing Switzerland, 2014.

González Fuster, Gloria and Serge Gutwirth, "The legal significance of individual choices about privacy and personal data protection", in Michael Friedwald, J. Peter Burgess, Johann Čas, Rocco Bellanova, Walter Peissl (eds.), *Surveillance, Privacy and Security. Citizens' Perspectives*, Routledge, 2017.

IRISS Consortium, *Handbook on Increasing Resilience in a Surveillance Society: Key considerations for policy-makers, regulators, consultancies, service providers, the media, civil society organisations and the public*, IRISS project, EC Grant Agreement No. 285593, 2014, http://irissproject.eu/?page_id=9

Kokott, Juliane and Christoph Sobotta, "The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR", *International Data Privacy Law*, Vol. 3. (2013) No. 4., pp. 222-228. http://dx.doi.org/10.1093/idpl/ipt017

van der Sloot, Bart, "Is the human rights framework still fit for the Big Data era? A discussion of the ECtHR's case law on privacy violations arising from surveillance activities", in Serge Gutwirth, Ronald Leenes and Paul De Hert (eds.), *Data Protection on the Move*, Springer Science+Business Media B.V., Dordrecht, 2016, pp. 411-436. http://dx.doi.org/10.1007/978-94-017-7376-8_15

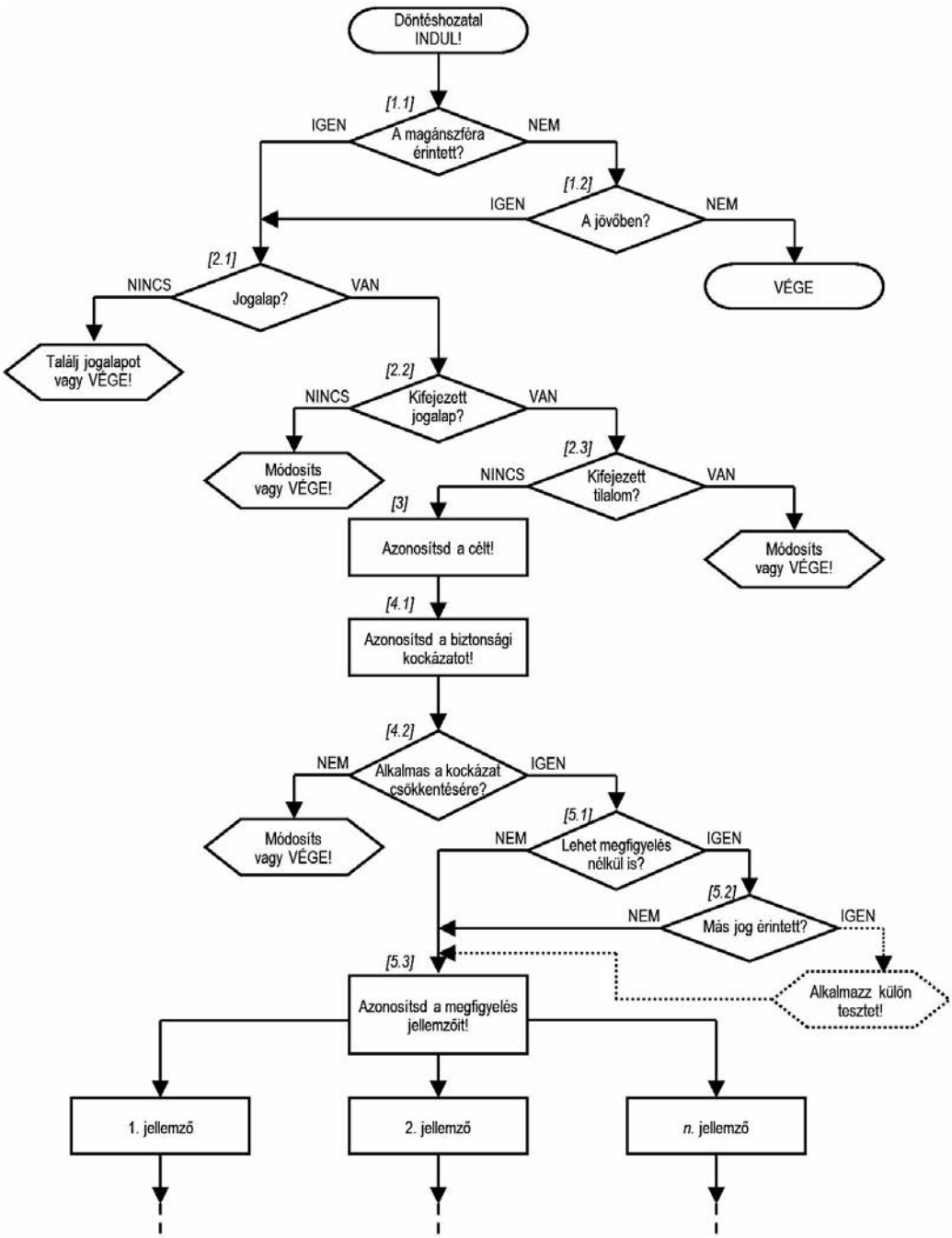
Solove, Daniel J., Marc Rotenberg and Paul M. Schwartz, *Privacy, information and technology,* Aspen Publishers, New York, 2006.

Westin, Alan, *Privacy and Freedom,* Atheneum, New York, 1967.

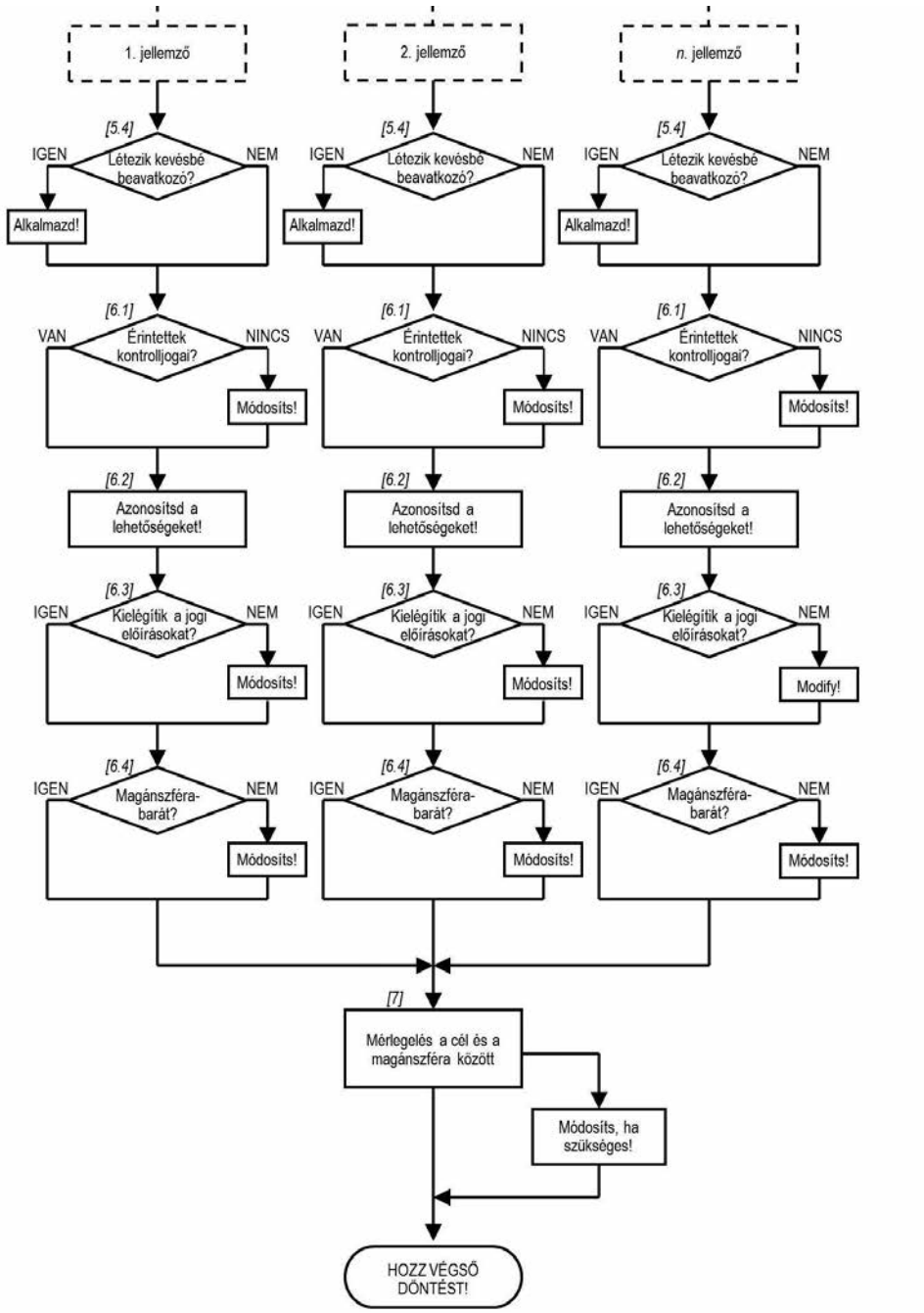
Székely Iván társadalmi informatikus, a Közép-európai Egyetem kutatóprofesszora, a BME docense. Kutatói érdeklődése és publikációi az információs autonómia, a nyilvánosság és titkosság, az emlékezés és felejtés, a megfigyelés, a magánélet, a reziliencia, az identitás és az archivisztika területeire irányulnak.

Somody Bernadette alkotmányjogász, az Eötvös Károly Intézet igazgatója, az ELTE Állam- és Jogtudományi Kar Alkotmányjogi Tanszékének oktatója. Kutatási területe az alapjogok védelme, az alapjogvédelmi intézményrendszer és az alapjogi bíráskodás.

Szabó Máté Dániel alkotmányjogász, a Társaság a Szabadságjogokért szakmai igazgatója. Szakmai és kutatói tevékenysége az alapvető szabadságjogok és az információs jogok védelmére, az információs önrendelkezés alkotmányos határainak vizsgálatára irányul.



5.a ábra: A megfigyelésekkel kapcsolatos döntéshozatal arányossági teszten alapuló lépései (1. rész)



5.b ábra: A megfigyelésekkel kapcsolatos döntéshozatal arányossági teszten alapuló lépései (2. rész)

Pásztor Emese

Magánélet és bizonytalanság – A jogi kontrollmechanizmusok szerepe a nemzetbiztonsági célú titkos információgyűjtés alapjogi kockázatainak mérséklésében

Bevezető

Jelen írásnak nem célja kétségbe vonni a nemzetbiztonsági szolgálatok működésének fontosságát, továbbá nem célja azon háborogni sem, hogy e szervek napi rutinja kifejezetten a transzparencia hiányára épül. A nemzetbiztonsági apparátus jogállamban értünk dolgozik, a külvilág számára nehezen átlátható működési elvek mentén – ha nem így volna, értelme sem volna. Nem nehéz ugyanakkor belátni, hogy a titkosság a visszaélések fokozott lehetőségét hordozza magában. A feladat adott: ezt a fokozott kockázatot megfelelő jogi kontrollmechanizmusok beiktatásával úgy kell a minimumra szorítani, hogy közben a nemzetbiztonsági védőhálót ne fedjük fel azok előtt, akik ellen okkal lett kifeszítve.

A következő néhány oldalon amellett fogok érvelni, hogy a nemzetbiztonsági célú titkos információgyűjtés esetében a magánszférához való jog tényleges érvényesülésének minimuma, hogy megfigyelést miniszteri engedély helyett *csak előzetes rendesbírósági döntésben adott felhatalmazás alapján* lehessen végezni. Ezen túlmenően kísérletet teszek egy olyan ideális rendszer felrajzolására, amely a terrorizmus elhárítására hivatott szervek működésének ellehetetlenítése nélkül az eljárás valamennyi szakaszában lehetőséget ad az egyén alapjogainak hatékony védelmére.[1] Az írás tehát két szempontot egyszerre dolgoz fel: a magánszférához való jog és ezzel összefüggésben egyúttal a hatékony jogorvoslathoz való jog támasztotta követelményeknek megfelelő megoldás feltárására irányul.

A titkos információgyűjtés intézményének visszásságai nem ma merülnek fel először, azonban az Emberi Jogok Európai Bíróságának egy közelmúltbeli ítélete[2] kényszerítő indokkal szolgál a terület teljes újraszabályozásához. Az ítélet kimondta, hogy a nemzetbiztonsági célú titkos információgyűjtés magyar jogi háttere az Emberi Jogok Európai Egyezményét[3] sérti, arra azonban nem adhatott választ, hogy ezt a sérelmet milyen tartalmú új szabályozással lehet kiküszöbölni.

Annyi bizonyos, hogy a hatékony külső jogi kontroll megvalósításának nem egy módja van, mindez a megfigyelés folyamatának több pontján, különböző természetű és ennek megfelelően különböző hatáskörökkel felruházott alapjogvédelmi szervek bevonásával is elképzelhető. A választás lehetőségeinek az európai alapjogvédelmi sztenderd és a magyar alkotmányos hagyomány szab határt – már csak az a kérdés, hogy ez a gyakorlatban mit jelent.

[1] Köszönöm Somody Bernadette, Székely Iván, valamint a névtelen bíráló értékes megjegyzéseit, melyekkel hozzájárultak a tanulmány elkészültéhez.

[2] *Szabó and Vissy v. Hungary*, judgment of 12 January 2016, no. 37138/14.

[3] Az emberi jogok és az alapvető szabadságok védelméről szóló, Rómában, 1950. november 4-én kelt Egyezmény.

Szabó és Vissy kontra Magyarország – Az ügy körülményei és a döntés

Két magyar állampolgár, Szabó Máté és Vissy Beatrix 2014 májusában az Emberi Jogok Európai Bíróságához fordult a nemzetbiztonsági célú titkos információgyűjtés hazai szabályozása miatt. Az indítványozók akkortájt a közhatalom mindenkori gyakorlóival szemben kritikus Eötvös Károly Intézet munkatársai voltak;[4] gondolhatnánk, hogy a kifogásolt szabályozás személyükben érintette őket. A könnyednek éppen nem nevezhető témát közelebb hozhatja az olvasóhoz, hogy a Bíróság[5] a kérelem befogadásakor nem tulajdonított kifejezett jelentőséget annak, hogy a kérelmezők a Kormány bírálata miatt fokozottan ki lehettek téve a megfigyelésnek. Mivel a titkos megfigyelés lehetséges érintettjeinek köre teljesen nyitott, a szabályozás hiányosságai azok puszta léte miatt valamennyiünk alapjogaira kockázatot jelentenek.

Az indítvány alapjául az szolgált, hogy a beadvány benyújtói szerint a Terrorelhárítási Központ számára e körben biztosított különleges jogosítványok és ezek engedélyezése az Egyezménynek a magánéletet védő 8. cikkébe ütközik. Bár kérelmüket a Bíróság megalapozottnak találta, a jelen idő továbbra is indokolt, mivel a szabályozás a kézirat lezárásának napjáig nem változott.[6]

A szövevényes jogszabályi hátteret összefoglalva, a rendőrségi törvény[7] a terrorizmus elleni hatékony fellépés érdekében olyan, a titkos információgyűjtés során gyakorolható, különleges jogosítványokkal ruházza fel a Terrorelhárítási Központot (TEK)[8], mely azt eredményezi, hogy a TEK az érintett személy hozzájárulása nélkül annak otthonában lényegében mindent megtehet, ami a titkos megfigyelés körében elképzelhető. Ennek keretében a TEK házkutatást végezhet, felvételeket készíthet, felbonthatja a megfigyelt személy postai küldeményeit, elektronikus úton továbbított kommunikációját megismerheti és rögzítheti.

A titkos információgyűjtési tevékenység két különböző indok alapján végezhető: valamilyen *konkrét bűncselekmény felderítéséhez kapcsolódva*, *vagy* pedig konkrét bűncselekmény gyanúja nélkül, *nemzetbiztonsági megfontolásokból*. Mindennek azért van jelentősége, mert engedélyezése attól függ, hogy e két ok közül melyik merül fel. Amennyiben ugyanis egy

[4] A szerző jelenleg is az Eötvös Károly Intézet munkatársa.

[5] A továbbiakban lásd még: EJEB.

[6] Az EJEB hatásköre a jogsértés megtörténtének megállapításán túl arra terjed ki, hogy ha szükségesnek látja, „igazságos elégtételt" nyújtson a kérelmezőnek. Arra, hogy a hazai hatóságok (például a bíróság vagy az Alkotmánybíróság) határozatait, vagy a hazai jogszabályokat megváltoztassa, illetve megsemmisítse, vagy törvénymódosításra kötelezze a nemzeti parlamenteket, nincs lehetősége. Attól függetlenül, hogy az EJEB ítéletei nem írják elő törvények kötelező megváltoztatását, ha az Egyezmény tiszteletben tartása csak törvénymódosítás által érhető el, akkor az elmarasztalt államnak ezzel az eszközzel kell elérnie az Egyezménynek való megfelelést. Az első fokú ítéletet a konkrét ügyben az EJEB 2016. január 12-én hirdette ki, amellyel szemben a magyar állam fellebbezett, ezért csak később, 2016. június 6-án vált véglegessé. A kézirat lezárására 2017. január 15-én került sor.

[7] A Rendőrségről szóló 1994. évi XXXIV. törvény (a továbbiakban: Rtv.) 7/E. §.

[8] A TEK 2010-ben jött létre azzal a céllal, hogy országos illetékességgel lássa el a terrorelhárítási feladatokat, valamint a terrorizmus elleni küzdelem koordinációját, elemzését, értékelését. Feladata leginkább a terrorcselekmény és az ahhoz kapcsolódó bűncselekmények felderítésére, megelőzésére és megszakítására terjed ki.

adott bűncselekmény felderítéséről van szó, a titkos információgyűjtés elrendelése bírósági engedélyhez kötött[9], ha viszont nemzetbiztonsági céllal történik, akkor az engedélyezés az igazságügyért felelős miniszter hatáskörébe tartozik.[10]

A rendőrségi törvény az előbbi körben taxatíve felsorolja, hogy pontosan mely bűncselekmények felderítése során vethető be a titkos információgyűjtés eszköztára, a lehetséges nemzetbiztonsági célok azonosításakor azonban már jóval nehezebb helyzetben van, aki a törvény szövege alapján tájékozódna. Az igazságügyért felelős miniszter a gyanútól elszakadva, terrorcselekmények elkövetésére irányuló törekvések megelőzése, felderítése és elhárítása, illetve külföldi fegyveres konfliktus vagy terrorcselekmény esetén magyar állampolgárok mentése érdekében engedélyezhet titkos információgyűjtést, mely ebben az esetben már nem a rendőrségi, hanem a nemzetbiztonsági törvény[11] rendelkezései szerint zajlik. A jogszabály eljárási garanciaként rögzíti, hogy a titkos információgyűjtés csak akkor alkalmazható, ha a szükséges információ máshogy nem szerezhető be, ezen kívül azonban hiába kutatunk konkrét támpontok után az elrendelés lehetőségeit illetően. Az intézkedés legfeljebb 90 napig tarthat, amely időszak a miniszter döntése alapján további 90 nappal meghosszabbítható, ráadásul ezt a döntést anélkül kell meghoznia, hogy jogosult lenne megismerni a folyamatban lévő információgyűjtés eredményét. A folyamat lezárultával a megszerzett lényegtelen információk sorsa is bizonytalan. A miniszter által engedélyezett titkos információgyűjtések külső ellenőrzését az Országgyűlés Nemzetbiztonsági Bizottsága és az alapvető jogok biztosa látja el – a kérelmezők által beszerzett adatok szerint azonban soha egyik szerv sem élt erre irányuló jogosítványaival.

A kérelmezők beadványukban azt állították, hogy ilyen körülmények között a nemzetbiztonsági célú titkos információgyűjtés keretében akár indokolatlan és a magánéletet aránytalanul sértő intézkedéseknek is alanyai lehetnek, különösen, ha mindez bírósági kontroll nélkül történik.[12]

Az ügy alapos vizsgálata után a Bíróság nem látta igazoltnak, hogy a nemzetbiztonsági célú titkos információgyűjtést szabályozó magyar jogszabály megfelelően pontos, hatékony és átfogó jogi garanciákat biztosítana a megfigyelő intézkedések elrendelésével, végrehajtásával és a vonatkozó jogorvoslati lehetőségekkel kapcsolatban, ezért megállapította az Egyezmény 8. cikkének megsértését.[13] Ennek puszta tényén kívül számunkra inkább az a lényeges, hogy a Bíróság az ítélet indokolásában tett utalásai alapján meglehetősen jól rekonstruálható, mit tekint a titkos információgyűjtés alapjogvédelmi biztosítékai jelenlegi minimumának.

A konkrét esetben a Bíróság dolgát „megkönnyítette", hogy Magyarországon gyakorlatilag semmilyen hatékonyként értékelhető kontrollmechanizmus nem működik a nemzetbiztonsági célú titkos információgyűjtés felett. Ilyen körülmények között a Bíróság nem szembesült annak nehézségeivel, hogy vajon a létező rendszer megfelel-e a strasbourgi

[9] Rtv. 7/E. § (2) bek.
[10] 7/E. § (3) bek.
[11] A nemzetbiztonsági szolgálatokról szóló 1995. évi CXXV. törvény.
[12] Álláspontjuk szerint továbbá az Egyezmény 8. cikke mellett a szabályozás az Egyezmény által biztosított tisztességes tárgyaláshoz és hatékony jogorvoslathoz való jogokat is sérti (6. és 13. cikk).
[13] A Bíróság megállapította továbbá, hogy az Egyezmény 8. cikkével együtt olvasott 13. cikkét is megsértették, ugyanakkor nem látta szükségesnek a panaszt a 6. cikk alapján is megvizsgálni.

minimumnak – mivel a felügyelet rendszere nincs kiépítve, az ítélet megállapításai sem a jelenlegi rendszer kritikáját jelentik, sokkal inkább értelmezhetőek útmutatásként a jövőbeni szabályozáshoz.

Az európai sztenderd

Ha európai alapjogvédelmi sztenderdekről beszélünk, figyelmünket elsősorban az Emberi Jogok Európai Bíróságának gyakorlatára érdemes összpontosítanunk. Az Emberi Jogok Európai Egyezménye és az annak kikényszerítésére hivatott alapjogvédelmi intézményrendszer gondoskodik – más alapjogok mellett – a magán- és családi élet tiszteletben tartásához való jog érvényesüléséről valamennyi részes államban. A nemzetbiztonsági célú titkos információgyűjtés kérdése kétségkívül ebbe a körbe tartozik; a Bíróság álláspontja szerint nem vitás, hogy a jogszabály puszta léte az állam beavatkozását jelenti a kérelmezők magánszférájába. Önmagában azonban nem mindenfajta beavatkozás jelenti egyúttal az Egyezmény megsértését is. Az egyezménysértés megítéléséhez maga az Egyezmény ad útmutatást[14], amikor kimondja, hogy a hatóság csak olyan, törvényben meghatározott esetekben avatkozhat be a magánélethez fűződő jog gyakorlásába, amikor az egy demokratikus társadalomban például a nemzetbiztonság, a közbiztonság védelme, illetve zavargás vagy bűncselekmény megelőzése érdekében szükséges. A jogkorlátozás céljait tehát az Egyezmény kimerítően felsorolja, ezek között szerepel is a nemzetbiztonság, ezért a nemzetbiztonsági célú titkos információgyűjtés esetében a célok legitimitása felől nem lehet kétség. A vizsgálat következő lépése annak eldöntése, hogy a magánszféra ilyen jellegű korlátozása szükséges-e egy demokratikus társadalomban. Ez a szükségesség a Bíróság gyakorlatában fokozott, a demokratikus intézmények védelme érdekében felfogott szükségességet jelent, annak elismerése mellett, hogy az állami hatóságoknak van bizonyos mértékű mérlegelési joguk annak megítélésében, hogy milyen eszközöket választanak a nemzetbiztonság védelmére (margin of appreciation). A teszt utolsó eleme az arányosság értékelése, mellyel a Bíróság csak akkor foglalkozik, ha a korlátozás valamennyi korábbi, egymásra épülő lépcsőfok próbáját kiállta.

A fenti elemekből áll össze az a teszt, melynek alapján az EJEB megítéli, hogy egy adott alapjogkorlátozó intézkedés az Emberi Jogok Európai Egyezményébe ütközik-e. A visszaélések megelőzésére egy összetett garanciarendszer hivatott, a Bíróság pedig a jogi kontrollmechanizmusokra ennek egyik elemeként tekint. A kontrollmechanizmusok célja annak biztosítása, hogy az állam csak olyan esetekben avatkozzon be a polgárok magánszférájába, amelyek egy demokratikus társadalomban a szigorú szükségesség feltételének megfelelnek.[15]

[14] 8. cikk 2. bekezdés.

[15] A jogi kontrollmechanizmusok hatékony működése mellett jelentősége van még az intézkedés jogszabályi hátterének (az intézkedés jellege, köre, időtartama, jogalapja), melyekkel kapcsolatban a Bíróság szintén megfogalmazott minimális garanciákat. Ilyen például, hogy törvényben kell szabályozni a beavatkozást elrendelő végzés alapjául szolgáló bűncselekmények jellegét, az érintett személyek kategóriáinak meghatározását, a lehallgatás időtartamára vonatkozó korlátokat, a megszerzett adatok sorsára vonatkozó eljárás szabályait, valamint az adatok törlésére vagy megsemmisítésére vonatkozó rendelkezéseket. Mivel ez a mostani elemzés a jogi kontrollmechanizmusokra koncentrál, a döntés az ezekkel kapcsolatos megállapításaira nem tér ki.

Általánosságban elmondható, hogy a Bíróság a titkos információgyűjtést egy folyamatként látja, és ennek megfelelően megkülönbözteti az előzetes engedélyezést és a folyamat közben, illetve annak végeztével gyakorolt felügyeletet. Az egyes fázisok egy idővonalon állomásokként szemléltethetők, fontos azonban hangsúlyozni, hogy a Bíróság nem egymástól elszigetelten vizsgálja az egyes állomások garanciális jelentőségét. A jogállamiság fogalmából kiindulva az érvek a *hatékonyság* központi követelménye köré rendeződnek, a Bíróság szerint ugyanis jogállamban az egyén jogaiba a végrehajtó hatalom csak hatékony kontroll mellett avatkozhat be, a bevont intézményeknek és a számukra biztosított hatásköröknek ennek megfelelően *összességükben* kell a hatékony jogvédelmet garantálniuk.

a) Előzetes engedélyezés

Amennyiben a titkos információgyűjtés folyamatában beszélhetünk szokásos ügymenetről, e szerint az első lépés a megfigyelés elrendelésének engedélyezése. A rendelkezésre álló esetjog alapján a Bíróság a részes államokat abba az irányba tereli, hogy az engedélyt *lehetőleg bíróság* adja ki, ezt azonban nem mondja ki kényszerítő követelményként.[16] Ezt a józan észre ható terelgetést érhetjük tetten, amikor a magyar példa kapcsán a Bíróság kifejti, hogy a rendesbíróság lenne alkalmas arra, hogy egy bevett értelmezési gyakorlatot kialakítva szűkítse a TEK mérlegelési lehetőségeit az érintettek körének meghatározásában.[17]

A hatékonyság kulcsa a függetlenség: vagy független testületnek kell engedélyeznie a megfigyelést, vagy az engedélyező testület tevékenységét kell a bíróságnak vagy – a függetlenség fokában ehhez hasonló – testületnek ellenőriznie.[18] Ehhez képest minden egyéb megoldás kivételként fogadható el, melyek indokoltságát alaposan meg kell vizsgálni.[19] A fentiek erejéből sokat elvesz, hogy az előzetes engedélyezést a Bíróság nem tekinti abszolút követelménynek arra hivatkozva, hogy ahol kiterjedt utólagos felügyelet működik, ott ez ellensúlyozhatja a rendszer hiányosságait.[20] Ezzel kapcsolatban fontos rámutatni a Bíróság álláspontjának vitathatóságára. Az előzetes engedélyezés a jogsértés megelőzésére hivatott, így funkcióját tekintve tér el az utólagos felügyelet intézményétől. Amennyiben az előzetes engedélyezés hiánya miatt megtörténik az alapjogsértés, az utólagos felügyelet már csak a jogsértés megtörténtét tárhatja fel, az alapjog alanya szempontjából aligha ellensúlyozva ezzel a magánszféra megsértését.

A „normál" ügymenethez képest is kivételesek azok a vészhelyzetek, ahol technikailag kivitelezhetetlen, vagy rendkívül célszerűtlen és időpazarló lenne egy független szerv engedélyéhez kötni az információgyűjtés megkezdését. A kivételes engedélyezés igényének jogossága az európai sztenderd szerint sem vitatott, nem kizárt, hogy a fentiek-

[16] Speciális esetekben volt rá példa, hogy a Bíróság feltétlenül előzetes bírósági engedélyeztetést követelt meg, például a médiára irányuló titkos megfigyelések esetén (*Telegraaf Media Nederland Landelijke Media B.V. and Others v. the Netherlands*, judgment of 22 November 2012, no. 39315/06, *Kopp v. Switzerland*, judgment of 25 March 1998, no. 13/1997/797/1000).

[17] *Szabó and Vissy v. Hungary,* 73., valamint *Roman Zakharov v. Russia*, judgment of 4 December 2015, no. 47143/06, 249.

[18] *Dumitru Popescu v. Romania*, judgment of 26 April 2007, no. *71525/01*, 70-73.

[19] *Klass and Others v. Germany*, judgment of 6 September 1978, no. 5029/71, 42, 55.

[20] *Kennedy v. The United Kingdom*, judgment 18 May 2010, no. 26839/05, 167.

ben részletezett engedélyezés nélkül is megkezdődhessen a megfigyelés. Az érintett időtartam világos jogi szabályozásán túl ennek garanciális eleme, hogy az ilyen sürgősségi intézkedést mindig utólagos felülvizsgálathoz kell kötni.

b) Felügyelet

Arra nézve, hogy az engedélyezés után, de még a megfigyelés tartama alatt milyen kritériumai vannak a hatékony külső kontrollnak, kevesebb utalást találunk az esetjogban. Általános követelmény, hogy a rendesbíróságokat – mint azt a szervtípust, amely a függetlenség, a pártatlanság és a megfelelő eljárás legjobb garanciáját nyújtja[21] – valamilyen módon be kell vonni a felügyeletbe. Hiába a titkos megfigyelések jellege miatt indokolt elvi jelentőség[22], itt is vannak kivételek: adódott arra is példa, hogy a Bíróság elfogadhatónak talált egy olyan egyesített felügyeleti modellt, amelyben nem volt bírósági kontroll, de „az ellenőrzés első körét bírói hivatal betöltésére képesítéssel rendelkező tisztviselő végezte".[23] Érdekes megfigyelni, hogy a Bíróság annak ellenére is megelégszik a képesítés meglétével, hogy a képesítés önmagában nem jelenti a bírói hivatal tényleges betöltésével járó független státusz meglétét is. Ebből kiindulva úgy tűnik, hogy a Bíróság az alapjogvédelmi minimum szempontjából *fontosabbnak tartja a szakértelmet* a döntéshozó személyi és szervezeti függetlenségénél.

Általánosságban annyi mégis elmondható, hogy ha valahol, legalább az eljárás utolsó fórumaként elvárásként jelenik meg a bíróság bevonása. Ez az utólagos felülvizsgálati elem az előzetes engedélyezés beiktatásától függően kötelező. Ha a megfigyelést előzetesen nem bírósági szerv engedélyezte, akkor szükséges, hogy a bírósági kontroll legalább utólag biztosítva legyen. A bírósági felülvizsgálattal kapcsolatban utalunk a nyilvánosság követelményére, amely egyértelműen kizárja a nem publikus bizottsági jelentések útján megvalósuló felülvizsgálatot az elfogadható ellenőrzési mechanizmusok sorából.[24]

Külön kérdés, hogy az eljárás végén a bíróság hivatalból ellenőrzi-e a folyamat jogszerűségét, vagy emellett – akár ehelyett – az érintett kérelmére nyílik meg a jogorvoslat lehetősége. A Bíróság ezzel kapcsolatban kifejtette, hogy ha a titkos információgyűjtéssel érintett állampolgárok nem értesülnek titkos megfigyelésükről, erősen megkérdőjelezhető a jogorvoslati lehetőség fenntartásának értelme.[25] Erre való tekintettel a Bíróság gyakorlata

[21] *Szabó and Vissy v. Hungary,* 77.
[22] *Klass and Others v. Germany, 55, 56.*
[23] *Klass and Others v. Germany, 56.*
[24] *Roman Zakharov v. Russia*, 283.
[25] E körben az európai védelmi szint elméleti síkon meglehetősen egyértelmű. A Bíróság osztja a Velencei Bizottság megállapítását, miszerint a jogorvoslat hatékonysága azon múlik, hogy az egyén értesült-e a feltételezett túlkapásról, és tudja-e ezt hitelt érdemlően bizonyítani a Bíróság előtt (a Velencei Bizottság 71. plenáris ülésén a biztonsági szolgálatok demokratikus felügyeletének tárgyában elfogadott CDL-AD(2007)016-e számú jelentés 243. pontja). http://www.venice.coe.int/webforms/documents/CDL-AD(2007)016.aspx
Mindemellett ugyanakkor a „margin of appreciation" teszt gyakorlati alkalmazásakor ez az elméleti tisztaság veszíthet egyértelműségéből. A tájékoztatás elmaradását az államok adott esetben kimenthetik arra való hivatkozásukkal, hogy a tájékoztatással a nemzetbiztonsági szolgálatok általános működésére és munkamódszerére nézve szivárognának ki értékes információk (*Klass and Others v. Germany 58.).*

még egy kötelező elemet rögzít: feltétlenül értesíteni kell utólag az érintettet a vele szemben alkalmazott intézkedésről, amint az értesítés a nemzetbiztonsági cél veszélyeztetése nélkül kiküldhető.[26]

Azon túl, hogy a Bíróság szemüvegén át a felügyelet ideális esetben szintén a bíróságok kezében van, néhány szervtípust az esetjog egyértelműen kizár a felügyeleti hatáskör letéteményeseként elfogadható intézmények sorából. Ilyen például a miniszter vagy a végrehajtó hatalom bármely politikai felelősséget viselő tagja. Az ilyen szervek eljárása politikai karakterük miatt a Bíróság szerint is a visszaélések fokozott kockázatát hordozza magában, ráadásul ezek lényegüknél fogva alkalmatlanok a szigorú szükségesség követelményének értékelésére. Nem ilyen tiszta a helyzet az ombudsman-típusú intézmények megítélésében. Az alapvető jogok biztosával kapcsolatban elvi szinten a Bíróság egyedül azt nem látta kétségtelenül igazoltnak, hogy a biztos szükségképpen bírói tisztség betöltésére alkalmas személy – az ombudsmani-jellegű szervek (hatályos jogunkban az alapvető jogok biztosa, korábban például az állampolgári jogok biztosa vagy az adatvédelmi biztos) függetlenségére nézve nem tett megállapítást. Az EJEB döntéséből kirajzolódó elvárásokat az 1. ábra és az 1. táblázat összegzi.

1. ábra: Idővonal, a titkos megfigyelés folyamatának strasbourgi követelményei

	kivételes engedélyezés	előzetes engedélyezés	a végrehajtás felügyelete	utólagos értesítés a megfigyelésről	utólagos felügyelet
Kötelező vagy fakultatív elem?	kötelező felülvizsgálat mellett elfogadható	akkor kötelező, ha a kontroll hatékonysága utólagos felügyelettel nem biztosítható	nem kötelező	a nemzetbiztonsági cél veszélyeztetésétől függően kötelező	akkor kötelező, ha az előzetes engedélyezést nem bírói szerv végezte
Milyen szerv végezheti?	a titkos megfigyelés végrehatásáért felelős szerv	független szerv, lehetőleg bíróság. az engedélyezést bíró ellenőrizze	ha van, akkor független szerv	a titkos megfigyelés végrehajtásáért felelős szerv	lehetőleg bíró, de az eljárás valamely pontján mindenképp legyen bevonva a bíróság

1. táblázat: A titkos megfigyelés folyamatának strasbourgi követelményei

[26] *Weber and Saravia v. Germany*, judgment of 29 June 2006, no. 54934/00, 135., *Roman Zakharov v. Russia*, 287.

A hazai alkotmányos háttér

A magyar alkotmányos hagyományt vizsgálva talán a legfontosabb forrás az EJEB döntése által is idézett 32/2013. (XI. 22.) AB határozat, mely a rendőrségi törvény témánk szempontjából releváns szakaszával foglalkozik.

Az Alkotmánybíróság a nem bűnüldözési célból folytatott titkos információgyűjtés szabályait 2013 előtt nem vizsgálta. Az ekkor megszületett határozat megítélése szempontjából azonban jelentőséggel bír, hogy a testület már korábban, 2007-ben, még az Alaptörvény hatályba lépése előtt rögzítette azokat a szempontokat[27], amelyek alapján eldönthető, hogy mikor fogadhatóak el egy demokratikus jogállamban a titkos információgyűjtés eszközei és módszerei. Ezen eszközök és módszerek szükségességét a testület azzal támasztotta alá, hogy bizonyos, a társadalom rendjét súlyosan sértő bűncselekmények ellen hagyományos eszközökkel nem lehet hatékonyan fellépni, a titkos megfigyelés pedig alkalmas lehet arra, hogy a társadalom védelme érdekében „behozza a bűnüldöző szerveknek a bűnözéssel szemben esetlegesen fennálló lépéshátrányát".[28] Noha az idézett részlet kifejezetten a bűnüldözési célú titkos információgyűjtésre vonatkozik, az Alkotmánybíróság ugyanebből a tételből indult ki a nem bűnüldözési célból folytatott titkos információgyűjtés alkotmányosságának megítélésekor.[29] Ennél egy fokkal világosabb, hogy miért ragaszkodott azokhoz a szintén 2007-ben lefektetett alapelvekhez, melyek szerint a jogállamiság és az alapjogok védelme a titkos információgyűjtés felhasználási rendjének részletes és differenciált szabályozását követeli, a magánszférába történő beavatkozás súlyossága miatt pedig kivételesen, átmenetileg és végső megoldásként képzelhető el az eszköz alkalmazása.

32/2013. (XI. 22.) számú határozatában az Alkotmánybíróság elutasította a rendőrségi törvény azon rendelkezésével szemben benyújtott beadványt, amely a terrorelhárításért felelős szervet titkos információgyűjtésre hatalmazta fel. Ez a beadvány felépítésében eltért a Bírósághoz benyújtott indítványtól, lényegében arra irányult, hogy a terrorizmust elhárító szerv által folytatható nemzetbiztonsági célú titkos információgyűjtés ne a nemzetbiztonsági törvény, hanem a szélesebb garanciákat biztosító rendőrségi törvény, vagy arra legalábbis jobban emlékeztető rendelkezések szerint folyjon, biztosítva ezzel például a folyamat bírósági engedélyhez kötöttségét. Anélkül, hogy részletesen ismertetném azt a szükségességi-arányossági követelményrendszert, amelyen belül az Alkotmánybíróság következtetéseit levonta, a külső jogi kontrollmechanizmusokra vonatkozó sztenderd azonosítása szempontjából legfontosabb megállapításokat veszem sorra.

Az indokolásban az Alkotmánybíróság már elszakad attól az elméleti kiindulóponttól, hogy a nem bűnüldözési célú titkos megfigyelések szükségességét a bűnüldözési célú megfigyelés szükségességéhez mérje, sőt, megállapítja, hogy a nemzetbiztonsági feladatok *össze sem hasonlíthatók* a bűnüldözési célból folytatott, bírói engedélyhez kötött titkos információgyűjtéssel. Ezt azzal indokolja, hogy „a nemzetbiztonsági feladatok sokkal szélesebb spektrumot fognak át, mint a bűnüldözési feladatok, a valóságot elsősorban nem az

[27] 2/2007. (I. 24.) AB határozat

[28] 2/2007. (I. 24.) AB határozat, ABH 2007, 65, 100.

[29] Mivel az Alaptörvény a jogállamiságot deklaráló B) cikk (1) bekezdése és a korábbi Alkotmány 2. § (1) bekezdése tartalmilag megegyezik, az Alkotmánybíróság az Alaptörvény hatályba lépését követően is fenntartotta e körben tett megállapításait.

események büntetőjogi relevanciájának szemszögéből vizsgálják és nem is feltétlenül járnak büntetőeljárási következményekkel." A határozat különösebb magyarázat nélkül magától értetődőnek veszi, hogy a nemzetbiztonsági kockázatok mérlegelése *politikai döntést igényel*, ezért az ilyen kockázatok kezelése, és egyáltalán, a megfigyelés engedélyezése a végrehajtó hatalom hatáskörébe tartozik.[30] Ebben a megközelítésben az igazságügyért felelős miniszter személyének alkalmassága nem kérdőjeleződik meg. A testület azt az egyedüli kritériumot támasztja vele szemben, hogy az engedélyezéskor mérlegeljen a nemzetbiztonsági érdek és az alapjogsérelem között. A mérlegelés sarokpontjainak vizsgálatakor az Alkotmánybíróság párhuzamot von a bűnfelderítési célú titkos információgyűjtéssel, megállapítva, hogy a nemzetbiztonsági célú titkos megfigyelés esetében az a garancia, amely a titkos megfigyelést csak minden egyéb eszköz hatástalanságakor teszi alkalmazhatóvá, ugyanazt a célt szolgálja, mint a bűnfelderítési információgyűjtés esetében az alkalmazás alapjául szolgáló bűncselekmények törvényi rögzítése.

Az alapjogkorlátozás alkotmányosságának másik garanciáját az Alkotmánybíróság a külső ellenőrzésben látja, ezzel kapcsolatban részletesen elemzi is az Országgyűlés Nemzetbiztonsági Bizottságának és az alapvető jogok biztosának a hatásköreit. A szabályok részletes ismertetését követően meg is állapítja azt a kétségtelen tényt, hogy a nemzetbiztonsági törvény elvileg lehetővé teszi az igazságügyért felelős miniszter engedélyezési eljárásának a végrehajtó hatalomtól független szervek általi ellenőrzését, arra nézve azonban semmilyen megállapítást nem tesz, hogy az az ellenőrzés mennyiben tekinthető hatékonynak. A szabályozást elnézve ez pedig nem volna haszontalan. Az Országgyűlés Nemzetbiztonsági Bizottsága a titkos információgyűjtés elrendelése és végrehajtása felett egyaránt ellenőrzést gyakorol, információit a nemzetbiztonsági szolgálatok irányításáért felelős miniszter (a belügyminiszter, az egyes szakosodott szervezetek esetében pedig a Miniszterelnökséget vezető miniszter, valamint a honvédelemért felelős miniszter) és az elrendelést engedélyező miniszter (az igazságügyminiszter) tájékoztatásaiból, állampolgári panaszokból, valamint a szolgálatok munkatársainak bejelentéseiből szerzi. Erősen elgondolkodtató, hogy mennyiben várhatja a bizottság saját magukra nézve terhelő információk szolgáltatását a titkos megfigyelés folyamatában hatáskörökkel rendelkező szervektől, illetve milyen állampolgári bejelentésekre számít, ha a titkos megfigyeléssel érintett személyt a döntéshozó nem tájékoztathatja a megfigyelés elrendeléséről.[31] A hatályos szabályozás szerint tehát a titkos információgyűjtést engedélyező miniszter eljárásáról, illetve a titkos információgyűjtés tényéről az érintettet nem tájékoztathatja, olyan szabály pedig nem létezik, mely előírná, hogy a szolgálatok az érintettet proaktív módon tájékoztatni lennének kötelesek. Ennek fényében a nemzetbiztonsági törvény által bevezetett panaszmechanizmus hatékonysága is megkérdőjelezhető[32], és hasonló a helyzet a határozat

[30] 32/2013. (XI. 22.) AB határozat, ABH 2013, 924, 105.

[31] Nbtv. 58. § (6) bek.

[32] Az Nbtv. 11. § (5) bekezdése felhatalmazza a minisztert a nemzetbiztonsági szolgálatok tevékenységével kapcsolatos panaszok kivizsgálására. Ezzel összefüggésben érdemes felhívni a figyelmet arra is, hogy az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (a továbbiakban: Infotv.) 14. § a) pontja alapján az érintett kérelmezheti az adatkezelőnél (így a szolgálatoknál is) tájékoztatását személyes adatai kezeléséről. E két valóban létező jogérvé-

által szintén részletesen ismertetett, de a gyakorlatban ezen a területen soha sem alkalmazott ombudsmani kontrollal is.[33] Kevéssé valószínű, hogy bárki eljárásokat indítana alapjogai védelmében, ha hozzá semmiféle jel nem jut el, melyből alapjogainak sérelmére következtethetne.

Árulkodó az a kiszólás, melyben az Alkotmánybíróság kezeit széttárva állapítja meg, hogy a titkos megfigyelés *sajátos jellege* kizárja a jogorvoslatot.[34] Ez a megállapítás ebben a formában nem helytálló, mivel a titkos megfigyelés jellege önmagában egyáltalán nem zárja ki, hogy a megfigyelés elrendelésének jogossága és a megfigyelés végrehajtásának jogszerűsége utólag kivizsgálható legyen. A titkos megfigyelés jellegével szemben a jogorvoslat hiányában kizárólag annak van szerepe, hogy a megfigyelt személy még utólag sem értesül a megfigyelés megtörténtéről. Ezt a megállapítást a testület arra használja, hogy ezzel az engedélyezés kötelező miniszteri indokolása mellett érveljen. Az indokolási kötelezettséget a testület alkotmányos követelményként is megfogalmazza, ami a határozat egyértelmű erénye.[35] Ugyanakkor azzal, hogy az utólagos értesítés hiányát az Alkotmánybíróság kész ténynek veszi, és nem kéri számon a jogalkotón, a rendszer lényegi hibájáról tudomást sem vesz, és úgy tesz, mintha az alapvetően megváltoztathatatlan lenne. Ennek indokai nem világosak. A nemzetbiztonsági érdek megköveteli, hogy a megfigyelt személy az információgyűjtés kezdetén és annak tartalma alatt ne értesüljön az intézkedésről, nehogy viselkedését ahhoz igazítsa. Ez az érdek ugyanakkor a titkos információgyűjtés lezárultával elenyészik: ha a titkos információgyűjtés nem igazolta vissza, hogy a megfigyelt személy nemzetbiztonsági kockázatot jelent, nem indokolható, hogy utólag miért ne értesülhetne a történtekről.

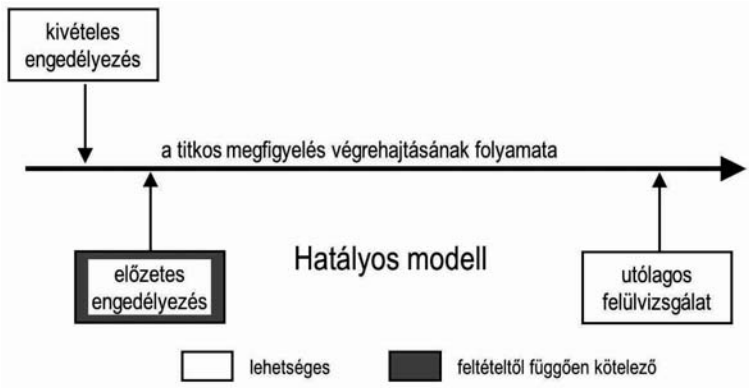
Az Országgyűlés Nemzetbiztonsági Bizottságán és az alapvető jogok biztosán keresztül a felügyelet formális értelemben biztosított, ez azonban patyomkin-felügyelet, mely a gyakorlatban sosem lépett működésbe, és a szabályozás jellegéből fakadóan erre nem is lenne alkalmas. Az európai mérce bemutatásakor használt idővonalon szemléltetve a hatályos szabályozás a következőképpen fest (2. ábra):

nyesítési lehetőség hatékonyságát ugyanakkor egyértelműen aláássa az a fentiekben is említett szempont, hogy az érintettnek nincs oka gyanakodnia megfigyelés lefolytatására, ráadásul az Nbtv. 48. § (1) bekezdése szerint a nemzetbiztonsági szolgálatok által kezelt adatokról az érintett kérelmére történő tájékoztatást a nemzetbiztonsági szolgálat főigazgatója diszkrecionális jogkörben megtagadhatja – mindehhez elegendő a nemzetbiztonság érdekére vagy mások jogaira hivatkoznia.

[33] Az ellenőrzés jogalapját az alapvető jogok biztosáról szóló 2011. évi CXI. törvény 18. § (1) bekezdés f) pontja szolgáltatja.

[34] 32/2013. (XI. 22.) AB határozat, ABH 2013, 924, 132.

[35] Az Nbtv. 58. § (3) bekezdésében kifejezetten nem szerepel, hogy az engedélyezőnek határozatában indokolnia kellene az engedély megadását. Az Alkotmánybíróság a részletes indokolás kötelezettségét mondta ki alkotmányos követelményként, a törvény ezzel összhangban álló módosítására azonban továbbra sem került sor.



2. ábra: Idővonal, a titkos megfigyelés folyamatának hatályos hazai modellje

	kivételes engedélyezés[36]	előzetes engedélyezés	utólagos értesítés a megfigyelésről	utólagos felügyelet
Létezik vagy nem létezik hatékonynak tekinthető formában?[37]	☒	☒	–	–
Milyen szerv végzi?	a titkos megfigyelés végrehajtásáért felelős szerv	az igazságügyért felelős miniszter	–	–

2. táblázat: A titkos megfigyelés folyamatának hatályos hazai modellje

A fentieket látva az Emberi Jogok Európai Bírósága helyettünk is levonta a következtetést: a hazai szabályozás alapjogvédelmi szintje elmarad az európai sztenderdtől. Egy tisztán elméleti kiindulópontból világosan látható, mekkora az a lehető legalacsonyabb küszöb, melyet egy képzeletbeli országnak elegendő átlépnie a strasbourgi mérce teljesítéséhez. Az előzetes engedélyezés intézményét legalábbis valamilyen bírói tisztség betöltésére alkalmas személyből vagy személyekből álló, a végrehajtó hatalomtól független szerv kezébe kell helyezni, emellett pedig gondoskodni szükséges a megfigyelt személyek utólagos, a nemzetbiztonsági célt nem veszélyeztető időpontban való értesítéséről. A *hatékonyság* követelményének kielégítéséhez mindez mégis kevés. Ha a felállított intézményrendszer az adott ország alkotmányos közegében működésképtelen, hiába felel meg minden elméleti kívánalomnak, nem lesz alkalmas a hatékony jogorvoslat biztosítására – ebből a szempontból jelentősége van a hazai alkotmányos hagyomány adta lehetőségeknek.

[36] Az Nbtv. 59. § (1) bekezdése szerint a nemzetbiztonsági szolgálatok főigazgatói a titkos információgyűjtés folytatását legfeljebb az engedélyező döntéséig engedélyezhetik, ha a titkos információgyűjtés külső engedélyeztetése olyan késedelemmel járna, amely az adott ügyben nyilvánvalóan sértené a nemzetbiztonsági szolgálat eredményes működéséhez fűződő érdeket.

[37] A táblázat a főszövegben kifejtettek alapján kizárólag azokat a jogérvényesítési lehetőségeket összegzi, melyek a hatályos szabályozás alapján hatékony formában érvényesülnek. A létező, de a gyakorlatban nem érvényesülő jogérvényesítési lehetőségeket a fent hivatkozott indokok alapján nem értékelem ilyenként.

Az alapjogvédelmi intézményrendszer kínálati oldala – lehetőségek és modellek

A következőkben az alapjogvédelmi intézményrendszer hazai „kínálati oldalát" elemzem, a hozzájuk tapadó alkotmányos hagyomány szempontjából értékelve a kontrollba bevonható intézmények alkalmasságát. A paletta áttekintésekor egy sor olyan alkotmánybírósági határozatból és egyéb forrásból meríthetünk, melyek a titkos információgyűjtés feletti külső kontroll folyamatába potenciálisan bevonható szervek alkotmányos státuszát tárgyalják – ezek közül a közelmúltban zajló folyamatokat előtérbe helyezve válogatok. A vizsgálódás középpontjában intézmények állnak, mivel a külső kontroll objektivitása és hatékonysága leginkább az abba bevont szervek függetlenségének fokától, az ott összpontosuló speciális szakértelemtől, és az adott szerv számára biztosított hatásköröktől függ, melyeket a szerv típusa bizonyos fokig szükségképpen meghatároz. A számvetés nem tér ki a civil kontroll szerepére. Ennek oka, hogy az alapjogok védelme alapvetően az állam kötelezettsége, melyet a civil szféra hatékonyan segíthet, de a terhet magát az EJEB értelmezésében sem veheti le az állam válláról.

Bírói típusú alapjogvédelem

Láthattuk, hogy az Emberi Jogok Európai Bírósága szerint is a független bíróság az első számú választás a rendelkezésre álló lehetőségek közül – ez az ideális megoldás, melyhez képest minden más elképzelés kivétel, melynek alkalmazását indokolni kell. Ennek oka – ahogyan azt fentebb idéztem –, hogy az EJEB megfogalmazásában a bíróság az a szervtípus, mely „a függetlenség, a pártatlanság és a megfelelő eljárás legjobb garanciáját nyújtja". Az EJEB azonban szükségképpen az általa ismert tapasztalatokból indult ki, ezért ahhoz, hogy a bírósági kontrollt hatékony eszköznek minősítsük, nem kerülhető meg a bírói hatalmi ág jelenlegi hazai állapotának értékelése. Ennek során elsősorban azt vizsgálom, hogy a bíróságok függetlenségének alkotmányos garanciái valóban lehetővé teszik-e azt, hogy a bíróságok hazai viszonyok között is a fair eljárás legmagasabb szintű biztosítékait garantálják.

Az aktuális folyamatok értelmezéséhez érdemes egy pillantást vetnünk a bírák kényszernyugdíjazásáról szóló alkotmánybírósági határozat[38] fontosabb megállapításaira. Ebben a döntésében a testület már az Alaptörvény rendelkezései alapján járta körül a bírói függetlenség főbb kérdéseit. A döntést azért lehet a bírói függetlenség próbakövének tekinteni, mert a 62. életévüket betöltött, jellemzően ekkor már magasabb beosztásban ítélkező bírók a korábbi szabályozás szerint 70. életévük betöltéséig háborítatlanul folytathatták tevékenységüket, az alkotmánybírósági határozat tárgyát képező szabályozás viszont a rájuk irányadó öregségi nyugdíjkorhatár betöltésekor kötelező felmentésüket írta elő. Túl a bírák elmozdításának az életpálya szempontjából nyilvánvaló személyes következményein, a törvénymódosítás az igazságszolgáltatási hatalmi ág függetlenségét egészében érintette, mivel intézményi szinten „fejezte le" a bírósági szervezetrendszert.

A probléma súlyosságára az Alkotmánybíróság is reagált, hatályba lépésének napjára visszaható hatállyal semmisítette meg a bírák jogállásáról és javadalmazásáról szóló 2011. évi CLXII. törvény érintett szakaszait.[39]

[38] 33/2012. (VII. 17.) AB határozat.

[39] Túlzás volna ugyanakkor állítani, hogy a határozatot teljes egyetértés övezte: a határozat meghozatalakor hivatalban lévő tizenöt bíróból hét bíró csatolt különvéleményt, kifejezve egyet nem értését.

Arra támaszkodva, hogy az Alaptörvény a történeti alkotmány vívmányaira az alkotmányértelmezés egyik forrásaként hivatkozik, az Alkotmánybíróság egészen 1869-ig nyúlt vissza a bírói függetlenség hagyományainak összegzésében.[40] Ezzel az Alaptörvény bírói függetlenséget rögzítő rendelkezését[41] történeti kontextusba helyezte, kimondva, hogy a bírói függetlenség és az abból eredő elmozdíthatatlanság elve nemcsak tételes alaptörvényi szabály, hanem a történeti alkotmány egyik vívmánya, ezáltal pedig olyan értelmezési alapelv, amelyet az Alaptörvény más szabályai lehetséges tartalmának feltárásakor is alkalmazni kell.[42]

A bírói függetlenség garanciája két pilléren nyugszik: a szervezeti és a státuszbeli biztosítékokon. Személyi értelemben a bírói függetlenség azt jelenti, hogy a törvényeknek való alávetettségen túl vele szemben *minden* más *függés kizárt* (Kukorelli 2007: 530). Ezt a teljes függetlenséget bontják ki azok a részletszabályok, melyek értelmében a bíró nem utasítható, illetve tisztsége „egy életre szól", legalábbis csak sarkalatos törvényben meghatározott okokból és eljárás eredményeként mozdítható el belőle.[43] Ezek a személyi garanciák a befolyásmentes ítélkezéshez szükséges szabadságot hivatottak biztosítani, döntési autonómiát garantálva a bírónak, kizárva annak lehetőséget, hogy ítélete miatt szolgálati retorzió érje. A személyi dimenziót nem lehet elválasztani ugyanakkor a szervezetitől, mivel a bírák elmozdíthatatlansága ugyanúgy jelenti a bírói jogállás, mint a független, pártatlan bírósághoz való jog garanciáját.[44] A szervezeti függetlenséget a bíró szemszöge helyett sokkal inkább a polgárok pozíciójából lehet megragadni: a független bíróság nem a bíró, hanem a bíróság előtt folytatott eljárások alanyai számára garancia.[45] Adott esetben mindebből az Alkotmánybíróság azt a következtetést vonta le, hogy az Alaptörvény rendelkezései a korhatárcsökkentés módjában és határidejében kötik a törvényalkotót[46], a bírák számára kedvezőtlen korhatárváltozásnak csak fokozatosan, megfelelő átmeneti idő alatt lehet helye[47] úgy, hogy az a bíró elmozdíthatatlanságának elvét – ezáltal pedig a bíró személyi és a bíróság szervezeti függetlenségének elvét általában – ne sértse.

[40] Az Alaptörvény R) cikk (3) bekezdése szerint az Alaptörvény rendelkezéseit azok céljával, a benne foglalt Nemzeti hitvallással és történeti alkotmányunk vívmányaival összhangban kell értelmezni. A határozat erre hivatkozva két, a polgári átalakulás szempontjából jelentős törvényre hivatkozik: a bírói hatalom gyakorlásáról szóló 1869: IV. törvénycikkre, és a bírák nyugdíjazását is tárgyaló 1871: IX. törvénycikkre.

[41] Az Alaptörvény 26. cikk (1) bekezdése szerint a bírák függetlenek, és csak a törvénynek vannak alárendelve, ítélkezési tevékenységükben nem utasíthatóak. A bírákat tisztségükből csak sarkalatos törvényben meghatározott okból és eljárás keretében lehet elmozdítani.

[42] 33/2012. (VII. 17.) AB határozat, ABH 2012, 99, 80.

[43] 33/2012. (VII. 17.) AB határozat, ABH 2012, 99, 83.

[44] 33/2012. (VII. 17.) AB határozat, ABH 2012, 99, 84.

[45] Az Alaptörvény XXVIII. cikkének (1) bekezdése szerint mindenkinek joga van ahhoz, hogy az ellene emelt bármely vádat vagy valamely perben a jogait és kötelezettségeit törvény által felállított, független és pártatlan bíróság tisztességes és nyilvános tárgyaláson, ésszerű határidőn belül bírálja el.

[46] 33/2012. (VII. 17.) AB határozat, ABH 2012, 99, 84.

[47] 33/2012. (VII. 17.) AB határozat, ABH 2012, 99, 106.

A határozatból és az abban összegzett és fenntartott korábbi alkotmánybírósági gyakorlatból[48] valóban a függetlenség erős modellje rajzolódik ki[49], az EJEB elvárása tehát a hazai viszonyok fényében sem tűnik alaptalannak.

Nem bírói típusú alapjogvédelmi szervek

Akár a bíróságokra, akár nem bírói szervekre bízzuk a nemzetbiztonsági célú titkos megfigyelések külső jogi kontrollját, ha a külső kontrolltól alapjogi szempontú mérlegelést várunk – márpedig az EJEB ítélete szerint ezt kell tőle várnunk –, akkor kizárólag alapjogvédelmi karakterű intézményekben gondolkodhatunk. Ebből az összesítésből éppen ezért marad ki az Országgyűlés Nemzetbiztonsági Bizottsága, amely már ennek a követelménynek az előszobájában elbukik: nemhogy alapjogvédelmi, de egyáltalában jogi kontroll megvalósítására sem lehet alkalmas egy olyan intézmény, amelynek eljárásában a politikai elemeknek van túlsúlya. Ehhez hasonlóan reménytelen várakozás jogi kontrollt számon kérni az igazságügyért felelős miniszteren, akit ezért szintén nem értékelek számba vehető szereplőként.

A nem bírói típusú alapjogvédelmi szervek valamilyen szempontból nem rendelkeznek a bíróságokat megillető jogállási és hatásköri jellemzők teljességével. Ez jelentheti a függetlenség korlátozottságát ugyanúgy, mint azt, hogy az adott szerv nem feltétlenül hozhat kötelező döntést (ehelyett például csak ajánlást tehet), illetve döntése bíróság előtt megtámadható, tehát nem végleges (Somody 2010: 5). E szervek eljárásainak azonban nem csak hátrányai vannak: gyorsaságuk és rugalmasságuk az alapjogvédelmi intézményrendszer értékes, a rendesbíróságok tevékenységét jól kiegészítő elemeivé teheti őket. A létező intézményrendszert szemlélve az alapvető jogok biztosa és a Nemzeti Adatvédelmi és Információszabadság Hatóság (a továbbiakban: NAIH) alkalmasságát érdemes vizsgálatnak alávetni.

a) Alapvető jogok biztosa

Az ombudsman-típusú alapjogvédelem a rendszerváltás óta része a hazai intézményrendszernek. Az állampolgári jogok országgyűlési biztosa és a szakosított biztosok által alkotott rendszer kezdeti formájához képest mára teljesen átalakult, 2012 óta az alapvető jogok biztosa tölti be az általános hatáskörű ombudsman szerepét. Az egykori szakosított biztosok

[48] 54/2001. (XI. 29.) AB határozat, 13/2002. (III. 20.) AB határozat, 1/2008. (I. 11.) AB határozat, 21/2010. (II. 25.) AB határozat.

[49] Ebben a koherens rendszerben, az ügy fokozott politikai érzékenysége miatt egyfajta átmeneti megingásként lehet értékelni a 2006 őszi tömegoszlatásokkal összefüggő elítélések orvoslásáról szóló 2011. évi XVI. törvény (az úgynevezett semmisségi törvény) alkotmányosságát kimondó 24/2013. (X. 4.) AB határozatot. Az ügy alapjául szolgáló törvény 2011-ben, évekkel a 2006-os események után azt mondta ki, hogy a tömegoszlatásokhoz kapcsolódóan a törvényben meghatározott bűncselekmények elkövetését megállapító ítéletek semmisnek tekintendők, amennyiben az elítélés vagy a megállapítás alapját kizárólag rendőri jelentés, illetve rendőri tanúvallomás képezte. A határozatot a bírói függetlenségre jelentett kockázatok szempontjából részletesen elemezte Majtényi, Somody és Vissy (2013).

közül ketten igen korlátozott jogosítványokkal az általános biztos helyetteseivé váltak[50], az adatvédelmi biztos intézménye pedig megszűnt, hasonló szerepet a NAIH volna hivatott betölteni.[51]

Az alapvető jogok biztosa független parlamenti méltóság, jogállását az Alaptörvény szabályozza.[52] Az Országgyűlés a képviselők kétharmadának szavazatával választja, tevékenységéről évente be kell számolnia. Csak a törvényeknek van alárendelve, tevékenységével összefüggésben nem utasítható. Hatásköre általános jellegű, valamennyi alapjogi visszásság ügyében vizsgálódhat szinte valamennyi hatóságnál, lehetősége van egyebek mellett a rendvédelmi szerveknél, így a Terrorelhárítási Központnál tapasztalható visszásságok kivizsgálására is.[53] Általában egyedi kérelmek alapján, kivételesen azonban hivatalból is eljárhat. Vizsgálati jogosítványait a törvény meglehetősen széles körben állapítja meg. Intézkedései ajánlás-jellegűek, a kötelező erőt nélkülözik – az intézmény jellege miatt tekintélyét a nyilvánosság ereje alapozza meg.

A hozzá hasonló nemzeti intézmények függetlenségének megítélésében kulcsszerepe van a Párizsi Elveknek[54], melyek számos garanciális követelményt támasztanak például a jelölési és megválasztási folyamattal, a szükséges szavazati többséggel, a biztosítandó mentelmi joggal és a költségvetési függetlenséggel kapcsolatban. 2016-ban az alapvető jogok biztosa az elveknek való megfelelés szempontjából a legmagasabb, „A" jelű minősítést kapta a 2014 októberét megelőző egyéves időszakra.[55]

Összefoglalóan megállapítható tehát, hogy a jogszabályi háttér alkalmas az alapvető jogok biztosa független státuszának biztosítására. A képet némileg árnyalja, hogy míg a Párizsi Elvek szerint például a nemzeti intézmények civil szervezetekkel való kapcsolattartása esszenciális kritérium a hatékony működéshez (Sziklay 2011: 87), az alapvető jogok biztosát 2014 szeptemberében meglehetősen megalázó körülmények között rendelte maga elé a parlament igazságügyi bizottsága, mivel a Magyar Nemzet megírta, hogy a biztos hivatala egyeztetett a Társaság a Szabadságjogokért (TASZ) nevű civil szervezettel a tűcsere-programról szóló jelentésük közzététele előtt.[56] Az ügyben végül kifejezetten azért

[50] Plasztikus látleletet ad erről a 3002/2012. (VI. 21.) AB végzés. Önálló hivatala betöltésének utolsó napjaiban a jövő nemzedékek országgyűlési biztosa a néhány nappal később hatályba lépett, és őt hatásköreitől megfosztó, az alapvető jogok biztosáról szóló 2011. évi CXI. törvény egyes rendelkezései megsemmisítését kérte. Az Alkotmánybíróság a beadvánnyal érdemben nem foglalkozott, a beadvány visszautasításának oka az volt, hogy a jövő nemzedékek biztosa az új jogszabály hatályba lépésével elveszítette önálló indítványozási jogát, felettese, az alapvető jogok biztosa pedig nem osztotta alkotmányossági aggályait.

[51] Ezzel a kvázi jogutódlással a következő pontban foglalkozom.

[52] Alaptörvény 30. cikk.

[53] Ajbtv. 18. § (1) bekezdés f) pont.

[54] Principles relating to the Status of National Institutions (The Paris Principles). Adopted by General Assembly resolution 48/134 of 20 December 1993.

[55]Global Alliance of National Human Rights Institutions: Chart of the Status of National Institutions, Accreditation status as of 5 August 2016.
http://www.ohchr.org/Documents/Countries/NHRI/Chart_Status_NIs.pdf

[56] „Ombudsmani meghallgatás: fegyelmit kapott az egyik ügyintéző", Mandiner, 2014. szeptember 30. http://jog.mandiner.hu/cikk/20140930_ombudsmani_meghallgatas_fegyelmit_kapott_az_egyik_ugyintezo

vonták felelősségre az ombudsmani hivatal egyik munkatársát, mert egy érintett civil szervezettel levelezést folytatott a jelentés közzétételéről. Az egyeztetés tényét a parlament igazságügyi bizottsága egyfajta *vádként* fogalmazta meg az alapvető jogok biztosával szemben, aki először *tagadta* a történteket, majd *elismerte*, hogy kommunikáltak a TASZ-szal, azzal, hogy a jelentés közzétételének idejéről nem egyeztettek. A meghallgatás során fel sem merült, hogy a Párizsi Elvek értelmében a történtek a hivatal normális működésének kereteibe tartoznának, és az eset csak annyit jelez, hogy az ombudsman ellátja feladatait. A konkrét esetben az alapvető jogok biztosát a Párizsi Elvek betartása miatt számoltatta el az Országgyűlés, megvalósítva ezzel az elvek megsértését.

Majtényi László megfogalmazásában az ombudsman intézménye lehet egyfajta „szépségtapasz", a demokráciaépítés legjobb szándéka mellett egyúttal a demokrácia hiányát is leplező szerepben (Majtényi 2014: 1) – ennek megítélése egészen biztosan nem önmagában a szabályozási háttér minőségének függvénye. Mégis elmondható, hogy bár az alapvető jogok biztosának függetlensége is összetett kérdés, a jogszabályi háttér a független státuszt megfelelően biztosítja, ezért a biztost nem volna meggyőző a függetlenség hiánya miatt kizárni az alkalmas intézmények közül.

Az alapvető jogok biztosával szemben felvethetőek ugyanakkor hatásköri érvek: hogyan akadályozna meg az ombudsman bármilyen alapjogsérelmet a titkos információgyűjtés folyamatában, ha nem rendelkezik az ehhez szükséges eszköztárral?[57] Az, hogy az alapvető jogok biztosa akár az engedélyezés, akár a felügyelet körében valódi funkciókat lásson el, hatósági karakter nélkül elképzelhetetlen. Példaként említhető, hogy korábban az adatvédelmi biztosnak voltak bizonyos hatósági jogosítványai – határozatban rendelhette el a jogosulatlanul kezelt adatok zárolását vagy törlését, megtilthatta a jogosulatlan adatkezelést vagy adatfeldolgozást, illetve felfüggeszthette az adatok külföldre továbbítását. A határozattal szemben bírósági felülvizsgálatnak volt helye. Hasonló volt a helyzet a ritkán alkalmazott titokfelügyeleti eljárásban, melynek során, ha az adatvédelmi biztos a minősített adat minősítésének megszüntetésére vagy módosítására szólította fel a titokgazdát, amennyiben a titokgazda nem fordult bírósághoz, a minősítés meghatározott határidő elteltével a biztos felszólításában foglaltaknak megfelelően módosult (Jóri 2010: 24).

Az alapvető jogok biztosának hatásköre csak a jogszabályi környezet függvénye, bevonása egy nemzetbiztonsági célú titkos információgyűjtésre vonatkozó speciális, kifejezetten erre a célra létrehozott, hatósági típusú eljárásban elfogadható megoldás. Fontos ugyanakkor hangsúlyozni, hogy szerepe nem lehet kizárólagos: határozatainak bírósági felülvizsgálatát minden esetben biztosítani kell.

b) Nemzeti Adatvédelmi és Információszabadság Hatóság

A két másik szakosított biztossal ellentétben az adatvédelmi biztos nem vált az alapvető jogok biztosának harmadik helyettesévé. A hivatalban lévő adatvédelmi biztos megbízatása az Alaptörvény hatálybalépésével megszűnt, helyette pedig megkezdte működését a

[57] Hasonló fontosságú kérdés az alapvető jogok biztosa vizsgálati jogköreinek korlátozottsága a nemzetbiztonsági szolgálatokat érintő vizsgálata során (Ajbtv. 22. § (2) bekezdés és Ajbtv. 23. §).

NAIH, melynek létrehozatalára az Alaptörvény adott felhatalmazást. A miértekkel kapcsolatban olvasható nem hivatalos magyarázatok a függetlenség szempontjából sem kifejezetten megnyugtatóak.[58]

A kimondott indokolás szerint a jogalkotó az adatvédelmi biztos intézménye megszüntetését kifejezetten egy hatósági jogkörökkel rendelkező intézmény felállításának szükségességével támasztotta alá. Az elvek szintjén valóban sikerült az új intézményt az Európai Unió által megkívánt független adatvédelmi ellenőrző hatóság koncepciójával összehangolni, a NAIH első ránézésre úgy tűnik, hogy megfelel egy független szervvel szemben támasztható követelményeknek (Szabó és Hidvégi 2014, 72.). A NAIH autonóm államigazgatási szerv, feladatkörében nem utasítható, feladatát más szervektől elkülönülten, befolyástól mentesen látja el, költségvetése az Országgyűlés költségvetési fejezetén belül önálló címet képez. Mint az autonóm államigazgatási szervekre általában, a NAIH-ra is igaz ugyanakkor, hogy függetlensége relatív, a végrehajtó hatalomtól paradox módon pont az államigazgatás részeként kellene elkülönülnie.

A függetlenségdeficit tetten érhető eleme, hogy míg az adatvédelmi biztost a köztársasági elnök javaslatára a képviselők kétharmada választotta, a NAIH elnökét a miniszterelnök javaslatára a köztársasági elnök nevezi ki. Tehát egyszerűen fogalmazva, a hatóság elnöke az lesz, akit erre a pozícióra a miniszterelnök alkalmasnak talál. Mindez elsősorban nem államszervezeti értelemben kérdőjelezi meg a NAIH függetlenségét, hanem kifejezetten az ellenőrzött szervezetektől való függetlenség iránt támaszt kétségeket (Szabó és Hidvégi 2014: 72). Ezt az általuk megfogalmazott gyanút Szabó és Hidvégi alá is támasztotta, amikor a NAIH adatvédelmi hatósági eljárásait értékelve megállapították, hogy a NAIH az állammal szemben a magán-adatkezelőkhöz képest mind a lefolytatott eljárások számát, mind a jogsértések megállapítását, mind pedig a kiszabott bírságok nagyságát tekintve jelentősen nagyobb megértést tanúsít. A vizsgálat az önkormányzatokat érintő hatósági eljárások áttekintése során politikai elfogultságot is megállapított (Szabó és Hidvégi 2014: 73-74).[59]

Ennek alapján megalapozottan állítható, hogy a NAIH a függetlenség hiánya miatt nem alkalmas arra, hogy a titkos információgyűjtés feletti kontroll részese legyen.

[58] „Az adatvédelmi biztos esetében ez az út azért nem volt járható, mert az Európai Unió szigorú irányelve a tagországok adatvédelemre létrehozott szervének teljes függetlenségét ('complete independence') írja elő, melyet az EU Bírósága egy 2010 márciusában Németországot elmarasztaló ítéletében meg is erősített. Az adatvédelmi biztost ezért nem lehetett se helyettessé degradálni, sem pedig egyszerűen felszámolni. Ki kellett találni egy új szervet – a kormányfő javaslata alapján 9 évre kinevezett – vezetővel az élén, mégpedig egy újszerűnek tűnő másik adatvédelmi törvénybe ágyazva." (Kerekes 2012: 80)
A szándéktól függetlenül érdemes megjegyezni, hogy a luxemburgi bíróság az adatvédelmi biztos pozíciójának megszüntetésével kapcsolatban az Európai Bizottság által megindított kötelezettségszegési eljárásban kimondta, hogy Magyarország megsértette az uniós jogot, mivel a személyes adatok védelméért felelős hatóságok függetlensége megköveteli, hogy a tagállamok tiszteletben tartsák a megbízatások időtartamait.

[59] A vizsgálat a 2012-től 2014. első hét hónapjának végéig terjedő időszakot fedte le.

Következtetések

Áttekintve az eldöntendő kérdéseket, a tanulmányban arra kerestem a választ, hogy melyik az a szerv, amely a függetlenség foka, illetve a rendelkezésére álló hatáskörök és a szakértelem szempontjából a legalkalmasabb a titkos információgyűjtés feletti kontroll ellátására, és az információgyűjtés folyamatának melyek azok a pontjai, melyeken a kontrollt végző szerv számára a magánszféra védelmében beavatkozási lehetőséget szükséges biztosítani.

A függetlenség és a szakértelem szempontjai között rangsorolva a Bíróság mérlegelésével ellentétben a függetlenséget helyezem előtérbe, mert azt semmi sem zárja ki, hogy egy megfelelő hatáskörökkel felruházott, a végrehajtó hatalomtól megfelelően elkülönült szerv idővel megszerezze a hatékony külső kontroll biztosításához szükséges ismereteket – ez az út a másik irányba viszont nem járható. Ebből a kiindulási pozícióból a végrehajtó hatalom részeseként politikai szempontokat érvényesítő minisztert zárom ki először az alkalmas szervek sorából. A miniszternek sem az engedélyezés, sem a folyamat bármely későbbi eleme során nem juttatható szerep. A Bíróság döntése alapján egyértelműen kizárható továbbá bármilyen olyan szerv, melynek működése a nyilvánosság elől rejtve zajlik. Ez a következtetés szintén összeegyeztethető a függetlenség követelményével: mivel a nyilvánosság a függetlenség első számú biztosítéka, a külső kontrollt nem bízhatjuk sem az Országgyűlés Nemzetbiztonsági Bizottságára, sem más hasonló formációra. Az általa végzett feladatok jellegét tekintve logikus választás volna a NAIH, ez a szerv azonban a függetlenség előkérdésén szintén elbukik. A titkos információgyűjtés az alapjogokra kiemelt kockázatot jelent, a végrehajtó hatalom féken tartását aligha várhatjuk egy olyan szervtől, melynek vezetőjét a végrehajtó hatalmi ág vezetője ülteti székébe. Az elemzés a létező intézményrendszerre koncentrált, de természetesen a külső kontroll megvalósítása elképzelhető bármilyen új, kifejezetten erre a célra létrehozott független szerv bevonásával is. Ennek lehetőségeiről csak találgathatunk, az azonban nagy biztonsággal állítható, hogy az ellenőrzött szervektől való függetlenséget a NAIH-nál magasabb szinten kell biztosítani.

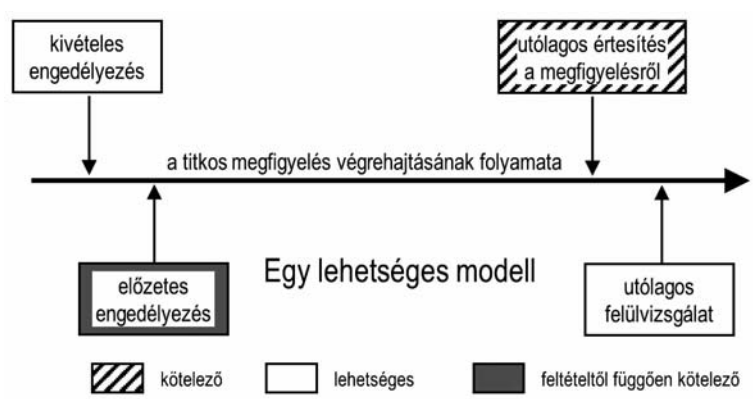
A függetlenség szempontjából a vizsgált szervek közül az alapvető jogok biztosa kiállja a próbát. A hatáskörének soft-jellegével kapcsolatos érvek szintén kezelhetők, elképzelhető volna, hogy a titkos információgyűjtés kontrolljának újraszabályozásakor a jogalkotó olyan hatáskörökkel vértezze fel a biztost, mely a vizsgálódáson túl alkalmassá tenné őt az észlelt alapjogsértések azonnali megszakítására is. A Bíróság az ombudsmanon a bírói hivatás betöltésére való alkalmasságot kérte számon, az esetjog rugalmasságát látva azonban úgy tűnik, hogy ezt a követelményt is át lehetne hidalni, ha a biztosnak a kontroll ellátására nem csak jogszabályi lehetősége volna, hanem azt valóban el is látná.

Az alapjogvédelmi intézmények közül egyedül a rendesbíróság az, melynek függetlenségét összességében a közelmúlt eseményei sem kezdték ki számottevő mértékben, hatáskörei pedig egyúttal a terület jelentős újraszabályozása nélkül is alkalmassá teszik a feladat ellátására. A bíróságokba vetett bizalom szempontjából fontos hangsúlyozni, hogy a garanciák teljességét a rendesbírósági intézményrendszer tekintetében is csak akkor feltételezzük, ha a titkos információgyűjtés feletti kontroll a bírósági intézményrendszer szerves részévé válik, nem pedig egy elszigetelt, a végrehajtó hatalom által könnyebben megkörnyékezhető különbíróság keretein belül szerveződik.

A Kormány a bíróságokat az EJEB előtt folyó eljárásban a szükséges speciális szakértelmet nélkülöző, a feladat ellátására alkalmatlan szervekként írta le, mindezt a meg-

vizsgálandó adatok jellegével, a kockázatértékelésben rejlő szubjektivitással, a nemzetbiztonság politikai természetével, valamint a Kormánynak biztosított széles mérlegelési jogkörrel alátámasztva. Ebben a felsorolásban a Kormány, szándékával ellentétben, éppen annak adta kimerítő számba vételét, hogy miért volna égető szükség a bíróságok bevonására. Az alapjogok védelme kifejezetten a mérlegelés szubjektivitásának korlátozását, valamint a politikai megfontolások és a Kormány mozgásterének jogi eszközökkel való féken tartását követeli, függetlenül attól, hogy a végrehajtó hatalom maga igényli-e saját hatásköreinek korlátozását. Fontos kiegészítő szempont, hogy a Kormány szerint nem lehet olyan pozitív jogot létrehozni a szóban forgó területen, amely a bírósági döntéseknek jogalapot szolgáltató egzakt kritériumokat határoz meg. Ezt az álláspontot az Emberi Jogok Európai Bírósága nem osztotta, az ítélet szerint nem csak a kontroll rendszerén, hanem a szabályozás színvonalán is változtatni kell az egyezménysértés kiküszöböléséhez. Mindenesetre az egészen biztos, hogy ha a Kormánynak nincsenek érvei a bíróságok meggyőzésére az információgyűjtés engedélyezésének szükségességéről és a folyamat jogszerűségéről, ennek okát nem a bírói kar felkészületlenségében kell keresni. A szakértelem hiánya kapcsán továbbá érdemes rögzíteni, hogy a bíróság az igazságügyi szakértői hálózatra támaszkodva problémamentesen boldogul a jogon kívül eső, különleges szakértelmet igénylő ügyekben is.

A beavatkozások ütemezése elsősorban a terrorelhárításért felelős szerv munkájának zavartalansága miatt fontos. Ebből a szempontból a bűncselekmények gyanúja miatt elrendelt titkos információgyűjtésnél működő kivételes engedélyezés lehetőségének fenntartása mellett foglalok állást, azzal, hogy ezt a sürgősségi intézkedést rövid és szigorúan meghatározott időtartamon belüli bírósági felügyeletnek kell alávetni. Ha a kivételes engedélyezés esete nem áll fenn, a bíróság előzetes engedélyező szerepétől nem lehet eltekinteni, hiszen ha a jogsértés megtörtént, azt semmiféle utólagos felülvizsgálat nem fordíthatja vissza. Az érintett utólagos, nemzetbiztonsági kockázatot nem jelentő időpontban történő értesítése szintén nem mellőzhető, másként a jogorvoslathoz fűződő alapjog teljesen kiüresedik. Ha a folyamat két végpontján megfelelő garanciák biztosítják a magánszféra védelmét, a folyamat közben a nemzetbiztonsági célú titkos megfigyelések zavartalansága a prioritás, ehhez azonban szükséges további garancia, hogy az ellenőrzéssel lefedett időtartam ne legyen túl hosszú, a hosszabbítást pedig szintén bíróság engedélyezze, méghozzá az ezt alátámasztó indokok ismeretében.



3. ábra: Idővonal, a titkos megfigyelés folyamatának egy lehetséges modellje

	kivételes engedélyezés	előzetes engedélyezés	utólagos értesítés a megfigyelésről	utólagos felügyelet
Létezzen vagy ne létezzen?	☒	☒	☒	☒
Milyen szerv végezze?	a titkos megfigyelés végrehajtásáért felelős szerv	bíróság	a titkos megfigyelés végrehajtásáért felelős szerv	bíróság

3. táblázat: A titkos megfigyelés folyamatának egy lehetséges modellje

Zárszó és jövőkép

Magánélet és bizonytalanság – a cím arra utal, hogy az öntudatlanul elfogadott tradeoff jegyében könnyedén hozunk áldozatokat magánszféránkból, az áldozat nagysága azonban ugyanúgy bizonytalan, mint az ettől remélt biztonság bekövetkezése (Székely, Somody és Szabó 2017a, 2017b).[60] A terrorizmus fenyegetéseitől megrendült biztonság helyreállítása nemzetbiztonsági szakkérdés, a magánszférára leselkedő kockázatok mérséklése azonban ettől eltérően elsősorban jogi kérdés, melyet nem a biztonságunkra jelentett fenyegetések elhárítására hivatott szervek igényeinek megfelelően kell megválaszolni.

A titkos információgyűjtés az elrendelés okára való tekintet nélkül igen mély beavatkozást jelent az egyén magánszférájába. Az alapjogkorlátozás alkotmányos tesztje alapján a magánszférához való jog lényeges tartalmát a korlátozás nem érintheti. De ugyan mi marad a lényeges tartalomból, ha valakinek minden on- és offline közlését megismerik, Google keresései alapján gondolatai jó részét kifürkészik és a nemzetbiztonsági szolgálatok munkatársai élőben figyelik, ahogy gyerekeinek mesét olvas, lecsót készít, vagy zuhanyzáshoz készülődve levetkőzik? Ilyen súlyos kockázat esetén különösen fontos kételkednünk minden, a szükségességi-arányossági logikán rést ütő, és az alapjogkorlátozást homályos politikai indokokkal alátámasztani igyekvő érv helyességében.

A technológia fejlődésével magánéletünk kiszolgáltatottsága inkább fokozódik, mint csökken. Az Emberi Jogok Európai Bírósága arra figyelmeztetett, hogy a technológiai fejlődés egyre égetőbbé teszi a magánélethez való jog Egyezmény szerinti védelmét; ideális esetben a megfigyelési módszerek fejlődésével együtt fejlődnének az alapjogokat védő garanciák.[61] A Belügyminisztériumban jelenleg is folyamatban van az új törvényjavaslat szövegezése, a tét pedig igen magas. Nyilvános vita híján egyelőre csak bizakodhatunk, hogy a minisztérium olyan szabályozási megoldásban gondolkodik, amely a választott intézményeket tekintve alkalmas az alapjogvédelem szempontjainak hatékony érvényesítésére. Az elemzés a mérlegelendő szempontok tisztázásához kívánt hozzájárulni.

[60] A privacy-security tradeoff tarthatatlanságának jól feldolgozott nemzetközi szakirodalma van, e körben említhető például Pavone és Degli Esposti (2010), illetve Moore (2011) ezzel foglalkozó tanulmánya.

[61] *Copland v. The United Kingdom*, judgment of 3 July 2007, no. 62617/00, 41.

Irodalom

Jóri András, „Az adatvédelemért és az információszabadságért felelős biztos intézményéről", *Fundamentum*, XIV. évf. (2010) 2. szám, 20-29. old. http://www.fundamentum.hu/sites/default/files/10-2-02.pdf

Kerekes Zsuzsa, „Lejtőn az információszabadság", *Fundamentum*, XVI. évf. (2012) 2. szám, 74-89. old. http://www.fundamentum.hu/onkormanyzatisag/cikk/lejton-az-informacioszabadsag

Kukorelli István (szerk.), *Alkotmánytan I.*, Osiris Kiadó, Budapest, 2007.

Majtényi László, „A független ombudsmanintézményeket helyre kell állítani, az alapvető jogok biztosától pedig továbbra is elvárható a jogállami jogvédelem", *MTA Law Working Papers*, 2014/47. http://jog.tk.mta.hu/uploads/files/mtalwp/2014_47_Majtenyi.pdf

Majtényi László, Somody Bernadette és Vissy Beatrix, „Jobbhorog a bírói függetlenségre", *Élet és Irodalom*, LVII. évf. (2013) 43. szám. http://www.ekint.org/fuggetlen-igazsagszolgaltatas/2013-10-25/majtenyi-laszlo-somody-bernadette-vissy-beatrix-jobbhorog-a-biroi-fuggetlensegre

Moore, Adam D., „Privacy, security, and government surveillance: Wikileaks and the new accountability", *Public Affairs Quaterly*, Vol. 25. (2011) No. 2., pp. 141-156 https://www.law.upenn.edu/institutes/cerl/conferences/ethicsofsecrecy/papers/reading/Moore.pdf

Pavone, Vincenzo and Sara Degli Esposti, „Public assessment of new surveillance-oriented security technologies: Beyond the trade-off between privacy and security", originally published online 26 August 2010 http://dx.doi.org/10.1177/0963662510376886

Szabó Máté Dániel és Hidvégi Fanny, „Két ítélet és végrehajtásuk. Az Európai Bíróságnak az adatvédelmi biztosról és az adatmegőrzésről szóló ítéletei és azok utóélete Magyarországon", *Fundamentum*, XVIII. évf. (2014) 4. szám, 69-82. old. http://www.fundamentum.hu/sites/default/files/14-4-06.pdf

Somody Bernadette, „Alapjogvédelem a bíráskodáson túl – Ombudsmanok és alapjogvédő hatóságok Magyarországon", *Fundamentum*, XIV. évf. (2010) 2. szám, 5. old. http://www.fundamentum.hu/sites/default/files/10-2-01.pdf

Székely Iván, Somody Bernadette és Szabó Máté Dánie, „Biztonság és magánélet: az alku-modell megkérdőjelezése és meghaladása I. rész: Társadalomelméleti és szociológiai megközelítések", *Replika*, 103. szám (2017a)

Székely Iván, Somody Bernadette és Szabó Máté Dánie, „Biztonság és magánélet: az alku-modell megkérdőjelezése és meghaladása II. rész: Jogi és döntéstámogatási megközelítések", *Információs Társadalom*, XVII évf. 1. szám (2017b), 7-23. old. http://dx.doi.org/10.22503/inftars.XVII.2017.1.1

Sziklay Júlia, „Az ombudsman nemzeti emberi jogi intézményi (NHRI) státusa", *Nemzet és Biztonság*, IV. évf. (2011) 10. szám, 86-90. old. http://www.nemzetesbiztonsag.hu/cikkek/sziklay_julia-az_ombudsman_nemzeti_emberi_jogi_intezmenyi__nhri__statusa.pdf

Pásztor Emese 2011-ben végzett az ELTE Állam- és Jogtudományi Karán. Jelenleg az Eötvös Károly Intézet kutatója, emellett pedig az ELTE Állam- és Jogtudományi Doktori Iskolájának és az egyetem Master in European Human Rights képzésének hallgatója. Korábban tanácsadóként dolgozott a közigazgatásban, rendészeti jogi területen. Alkotmányjogi PhD tanulmányait 2014-ben kezdte, kutatási területe a magánszféra védelme és a magánszférát érintő állami beavatkozások terjedelme, különös tekintettel a család magánszférájára. 2016-ban jogi szakvizsgát tett, magyarul, angolul és spanyolul beszél.

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 iránt uk 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.

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.

Kiss Attila – Krasznay Csaba

A felhasználói viselkedéselemzés kiberbiztonsági előnyei és adatvédelmi kihívásai

Bevezetés

Azok számára, akik évek, évtizedek óta az információbiztonság területén dolgoznak, nem meglepő, hogy egyre több és egyre komplexebb támadás indul az információs infrastruktúrák ellen. Azzal azonban, hogy a média is egyre többet foglalkozik a kibertámadásokkal, illetve hogy a mindennapi ember is a saját bőrén érezheti ezek hatását, például a zsarolóvírusok jelentette közvetlen károk útján, kezd folyamatosan a közbeszéd részévé válni ez a fenyegetés. A kiberbiztonság objektív mutatói mellett tehát a szubjektív percepció is romlik, így a védelemmel foglalkozó szakértőknek olyan megoldásokat kell keresni, melylyel érdemben lehet javítani a helyzeten.

Mivel a biztonsági problémák okaként első helyen a felhasználók ismerethiányát szokták feltüntetni, napjainkban fokozottan jelenik meg a biztonságtudatossági oktatások fontossága. Ez azonban nem elégséges. A szofisztikált támadások során a tapasztalatok szerint a támadók biztosan megtalálják azokat a felhasználókat, akiknek a hibáit kihasználva be lehet jutni egy rendszerbe. Ezért a megoldásszállítók között folyamatos a versenyfutás a kiberbiztonság „Szent Gráljának" a megtalálásában, melynek segítségével a támadási kísérletek még korai fázisban észlelhetők és megállíthatók. Ilyen csodafegyver azonban valószínűleg nincsen. A létező technológiák jó összehangolása és a stratégiai gondolkodás vezethet oda, hogy a számítógépes rendszerekre leselkedő veszélyeket elfogadható szintre lehessen csökkenteni.

Ez persze nem jelenti azt, hogy ne lennének olyan innovatív megoldások, amelyek érdemben képesek javítani a kiberbiztonság állapotán. Az egyik ilyen megoldás a felhasználói viselkedés elemzése. Az informatikai erőforrások robbanásszerű fejlődése lehetővé tette, hogy a nagy mennyiségű digitális adatból, amelyet egy felhasználó a munkája során generál, létre lehessen hozni egy olyan profilt, amely a felhasználóra jellemző, „szokásos" tevékenységet mutatja be. Ezt használják ki az elektronikus kereskedelem során, például a közösségi oldalakon látható célzott, személyre szabott hirdetések a felhasználói profil alapján kerülnek megjelenítésre. Ha azonban ismert a „szokásos", akkor ismert a „szokatlan" tevékenység is. Ez ad lehetőséget a védelmi megoldások tervezésére, építve arra, hogy ha egy felhasználót sikeresen támadnak, majd a hozzáférési jogosultságaival visszaélve bejutnak a rendszerbe, akkor a humán karakterisztikák megváltoznak, hiszen más ember, más szokásokkal fogja a rendszert használni. Ezt a változást pedig jó eséllyel detektálni tudja a rendszer.

A jó védelem azonban folyamatos megfigyeléssel jár, hiszen ez az alapja a hatékony felhasználói profil felépítésének. Ahol pedig megfigyelés van, ott fokozottan kell figyelni a személyes adatok kiemelt védelmére is, hiszen a begyűjtött adatok részletes információt nyújtanak még a felhasználó által végzett legapróbb tevékenységről is. Ezzel pedig el is érkeztünk a biztonság kontra személyes adatvédelem kérdéskörhöz, mely a Snowden-féle szivárogtatás óta kiemelt figyelmet kapott az egész világon. Érdemes tehát részletesebben is megismerni, mit nyerhet és milyen áron a társadalom a mesterséges intelligencia és a Big Data elemzés elterjedésével!

A kiberbiztonság aktuális kihívásai

Sokan, sokféleképpen próbálják megbecsülni, mekkora kárt okoz a globális gazdaság számára a kiberbűnözés. A Cybersecurity Ventures (2016) elemzése 3 billió dollárra teszi a jelenlegi károsszeget, mely véleménye szerint 2021-re akár 6 billió dollárra is felkúszhat, beleértve ebbe minden direkt és indirekt káreseményt, így a személyes adatok szivárgása okozta kárt, üzleti titkok nyilvánosságra kerülését, esetleg (kritikus) infrastruktúrák sérülését. A Ponemon Institute (2016) riportja szerint egy nagy szervezetnek évente átlagosan 4 millió dollár kárt okoznak a kibertámadások. Bár ezek a számadatok nem feltétlenül pontosak, még ha nagyságrendi tévedések is vannak bennük, mutatják, hogy mekkora gazdasági kárt okoz az informatikának való kitettség. Egyben mutatja azt is, hogy a kiberbűnözéssel foglalkozó csoportok bevétele is milliárd dollárokban mérhető, bár erre leginkább az egyes online identitások feketepiaci áraiból lehet következtetni. A Dell Secureworks (2016) gyűjtése szerint például egy „átlagos" üzleti felhasználói fiók ára a Darkweben 20 és 149 dollár között van, egy európai bankkártya adatait pedig 40 dollárért lehet megvásárolni. Ilyen digitális adatok pedig milliószámra állnak rendelkezésre az erre szakosodott bűnszervezeteknél.

Nehezen választható el a kiberbűnözéstől az államilag támogatott kiberkémkedés és a kiberhadviselés, hiszen ezek személyi és technológiai háttere gyakran összefolyik. Miután a NATO a 2016-os varsói csúcson hivatalosan is műveleti területté nyilvánította a kiberteret, nem csak a szervezetek egyéni védelmében, hanem a nemzetvédelemben is kritikussá vált az információbiztonság kiemelt kezelése – hivatalosan is (Minárik 2016). Nem véletlen, hogy napjaink politikai diskurzusában az egyik első kérdés, amit a megválasztott politikai vezető megkap, a kiberbiztonsággal kapcsolatos terveiről szól (Lee 2016).

Függetlenül attól, hogy mi a támadói motiváció, a végrehajtás eszköztára nagyon hasonló minden esetben. Hutchins és szerzőtársai (Hutchins et al. 2011) alapműnek számító cikkükben mutatták be a modern kibertámadások folyamatát és az elhárítás eszközeit. A folyamat az 1. ábrán látható. A jelen tanulmány szempontjából kulcsfontosságú Kézbesítés pontnál a következő megfogalmazás olvasható: „A fegyverként használható tartalmak három leginkább elterjedt célbajuttatási módszere a Lockheed Martin Computer Incident Response Team (LM-CIRT) 2004-2010 közötti megfigyelései alapján az e-mail csatolmányok, a weboldalak és a hordozható USB eszközök". Ez a megállapítás továbbra is igaz, egyben jelzi, hogy a támadó és a célpont közötti elsődleges kapcsolat egy, a szervezet infrastruktúrájához hozzáféréssel rendelkező személy. A védekezésben pedig éppen ezért kiemelt szerepe van az éber felhasználónak, aki képes a támadást észrevenni.

Pusztán a felhasználói éberségre azonban nem lehet építeni. A Nemzetközi Távközlési Unió adatai szerint 2016 végén a világ népességének 47%-a használja az internetet (ITU 2016). Egy nagyvállalatnál több tízezer ember rendelkezik valamilyen szintű hozzáféréssel az informatikai rendszerhez. Ebben a tömegben elég egy figyelmetlen vagy képzetlen felhasználó és a legfontosabbnak tartott védelmi vonal máris elesett. Nemeslaki és Sasvári (2014) a hazai biztonságtudatosság helyzetét vizsgálva is hasonló megállapításra jut, felmérésük alapján az üzleti és a közszférában dolgozók több mint harmada meg van győződve arról, hogy a számítógépük nem potenciális célpontja egy rosszindulatú támadásnak. Éppen ezért ma már minden szakembernek azzal kell számolnia, hogy a Kézbesítés sikeres lesz, így a későbbi fázisokban kell a megfogni a támadást.

1. ábra: Pusztítási lánc a kibertérben
(Hutchins et al. 2011)

A későbbi fázisokat elsősorban műszaki eszközökkel lehet kontroll alatt tartani. A hagyományos védelmi filozófia a megelőző (preventív) intézkedéseket részesíti előnyben, azaz olyan technológiák használatát, melyek nem engedik végrehajtódni a pusztítást kifejtő kódokat, illetve blokkolják a kompromittált erőforrásokhoz való távoli hozzáférést. Ezeknek a preventív megoldásoknak azonban hátránya, hogy elsősorban a korábbról már ismert támadási mintákat képesek kezelni, azaz a minta kis változtatásával a védelmi hatékonyság drasztikusan csökkenthető. Az elmúlt években emiatt a stratégiai gondolkodás változik, egyre jobban előtérbe kerülnek a felismerő (detektív) megoldások, melyek a több forrásból érkező információk alapján próbálják segíteni a támadások felismerését.

A klasszikus felismerő védelmi intézkedések közös tulajdonsága, hogy minél több forrásból érkező adat feldolgozásával segítik a döntéshozatalt, azaz annak eldöntését, hogy valójában kiberbiztonsági incidens történt-e. A két legrégebben használt technológia ezen a területen a behatolás-detektáló rendszer (Intrusion Detection System – IDS) és a rendszerek naplóadatait feldolgozó rendszer, melynek jelenleg bevett elnevezése biztonsági incidens- és eseménymenedzsment rendszer (Security Incident and Event Management – SIEM). A két rendszer között több a hasonlóság, mint a különbség. A fő eltérés az, hogy míg az IDS a hálózati forgalom elemzésére támaszkodik, a SIEM rendszerek a különféle naplóadatok közötti korrelációkból építkeznek. Ezen túlmenően főleg a hasonlóságokat érdemes vizsgálni!

A két technológiában közös, hogy hatalmas mennyiségű adatból tudnak építkezni, mely adatok strukturáltak ugyan, de az egyes források adatformátuma jellemzően különböző. A döntéstámogatást szabályalapon segítik, azaz a rendszerek által korábbról már ismert mintázatok alapján jelzik az esetleges behatolást. Hatalmas mennyiségű riasztást generálnak, így a nem megfelelően finomhangolt rendszer riasztásainak áttekintéséhez jelentős emberi erőforrás szükséges. Nagyon gyakoriak a hamis pozitív riasztások, melyek miatt a szabályrendszert folyamatosan finomítani kell. Eközben a valódi támadások, me-

lyek nem szerepelnek az ismert mintázatok között, könnyen rejtve maradhatnak.

Ezek a kihívások vezettek el ahhoz a felismeréshez, hogy mindkét technológiát érdemes olyan irányba fejleszteni, amely felhasználja a mesterséges intelligenciával kapcsolatos aktuális kutatásokat, hiszen alapvetően minden rendelkezésre áll a számítógéppel támogatott döntéshozatalhoz – a nagy mennyiségű adat és az igény arra, hogy ezekből minél hasznosabb információ álljon elő. A 2000-es évek közepén már számos kutató publikált az IDS-ek jövőjéről, például Abraham és szerzőtársai (2005) így fogalmazták meg a state-of-the-art helyzetet:

> „A behatolás-detektálásnak két típusa van: a nem szabályszerű használat és az anomália detektálása. A nem szabályszerű használat azonosításához a támadás azon jól definiált mintázatát használják, melynek segítségével ki lehet használni egy rendszer vagy alkalmazás sebezhetőségét. Ezek a mintázatok előre be vannak kódolva a rendszerbe és pontosan meg kell egyezniük a felhasználói tevékenységgel a behatolás detektálásához. Az anomália alapú behatolás-detektálás a normális felhasználás mintázatát használja a behatolás érzékeléséhez. A normális felhasználás mintázatát a rendszerek statisztikai értékeiből állítják elő. A felhasználó viselkedését ebben az esetben folyamatosan megfigyelik és bármilyen eltérést az összeállított normális viselkedésmintától behatolásként érzékelnek."

Elemzésük célja annak kimutatása volt, hogy mennyire hatékonyak az egyes gépi tanulási algoritmusok a kor lehetőségei mellett. Megállapították, hogy a mesterséges intelligencia jelentős segítséget nyújt a támadások észlelésében, de így fogalmazták meg a szükséges kompromisszumokat: „Az IDS által ellenőrizendő adathalmaz hatalmas, még egy kis hálózat esetében is. Az elemzés rendkívül nehéz még számítógépes támogatással is, mivel bizonyos elemzési módok nehézzé teszik a gyanús viselkedési mintázatok felfedezését. Az elemzési eredmények között komplex kapcsolatok vannak, melyeket a gyakorlatban emberi értelemmel lehetetlen felfedezni. Az IDS-ben ezért csökkenteni kell a feldolgozott adatok mennyiségét."

Hasonló kihívásokkal szembesültek a SIEM rendszerek üzemeltetői és a kor színvonala mellett hasonló irányban folytak a kutatások is. A matematikai és az informatikai háttér fejlődésével azonban folyamatosan jelentek meg azok a megoldások, amelyek lehetővé tették a nagy mennyiségű strukturált (és nem strukturált) adat hatékony elemzését, közel valós időben. 2010 környékén már a közösségi hálózatokat és a keresőmotorokat fejlesztő cégek elsődleges üzleti modelljévé vált a „normális" viselkedés, a felhasználók érdeklődési körének egyre pontosabb kiismerése. Csak idő kérdése volt, hogy mikor jelenik meg a kiberbiztonságban is ez a technológia, amely segíteni tud a „szokatlan" viselkedés azonosításában, ezzel megoldást kínálva arra, hogy túl lehessen lépni a hagyományos, szabályalapú megelőző és észlelő védelmi rendszerek adta határokon.

Felhasználói viselkedéselemzés a kiberbiztonságban

A bűncselekmények előrejelzése, ezzel pedig a biztonság növelése régóta foglalkoztatja az emberiséget. Elég csak Philip. K. Dick klasszikus novellájára, a Különvéleményre gondolni, mely már 1956-ban felvetette azt a kérdést, milyen kihívásokkal jár az, ha a „mes-

terséges" intelligencia segíti az emberiséget a bűnmegelőzésben, lényegében bizonyítékok nélkül ítélve bűnösnek a jövőbeni elkövetőt. Bár sokaknak eszébe jut ez az analógia a Big Data elemzés, a mesterséges intelligencia és a biztonság kapcsán, a társadalmi nyereség mégis olyan előnyösnek látszik, hogy az államok egyre jobban támaszkodnak ezekre a technológiákra, szélesebb körben kívánják azokat alkalmazni, akár az állampolgárok magánszférájának, információs önrendelkezési jogának korlátozása, szűkítése mellett is.

Természetesen számos olyan terület létezik, ahol közmegegyezés van az államok és az állampolgárok között abban, hogy a biztonság javítása érdekében a személyes adatok védelmét valamennyire háttérbe kell szorítani. Iverson (2015) kutatásában hat ilyen területet jelölt meg: a nemzetbiztonságot, a közbiztonságot, a tulajdon biztonságát (például kamerás megfigyeléssel), az információbiztonságot, a családok biztonságát (egészségügy) és a pénzügyi biztonságot.

A magánszféra védelméhez fűződő alapjog korlátozása ezeken a területeken jellemzően törvényi szinten került rögzítésre[1], de az információbiztonság és a hozzá kapcsolódó tulajdon biztonsága területén főleg a kialakult adatvédelmi joggyakorlat és a nemzeti adatvédelmi hatóságok, bíróságok jogértelmezése adhat csak iránymutatást. A rögzített jogok és kötelezettségek többnyire világosak, a Big Data és a mesterséges intelligencia azonban olyan értelmezési nehézségeket, kiskapukat hoztak a rendszerbe, melyek számos új kérdést vetnek fel a biztonság és az adatvédelem kapcsolatában.

Ezt legerőteljesebben Edward Snowden, a Booz Allen Hamilton cégen keresztül az amerikai National Security Agencynek (NSA) dolgozó elemző világot megrengető szivárogtatása támasztotta alá. Az NSA megfigyelési tevékenysége súlyosan sértette azokat az adatvédelmi elveket, melyeket az Európai Unióban természetesnek veszünk, de még a jóval megengedőbb, az információ szabadabb áramlását támogató amerikai jogrenddel is ellentétes volt a kialakított adatgyűjtési gyakorlat. Lyon (2014) összefoglaló cikkében mutatja be mindazt, amit a Snowden szivárogtatás által tudott meg a világ a Big Data felhasználásáról a nemzetvédelmi szektorban. Cikkének konklúziójaként két megállapítást tesz.

> „Egyrészt, milyen módon és milyen mértékben jelzi a Snowden-szivárogtatás azt, hogy a Big Data alkalmazása egyre fontosabb a megfigyelésben? A válasz egyértelműen az, hogy nagyon fontos. A legfontosabb Snowden-felfedések, különösen azok, amelyeknél a metaadatok kiemelt fontosságúak, függést mutatnak a Big Datától. A második kérdés az, hogy mennyire változtatják meg ezek a technikák a megfigyeléssel kapcsolatos politikát és gyakorlatot? Új trendek vannak, vagy a korábbiak kiterjesztéséről van szó? A bizonyítékok ismét arra utalnak, hogy a Big Data használata erősen torzítja a megfigyelést a technológiai

[1] Lásd például a tájékoztatáshoz fűződő jog korlátjaként az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (a továbbiakban: Infotv.) 19.§-ban megjelenő területeket, ahol az érintett jogait törvény korlátozhatja: „az állam külső és belső biztonsága, így a honvédelem, a nemzetbiztonság, a bűncselekmények megelőzése vagy üldözése, a büntetés-végrehajtás biztonsága érdekében, továbbá állami vagy önkormányzati gazdasági vagy pénzügyi érdekből, az Európai Unió jelentős gazdasági vagy pénzügyi érdekéből, valamint a foglalkozások gyakorlásával összefüggő fegyelmi és etikai vétségek, a munkajogi és munkavédelmi kötelezettségszegések megelőzése és feltárása céljából – beleértve minden esetben az ellenőrzést és a felügyeletet is –, továbbá az érintett vagy mások jogainak védelme érdekében."

megoldástól való függés irányába (...) megnövelve a prediktív analitika fontosságát annak érdekében, hogy előre lehessen látni, meg lehessen jósolni bizonyos történéseket."

Ez a fajta függés a technológiától azonban nagyon veszélyes. Boyd és Crawford (2012) részletesen kifejti, mennyi kérdést vet fel a Big Data elemzés használata. Cikkükben hat olyan területet fogalmaznak mely, amelyeknek mindenkit aggodalommal kell eltölteniük a Big Data korlátlan használata esetén. Tanulmányunk szempontjából talán a legérdekesebb kritikai észrevétel az, hogy a kontextusból kiragadott Big Data eredmény elveszíti a jelentését, valamint az, hogy attól még, hogy valami hozzáférhető, még nem feltétlenül etikus a felhasználása. A biztonsági rendszerek sajátossága, hogy bár hihetetlen mennyiségű információt lehet belőlük kinyerni, kiemelt figyelmet kell fordítani arra, hogy a döntés meghozatalánál ezt az információhalmazt etikusan, a kontextus ismeretében használják fel.

Egy számítógép azt teszi, amit a programozója mond, így komoly hiba lenne egy program kimenetére bízni egy automatikus döntést. A Big Data és a mesterséges intelligencia azonban olyan lehetőség a biztonsági szakma kezében, amelyet egyértelműen használni kell. Olyan megoldásokat kell tehát fejleszteni, amelyek figyelembe veszik azokat az etikai elveket, amelyek egyébként az egyes európai és nemzeti adatvédelmi szabályokból is levezethetők.

A felhasználói viselkedéselemzés jogi szemszögből

Fel kell tennünk a kérdést ugyanakkor, hogy mennyiben jelenthetnek jogszerű megoldást a kibertér kihívásaira az itt bemutatott megoldások, illetve az azok továbbfejlesztésének eredményeképpen született – a viselkedést egyre több adatot felhasználva, még több szemszögből, hatékonyabban elemző és már előre is jelző – új rendszerek.

Általánosságban elmondható, hogy a viselkedésminta kialakítása, vagy az információs rendszer szokásos adatforgalmának meghatározása érdekében az érintett felhasználó számos adata rögzítésre kerül. Az elemző rendszerek figyelhetik a böngészési szokásait, elektronikus levelezését, a letöltött csatolmányainak tartalmát, a belső munkahelyi információs rendszer használatát, sőt a metaadatok mellett rögzíthetik akár az elektronikus kommunikáció tartalmát is.

Ha ezek az adatok később külön-külön, vagy akár kombinálva összefüggésbe hozhatóak maradnak az egyes felhasználókkal, vagy azokból következtetés vonható le az érintett természetes személyre, akkor – annak helytállóságától, etikai megítélésétől, jogszerűségétől, esetleges következményeitől függetlenül – személyes adatok kezeléséről beszélünk (Adatvédelmi Munkacsoport 2010 és Infotv. 3.§).

Gyakran hallani a profilozást folytató adatkezelőktől, hogy valójában nem kezelnek személyes adatot, hiszen csak a hálózathoz csatlakoztatott eszközöket figyelik, nem az azt használó magánszemélyt. Szintén gyakori érv, hogy a gyűjtött adatokat álnevesítik[2], illetve

[2] A közhiedelemmel ellentétben nem elegendő a természetes azonosító adatot egy számsorra cserélni, az álnevesítés adatvédelmi és adatbiztonsági követelményeit a 29. cikk szerinti Adatvédelmi Munkacsoport 05/2014. számú véleményében találjuk.

anonim módon gyűjtik, tehát ők nem kötelesek megfelelni adatvédelmi jogi követelményeknek. Ohm (2009) kutatási eredményei ugyanakkor azt mutatják, hogy az anonim adattárolás illúzió[3] az olyan adatgyűjtések esetében, ahol elegendően nagyszámú adat és idő áll rendelkezésre, így tipikusan a profilozás során is. Alexin (2014) bemutatja, hogy már három, első ránézésre az érintetthez szorosan nem kapcsolható azonosító (irányítószám, nem, születési dátum) összekapcsolásával is nagy valószínűséggel egyetlen személyt azonosíthatunk be. A viselkedéselemzést végző személy vagy szervezet (a továbbiakban: adatkezelő) tevékenysége pedig pont erre irányul – szeretné fokozatosan felismerni a felhasználó (jogi szóhasználatban: érintett) szokásait, gyakori hibáit, vagy érdeklődési körét, hogy aztán bizonyos esetekben egyre pontosabban tudja előre jelezni az érintett várható viselkedését egy adott élethelyzetben. A viselkedéselemzés – függetlenül attól, hogy a profilozás célja az információbiztonság fenntartása, a dolgozók teljesítményének (hasznosan töltött munkaidejének) monitorozása, vagy akár személyre szabott tartalmak, reklámok megjelenítése – veszélyt jelent az érintett alapvető emberi jogaira és szabadságaira (Nemzetközi Távközlési Adatvédelmi Munkacsoport 2013).

Számos nemzetközi dokumentum rögzíti az érintett magánélete tiszteletben tartásához fűződő jogát, beleértve kommunikációjának bizalmas jellegét és személyes adatai védelmét.[4] E jogoknak – bár esetenként korlátozottan – érvényesülniük kell a személyes adatok kezelésének valamennyi területén, beleértve a rendőrségi, igazságügyi, valamint a nemzetbiztonsági célú adatkezeléseket is.[5] Az Emberi Jogok Európai Bírósága kimondta emellett, hogy napjainkra a magán- és a szakmai élet kérdései nehezen különíthetők el egymástól, így a munkahelyi viselkedés és kommunikáció megfigyelése szükségszerűen beavatkozást jelent az érintettek magánéletébe is.[6] A levélküldemények felbontását és a telefonok lehallgatását vizsgáló döntéseken[7] túl a Bíróság kimondta azt is, hogy a munkahelyi e-mailek tartalma, sőt kommunikációjának metaadatai is az érintett védendő személyes adatai.[8]

Fontos kiemelnünk, hogy nem vonatkozik azonban adatvédelmi jogi előírás azokra az adatkezelésekre, amelyek kizárólag magáncélból történnek. Ennek tekinthető például, ha egy profilozást végző természetes személy pusztán a saját információs rendszere védelme érdekében vesz igénybe egy monitorozást végző terméket, és így készít viselkedésmintát saját magáról, amelyhez más, még az elemző szoftver gyártója sem férhet hozzá.

Ettől a nem túl gyakori esettől eltekintve azonban az Európai Unió valamennyi tagállamában szigorú jogszabályi követelmények kapcsolódnak az üzleti életben és a közszfé-

[3] *A deanonimizálás lehetőségeiről részletesen ír jelen lapszámunkban Gulyás Gábor György – a szerk.*

[4] A Liszaboni Szerződéssel 2009-ben elfogadott Európai Unió Alapjogi Chartájának 7. és 8. cikke tovább pontosította az Európa Tanács országai által 1950-ben elfogadott Emberi Jogok Európai Egyezményének 8. cikkében kifejtett alapjogot.

[5] Az EU adatvédelmi tárgyú jogszabályai 2018. májusig csak a nemzetközi adatáramlás kapcsán tartalmaznak kötelező előírásokat e területen, de az Infotv. hatálya és az Európa Tanács 108. egyezménye már most is kiterjed ezekre.

[6] Elsők között a Niemietz kontra Németország (13710/88) ügyben mondja ki az Európa Tanács 108. egyezménye kapcsán, de az ebben lefektetett elveket később az Európai Unió Bírósága is átveszi.

[7] Lásd például az Emberi Jogok Európai Bíróságának Halford v. Egyesült Királyság (1997) 20605/92. ügyében.

[8] Lásd bővebben az Emberi Jogok Európai Bíróságának Copland v. Egyesült Királyság (2007) 62617/00. ügye.

rában is a személyes adatok gyűjtéséhez, elemzéséhez, összefoglalóan kezeléséhez. Ezek azonban főleg az elveket rögzítik, ritka az egyes technológiákra vonatkozó speciális előírás, így a viselkedéselemzésen alapuló megoldások esetében is főleg az adatvédelmi hatóságok jogértelmezése, gyakorlata az irányadó.

Az alapelvek jelentősége

Az adatkezelés, így a profilozás is csak megfelelő korlátok között, jogszerű célhoz kötötten és megfelelő jogalap birtokában, az érintett jogait – kiemelten a tájékoztatáshoz (hozzáféréshez) fűződő jogát – tiszteletben tartva, valamint az adatok biztonságát garantálva válhat jogszerűvé.

Az adatminimalizálás és célhoz kötöttség elve alapján csak a jogszerű adatkezelési cél megvalósításához feltétlenül szükséges adatok gyűjthetőek, és csak olyanok, amelyek alkalmasak is annak eléréséhez. Az így gyűjtött adatokat ezt követően is csak az eredeti célhoz kötötten lehet felhasználni. Jogellenes például az információbiztonság, a rendszer védelme céljából gyűjtött adatok alapján meghatározni a dolgozó munkával töltött idejét, pártállását, vagy szabadidős érdeklődési körét. Szintén tilos az előre meghatározott cél nélküli, későbbi felhasználás érdekében történő úgynevezett „készletező adatgyűjtés".

A törvényes cél érdekében is csak akkor kezelhető személyes adat, ha megfelelő jogalappal történik. Meg kell különböztetnünk az érintett hozzájárulásán alapuló adatkezelést (Infotv. 5.§ (1) a)), törvény vagy – törvény felhatalmazása alapján, az abban meghatározott körben – helyi önkormányzat rendelete által előírt „kötelező" adatkezelést (Infotv. 5.§ (1) b)), illetve az érdekmérlegelésen alapuló eseteket (Infotv. 6.§).

A viselkedéselemzéshez közvetlenül kapcsolódó követelmény az adatminőség elvének való megfelelés is, amely előírja, hogy csak naprakész, pontos, és jogszerű forrásból származó adatok alapján vonjunk le következtetést a felhasználóról. Ide kapcsolódik az Európai Unió Bírósága által kifejtett[9], és az EU adatvédelmi reformjában is megjelenő „jog az elfelejtődéshez" (Right to be forgotten)[10] elve. Székely (2013) szerint e jog „érvényesíthetőségének előfeltétele, hogy az emberek egyáltalán tudatában legyenek annak, hogy ki, milyen célból, milyen adataikat kezeli – azaz gyűjti, elemzi és felhasználja – és azok törlését hol követelhetik. Ellenkező esetben hiába lesz jogunk ahhoz, hogy elfelejtsenek és töröljenek, ennek gyakorlati érvényesíthetőségétől egyre messzebb kerülünk." Az elfelejtődéshez való jog tehát úgy garantálható, ha az érintett tisztában van azzal, hogy milyen adatkezelés alanya (titkos megfigyelés csak bírói felügyelettel, törvény alapján végezhető), a cél megvalósulása érdekében pedig a lehető legkorábban tájékoztatni kell a profilozásról.

További előírásokat találhatunk még az adatkezelés időtartamára, az adatfeldolgozó igénybevételére és az adattovábbításra vonatkozóan is, valamint az adatkezeléseket be kell jelenteni az adatvédelmi hatóság, nálunk a Nemzeti Adatvédelmi és Információszabadság Hatóság (a továbbiakban: NAIH) által vezetett adatvédelmi nyilvántartásba.

[9] Lásd C-131/12. Google Spain v AEPD and Mario Costeja Gonzalez ügy.
[10] Más fordításban: Jog ahhoz, hogy elfelejtsenek.

A viselkedéselemzés jogszerű alkalmazási területei

A korábbiakban elemzett biztonsági kihívások miatt az új védelmi technológiák alkalmazása néhány területen a veszélyek ellenére is indokoltnak tűnik. Az állami szereplők oldaláról komoly nemzetgazdasági, bűnüldözési, nemzetbiztonsági, honvédelmi érdek fűződik a tömeges adatgyűjtésen alapuló detektív megoldások rendszeresítéséhez, míg a piaci szektor gazdasági megfontolások alapján – a munkavállalók okozta biztonsági kockázatok csökkentése, esetleg a teljesítményük mérése, javítása érdekében – vezetné be széles körben azokat. Kevés kritika éri az ügyfelek bankkártyás tranzakcióinak bankok általi monitorozását, amely lehetővé teszi a szokásostól eltérő helyen, vagy időpontban történő fizetések észlelését, az esetleges visszaélések megelőzését (Tamásné 2015). Nem szabad elfelejtkeznünk a jelenleg legszélesebb körben alkalmazott marketing célú profilozásról sem, amikor a közösségi oldalak és egyéb online üzleti szereplők a vásárlók szokásainak megismerésével kívánják javítani keresési eredményeiket – és ahhoz szorosan kapcsolódva eladási statisztikáikat.

Ezek a célok szintén visszavezethetőek az adatkezelők olyan alapjogi szinten is elismert jogaihoz, mint a vállalkozás szabadsága vagy a tulajdonhoz való jog.[11] Ezért a profilozást néhány területen tekinthetjük jogszerű célnak, azok szűk körben történő alkalmazására már most is lehetőséget (jogalapot) biztosít a magyar és az Uniós adatvédelmi jog is.

A tudományos diskurzus és az adatvédelmi hatóságok elsősorban a közvetlen üzletszerzés érdekében történő (reklám célú) viselkedéselemzés vizsgálatából indultak ki[12], és az EU 2018-tól alkalmazandó új adatvédelmi jogszabálycsomagja is különös hangsúlyt fektet a keresőoldalak és a közösségi oldalak komoly profitot eredményező profilozó tevékenységére. Ezekben az esetekben a felhasználó többnyire valamely szolgáltatás díjmentes igénybevételéhez kapcsolódva, annak szerződési feltételei között olvasható tájékoztatás birtokában, *hozzájárul* ahhoz, hogy róla adatokat gyűjtsenek. Bár ebből hátrányai származhatnak, de dönthet úgy, hogy nem regisztrál egy közösségi oldalra, vagy másik keresőoldalt vesz igénybe, esetleg letiltja az operációs rendszer naplózási funkcióját, vagy törli magát a levelezőrendszerből, ha nem kíván alanya lenni a viselkedéselemzésnek. Az elemzés során az adatkezelésnek végig meg kell felelnie a korábban bemutatott alapelveknek, igaz, a gyakorlat az mutatja, hogy ezek a súlyos adatvédelmi bírságok ellenére sem valósulnak meg a nagy nemzetközi vállalkozások esetében (lásd Google- és Facebook-perek szerte Európában).

A hatályos uniós jog, és a 2018-tól alkalmazandó szabályok alapján is a tagállamok szuverén joga marad, hogy *közérdeken alapuló célból jogszabályban* előírjanak egyes adatkezeléseket, így például lehetővé tegyék a viselkedéselemzést nemzetbiztonsági vagy honvédelmi érdekből néhány területen, vagy korlátozzák az érintett hozzáférési jogát a róla gyűjtött adatokhoz (például bűnüldözési érdekből). Hazánkban ágazati törvények lehetővé tehetik a viselkedéselemzést, amennyiben alkalmazásának feltételeit és korlátait megfelelően meghatározzák. Annak gyakorlati végrehajtása során azonban már figyelemmel kell

[11] Az Európai Unió Alapjogi Chartájának 15-17. cikkei is nevesítik ezeket.

[12] A tagállami adatvédelmi hatóságok egységes jogértelmezésük kialakítása céljából az EU adatvédelmi irányelvének 29. cikke szerinti Adatvédelmi Munkacsoportban (a továbbiakban: Adatvédelmi Munkacsoport) közös véleményt fogalmaztak meg a témában (2010 és 2011).

lennie az adatkezelőnek az adatvédelmi alapelvekre, csupán a jogalapjában tér el az érdekmérlegelésen, vagy az érintett hozzájárulásán alapuló adatgyűjtéstől.[13]

Noha a hatályos jogban nem találunk az információbiztonsági célból történő viselkedéselemzést előíró közvetlen jogszabályt, a jogalkotó is elismeri az információbiztonság jelentőségét, hiszen a személyes adatok védelme sem valósítható meg az adatbiztonsági elvárások (Infotv. 7.§) teljesülése nélkül. Az adatvédelmi incidens naplózásának előírásával (Infotv. 15.§) azt már nemcsak célként, hanem törvényes jogalapként is értelmezhetjük arra, hogy a rendszert folyamatosan ellenőrizzük, a hálózati adatforgalmat naplózzuk.

Az is felmerülhet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény hatálya alá tartozó szervek esetében, hogy adatgyűjtésük céljaként a törvénynek való megfelelést nevesítsék, ennek érdekében pedig – már az *érdekmérlegelés* jogalapját segítségül hívva, a szükséges érdekmérlegelési tesztet elvégezve – viselkedéselemzést alkalmazzanak.

Számos kérdés merülhet fel azonban a munkaviszonyhoz, tagsági viszonyhoz kötődő profilozás kapcsán, amelyeket munkajogi és adatvédelmi jogi szempontból is szükséges vizsgálnunk. Amennyiben egy szervezet munkavállalóinak monitorozásáról beszélünk, akkor a rendszer által gyűjtött adatok és az abból levonható következtetések (úgynevezett prediktív profil) szükségszerűen kiegészíthetővé válnak az offline világból rendelkezésre álló adatokkal, így a felhasználók még pontosabb beazonosítását teszik lehetővé (explicit profil). Ha a munkáltató nem csak metaadatokat, hanem a kommunikáció tartalmát is vizsgálja – például kártékony kódok terjedésének, vagy üzleti titkainak szivárgását megelőzendő –, akkor fennáll a veszélye annak is, hogy olyan különleges adatok (egészségügyi állapot, szexuális érdeklődés, pártállás, vallás stb.) is az adatkezelő tudomására jutnak így, melyeket jogszerűen nem kezelhet. A beérkező kommunikáció vizsgálata szintén problémát vethet fel, hiszen feladójának személyes adatai is veszélybe kerülhetnek, aki nem járulhatott hozzá az adatgyűjtéshez, nem kaphatott tájékoztatást az adatkezelésről (Bankó és Szőke 2015).

Fentiek, és a NAIH jogértelmezése alapján munkaviszonyhoz kapcsolódóan az érintett saját profilozásához való hozzájárulása nem tekinthető megfelelő jogalapnak, hiszen alárendeltségi viszonyából következően, döntése esetleges következményei miatt nem tudja önkéntes, befolyástól mentes hozzájárulását adni az adatkezeléshez.

A munkáltató jogos érdekeire tekintettel azonban szigorú garanciák érvényesülése mellett mégis ellenőrizhető az internethasználat és a munkahelyi eszközök adattartalma, ha az törvényi rendelkezésen, illetve megfelelő érdekmérlegelésen, valamint előzetes tájékoztatáson alapul. A NAIH munkahelyi adatkezelések jogszerűségéről szóló 2016 novemberi tájékoztatója kitér az internethasználat ellenőrizhetőségére is. A NAIH jogértelmezése szerint a Munka Törvénykönyvéről szóló 2012. évi I. törvény 11. §-a megfelelő jogalapot ad a munkáltatónak, hogy ellenőrizze a munkavállaló online tevékenységét, és adott esetben munkajogi jogkövetkezményt alkalmazzon a munkavállalóval szemben. Az ellenőrzés eszközének kiválasztásához és kereteinek meghatározásához a munkáltatónak el kell végeznie az érdekmérlegelés tesztjét, valamint meg kell határoznia, hogy milyen

[13] A követelményekről lásd az Adatvédelmi Munkacsoport az elektronikus kommunikáció hírszerzési és nemzetbiztonsági célú megfigyeléséről szóló 4/2014. számú véleményét (WP 215), valamint az azt alátámasztó jogi értékelését (WP 228).

céllal, milyen érdekei mentén ellenőrzi az internethasználatot. Fontos elvárás, hogy az ellenőrzés kereteit megadó belső szabályzatot készítenie, és az ellenőrzésnek a munkavállaló munkaköréhez igazodónak kell lennie. A munkáltatónak kötelessége a munkavállalót részletesen tájékoztatni az ellenőrzés előtt, és a vizsgálat csupán arra terjedhet ki, hogy a munkavállaló betartotta-e a belső szabályzatokban rögzített munkáltatói rendelkezést (tiltott oldalak, vagy kommunikáció, például chat), tehát a munkavállaló részletes tevékenységének feltérképezése nem megengedett.

Álláspontunk szerint a NAIH által meghatározott – munkáltatói ellenőrzési célú, és teljesítménymméréshez kötődő – ellenőrzéshez képest közvetlenebb gazdasági érdeke fűződik a munkáltatónak a biztonsághoz. Ezért a fenti korlátok ellenére a védelmi célú profilozás érdekmérlegelési tesztje megengedőbb eredményt hozhat. Boehm, Hey és Ortner (2016) egy jogszerűen kialakított viselkedéselemzési megoldás (biztonságtudatossági teszt) bemutatása kapcsán felhívja a figyelmet arra, hogy a profilozás korlátait és feltételeit meghatározó jogszabályi felhatalmazás hiányában is lehetőséget ad az uniós adatvédelmi jog arra, hogy – az adatkezelésre vonatkozó alapelvek és előírások betartása mellett – az adatkezelő jogos érdekének érvényesítése céljából gyűjtse az adatokat. Ehhez szükséges, hogy az adatok gyűjtését a lehető legszűkebb körben és ideig végezze a munkáltató, majd ezt követően azokat álnevesítve, vagy anonim formában értékelje, és eltérő célból azokat ne használja fel.

Az új adatvédelmi szabályozás

Az EU adatvédelmi reformjának eredményeként 2012-től érezhetően nőtt az adatvédelmi szabályozás jelentősége Európában. Ezt nem csak a formálódó rendeletszöveghez kapcsolódó lobbitevékenység (Nielsen 2013a), illetve a rendelet-tervezethez az Európai Parlament fennállása óta érkezett egyik legtöbb módosító javaslat beérkezése mutatta (Nielsen 2013b), hanem az is, hogy az Európai Unió Bírósága számos nagy horderejű döntésben terjesztette ki az adatvédelmi jog hatályát.[14] A tagállamonként eltérő módon átültetett EU adatvédelmi irányelv (95/46/EK) helyébe 2018. május 25-én az EU Általános Adatvédelmi Rendelete[15] lép, amely közvetlenül alkalmazandó jogszabályként egységesen magas elvárásokat határoz meg a megfigyelést és profilozást végző adatkezelőkre szerte Európában. Újdonság, hogy hatálya nemcsak az itt működő szervezetekre, de az EU-n kívüli adatkezelőkre is kiterjed, ha az Unióban tartózkodó érintetteknek nyújtanak szolgáltatást, vagy árusítanak terméket, illetve, ha az érintettek viselkedésének megfigyelése érdekében kezelnek róluk adatokat – feltéve, hogy az Unió területén belül tanúsított viselkedésükről van szó (Rendelet 3. cikk (2)).

[14] Lásd a C-131/12. Google Spain v AEPD and Mario Costeja Gonzalez ügy az elfelejtődéshez való jogról, illetve a C-362/14. számú Maximilian Schrems v Data Protection Commissioner ügyben hozott határozatát, melyben a Snowden-ügyet követően kimondta, hogy az Egyesült Államok nem minősül adatvédelmi szempontból biztonságos harmadik országnak, és a Safe Harbor keretrendszert érvénytelennek nyilvánította.

[15] 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 rendelet hatályon kívül helyezéséről (a továbbiakban: Rendelet).

A Rendelet már egyértelműen adatkezelésként nevesíti a profilozást (4. cikk 4. pont), és személyes adatként az IP-címet, böngésző sütiket és a helymeghatározó adatokat is, csakúgy, mint a naplóállományokat, amennyiben azok egyéb információkkal összekapcsolva felhasználhatóak a természetes személyes profiljának létrehozására és az adott személy azonosítására (30. Preambulum).

A Rendelet is átveszi a jogos érdeket, mint adatkezelési jogalapot. Erre alapozva jogszerűnek nyilvánítja az olyan mértékű információbiztonsági célú személyes adatkezelést, „amely a hálózati és informatikai biztonság garantálásához feltétlenül szükséges és arányos, vagyis adott titkossági szinten az érintett hálózat vagy információs rendszer ellenálló képessége az e hálózatokon és rendszereken tárolt vagy továbbított adatok, valamint az e hálózatok és rendszerek által nyújtott vagy rajtuk keresztül elérhető kapcsolódó szolgáltatások hozzáférhetőségét, hitelességét, integritását és bizalmas jellegét sértő véletlen eseményekkel, illetve jogellenes vagy rosszhiszemű tevékenységekkel szemben." (49. Preambulum).

A monitorozás céljától függetlenül a jogos érdek csak akkor állapítható meg, ha az érintett észszerűen számíthat arra, hogy adatkezelésre az adott célból a személyes adatok gyűjtésének időpontjában és azzal összefüggésben kerülhet sor, tehát már előre tudnia kell a profilalkotási eljárások alkalmazásáról. Széles körű hozzáférési (tájékoztatási) jogot kap az érintett a profilozáshoz kapcsolódva, ám a jelenlegi szabályoknál kevesebb eszköze lesz az ellen fellépni az érdekmérlegelés következtében. Amennyiben a profilalkotás során kialakult eredményre olyan döntés épül, ami az érintett helyzetét jelentős mértékben érinti (például munkáltatói döntések), akkor a tevékenység megkezdése előtt kötelező lesz az adatvédelmi hatásvizsgálat (35. cikk) lefolytatása is. A Rendelet ugyanakkor számos adatbiztonsági előírást tartalmaz (32. cikk), valamint javasolja az álnevesítés alkalmazását, ami azonban nem vezethet arra az eredményre, hogy a továbbiakban ne minősülne az adat személyes adatnak.

A Rendelet nem alkalmazható a bűnügyi és igazságügyi célú adatkezelésekre (2. cikk). A bűnügyi és igazságszolgáltatási célú adatkezelések szabályait rögzítő 680/2016 (EU) irányelv[16] már egységes szabályokat állapít meg az EU valamennyi bűnüldöző szerve számára, míg korábban ezen a területen csak a határon átnyúló adatáramlást szabályozták. A Bűnügyi irányelv 11. cikk (1) bekezdése kimondja, hogy „az olyan, kizárólag automatizált adatkezelésen – ideértve a profilalkotást is – alapuló döntés, amelynek joghatása az érintettre nézve hátrányos vagy őt jelentős mértékben érinti, tilos, kivéve, ha (…) uniós vagy tagállami jog teszi lehetővé, amely az érintettek jogaira és szabadságaira vonatkozó megfelelő garanciákról is rendelkezik, ideértve legalább az érintett jogát arra, hogy az adatkezelőtől emberi beavatkozást kérjen."

A nemzetbiztonsági és honvédelmi célú adatkezelések a fenti jogszabályok hatályán kívül esnek, továbbra is tagállami jog alá tartoznak majd.

[16] Az Európai Parlament és a Tanács (EU) 2016/680 irányelve (2016. április 27.) a személyes adatoknak az illetékes hatóságok által a bűncselekmények megelőzése, nyomozása, felderítése, a vádeljárás lefolytatása vagy büntetőjogi szankciók végrehajtása céljából végzett kezelése tekintetében a természetes személyek védelméről és az ilyen adatok szabad áramlásáról, valamint a 2008/977/IB tanácsi kerethatározat hatályon kívül helyezéséről (a továbbiakban: Bűnügyi irányelv).

Biztonság és/vagy magánszféra? A beépített adatvédelem elve

Az EU „Europe 2020" stratégiája keretében induló adatvédelmi reformjának egyik kiemelt célja volt a felhasználók új technológiákba és az online térbe vetett bizalmának növelése. Ennek elsődleges eszközeként a digitális ügyekért felelős biztos, Viveane Reding (2011) a személyes adatok fokozottabb védelmét és az információbiztonság erősítését, mint egymást kölcsönösen feltételező és kiegészítő garanciát jelölte meg.

A szabályozás az elvek mellett ismét figyelmet fordít a technológiai fejlődés jelentette kihívásokra, a Rendelet és a Bűnügyi irányelv is kötelezően előírja a beépített és az alapértelmezett adatvédelem elvének alkalmazását, valamint az adatvédelmi szempontú előzetes hatásvizsgálat lefolytatását a magas adatvédelmi kockázatot rejtő új adatkezelések azonosítása érdekében.

A beépített adatvédelem (Privacy by Design) elvének kidolgozása Kanada korábbi adatvédelmi biztosának, Ann Cavoukiannek a nevéhez fűződik, aki a 90-es években, főleg az Egyesült Államokban megjelenő „Surveillance by Design" felfogásra keresett választ. A megfigyelésközpontú társadalom létrehozásának elve, és a kapcsolódó törvénytervezetek azt állították[17], hogy az állampolgárok biztonsága csak a magánszférájuk védelmének rovására biztosítható. Az elv hívei szerint minél inkább figyelembe vesszük a magánszféra védelmét és az adatvédelmi elveket, annál nagyobb lesz a kockázata akár egy, a kibertérből érkező, akár egy terrorizmussal összefüggő támadásnak. A napjainkban sem idegen felfogás gyakorlati megvalósulása a közterületi kamerázás rohamos terjedése és korlátlan megfigyelési funkció integrálását jelenti a kommunikációs technológiákba olyan mértékben, amelynek segítségével a rendvédelmi szervek bármilyen adathoz hozzáférhettek (Davies 2010). A Big Data-alapú megoldások terjedésével megnőtt azon fejlesztők versenyelőnye, akik olyan rendszereket képesek előállítani, amelyekben a felügyelet az általános napi működés részét képezi, a felhasználói viselkedéselemzés költségeinek csökkenése pedig magával hozhatja az adatkezelők oldalán az elv újjászületését.

A Privacy by Design elve ezzel szemben annak a filozófiája, hogy a magánszféra-védelem és az adatvédelmi szabályozás elveit integrálni kell a különböző adatkezelő technológiák követelményrendszerébe, amely így a számítástechnikai és üzleti alkalmazások integráns részévé válik anélkül, hogy azok funkcionalitást korlátozná. Elismeri a biztonság jelentőségét, de úgy kíván eredményeket elérni, hogy közben nem sérti szükségtelenül az érintettek széles körének magánszféráját, kölcsönös előnyökre törekszik (Cavoukian 2016).

Az elv gyakorlati megvalósulásának egyik legfontosabb eleme a Székely (2008) által Privátszférát Erősítő Technológiáknak fordított „Privacy Enhancing Technologies", azaz PETs-ek fejlesztése, alkalmazása, és azok terjedésének elősegítése.

A PETs kifejezésre nem található általánosan elfogadott meghatározás, leggyakrabban azonban az egyén identitását, személyazonosságát védő technikai és szervezeti megoldások gyűjtőneveként alkalmazzák (London Economics 2010). Az adatszivárgások, visszaélési botrányok magas száma jól mutatja, hogy önmagában a szabályozás, önszabá-

[17] Az érvek 1994-ben az Egyesült Államok "Communications Assistance for Law Enforcement Act" (CALEA) című törvényének vitájakor, majd a digitális távközlési hálózatok lehallgatását szabályozó 1999-es törvényjavaslat kapcsán is felmerültek. http://w2.eff.org/Privacy/Surveillance/CALEA/1999/

lyozás és a jogalkalmazás sem tudnak elegendő védelmet nyújtani a felhasználóknak a tömegesen előforduló visszaélésekkel szemben. Ugyanakkor az adatkezelők sem lehetnek biztonságban az egyre újabb, a személyes adatok megszerzésére tervezett műszaki és Social Engineering típusú támadások ellen, pedig az adatbiztonság garantálása a Rendelet hatályba lépésével (32. és 33. cikk) égető problémaként jelenik meg.

A PET-ek alkalmazásának különös jelentősége van minden olyan technológiai fejlesztés során, amelyek esetében magányszemélyek (érintettek) személyes adatait gyűjtik, elemzik, hasznosítják, tehát adatkezelés történik. E technológiák és eszközök alapvető célja, hogy ne csak az adatokat információbiztonsági szemszögből, hanem az adatalanyokat, az érintetteket is védjék a visszaélések ellen, és elősegítsék az információs önrendelkezéshez való joguk érvényesíthetőségét, ami Goldberg (2002) szerint a jogi előírások és az önszabályozás mellett a technológia által is elősegíthető lehet. Az elmúlt két évtizedben a beépített adatvédelem elve és az azt gyakorlatba átültető megoldások lassan terjedtek, létjogosultságukat azóta is sokan kétségbe vonják. Ennek egyik fő oka – a felhasználók adatvédelmi tudatosságának és ahhoz kapcsolódó aktivitásának alacsony szintje mellett (Szőke 2015) – a kötelező alkalmazásukat előíró jogszabályok hiánya volt (London Economics 2010).

Szőke és Böröcz (2013) a Privacy by Design elvének uniós átültetése kapcsán kiemeli, hogy az eredetileg a PETs megoldásokhoz kapcsolódva megjelenő, kifejezetten a technológiára fókuszáló elv a Rendeletben (25. cikk) és a Bűnügyi irányelvben (20. cikk) már átfogóan, a tervezési, üzleti, és üzemeltetési folyamatokban is kötelezően megvalósítandó előírás. Gyakorlati alkalmazása azonban továbbra is bizonytalanságot okoz, mivel a megfogalmazott elvek sokkal inkább egy szemléletet, hozzáállást tükröznek, mintsem olyan normatív követelményrendszert, amelynek betartása vagy be nem tartása könnyedén megállapítható, mérhető volna (Davies 2010).

Az elv tartalmának kidolgozása a tagállamok adatvédelmi hatóságaira hárul majd, de a beépített adatvédelem megvalósításának (Privacy Engineering) területével foglalkozó mérnökök, informatikusok már több területen is szép eredményeket értek el az álnevesítés alkalmazásával.[18] Az információbiztonsági célú felhasználói viselkedéselemzést támogató megoldások esetében is fontos cél lehet ezért a magánszféra védelmét garantáló, de ugyanakkor az elvárt biztonsági szintet még nyújtó PET-ek fejlesztése, kidolgozása.

Összefoglalás

A felhasználói viselkedéselemzés kiváló lehetőség az új típusú kiberbiztonsági kihívások kezelésére, de különös figyelmet kell fordítani annak adatvédelmi aspektusaira is. Pardo és Siemens (2014) gyűjtése alapján a következő etikai és adatvédelmi elvek mentén lehet a gépi tanulást hadrendbe állítani.

- Transzparencia: a megfigyelteknek tisztában kell lenniük azzal, hogyan működik az elemzési eljárás, és azzal, hogy milyen információkat használnak fel ennek során.

[18] Lásd az okos mérők alkalmazása során a villamosenergia-szektorban, a budapesti Groupama Aréna beléptetőrendszerének hash kóddal átalakított biometrikus beléptető adatai esetében, vagy Cavoukian (2011) összefoglalójában a nemzetközi eredményekről.

- Kontroll az adatok felett: a megfigyeltnek lehetőséget kell biztosítani arra, hogy hozzáférhessen és korrigálhassa a róla gyűjtött adatokat.
- Hozzáférési jogok: egyértelműen meg kell határozni, hogy ki és milyen körülmények között férhet hozzá és használhatja fel a gyűjtött adatokat.
- Elszámoltathatóság és ellenőrzés: egyértelműnek kell lennie, hogy ki és milyen felelősséggel bír a folyamatban.

Problémát jelenthet, hogy bár a 2018-ig alkalmazandó európai és hazai jog nem zárja ki a felhasználói viselkedéselemzésen alapuló védelmi célú mechanizmusok használatát, a tagállamok szabályozása nem egységes és az adatvédelmi hatóságok gyakorlata is különbözhet az érdekmérlegelési teszt kapcsán, így eltérő feltételekhez kötheti alkalmazásukat.

A részletszabályok kidolgozása még folyamatban van, de a Rendelet és a Bűnügyi irányelv ebben komoly változást hoz. A Rendelet már adatkezelési jogalapnak tekinti az engedély nélküli hozzáférés és a rosszindulatú programterjesztés megakadályozásához, továbbá a szolgáltatás megtagadásával járó támadások (DDOS), valamint a számítógépes és elektronikus kommunikációs rendszerekben való károkozás megállításához fűződő jogos érdeket (49. Preambulum). Az e célra fejlesztett új műszaki megoldások, szolgáltatások tervezésekor, illetve a működő rendszerek üzemeltetése során ezért mindenképpen javasolt már most figyelembe venni a Rendelet új előírásait és alapelveit is. Az érintettek megfelelő tájékoztatása mellett a beépített adatvédelem elvének megfelelően, ahol lehet, álnevesítést, PET technológiákat, valamint titkosított rendszerű kommunikációt és adattárolást alkalmazzunk.

Irodalom

A 29. cikk alapján létrehozott Adatvédelmi Munkacsoport, „2/2010. számú vélemény a viselkedésalapú online reklámról" (WP 171) 00909/10/HU, 2010.06.22. http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp171_hu.pdf

A 29. cikk szerinti Adatvédelmi Munkacsoport, „16/2011. sz. vélemény a viselkedésalapú online reklám bevált gyakorlatára vonatkozó EASA/IAB-ajánlásról" (WP 188) 2011.12. 08. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp188_hu.pdf

A Nemzeti Adatvédelmi és Információszabadság Hatóság tájékoztatója a munkahelyi adatkezelések alapvető követelményeiről. 2016.11.15. https://www.naih.hu/files/2016_11_15_Tajekoztato_munkahelyi_adatkezelesek.pdf

Abraham, Ajith, Crina Grosan and Yuehui Chen, "Cyber security and the evolution of intrusion detection systems.", *i-Manager's Journal on Future Engineering and Technology* 1.1 (2005): 74.

Alexin Zoltán, „Does fair anonymization exist?", *International Review of Law, Computers and Technology*, Vol. 28. (2014) No. 1., pp. 21-44. http://dx.doi.org/10.1080/13600869.2013.869909

Bankó Zoltán és Szőke Gergely László, „Az információtechnológia hatása a munkavégzésre", Pécs, Utilitates Bt., (2015) pp. 55–66.

Boehm, Franziska, Tim Hey and Robert Ortner, "How to measure IT security awareness of employees: a comparison to e-mail surveillance at the workplace", *European Journal of Law and Technology*, Vol 7. (2016), No 1. http://ejlt.org/article/view/500/633

boyd, danah and Kate Crawford, "Critical Questions for Big Data", *Information, Communication & Society*, 15:5 (2012), pp. 662-679. http://dx.doi.org/10.1080/1369118X.2012.678878

Cavoukian, Ann, "Embed Privacy by Design, or Risk Losing Privacy Forever", Berkeley Center for Law & Technology, 2016. https://www.law.berkeley.edu/wp-content/uploads/2016/03/Ann-Cavoukian.pdf

Cavoukian, Ann, *Privacy by Design. Strong Privacy Protection – Now, and Well into the Future. A Report on the State of PbD to the 33rd International Conference of Data Protection and Privacy Commissioners*, 2011. https://www.ipc.on.ca/wp-content/uploads/Resources/PbDReport.pdf

Davies, Simon, *Why Privacy by Design is the next crucial step for privacy protection – A discussion paper*, 2010. http://i-comp.org/wp-content/uploads/2013/07/privacy-by-design.pdf

Dell SecureWorks, *Underground Hacker Markets*, 2016.

Goldberg, Ian, "Privacy-enhancing technologies for the Internet, II: Five years later." in Roger Dingledine and Paul Syverson (eds.), *Privacy Enhancing Technologies. Second International Workshop, PET 2002 San Francisco, CA, USA, April 14–15, 2002 Revised Papers*, Springer-Verlag, Berlin-Heidelberg-New York, 2002. http://dx.doi.org/10.1007/3-540-36467-6_1

Hutchins, Eric M., Michael J. Cloppert and Rohan M. Amin, "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains", in Julie Ryan (eds), *Leading Issues in Information Warfare and Security Research, Vol. 1.*, Academic Conferences Limited, Reading, 2011, pp. 80-106.

International Telecommunication Union, *ICT Facts and Figures 2016*, ITU, Geneva, 2016.

Iverson, Brian, "Maverick: The Unbearable Cost of Privacy", Gartner, 2015.

Lee, Dave, "Obama presses Trump on cybersecurity", *BBC News*, 3 December 2016, http://www.bbc.com/news/technology-38193663

London Economics, *Study on the economic benefits of of privacy-enhancing technologies (PETs)*. Final Report to The European Commission DG Justice, Freedom and Security, 2010. http://ec.europa.eu/justice/policies/privacy/docs/studies/final_report_pets_16_07_10_en.pdf

Lyon, David, "Surveillance, Snowden, and big data: Capacities, consequences, critique", *Big Data & Society* Vol. 1. (2014) Issue 2., pp. 1-13. http://dx.doi.org/10.1177%2F2053951714541861

Minárik, Tomáš, "NATO Recognises Cyberspace as a 'Domain of Operations' at Warsaw Summit", Tallin, 21 July 2016, https://ccdcoe.org/nato-recognises-cyberspace-domain-operations-warsaw-summit.html

Morgan, Steve (ed.), *Hackerpocalypse: A Cybercrime Revelation*, Cybersecurity Ventures, 2016.

Nemeslaki András és Sasvári Péter László, „Az információbiztonság-tudatosság empirikus vizsgálata a magyar üzleti és közszférában", *Infokommunikáció és Jog*, 60. szám (2014), pp. 169-177.

Nemzetközi Távközlési Adatvédelmi Munkacsoport, *Webtracking és magánszféra: a kontextus, az átláthatóság és az ellenőrzés alapvető fontosságú marad*", Munkadokumentum, 53. Ülés, Prága, 2013. április 15-16. https://www.naih.hu/files/IWGDPT–Webtracking-es-maganszfera–HUN.pdf

Nielsen, Nikolaj, "MEPs copy-pasting amendments from US lobbyists", *euobserver*, 12 February 2013, https://euobserver.com/justice/119028 (2013a)

Nielsen, Nikolaj, "The man behind the EU parliament's data regulation", *euobserver*, 06 May 2013, https://euobserver.com/justice/119951 (2013b)

Ohm, Paul, "Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization", *UCLA Law Review* Vol. 57. (2010) Issue 6., pp. 1701-1777. http://www.uclalawreview.org/pdf/57-6-3.pdf

Pardo, Abelardo and George Siemens, "Ethical and privacy principles for learning analytics", *British Journal of Educational Technology*, Vol. 45. (2014) Issue 3., pp. 438-450. http://dx.doi.org/10.1111/bjet.12152

Ponemon Institute LLC, *2016 Cost of Data Breach Study: Global Analysis*, Ponemon, Traverse City, 2016.

Reding, Viviane, "The upcoming data protection reform for the European Union," *International Data Privacy Law* Vol 1. (2011) Issue 1., pp. 3-5. https://doi.org/10.1093/idpl/ipq007

Székely Iván, „Jog ahhoz, hogy elfelejtsenek és töröljenek”, *Információs Társadalom* XIII. évfolyam (2013) 3-4. szám, 7-27. old. http://www.infonia.hu/digitalis_folyoirat/2013/2013_34/i_tarsadalom_2013_34_szekely.pdf

Székely Iván, „Privátszférát erősítő technológiák”, *Információs Társadalom*, VIII. évf. (2008) 1. szám, 20-34. old.

Szőke Gergely László és Böröcz István, „A beépített adatvédelem (privacy by design) elve”, *Infokommunikáció és Jog,* 56. szám (2013), 120-125. old.

Szőke Gergely László, *Az európai adatvédelmi jog megújítása. Tendenciák és lehetőségek az önszabályozás területén*, HVG-ORAC, Budapest, 2015.

Tamásné Szabó Zsuzsanna, „Nemcsak a Budapest Bank, több hazai nagybank ügyfeleitől is loptak pénzt”, *24.hu*, 2015. augusztus 13. http://24.hu/fn/penzugy/2015/08/13/tobb-hazai-nagybank-ugyfeleitol-is-loptak-penzt-a-kartyacsalok/

Dr. Kiss Attila infokommunikációs szakjogász, korábban a Nemzeti Közszolgálati Egyetem Államtudományi és Közigazgatási Karának oktatója. Jogász diplomáját 2011-ben szerezte a Pécsi Tudományegyetemen, 2009-ben az Egyesült Királyságban a Coventry University (Erasmus), majd 2010-ben Csehországban a brnoi Masaryk Egyetem (Visegrad Fund ösztöndíj) hallgatója volt. 2011 és 2014 között a PTE ÁJK Informatikai és Kommunikációs Jogi Tanszékének doktorandusz hallgatója, témavezetője Balogh Zsolt György. Kutatási területe elsősorban a személyes adatok és a képmás védelme, több tanulmánya vizsgálja a térfigyelő kamerázás jogi hátterét és az Európai Unió adatvédelmi reformját.

Dr. Krasznay Csaba, PhD okleveles villamosmérnök, a katonai műszaki tudományok doktora, jelenleg a Nemzeti Közszolgálati Egyetem Államtudományi és Közigazgatási Karának adjunktusa. MSc diplomáját a Budapesti Műszaki és Gazdaságtudományi Egyetemen szerezte 2003-ban, PhD fokozatát a Nemzeti Közszolgálati Egyetem Katonai Műszaki Doktori Iskolája bocsátotta ki 2012-ben. Korábban kutatóként dolgozott a Budapesti Műszaki és Gazdaságtudományi Egyetemen, valamint információbiztonsági tanácsadóként, szakértőként több mint 10 éves tapasztalata van a kiberbiztonság üzleti világából. 2011-ben az Év Útmutató IT Biztonsági Szakemberének választották. Kutatási területe a kiberbiztonság és az elektronikus közszolgálati rendszerek információbiztonsággal kapcsolatos kérdései.

Gulyás Gábor György

Gépi tanulási módszerek alkalmazása deanonimizálásra

Bevezető

Az okostelefonok, a különféle szenzorok elterjedése, az internetnek a magánéletbe való szoros integrációja megkönnyíti a mindennapi életet és munkát. Ezekből a forrásokból rendkívüli potenciállal rendelkező adatok származnak, amelyek üzleti, kutatási vagy akár a nyílt adatok elvén működő kormányzati szolgáltatások szempontjából korábban sosem látott lehetőségeket tartogatnak a társadalmak számára.

Az előnyök mellett azonban nem elhanyagolható problémát jelenthet az efféle adatgyűjtésnek a privátszférára gyakorolt hatása sem, hiszen már nem csupán az állami szereplők – köztük a nyomozó szervek – számára könnyíti meg a megfigyelést, új szereplőként megjelennek a technológiát létrehozó cégek és maguk a felhasználók is. Ebben az új rendszerben a cégek adatokat gyűjtenek felhasználóikról, amit által a szolgáltatásaikat fejleszthetik, az adatok értékesítésével további bevételekhez juthatnak, illetve a technológia megkönnyíti, hogy felhasználók egymás után leskelődjenek, sőt kontrollálják is egymást. Méltán nevezhetjük a létrejövő rendszert kukkoló társadalmaknak (Székely 2010).

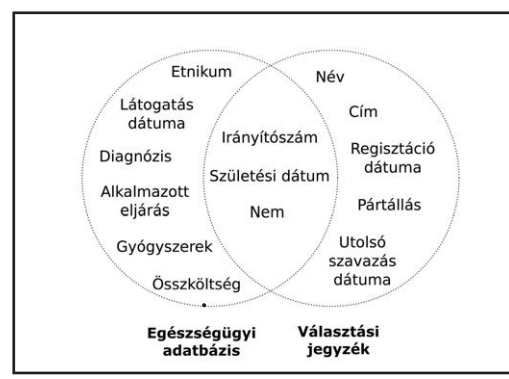
A kölcsönös „kukkolási" probléma enyhítésére a technológiai cégek privátszféravédő beállításokat fejlesztettek ki és tették elérhetővé felhasználóik számára. Például ilyenek a különféle, részletesen szabályozható láthatósági listák, amelyekkel üzenetek, profilok láthatóságát lehet beállítani. Ez azonban a szolgáltató oldaláról történő adatgyűjtés esetére nem oldja meg a privátszféra védelmét, amit indokol az adatokat kezelő cégek önvédelme, illetve megkövetelheti is ezt a jogi környezet. Az előbbire jó példát ad az America Online (AOL) esete, amikor 657 ezer felhasználójának három havi keresési előzményét tettek közzé kutatási célból, és emiatt a cég kénytelen volt perrel és a sajtónyilvánosságból fakadó presztízsveszteséggel szembenézni (Bangeman 2006). Az utóbbira pedig példa lehet az Európai Bizottság 95/46/EC direktívája, amely szerint az anonimizált adatokra már nem vonatkoznak az európai adatvédelmi irányelvek; így például az ilyen adatbázisok megosztása (eladása) elé kevesebb akadály hárul.

A védekezési módszerek legegyszerűbb formája a pszeudonimizálás (angolul *pseudonymization*), amely során megfosztják az adatokat az egyértelmű személyes adatoktól (mint nevek, felhasználónevek és egyéb azonosítók), és pszeudonim azonosítókra cserélik azokat (például véletlen számokra). Ennek célja, hogy az egyes rekordok ne legyenek triviális módon kapcsolatba hozhatóak az eredeti adatalanyokkal. Már több esetben is láthattunk rá „éles" demonstrációt, hogy ezek az eljárások nem megfelelőek (például Narayanan és Shmatikov (2008) és Barbaro (2006)). Az AOL előbb említett esete is ide tartozik: az AOL módosítás nélkül, de pszeudonim formában osztotta meg felhasználóinak körülbelül 20 millió keresésének szövegét. Ennek ellenére a keresések szövege alapján mégis be lehetett azonosítani egyes, a kereséseket végző személyeket, és ez nem volt különösebben bonyolult: a New York Times riporterének sikerült visszakövetnie és meg is szólaltatnia a 4417749-es számú felhasználót (Barbaro 2006).

Az AOL esetében a problémát egyértelműen az okozta, hogy ugyan a keresések nem kötődtek a kereső személyéhez, mégis minden egyes keresés közelebb vitt hozzá. Az anonimizálási eljárások (angolul *anonymization*) célja hasonló a pszeudonimizáláshoz, de az egyértelmű azonosítók eltávolításán túl az is elvárt, hogy az anonimizálás során létrejövő rekordokat ne lehessen hozzákötni az adatot szolgáltató eredeti személyhez, vagy hasonló módon az újságíró módszeréhez „szűkíteni a kört". Ez már érinti az AOL esetében látott információszivárgásokat is, ezért az anonimizálási eljárások az adatbázis nem azonosító jellegű mezőinek értékét is megváltoztatják.

A több, nem azonosító jellegű mező összevonásából létrejövő, úgynevezett kvázi-azonosítók kulcsfontosságúak a privátszféra védelme szempontjából. A kvázi-azonosítók segítségével összekapcsolhatóak különböző adatbázisok, és így az anonimizálás is visszafordíthatóvá válik, elég hozzá egy anonimizált adatbázisban szereplő rekordokat a kvázi-azonosítók mentén azonosítóval rendelkező rekordokkal párosítani. Ez utóbbit hívjuk deanonimizálásnak vagy újraazonosításnak (angolul rendre *de-anonymization* és *re-identification*).

Latanya Sweeney (2002) tanulmánya volt az egyik első prominens példa, ami felhívta a figyelmet a kvázi-azonosítók és újraazonosítás problémájára. Kutatóként hozzáférést kapott 135 ezer állami dolgozó és családja névtelen egészségügyi adataihoz, majd megvásárolta a Massachusetts-ben regisztrált szavazók listáját (20 dollárért). Az irányítószám, születési dátum és nem mezőkből formált kvázi-azonosítóval össze tudta kötni a két adatbázis rekordjainak egy részét, amelyet Massachusetts kormányzója egészségügyi adatainak kikeresésével demonstrált (1. ábra).



1. ábra: Latanya Sweeney a név nélkül módon publikált egészségügyi adatokat a választási jegyzék segítségével kompromittálta: a két adatbázist az irányítószám, születési dátum és nem mezők segítségével össze lehetett vonni (Sweeney 2002)

Sweeney az úgynevezett k-anonimitás (angolul *k-anonymity*) anonimizálási módszert javasolta az újraazonosítással szemben: a k-anonimitás akkor teljesül egy adatbázisra, ha minden egyes rekordjához tartozik legalább k-1 olyan másik rekord, amelyeknek a kvázi-azonosítója megegyezik. A k-anonimitás célja, hogy ha valaki össze is tudna kötni a kvázi-azonosítóval két adatbázist, akkor is csak legfeljebb 1/k valószínűséggel tudja a rekordokat helyesen összekapcsolni.

Sweeney (2002) munkája után számos tudományos cikk jelent meg, amelyek a módszer hibáit igyekeztek javítani, további adattípusra javasoltak anonimizálási eljárásokat, vagy éppen deanonimizálási algoritmusokat. E tanulmányban a deanonimizálási eljárások egy új típusát vizsgáljuk, nevezetesen azokat, amelyek gépi tanulási módszerekre (angolul *machine learning*) épülnek. A gépi tanulási módszerek automatizált adatelemzési módsze-

rek, amelyek során az adat modellezését az algoritmus a minták alapján maga tanulja meg (például kellő minta esetén fel tudja ismerni addig nem látott képeken is a macskákat). Pontosan ez a tulajdonságuk teszi a gépi tanulási módszereket vonzóvá az újraazonosítási támadásokban is: alkalmazásuk esetén például nem szükséges a tervezőnek pontosan értenie, hogy a két adathalmaz egyes rekordjai a különféle attribútumok alapján miképpen hasonlítanak egymásra (és így hogyan köthetőek össze) – az összerendelést végző függvényt a gépi tanulási módszer automatikusan képes megtalálni.

A deanonimizálási algoritmusok „történelme"

Sweeney demonstrációja a táblázatos adatokra és a k-anonimitás nagy visszhangot váltott ki, több száz művet inspirálva a következő években. A táblázatos adatok azonban csak egy speciális esetét képviselik az új technológiákból származó adatbázisoknak, ugyanis csak az esetek kisebb részében beszélhetünk egyáltalán relációs adatbázis jellegű felépítésről, vagy zárt attribútumhalmazról, amelyek azonosítókat tartalmaznak vagy kvázi-azonosítókként felhasználhatók. Az esetek többségében az egyes rekordokat leíró mezők (vagy attribútumok) száma nem zárt, folyamatosan bővül és nagy számú. Gondoljunk például egy webáruházra, ahol a felhasználók értékelik a termékeket: ez esetben a termékek száma nagy és folyamatosan nő, és a felhasználók jellemzően csak a termékek kis töredékét értékelték valaha. Ugyanilyen elrendezést kapunk, ha mondjuk egy közösségi hálózat kapcsolatrendszerének gráfját szomszédsági mátrixszal írjuk le. Ezeket nagy attribútumszámú vagy nagy dimenziójú adathalmazoknak hívjuk.

Viszonylag korán kiderült, hogy ezekben az esetekben a k-anonimitás nem megfelelő védekezési eljárás és legfeljebb csak kompromisszumot lehet keresni az anonimitás szintje és az adatbázis hasznossága között (Aggarwal 2005). Ennek oka az, hogy ahogy nő az attribútumok száma, úgy nő a potenciális kvázi-azonosító kombinációk száma is, ami miatt a rekordok egyre kevésbé hasonlítanak egymásra, és ez megnehezíti az anonimizálást, hiszen a k-anonimizálás csak sok attribútum törlésével lesz lehetséges.

A táblázatos adatoktól a tetszőleges struktúra felé

A Netflix cég a 2000-es évek elején DVD kölcsönzési tevékenységet folytatott, és rendszerének egyik kulcskomponense a Cinematch elnevezésű ajánlórendszere volt, amely a felhasználó értékeléseit figyelembe véve ajánlott számára további filmeket. A Netflix a Cinematch algoritmus továbbfejlesztésére versenyt indított, amelyhez 2006 októberében közzé tette körülbelül félmillió felhasználójának 1998 október és 2005 december közötti értékeléseit (Bennett és Lanning 2007). A cég közleményében is hangsúlyozta, hogy az adatokat név nélkül, azonosítókkal ellátva tették közzé, és az értékeléseket is kis mértékben módosították, hogy konkrét személyek értékeléseit nehezebb legyen visszakeresni.

A Netflix adatbázis szolgáltatott alapot az első nem táblázatos, nagy attribútumszámú adatbázis deanonimizálás demonstrációjára (Narayanan és Shmatikov 2008). Narayanan és Shmatikov a Netflix adathalmaz inspirációjára javasolta a Scoreboard algoritmust, amely egy általános deanonimizálási sémát követ, így a Netflix-specifikus alkalmazáson túlmenően tetszőleges nagy dimenziójú adatra alkalmazható.

A Scoreboard feltételezi, hogy a támadó rendelkezik olyan D' adatbázissal a deanonimizálás célpontjairól (ez az úgynevezett háttértudás, vagy kiegészítő információ), amely legalább részben megtalálható az anonimizált D adatbázisban, és az sem kritérium, hogy ez pontos információ legyen. A Scoreboard összehasonlítja a háttérinformációban szereplő $r' \in D'$ rekordokat az anonimizált adat $r \in D$ rekordjaival, és pontozza a potenciális $(r; r')$ párosításokat a hasonlóságuk alapján. A pontozásban a kevésbé gyakori jellemzők nagyobb hangsúlyt kapnak, ami a filmes vonatkozásban könnyen értelmezhető, hiszen például az kevesebbet árul el valakiről, hogy látta a Men in Black-et, mint mondjuk a Citizenfour-t. Ezután az algoritmus a legnagyobb pontszámú r'' rekordot jelöli ki a deanonimizálás eredményének, hogyha annak pontszáma a többi potenciális jelölthöz képes kellően kiemelkedő.

Az algoritmus tesztelésénél először azt ellenőrizték, hogy egy-egy véletlenszerűen választott felhasználót jól be tud-e azonosítani az algoritmus, majd pedig azt, hogy ha törlik az adatbázisból, ezt képes-e jelezni (téves alternatívák ajánlása helyett). Az előbbihez a felhasználótól mindössze 2-8 értékelést választottak ki a Scoreboard számára mint háttérinformációt (a felhasználók túlnyomó többsége 20 vagy több értékeléssel rendelkezik az adatbázisban). Ha a film pontozása pontosan ismert volt (1-5 csillag), a dátum pedig ±3 és ±14 nap pontosságú, akkor az algoritmus már mindössze 5/6 értékelés (6 értékelésből 5 helyes) alapján több mint 80%-os bizonyossággal volt képes a helyes deanonimizálásra, illetve ha az adatbázisban nem szerepelt a rekord, akkor annak elutasítására. 7/8 értékelésnél a deanonimizálás esélye bőven 90% felé nőtt. A kiegészítő információ pontatlanságát jól lehet ellensúlyozni az értékelések számával. Ha a film pontozásánál ±1 csillag eltérés volt megengedett, a dátumnál pedig a ±14 nap pontosság, akkor a 4/8-8/8 értékelések esetén a deanonimizálás valószínűsége körülbelül 60%-95% között mozgott.

A Scoreboard algoritmus akkor hatékony, hogyha megfelelő háttérismerettel rendelkezik a támadó, ennek feltárása azonban nem igényel különösebb nyomozói tevékenységet. Narayanan és Shmatikov munkájukban cáfolták, hogy a Netflix által kiadott adathalmaz jelentősen módosítva lenne: egyrészt két ismerősüknél, akiket megtaláltak az adatbázisban, mindössze legfeljebb 1/306 és 5/229 értékelés tért el az eredetitől, illetve a módosítást az adathalmaz statisztikai jellemzői sem támasztották alá túl meggyőzően. Ez viszont azt jelenti – tekintettel az algoritmus hibatűrési képességére –, hogy akár egy rövidebb munkahelyi csevegés vagy néhány értékelés az IMDb-n[1] is visszakereshetővé teszi azokat, akiknek értékeléseit a Netflix publikálta. (Ha pedig valaki mégsem szerepelne benne, az algoritmus ezt is hatékonyan jelzi.)

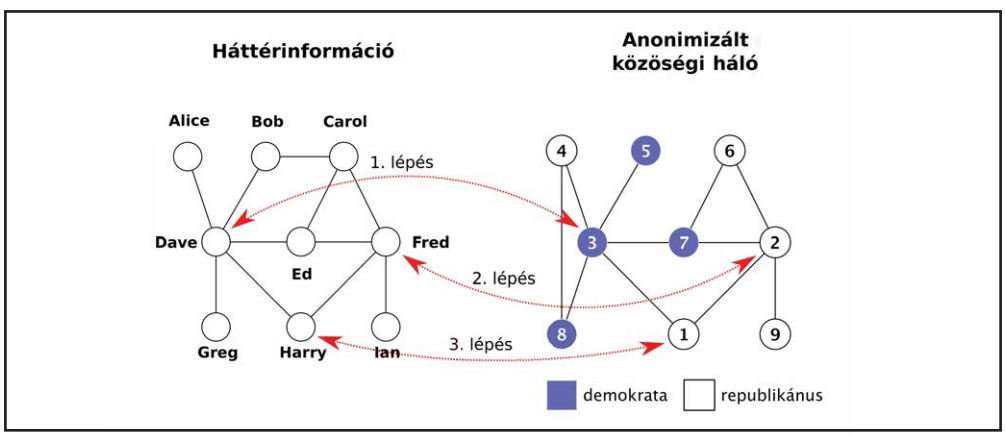
Hatékonyságnövelés: százezres közösségi hálózatok deanonimizálása

Bár a deanonimizálás valószínűsége (és pontossága) elég magas volt a Scoreboard algoritmus esetén, hatékonyságát jelentősen rontotta, hogy a háttérinformáció elemeit a teljes anonim adatbázissal összehasonlította. Ez a keresési séma nem működőképes, ha nem célzott támadásról van szó, hanem tömeges deanonimizálásról: azaz a Scoreboard csak addig hatékony, amíg a háttérinformáció néhány rekordot tartalmaz, de ha két teljes adatbázist kell összehasonlítani, akkor a számításigénye elfogadhatatlanul megnő.

[1] http://www.imdb.com

A másik probléma a fals-pozitív paradoxon, ami akkor áll fenn, ha a téves találatok aránya nagyságrendekkel több, mint a helyes. Ezt a filmes példánál maradva a következőképpen képzelhetjük el. Tegyük fel, hogy van egy a Scoreboardhoz hasonló algoritmus, amelynek ha megmutatunk egy $(r; r')$ felhasználó-párt ($r \in D$ anonim és $r' \in D'$ identitása ismert), akkor ha a párosítás helyes, az algoritmus 99% valószínűséggel ezt megmondja, míg hogyha helytelen, akkor 0,01% valószínűséggel téved csupán. Ha ezen feltételek mellett keresünk egy felhasználót az értékelései alapján egy 100 milliós halmazban, akkor az algoritmus körülbelül 10 000 találatot fog visszaadni, amiből azt az egy darab helyes találatot még ki kell valahogyan szűrni. (Ezért a Scoreboard-ban a legkevésbé egyező értékelés alapján diszkriminálták a téves találatokat, de ez a megközelítés nem mindig alkalmazható.) Éppen e miatt a probléma miatt kételkedhetünk az olyan projektek sikerében, amelyek a különféle bűncselekményeket tömeges megfigyeléssel kívánják megelőzni vagy visszaszorítani (Parra-Arnau és Castelluccia 2015).

Narayanan és Shmatikov (2009) a Scoreboardban alkalmazott alapelvek mentén javasoltak egy olyan algoritmust közösségi hálózatok deanonimizálására, amely ezeket a problémákat kiküszöböli, és emiatt akár két többszázezres (vagy nagyobb) közösségi hálózat deanonimizálását is képes hatékonyan és pontosan elvégezni – csupán a kapcsolatrendszer (gráf struktúra) figyelembevételével. Egyszerű trükköt alkalmaztak: mivel közösségi hálózatról van szó, és az egyes felhasználókat kapcsolatok kötik össze, az algoritmus futása során a már meglévő deanonimizálásokat is figyelembe vették.



2. ábra: Közösségi hálózat deanonimizálásának bemutatása. Először a globálisan kiugró felhasználókat párosítja (1-2. lépés), majd ezt követően a meglévő párok felhasználásával folytatja a többivel (3. lépés)

Az algoritmus működési elvét a 2. ábra segítségével mutatjuk be, amelyen látható egy nevekkel ellátott G' közösségi hálózat mint háttérinformáció, valamint egy G anonimizált közösségi hálózat. Mivel G tartalmaz egy érzékeny információt (politikai preferencia) a felhasználókról, a példában a támadó célja G deanonimizálása G'-vel. Az első lépésben az algoritmus a jellemzőik alapján globálisan kiugró felhasználókat keres, ez az inicializálási fázis. Ilyen például a Dave nevű felhasználó, amelynek összesen öt kapcsolata van (vagyis

az őt reprezentáló csomópontnak a fokszáma öt), ami G'-ben a legtöbb és így ez a jellemző Dave-et egyedivé teszi. A másik hálózatban a 3-as felhasználó szintén öt kapcsolattal rendelkezik és egyedi, ezért a támadó úgy veszi, hogy a 3-as felhasználó Dave-nek felel meg – azaz létrehoz egy párosítást a két közösségi hálózat felhasználói között. Ugyanilyen logika mentén létrehozza a (Fred, 2) párosítást is.

A következő fázis célja a meglévő párosítások felhasználása új párosítások kereséséhez. Erre szükség is van, hiszen – a példánál maradva – a kapcsolatok számának összehasonlítása nem minden esetben működik: például Harrynek két kapcsolata van, de ez igaz Bobra is. Azonban ha felhasználjuk a már meglévő párosításokat, akkor feltételezhetjük, hogy ahogy Harry Dave és Fred barátja G'-ben, úgy a neki megfelelő jelöltre is igaznak kell lennie, hogy 3 és 2 barátja G-ben és valószínűleg két kapcsolata van. Ez viszont csak az 1-es felhasználóra igaz, így az algoritmus létrehoz egy új párosítást (Harry, 1) között.

A meglévő párosításokat a példához hasonló módon használja fel a javasolt algoritmus a potenciális találatok szűkítésére (a gráf egészéről egy szűkebb körre): az adott G'-beli felhasználónak megfelelő találatról feltételezi, hogy az ismerőseik nagyjából ugyanazok, csak G-ben (Narayanan és Shmatikov 2009). A kisebb keresési tér így lényegében megoldja a hatékonysági és fals-pozitív problémákat is. A továbbiakban az algoritmus egyébként ugyanúgy működik, mint a Scoreboard: a potenciális találatokat pontozza (a koszinusz hasonlósághoz hasonlóan), és ha van kiemelkedő találat, akkor azt választja meg a deanonimizálási párosításhoz.

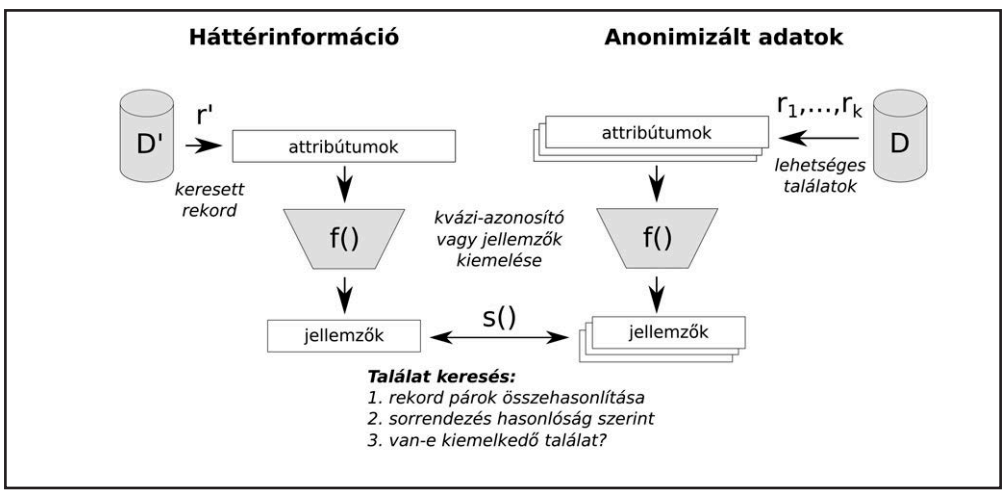
Az algoritmust élesben is tesztelték: egy 224 ezer felhasználóból álló Twitter kivonatot „deanonimizáltak” egy 3,3 millió felhasználóból álló Flickr kivonattal. A cél az volt, hogy az algoritmus párosítsa össze azokat a felhasználókat, amelyek mindkét kivonatban szerepelnek. Ehhez először, hogy az algoritmus eredményét ellenőrizni lehessen, meg kellett keresni valamilyen módszer alapján azokat a felhasználókat, akik ténylegesen mindkettőben szerepeltek. Ehhez felhasználták a felhasználónév, név és hely információkat, s ezekkel végül összesen 27 ezer felhasználót sikerült azonosítani mindkét adathalmazban. Az algoritmus inicializálásához kiválasztottak 150 felhasználót (akik rendelkeztek legalább 80 kapcsolattal). Az algoritmus a 27 ezer felhasználó 30,8%-át sikeresen megtalálta (ez a *felidézés*, a helyes találatok aránya az összes lehetséges találatokhoz képest), és csak 12,1%-nyi hibát vétett (ez a *hibaarány*: a hibás találatok száma az összes lehetséges találathoz képest). A későbbiekben is használni fogjuk a felidézés, precizitás és hibaarány fogalmakat; a precizitás a hibák aránya az összes találat között (angolul *precision*).

A 2009-ben publikált algoritmus az idő próbáját is kiállta. Egy 2015-ös cikkben szimulációs vizsgálatokkal összehasonlították az addig megjelent deanonimizáló támadásokat a legkorszerűbb anonimizálási eljárásokkal szemben (Ji et. al 2015), és eszerint egyetlen időközben publikált támadás sem múlta felül a Narayanan és Shmatikov által megalkotott algoritmus hatékonyságát. Az első, általában jobbnak tekinthető algoritmust Gulyás, Simon és Imre (2016) javasolta, ahol a 2015-ös összehasonlítást identikus módon megismételték, és az új algoritmust összemérték a korábbiak közül a legkiemelkedőbb eredményt nyújtóakkal. Ennek alapján az új algoritmus valamennyinél magasabb deanonimizálási arányt ért el alacsony hibaarány mellett.

Deanonimizálás gépi tanulás segítségével

A gépi tanulási módszereket jól körülhatárolható módon alkalmazzák a deanonimizálási eljárásokban. Az eddig tárgyalt példák alapján a következőképpen vázolhatjuk fel a deanonimizálási algoritmusok működési sémáját (3. ábra):

1. A támadás célja egy D anonimizált adathalmaz, melyből az egyértelmű azonosítók hiányoznak és az adatokat is módosították bizonyos mértékben. A támadó egy D' adathalmazt használ fel a D-beli rekordok deanonimizálására, amelyben a rekordok számossága adattípustól függően változó lehet.
2. A támadó az adat típusa alapján kiválasztja az $f(\cdot)$ és $s(\cdot)$ függvényeket. Az $f(\cdot)$ függvényt használja a rekordokból kvázi-azonosító előállítására, az $s(\cdot)$ függvény pedig két rekord kvázi azonosítóinak a hasonlóságát megadó függvény.
3. A támadó kiválaszt egy $r' \in D'$ rekordot, amelynek az anonimizált $r \in D$ párját keresi.
4. A támadó kiszámítja $f(r')$-et, majd valamennyi potenciális $r'' \in D$ rekordra szintén, és ezután kiszámolja a rekordok közötti $(f(r'), f(r''))$hasonlóságokat.
5. Ha van kiugró hasonlósággal bíró, vagy valamilyen más elfogadási kritériumnak megfelelő rekord, akkor ezt fogadja el $r=r''$ a helyes deanonimizálásnak.



3. ábra: A deanonimizálási eljárások jellemző sémája

A kvázi-azonosító kiválasztás a korábbi példákban bizonyos oszlopok kiválasztása volt (Sweeney 2002), illetve ennek felelt meg az egyes értékelések súlyozása a Netflix adathalmaz deanonimizálásában (Narayanan és Shmatikov 2008). Azonban ez nem mindig triviális feladat, például mit választanánk ki, ha hívásindítás és -fogadás idejéről és helyéről van egy adatbázisunk? Vagy mondjuk a telefon gyorsulás- és sebességmérőjéből származó információk alapján? Illetve az sem mindig egyértelmű, hogy a meglévő támadásokban használt választás a legoptimálisabb. Ezen okok miatt alkalmazták egyes esetekben a gépi tanulási módszereket a kvázi-azonosító, vagyis jellemző kiválasztására (angolul *feature selection*); azaz a $f(\cdot)$ függvényt helyettesítették olyan eljárásokkal, amelyek önállóan képesek azonosítani a releváns jellemzőket az adatban.

A másik tipikus alkalmazási terület az $s(\cdot)$ függvény helyettesítése gépi tanulási módszerekkel. Ennek az oka ugyanaz, mint az előbb: sok esetben nem ismert (különösen ha a jellemző kiválasztása is gépi módszerekkel történik), illetve előfordulhat, hogy gépi tanulással a szakértők által javasolt hasonlósági metrikánál jobbat lehet találni. A következő fejezetekben megvizsgáljuk, hogy különböző adattípusokra hogyan alkalmaztak gépi tanulási módszereket.

Gépi tanulás közösségi hálózatok deanonimizálásához

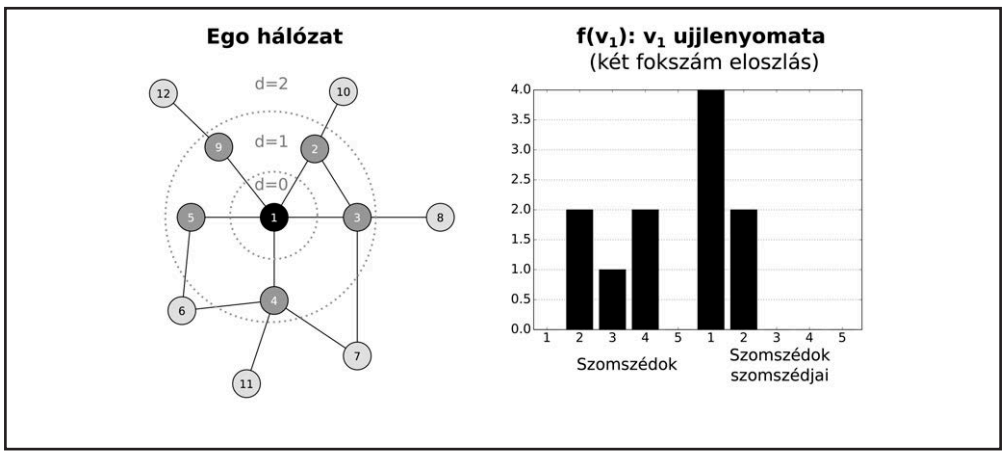
Az első közösségi hálózatokat gépi tanulás segítségével deanonimizáló algoritmust Pedarsani, Figueiredo és Grossglauser (2013) javasolta. Esetükben az algoritmus döntési mechanizmusa a Bayes-tételre épült, és jellemzőként az egyes felhasználók fokszámát és a gráf struktúrában már azonosított szereplőktől vett távolságait használta fel. Ahogy G' és G között nő a deanonimizált felhasználók száma, úgy tud egyre több információt az algoritmus a Bayes-döntés során figyelembe venni és egyre pontosabb döntéseket hozni. Az algoritmus további érdekessége, hogy ellentétben a Narayanan és Shmatikov által javasolt támadással, nem igényel inicializálást. Az algoritmus első lépésben a két közösségi hálózat legnagyobb fokszámú csomópontjai között keres párokat, majd a vizsgált csomópontok számát fokozatosan, iteratív módon kiterjeszti.

Az első teljesen átfogó összehasonlítást a közösségi hálózati deanonimizáló algoritmusokról Ji et al. (2015) készítette, amelyben a hét legkorszerűbb támadás közé beválasztották a Bayes-döntésen alapuló eljárást is. Az összehasonlításuk valós közösségi hálózatokon végzett mérésekre támaszkodott, amelyben az algoritmusokat többféle anonimizálási sémával szemben is alkalmazták. Noha az algoritmus jónak mondható eredményt ért el a helyesen deanonimizált felhasználókat tekintve, Ji et al. (2015) összehasonlító tanulmánya két jelentős részletet figyelmen kívül hagyott (amelyek a munka módszertana szempontjából is kritikusnak tekinthetők): a magas korrekt deanonimizálási arány mellé egészen magas hibaarány is társult (tehát alacsony volt a precizitás), illetve az algoritmus memóriaigénye, amely a meglévő deanonimizációs párosítások számától függően gyorsan növekszik (Gulyás, Simon és Imre 2016). Így az algoritmus eredményei kevésbé imponálóak; vélhetően az utóbbi probléma állhat annak a hátterében is, hogy az eredeti cikkben mindössze kétezer felhasználóból álló gráfon demonstrálták az algoritmus hatékonyságát (Pedarsani, Figueiredo és Grossglauser 2013), szemben a több tízezer csomópontból álló gráfokkal, amelyeket jellemzően alkalmazni szoktak az ilyen jellegű cikkekben.

A Sharad és Danezis (2014) által tervezett deanonimizáló algoritmus már általánosabb (de nem gépi tanulás által előállított) jellemzőket használt és véletlen erdőket (angolul *random forest*) a döntések meghozatalához. Az Orange 2012-es Data for Development (D4D) felhívása során ki akarta adni körülbelül 5 millió elefántcsontparti személy hívásinformációit (ki-kivel kommunikált), és előzetesen felkérte a kutatókat, hogy vizsgálják meg, hogy az adatok kellő mértékben anonimizáltak-e. Ez azt jelentette, hogy a kommunikációból létrejövő hálózatot ego hálózatokra (angolul *ego network*) szabdalták, amely egy felhasználóból és a körülötte lévő közvetlen kapcsolatokból állt (szomszédok és szomszédok szomszédai; lásd a 4. ábra, bal oldalt). Hamar kiderült, hogy ezek a darabok könnyen újra egyesíthetőek, ezért az Orange új, némileg módosított anonimizálási módszerrel állt elő. Hogy a macska-egér játéknak a kutatók elejét vegyék, megalkották a következőkben tárgyalt

algoritmust, amely az efféle apróbb módosítások esetén is működik és nem csupán ego hálózatok egyesítésére alkalmazható, hanem közösségi hálózat deanonimizáló algoritmusként is.

Sharad és Danezis a jellemző kiválasztásához az adott csomópont körüli szomszédok és azok szomszédjainak a fokszámának eloszlását javasolta (lásd a 4. ábra, jobb oldalt). Döntésük mögött az a megfontolás áll, hogy a különféle anonimizálási eljárások ellenére a fokszám eloszlás a hálózatban viszonylag érintetlen kell, hogy maradjon – különben az adatok felhasználhatósága (és üzleti, kutatási értéke) is jelentősen csökkenne.



4. ábra: Az 1-es felhasználó ego hálózata (a körök az egotól vett távolságot jelölik), és az 1-es felhasználóról (csomópontról) készített strukturális ujjlenyomat, amely a szomszédok és szomszédok szomszédjainak fokszámeloszlásának egymás után fűzése

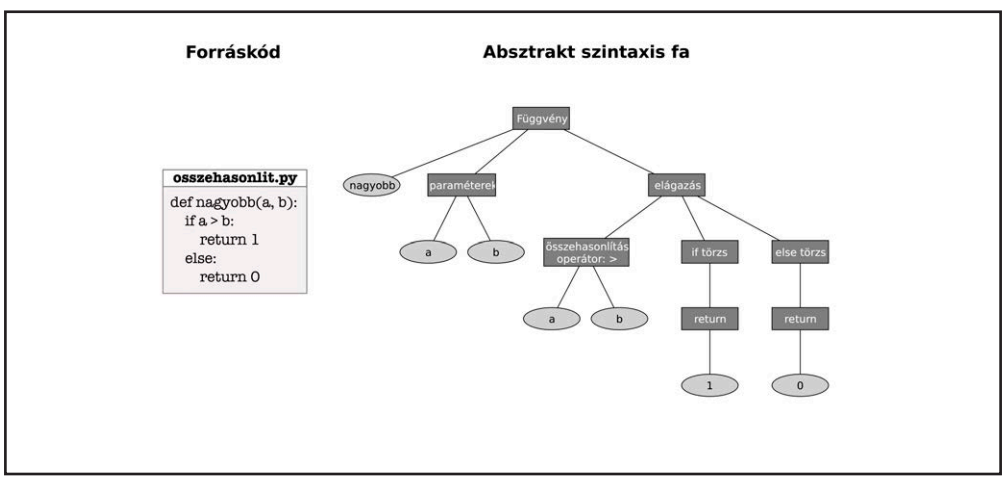
A deanonimizálási döntéshez pedig véletlen fákat használnak, a következő módon. Az algoritmus egy iterációjának bemenete $(v'v'')$ csomópont párok, amelyek egy, a háttérinformációból származó $v' \in G'$ csomópontból, és az ehhez tartozó összes potenciális $v'' \in G$-vel alkotott párosításokból állnak. Ezekhez az algoritmus kiszámolja a $(f(v'), f(v''))$ ujjlenyomatpárt, és ezeket a párokat adják bemenetként a véletlen erdőnek, amelynek kimenetként annyit kell kiadnia, hogy a két csomópont egyezik-e szerinte, vagy sem. Az algoritmus minden párosítást létrehoz, ahol a véletlen erdő egyező csomópontokat jelez. Ebből az is látszik, hogy az algoritmus egyedüli hátránya a Narayanan és Shmatikov (2009) támadásához képest, hogy nem veszi figyelembe a már deanonimizált felhasználó-párokat.

A támadást a Flickr szolgáltatásból származó adathalmazon tesztelték. A betanításhoz a véletlen erdőnek 5000 nem azonos (negatív minta), és változó számú, 10-1250 azonos felhasználó-párt mutattak (pozitív minta), a betanított modellt pedig 10 000 páron tesztelték le. Már 10 pozitív minta esetén is sikerült a felhasználók 16,74%-ának helyes deanonimizálása (felidézés), mindössze 1% hibaarány mellett. 50 pozitív mintával 22,01%-ra emelkedett a felidézés, és ezt érdemben a pozitív minták számával nem tudták növelni. Azonban nagyobb hibaarány tolerálása mellett ez is lehetséges, például 10% hibaarány mellett és 50 pozitív mintával 58,38% felidézést értek el. A szerzők által választott jellemző előállítási mód és a véletlen erdő alkalmazása kellően ellenállónak bizonyult.

Deanonimizálás programozási stílus alapján

Aylin et al. (2015) a programozók forráskód alapján történő deanonimizálását a fentiekhez hasonlóan gépi tanulási problémaként fogalmazták meg, amelyben a forráskód alapján létrehozott profilokról egy osztályozó gépi tanulási eljárás dönt, hogy ugyanattól a szerzőtől származnak-e, vagy sem. A korábbi munkákhoz képest fő újításként egy újszerű jellemzőkészletet dolgoztak ki programozók profilírozásához, illetve a módszerüket egy nagyobb, 250 programozót tartalmazó adathalmazon tesztelték, amely a Google Code Jam (GCJ) nemzetközi kódoló versenyről származik (a vizsgálatot a C++ forráskódú helyes megfejtésekre korlátozták). A támadás modellje a korábbival egyező sémára épül: rendelkezünk néhány forráskód-részlettel (anonim adat), amelynek szerzőjét keressük. Ehhez a rendelkezésünkre álló háttérinformáció egy forráskód-adatbázis, amely a keresett szerzőn kívül további szerzőktől is tartalmaz forráskódot.[2] A deanonimizálásnak ezen alkalmazási módja több pozitív felhasználási lehetőséggel is rendelkezik, például szerzői jog (bírósági előtti) bizonyításában, vagy plágium detektálásban, akkor is, ha konkrét kód-egyezés nincs a vizsgált művek között.

A jellemzők kinyeréséhez egy úgynevezett absztrakt szintaxis fát (angolul *abstract syntax tree*, AST) hoztak létre a forráskódból, erre látható egy egyszerű példa az 5. ábrán. Jól látszik, hogy például a függvények mélysége, az elágazások száma jól tükröződik ezen az ábrázolási módon, és ez összefüggésben áll a programozó absztrakciós képességével, ami máris egy jellemző.



5. ábra: Minta Python kód és a hozzá kapcsolódó absztrakt szintaxis fa

A kódolási profil háromféle jellemző csoportot tartalmazott mint szintaktikai, lexikai és kódelrendezés (vagy struktúra), és ezekből az első kettő tartalmaz több, az AST-ből származtatott jellemzőt is. Szintaktikai volt például az AST maximális mélysége, az egyes fa

[2] A cikk szerzői csak a zárt univerzum modell szerinti eseteket vizsgálták, amelyben a keresett programozó mindig szerepel a háttérinformációban. A nyílt világ modell vizsgálata még megoldandó kutatási feladat.

csomópontok relatív gyakorisága (de például a TF-IDF gyakoriság is (angolul *term frequency–inverse document frequency*), amely megmutatja, hogy egy adott szó a dokumentumon belül mennyire jelentős a korpusz egészéhez viszonyítva), átlagos mélysége, különböző csomópont bigramok relatív gyakoriságai (a bigram két csomópontegyüttes azonos sorrendű előfordulása, és általános formája az n-gram). Lexikai például az átlagos megjegyzéshossz logaritmusa, átlagos függvényszám logaritmusa fájlonként, míg az elrendezési jellemzők közé olyanok tartoznak, mint a szóközök, tabulátorok számának logaritmusa (fájlonként), illetve a tördelési szokások. A különféle n-gramok nélkül valamivel kevesebb, mint 300 jellemzőt határoztak meg, amelyek száma az n-gramokkal nagyságrendileg pár tízezerre nő.

Az így előállított profilokat véletlen erdőkkel hasonlították össze a Sharad és Danezis (2014) munkájában látott módhoz hasonlóan. Mivel a szerzők azonosítóit is közzétették a GCJ által publikált forráskódok mellett, így követni lehet éveken átívelően a munkásságukat. Ez megkönnyítette a modellek betanítását az egyes szerzők munkáinak felismerésére, hiszen nagyobb számú minta állt rendelkezésre.

Az így létrehozott programozó-azonosító rendszer magas találati arányt tudott elérni a különféle helyzetekben. Amikor 250 potenciális szerző közül kellett kiválasztania a megfelelőt, ez az esetek 95%-ában sikerült (plágiumkeresés jellegű alkalmazás), ha azonban csak két szerző között kellett választani, a rendszer az esetek 99%-ban sikeresen teljesítette a feladatot. További érdekesség, hogy megpróbálták egy kereskedelmi forgalomban elérhető kód-obfuszkáló programmal elrejteni a programozó identitását, de ez a találati arányon lényegében nem változtatott: kiderült, hogy a tesztelt alkalmazás a szintaktikai jellemzőket nem módosította, csupán néhány elrendezésbeli és lexikai jellemzőt[3], és ez nem volt elegendő.

Egy későbbi munkában Aylin et al. (2016) hasonló deanonimizálási támadást vizsgált bináris programok esetén, ami például fontos lehet rosszindulatú kódok szerzőjének a felderítésében. Azt találták, hogy bár a forráskódok bináris programmá alakítása (fordítás) során számos dolog visszaállíthatatlanul elvész, mint például a változónevek, illetve a fordító a program struktúráját is módosítja, azonban a szintaktikai jellemzők ez esetben is kevésbé sérülnek. Munkájukban megmutatták, hogy ezek visszanyerhetőek a bináris alkalmazások automatizált visszafordítása (angolul *decompile*) után, ugyanis a visszafordítás által létrehozott forráskódból kinyert absztrakt szintaxis fa továbbra is magán hordozza a programozó kézjegyét. Az AST-ből és további kiegészítésekkel olyan profilt tudtak létrehozni, amely koszinusz hasonlósága az eredeti program profiljához képest 80%-os volt, ami már elegendőnek bizonyult a véletlen erdő számára: 100 programozó esetén a deanonimizálás 78,1%-ban volt sikeres, de még 600 programozó esetén is 51,6%-ban.

Jövőkép: merre fejlődhetnek a támadások?

Az eddigi munkák eredményeit nem vonhatjuk kétségbe, azonban az is biztos, hogy nem értünk el a lehetőségek végére, több ponton lehet ezeket az eredményeket felülmúlni, vagy legalábbis jó eséllyel kísérletet tenni erre. A két legkézenfekvőbb trükk, amelyet

[3] Ez nem jelenti azt, hogy a programozó identitását ne lehetne anonimizálni ilyen szoftverrel, de azt igen, hogy ez az alkalmazás erre nem volt felkészítve. Lehet, hogy a teljes anonimizálás lehetséges, de ez további vizsgálatokat igényel.

gépi tanulási módszerek teljesítményének növelésénél alkalmazni szoktak, az a rendelkezésre álló adatok mennyiségének növelése, illetve *a döntési mechanizmusban alkalmazott gépi tanulási eljárások cseréje fejlettebbre*. A véletlen erdőket 1995-ben javasolták először (Ho 1995), és bár ma már „kulcskész" termékként elérhetőek különböző gépi tanulási könyvtárakban, nem minden esetben bizonyulnak a leghatékonyabb eszköznek.

Aylin et al. (2015) munkájának módszertanát követve Wisse és Veenman (2015) JavaScript programozókat azonosítottak AST-vel. Azonban munkájukban a véletlen erdőkkel (és néhány további eljárással) szemben lineáris kernelű *support vector machine* (SVM) eljárást alkalmaztak, mivel az jobb eredményt adott. Nem lenne meglepő, ha hamarosan kiderülne, hogy a mesterséges neurális hálózatok (angolul *artificial neural networks*, ANN) ennél is jobb eredményt képesek elérni: az elmúlt években az ANN-ek alkalmazása olyan eredményeket ért el különféle alkalmazásokban (mint például az arcfelismerés, vagy a beszédfelismerés), amely túlmutatott az addigi legjobb eredményen, bizonyos esetekben már az emberi pontosságot is elérve a problémák megoldásában (LeCun, Bengio és Hinton 2015). Az ANN-eket az emberi agy működése inspirálta, és az abban található neurális hálózatokat utánozzák. Bár az ANN-ek már évtizedek óta kutatott terület, az elmúlt évtizedben olyan új tanítási eljárások felfedezése hozott áttörést, amelyek a komplex és mélyebb struktúrájú hálózatok tanítását is hatékonyan el tudják végezni (illetve az ezzel párhuzamosan növekvő számítási kapacitás, amihez a videokártyák elterjedése is hozzájárult).

Szintén továbbfejlesztési lehetőség, ha a kvázi azonosítók helyett *automatizált jellemzőkinyerést* alkalmazunk az azonosítók precíz kézi megtervezése helyett. A komplex mesterséges neurális hálózatok ebben kiemelkedő eredményeket tudnak elérni: a hálózatok csak nyers adatot kapnak feldolgozásra, és maguk végzik el az adatok alapján a jellemzőkinyerést. Például az objektumfelismerésre szakosodott hálózatokban (ez az úgynevezett gépi látás szakterülete) a különböző neurális hálózati rétegek közvetlenül egymásra épülnek, és ahogy az információ feldolgozása történik, egyre komplexebb részletekkel dolgoznak. Arcfelismerés esetén míg az első neuron réteg csak a vonásokat fedezi fel (éldetektálás), a következő neuron réteg az ezekből összeálló részleteket, majd a harmadik pedig már az arc egyes részeit, mint szem, orr, stb. Ez a fajta jellemző-kiemelés hasznos lehet olyan esetekben, amikor a kézileg készített jellemzőkinyerés nem ismert, vagy kétséges, hogy a hatékonysága a legjobb.

Erre kiváló példa McPherson, Shokri és Shmatikov (2016) munkája, amelyben arcfelismerésre használt komplex neurális hálókat használtak elhomályosítással vagy kikockázással védett arcok felismerésére, az esetek 40-97%-ban sikeresen – ebben az esetben a jellemzőkinyerés nyilvánvalóan nem volt egyértelműen meghatározott.

A deanonimizálási probléma továbbá nagyon hasonlít a hitelesítés problémájához: van egy felhasználó (háttérinformáció) és az a kérdés, hogy egy adott felhasználói csoporton belül van-e vele egyező felhasználó (ami az anonimizált adathalmaznak felel meg). A legnagyobb különbség a két probléma között talán a felhasználók számában van: a hitelesítés(i eredményeket bemutató cikkek) jellemzően kisebb számú felhasználóval számol(nak) (lásd az alábbi példát), szemben a deanonimizálásnál látott ezrekkel, vagy többel. Ezért e korlát kiküszöbölése után várható csak, hogy a hitelesítésben alkalmazott áttörések megjelennek majd a deanonimizálási támadásokban is.

Gadelata és Rossi (2016) okostelefonok giroszkóp (sebességmérő) és gyorsulásmérő szenzorjaiból származó adatokat használtak hitelesítésre az okostelefonok felhasználói já-

rási stílusának elemzése alapján. A szenzorokból származó adatokat először is felosztották a járás ciklikussága szerint ablakokra, és ezekből az ablakokból származó mintákból nyertek ki egyéni jellemzőket komplex neurális hálózatokkal (úgynevezett konvolúciós neurális hálózatokkal). Munkájuk jól illusztrálja, hogy a hitelesítési problémában tipikusan mennyivel kisebb adathalmazokkal dolgoznak a kutatók: összesen 50 felhasználótól gyűjtöttek adatokat egy féléves periódus során, majd 35 alany adatait használták fel a jellemzőkinyerés betanítására, 15 felhasználó adatait pedig a hitelesítési mechanizmus tesztelésére.

Összegzés

Tanulmányunkban ismertettük a deanonimizáló támadásokat, amelyek az egyik legfőbb akadályát jelentik a különféle szolgáltatásokban gyűlő adatok publikálásának, hiszen sok esetben hatékonyan lehetővé teszik adathalmazok összekapcsolását, vagy anonimizálás esetén az eredeti identitás visszaállítását. Áttekintettük a korszerű deanonimizáló algoritmusokat, illetve a gépi tanulást alkalmazó támadásokat is. A jelen cikkben megjelenő trendből kitűnik, hogy – a privátszféra helyzetét tekintve – már most is jelentős fölénnyel bíró deanonimizáló támadások további, talán a felhasználói oldalon már egyáltalán nem ellensúlyozható előnyre tehetnek szert a gépi tanulási technikák alkalmazásával.

Ehhez vegyük hozzá, hogy nem egy olyan adattípus létezik (mint például a közösségi hálózatok struktúrája, vagy a telefonos kommunikációból származó helyzetinformáció), amelyre ugyan léteznek privátszféra-védő megoldások, de nincs általánosan elfogadott anonimizálási technika, amely a deanonimizáló támadásokkal szemben is megállja a helyét, és az alkalmazása az adat hasznosságát sem degradálja jelentősen. Emiatt egyelőre rövid és hosszú távon is csupán a jogi szabályozás tűnik megfelelő védelemnek, ami jelentheti azt, hogy az adat kurátora szerződésbe foglalva tiltja a deanonimizálást és az adatok további megosztását, illetve azt is, hogy törvényileg szabályozzák a deanonimizálás lehetőségét, például szigorú kutatási keretek közé szorítva a deanonimizálás lehetőségét. Erre láthatunk példákat, javaslat formájában már fel is merült az ausztrál törvényhozásban a deanonimizálás bűncselekménnyé nyilvánítása (Chirgwin 2016). Valamint az új európai adatvédelmi szabályozás (GDPR) is korlátozza az efféle visszaéléseket, ugyanis személyes adatnak tekinti az adatalanyhoz nem direkt módon köthető információkat is, amely a deanonimizálás célpontja lehet.

Irodalom

Aggarwal, Charu C., „On k-anonymity and the curse of dimensionality", in *Proceedings of the 31st international conference on Very large data bases (VLDB '05, Trondheim, Norway, August 30 - September 02, 2005)*, VLDB Endowment, 2005. pp. 901-909.

Bangeman, Eric, „AOL subscribers sue over data leak", *Ars Technica*, 26 September 2006. https://arstechnica.com/business/2006/09/7835/

Barbaro, Michael, „A Face Is Exposed for AOL Searcher No. 4417749", *The New York Times*, 9 August 2006. http://query.nytimes.com/gst/abstract.html?res=9E0CE3DD1F3FF93AA3575BC0A9609C8B63&legacy=true

Bennett, James and Stan Lanning, „The netflix prize", in *Proceedings of KDD Cup and Workshop 2007, San Jose, California, Aug 12, 2007*, ACM, 2007. https://www.cs.uic.edu/~liub/KDD-cup-2007/NetflixPrize-description.pdf

Caliskan-Islam, Aylin, Richard Harang, Andrew Liu, Arvind Narayanan, Clare Voss, Fabian Yamaguchi and Rachel Greenstadt, „De-anonymizing programmers via code stylometry", in Jaeyeon Jung (Ed.), *Proceedings of the 24th USENIX Conference on Security Symposium (SEC'15)*, USENIX Association, Berkeley, CA, USA, 2015, pp. 255-270.

Caliskan-Islam, Aylin, Fabian Yamaguchi, Edwin Dauber, Richard Harang, Konrad Rieck, Rachel Greenstadt and Arvind Narayanan, „When Coding Style Survives Compilation: De-anonymizing Programmers from Executable Binaries", *ArXiv preprint*, 1 March 2016. https://arxiv.org/abs/1512.08546

Chirgwin, Richard, „Australia wants law to ban de-anonymisation of anonymous data", *The Register*, 28 September 2016. http://www.theregister.co.uk/2016/09/28/oz_wants_to_ban_deanonymisation_ag_brandis/

Gadaleta, Matteo and Michele Rossi „IDNet: Smartphone-based Gait Recognition with Convolutional Neural Networks" *ArXiv preprint*, 19 October 2016. https://arxiv.org/abs/1606.03238

Gulyás Gábor György, Benedek Simon, Sándor Imre, „An Efficient and Robust Social Network Deanonymization Attack" in *Proceedings of the 2016 ACM on Workshop on Privacy in the Electronic Society (WPES '16, Vienna, Austria, 24 October 2016.)*, ACM, New York, NY, USA, 2016. pp. 1-11. https://doi.org/10.1145/2994620.2994632

Ho, Tin Kam, „Random decision forests" in *Proceedings of the Third International Conference on Document Analysis and Recognition Volume 1 (ICDAR '95, 14-15 August 1995.)*, IEEE Computer Society, Washington, DC, USA, 1995. pp. 278-283.

Ji, Shouling, Weiqing Li, Prateek Mittal, Xin Hu and Raheem Beyah, „SecGraph: a uniform and open-source evaluation system for graph data anonymization and de-anonymization", in Jaeyeon Jung (Ed.), *Proceedings of the 24th USENIX Conference on Security Symposium (SEC'15, Washington, D.C., 12-14 August 2015.)*, USENIX Association, Berkeley, CA, USA, pp. 303-318.

LeCun, Yann, Yoshua Bengio and Geoffrey Hinton, „Deep learning", *Nature*, Issue 521. (2015), pp. 436–444. http://dx.doi.org/10.1038/nature14539

McPherson, Richard, Reza Shokri and Vitaly Shmatikov, „Defeating Image Obfuscation with Deep Learning", *ArXiv preprint*, 6 September 2016. https://arxiv.org/abs/1609.00408

Narayanan, Arvind and Vitaly Shmatikov, „Robust De-anonymization of Large Sparse Datasets", in *Proceedings of the 2008 IEEE Symposium on Security and Privacy (SP '08, Oakland, 18-21 May 2008.)*, IEEE Computer Society, Washington, DC, USA, 2008, pp. 111-125. https://doi.org/10.1109/SP.2008.33

Narayanan, Arvind and Vitaly Shmatikov, „De-anonymizing Social Networks", in *Proceedings of the 2009 30th IEEE Symposium on Security and Privacy (SP '09, Oakland, 17-20 May 2009.)*, IEEE Computer Society, Washington, DC, USA, 2009, pp. 173-187. https://doi.org/10.1109/SP.2009.22

Parra-Arnau, Javier and Claude Castelluccia, „Dataveillance and the false-positive paradox", in *Proceedings of the 1st International Workshop on Privacy and Inference (PrInf 2015)*, Dresden, Germany, 2015.

Pedarsani, Pedram, Daniel R. Figueiredo and Matthias Grossglauser, „A Bayesian method for matching two similar graphs without seeds", in *51st Annual Allerton Conference on Communication, Control, and Computing (Monticello, 02-04 October 2013.)*, 2013, pp. 1598-1607. http://dx.doi.org/10.1109/Allerton.2013.6736720

Sharad, Kumar and George Danezis, „An Automated Social Graph De-anonymization Technique", in *Proceedings of the 13th Workshop on Privacy in the Electronic Society (WPES '14, Scottsdale, Arizona, USA — 3 November 2014.)*, ACM, New York, NY, USA, 2014, pp. 47-58. https://doi.org/10.1145/2665943.2665960

Sweeney, Latanya, „k-anonymity: a model for protecting privacy”, *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, Vol. 10. (2002) Issue 5., pp. 557-570. http://dx.doi.org/10.1142/S0218488502001648

Székely Iván: „Kukkoló társadalom - avagy van-e még függöny a virtuális ablakunkon?”, inTalyigás Judit (szerk.), *Az Internet a kockázatok és mellékhatások tekintetében*, SCOLAR, Budapest, 2010. 93-120. old.

Wisse, Wilco and Cor Veenman, „Scripting DNA: Identifying the JavaScript programmer”, *Digital Investigation*, Vol. 15. (2015. dec.), pp. 61-71. https://doi.org/10.1016/j.diin.2015.09.001

Gulyás Gábor György, PhD. Budapesten született 1984-ben. 2007-ben a BME Villamosmérnöki és Informatikai Karán szerzett diplomát az Infokommunikációs rendszerek biztonsága szakirányon, majd 2015-ben PhD fokozatot szerzett a BME-n a CrySyS Laboratórium tagjaként. Alapító tagja és rendszeres szerzője a Nemzetközi PET Portál és Blognak (2007-2015). Szervezője és előadója számos privátszféra-védelmet népszerűsítő előadásnak, eseménynek. Jelenleg az INRIA (Institut National de Recherche en Informatique et en Automatique, Franciaország) posztdoktori kutatójaként dolgozik a Privatics csoportban. Főbb kutatási területei a webes privátszféra-védelem (webes látogatók nyomkövetése és megfigyelése) és a (de-)anonimizálás témakörökre esnek.

Székely Iván

CPDP – Computers, Privacy and Data Protection, tizedszer

2017 januárjában tízéves jubileumához érkezett a CPDP[1], a számítógépek, a magánélet és az adatvédelem kapcsolatának talán legnagyobb és legjelentősebb, évente megrendezett nemzetközi konferenciája, amely magát „multistakeholder platform"-nak, vagyis olyan rendezvénynek határozza meg, ahol a témában bármilyen oldalról érdekelt, esetenként ellentétes érdekeket és álláspontokat képviselő szereplők találkozhatnak egymással, megismerhetik egymás nézeteit és nyíltan kifejthetik álláspontjukat. E beszámoló szerzőjének alkalma volt előadóként részt venni a legelső konferencián, majd számos azt követőn is, az utóbbi években pedig közreműködni a rendezvénysorozat szakmai irányító testületében és több programjában, ezért ez a beszámoló nemcsak a legutóbbi konferencia szerteágazó programjáról kíván rövid áttekintést adni, hanem igyekszik felvázolni azt a kontextust is, amely a CPDP-t kiemeli a hasonló tárgyú szakmai rendezvények sorából.

A CPDP előtörténete

2007 októberében Brüsszel flamand kulturális központjában, a *deBuren*-ben a jog, a technológia és a társadalom metszeteit kutató egyetemi intézetek[2] szervezésében „Reinventing Data Protection?" címmel rendeztek nemzetközi konferenciát a magánszféra és az adatvédelem különféle vetületeivel foglalkozó szakembereknek. A konferencia deklarált célja volt, hogy feltárja az adatvédelmi szabályozás problémáit és gyengeségeit, számbavegye a technológiai fejlődés kihívásait, összehozza a tudósokat a jogalkalmazókkal és az ipar képviselőivel, valamint hogy ajánlásokat fogalmazzon meg az EU adatvédelmi irányelvének reformja[3] érdekében. Az akkori résztvevők még ma is úgy emlékeznek vissza erre a rendezvényre, mint egy kivételesen színvonalas, sajátos hangulatú eseményre, amelynek előadásai könyv formában is megjelentek (Gutwirth et al. 2009). Kevesen tudták akkor, hogy az egyszeri rendezvény évenként megrendezett konferenciává, a válogatott szakmai kör pedig széleskörű közönséggé válik a következő években.

A konferencia nemsokára kinőtte a deBuren épületét (bár az intézmény azóta is állandó helyszíne a CPDP kapcsolódó rendezvényeinek, kiállításainak, nyilvános vitaestjeinek, könyvbemutatóinak), és átköltözött a Les Halles de Schaerbeek épületébe. A Les

[1] http://www.cpdpconferences.org

[2] Centre de Recherches Informatique et Droit (CRID, Namur-i Egyetem), Research Group on Law, Science, Technology and Society (LSTS, Brüsszeli Szabadegyetem), Tilburg Institute for Law, Technology, and Society (TILT, Tilburgi Egyetem), Instituut Permanente Vorming IPAVUB, Brüsszeli Szabadegyetem).

[3] A reform legfőbb eredménye a 2018 májusától alkalmazandó egységes európai adatvédelmi rendelet, a GDPR lett.

Halles egy funkcióját vesztett vásárcsarnok Brüsszel egyik multikulturális kerületében, a török negyed, a Gard du Nord pályaudvar és a piroslámpás negyed szomszédságában, vagyis nem az elegáns belvárosban fekszik. Az épület szerencsés sorsú, mert nem bontották le, hanem hatalmas tereit kulturális központtá alakították. A CPDP saját elnevezéseket alkalmaz a terek megjelölésére: a bárpulttal is rendelkező informális beszélgető hely a „sikátor" (La Ruelle), a kávészünetek, az ebéd, a fogadások és a díjkiosztó rendezvények helyszíne a „falu" (Le Village), a legérdekesebb előadások és viták helyszínéül szolgáló alsó szint a „pince" (La Cave), a két nagy helyszín pedig a mintegy 800 főt befogadó „nagyterem" (Grande Halle) és a szintén nagy méretű „kisterem" (Petite Halle). Mivel az évek során a CPDP résztvevőinek száma egyre nőtt, és a program is négy-öt, sőt néha hat párhuzamos szakcióban zajlik, ezért további helyszínekre volt szükség. Az épülettömb hátsó frontján lévő régimódi Maison des Arts palota, nyikorgó parkettájával és könyvtárszobájával, valamint különös hangulatú pincéjével a kisebb, nyugalmasabb környezetet igénylő előadások, beszélgetések helyszíne. Az épületet a Les Halles tetőzetén keresztül lehet megközelíteni, ahol egy – az utcáról nem látható – szürreális tetőkerten kell keresztülmenniük a résztvevőknek. Talán ez a rövid leírás is érezteti, hogy nem szokásos konferenciahelyszínről van szó.

A konferenciák arra alkalmas előadásaiból a Springer könyvsorozatot jelentet meg[4], az egyes kötetek címei a CPDP aktuális kiadásának címét viselik. A konferencia pedig szakmai rendezvényből „multistakeholder platform-má" vált; ez a folyamat nem volt vitáktól mentes: maradjon-e afféle „elit" konferencia, vagy nyisson a technológiai, üzleti, kormányzati, rendészeti és egyéb, adatvédelmi témákban érintett résztvevők felé. A nyitás megtörtént, a CPDP résztvevőinek száma pedig meghaladja az ezer főt, úgyhogy felvetődött a létszám limitálásának szükségessége, mind logisztikai, mind minőségbiztosítási okokból.

A konferencia megrendezése egész éves munkát és személyzetet igényel. A CPDP irányító személyei és testületei: az alapító igazgató (Paul De Hert), az ügyvezető igazgató és a programigazgató; a hattagú nemzetközi programbizottság, a még négytagú kibővített programbizottság; négy panelkoordinátor, valamint a 22 tagú nemzetközi tudományos bizottság, amely a konferencia általános irányvonalát van hivatva megszabni és véleményezni. A háttérintézmények között a legfontosabb szerepe a Brüsszeli Szabadegyetemnek és a Fraunhofer Intézetnek van.

A helyszín mellett a CPDP konferenciáknak más jellegzetességei is vannak. Első helyen kell említeni a fiatal pályakezdő kutatók, szakemberek támogatását. Ez nemcsak a részvételi díj elengedését és egyéb pénzügyi támogatást jelent, hanem külön a fiatal kutatók bemutatkozásának szentelt szekciók, az úgynevezett *academic sessions* rendezését is. Az ilyen szekciókban való részvételre előzetesen megírt tanulmányok benyújtásával lehet jelentkezni, amit gondos válogatás és lektorálás követ, majd pedig a szekciók során minden lektor élőben is értékeli az elhangzott prezentációkat, a doktori védéseknél kollegiálisabb stílusban; ezt nyilvános vita követi.

A CPDP konferenciákon számos díj kiosztása is megtörténik, ilyen például az Electronic Privacy Information Center (EPIC) által felajánlott és egy nagy tekintélyű zsűri által évente odaítélt International Champion of Freedom Award[5], vagy a legjobb interdiszcip-

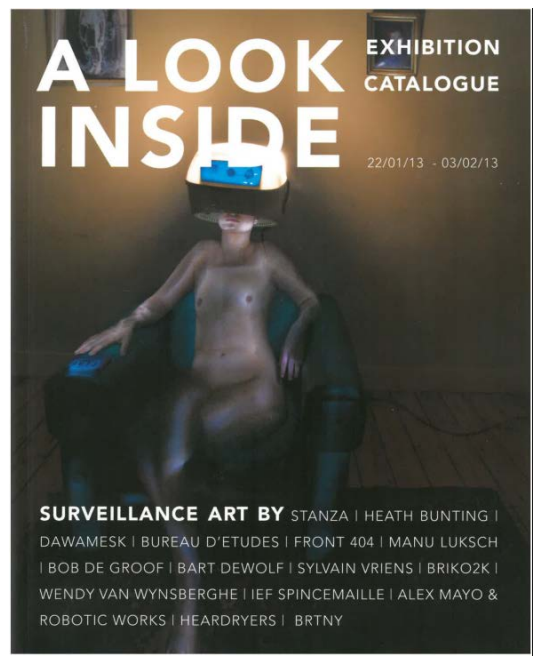
[4] A „Law, Governance and Technology" sorozat részeként.

[5] A díjat 2009-ben Prof. Stefano Rodota (Olaszország), 2010-ben Hon. Michael Kirby (Ausztrália), 2011-ben MEP Sophie In't Veld (Hollandia), 2012-ben Jennifer Stoddart (Kanada), 2013-ban Max Schrems (Ausztria), 2014-ben Jan Philipp Albrecht (Németország), 2015-ben Peter Hustinx (EU), 2016-ban Viviane Reding (EU) kapta.

lináris tanulmány szerzőinek szánt díj, amely egyúttal a Springer által kiadott könyvben való megjelenést is magában foglalja.

Innovatív témák első vagy elsők közötti nyilvános vitája is gyakran a CPDP paneleken hangzik el, például a drónok és a magánszféra viszonya, a post-mortem privacy és emberi méltóság jogi kezelése, vagy az algoritmikus döntéshozatal és az egyéni autonómia kérdései. Vannak zártkörű szekciók is, hagyományosan ilyen a filozófiai olvasókör, amelyre csak előzetes regisztrációval (és a kiadott művek előzetes áttanulmányozásával) lehet bejutni, de ilyen volt például 2015-ben az IRISS[6] nemzetközi kutatási projekt empirikus vizsgálatának eredményeiről rendezett kerekasztal-beszélgetés is, nevezetesen arról, hogy a kamerás megfigyeléssel gyűjtött adatok létéről és mibenlétéről az érintett polgárok hogyan szerezhetnek (vagy nem szerezhetnek) tudomást: erre a fűtött hangulatú vitára az adatvédelmi hatóságok képviselői kaptak meghívást, akik nem szerettek volna a nyilvánosság előtt beszélni az esetleges hiányosságokról e téren.

A CPDP konferenciák egész sor csatlakozó rendezvényt kínálnak; ilyenkor fontos politikai vonatkozású bejelentések is elhangoznak, mint 2012-ben a lengyel állandó EU-képviselet épületében rendezett fogadáson az új egységes európai adatvédelmi rendelet tervezetének benyújtása. Fontosak a nyilvános viták is, mint például 2015-ben a robotok magánéletéről, a sci-fi-ről és a jog eszköztáráról folytatott beszélgetés, amelyekre nemcsak regisztrált résztvevők jöhetnek el, hasonlóképpen a könyvbemutatókra, mint például 2013-ban David Lyon Zygmunt Baumannal folytatott beszélgetéseinek kiadott változata, a *Liquid Surveillance* című könyv bemutatása kapcsán szervezett beszélgetésre (Bauman és Lyon 2013).[7] Állandó kísérőprogramja a CPDP konferenciáknak a Surveillance Art[8] kiállítás, ahol a nemzetközi alkotógárda a legkülönfélébb hagyományos és innovatív műfajokban állít ki műveket, installációkat, többségükben a közönség interaktív bevonásával, a brüsszeli De Markten kiállítótereiben (1. ábra).



1. ábra:
A 2013-as Surveillance Art kiállítás katalógusa

[6] Increasing Resilience in Surveillance Societies, http://www.irissproject.eu Az empirikus vizsgálat eredményeiről könyv is megjelent (Norris et al. 2017).

[7] Az eseményen levetítették a Living in Surveillance Societies (LiSS) többéves nemzetközi kutatási projekt 2012-es budapesti rendezvénysorozatán készült kisfilmet is, lásd
https://www.youtube.com/watch?v=wLn7n6zc308

[8] A Surveillance Art olyan művészeti irányzat, amelynek központi tárgya a megfigyelés és a megfigyeltség.

Ugyancsak hagyományos eleme a rendezvénysorozatnak a konferencia helyszínén rendezett pecha kucha[9] is, valamint a filmvetítések: 2016-ban a két főszereplő, Jan Philipp Albrecht és Viviane Reding, valamint a rendező David Bernet személyes részvételével mutatták be a többszörös díjnyertes „Democracy – Im Rausch der Daten" című dokumentumfilmet „a pincében" (La Cave).[10] 2016-ban pedig az International Association of Privacy Professionals (IAPP) kiállítást rendezett Orwell *1984* című könyvének kiadásaiból „Privacy in Art – George Orwell 1984" címmel. Az IAPP az előző évben felvásárolta a könyv elérhető kiadásainak egy-egy példányát és Orwell kézirathagyatékának darabjait, és a négyszáz darabos gyűjtemény jelentős részét a konferencia időtartama alatt kiállította a Maison des Arts halljában. A könyvborítók sora a megfigyelés felfogásának és grafikai ábrázolásának elgondolkodtató változásait, sokszínűségét tükrözte a mű első, 1949-es kiadásától napjainkig.

A CPDP-nek előrendezvénye is van, a brüsszeli Saint Louis Egyetemen rendezett Privacy Camp[11], amely a magánélet és a személyes autonómia értékeiért küzdő civil szervezetek és aktivisták fóruma. Az itt elhangzó prezentációk és viták némelyike érdekességében felülmúlja a „hivatalos" konferencia-előadásokét.

Meg kell említeni „a faluban" megjelenő kiállítókat, akik részben cégeket, könyvkiadókat, részben nemzetközi szervezeteket, részben pedig kutatási projekteket és civil szervezeteket képviselnek. A kiállítók a konferencia teljes időtartama alatt az érdeklődők rendelkezésére állnak, időként élő demonstrációkkal, mint például egyes anonimizáló technológiák tesztelésével. Itt is látható tehát az üzleti szektor részvétele – mégis, a konferencia szellemisége szilárdan őrzi a magánélet fontosságát alapértéknek tekintő hozzáállást. Éppen ezért az üzleti résztvevők által szervezett előadások, panelbeszélgetések nem válhatnak „marketing bullshit" jelzővel illethető eseménnyé, erről a szervezők, illetve a tudományos bizottság tagjai igyekeznek gondoskodni. Hasonlóképpen limitált az üzleti és más szervezetek által felkínált támogatások aránya: ez nem haladhatja meg a konferencia összköltségvetésének 49 százalékát, illetve az egyedi támogatások maximális összege az összköltségvetés 7,5 százalékát. Ezzel együtt természetesen vannak platina és premier fokozatú támogatók, eseményszponzorok és médiapartnerek – érdemes végigtekinteni a támogatók során és a támogatások kategóriáján (2. ábra): látható, hogy a személyesadat-kereskedelemben és -felhasználásban alapvetően érdekelt multinacionális vállalatok is ott akarnak lenni a támogatók között, de a legérdekesebb az „erkölcsi támogatók" kategóriája, azoké, akik nyilvánvalóan nem pénzzel, hanem más módon támogatják a konferenciát.

2. ábra: Támogatói kategóriák és szponzorok, CPDP 2014

A CPDP olyan konferencia, ahol „mindenki ott van"; sokan a kapcsolattartás vagy kapcsolatteremtés kedvéért, avagy konkrét üzletkötés céljából vagy projekttervek megbeszéléséért jönnek el. A konferencia stílusa informális. Vannak ugyan nyakkendős, kiskosztümös panelek, de a többség öltözetében és beszédstílusában is laza és lényegretörő, ezzel is megőrizve a rendezvény egyetemi gyökereit. A multinacionális cégek elfogalt és elegáns fogadásokhoz szokott képviselői időnként panaszkodnak is, hogy ezért a részvételi díjért még sorban is kell állniuk az ebédosztásnál (de éppen az ő részvételi díjuk és szponzorálásuk teszi lehetővé a fiatalok támogatását). A CPDP-n mindenkihez oda lehet menni és ismerkedni, feltéve, hogy az illető ráér és nem foglalt másokkal folytatott beszélgetésekben. Kezdő kutatók közös ismerős bemutatása nélkül is megismerkedhetnek híres professzorokkal, aktivisták üzleti vezetőkkel és politikusokkal (akikkel egyébként talán más környezetben nem is állnának szóba, és vice versa...), vagyis olyanok is meghallgatják egymás érveit, akik amúgy nem keresik egymás társaságát, vagy egyenesen ellenfélnek tekintik egymást.

A konferencia januárban, az adatvédelem világnapjának hetén, három napon át reggeltől késő estig, egy nap előrendezvénnyel (Privacy Camp) és néhány utóprogrammal gyakorlatilag egy teljes hetet elfoglal, bár sokan csak bizonyos napokra jönnek emiatt. Ráadásul az öt, néha hat párhuzamos programfolyam miatt lehetetlen mindent meghallgatni, megnézni; szerencsére az informális stílushoz hozzátartozik a szabad mozgás is: senki nem sértődik meg azon, ha az előadása közben egyesek kimennek, vagy egy kevésbé érdekesnek tartott panelt otthagyva beülnek a nézők közé. Van egy furcsa tradíció, amit az új résztvevőknek meg kell szokniuk: egy jó hangú diák, a régimódi talárokat idéző köpenyben egy hatalmas kézi csengőt vagy inkább harangot rázva, sztentori hangon bekiabálja az idő múlását öt perccel a program vége előtt és az idő lejártakor. Ezzel lehet megelőzni a programok csúszását, illetve szinkronitásuk (ami a hallgatóság navigálásának feltétele) szétesését.

A felvezető plenáris előadáson kívül az összes többi előadás voltaképpen panelbeszélgetés formájában zajlik. Ez nemcsak arra jó, hogy minél több előadót lehessen színpadra küldeni, hanem arra is, hogy az előadók ne beszéljenek el egymás mellett, hanem rövid, vitaindító téziseket, provokatív állításokat fogalmazzanak meg, és vegyék figyelembe az előadótársak által mondottakat. Egy ekkora rendezvényen természetesen előfordul néhány gyengébb panel és előadó is, főként amiatt, hogy az új előadók nem mindig ismerik az itt megszokott elvárásokat, előismereteket, de az általános színvonal jó, egy-egy kimagasló panellel. Sok múlik a panel elnökén és főleg moderátorán. Ők javasolnak már előzetesen témát a szervezőknek, és ha elfogadják, ők szervezik meg, gyakran fél-háromnegyed évvel korábban a panel résztvevőit, egyeztetik a résztvevők fellépésének kereteit, és bonyolítják le a panelbeszélgetést.

Vannak állandó, évente ismétlődő panelek is: ilyen például az adatvédelmi biztosok és hatóságok tevékenységének, kapcsolatainak valamely aktuális aspektusát tárgyaló panel,

[9] A pecha kucha (japánul körülbelül bla-bla) eredetileg építészek által kitalált műfaj, amely az ötletek túlbeszélését megelőzendő, szigorúan kötött formában, 20 vetített kép egyenként 20 másodperces színpadi prezentálásával, személyenként 6 perc 40 másodperces keretben, moderátor (valamint kivetített stopper és automatikus képváltás) segítségével nyújt szórakoztató intellektuális élményt a nézőknek.

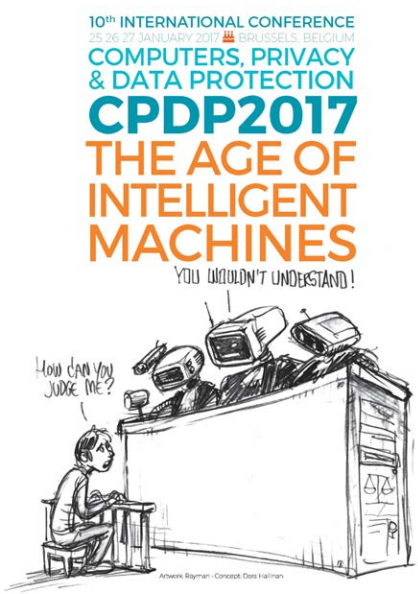
[10] A Democracy c. filmet 2016-ban Budapesten az évenkénti Verzió Nemzetközi Emberi Jogi Dokumentumfilm Fesztiválon is bemutatták.

[11] https://privacycamp.eu/

hat éve ugyanazon elnök és moderátor szervezésében és bonyolításában, de a panel résztvevői az aktuális téma függvényében változnak.[12] 2015-ben hunyt el a CPDP konferenciáknak, de egyúttal az egész privacy-közösségnek mindenki által ismert fenegyereke, Caspar Bowden, aki pótolhatatlan szerepet játszott a magánélet-sértő intézkedések feltárásában, megkérdőjelezésében, a politikai valótlanságok leleplezésében, a privátszférát erősítő technológiák elterjesztésében; emlékét a 2016. évi CPDP nyitónapján sajátos visszaemlékezésekkel és a róla készült kisfilmmel tisztelte meg a konferencia közönsége[13] – legalább is azok, akik valóban partnert vagy harcostársat láttak benne. Ettől kezdve új állandó panel, a Caspar Bowden emlékpanel is része a CPDP programjának.

Magyar előadók, résztvevők is vannak a CPDP konferenciákon, ha nem is sokan – az elmúlt években például Jóri András, a hivatalától megfosztott adatvédelmi biztos, aki az adatvédelmi biztosok függetlenségéről szóló panelben vett részt, Hidvégi Fanny, az AccessNow civil szervezet képviseletében, vagy a fiatal kutatók számára rendezett tudományos panelek magyar résztvevői.

CPDP 2017



Az idei Computers, Privacy and Data Protection konferencia címe és vezérgondolata „A gondolkodó gépek korszaka" volt (3. ábra). Számos panel és előadás foglalkozott az automatikus döntéshozatal, az algoritmikus kormányzás, a mesterséges intelligencia és a jogi szabályozás, vagy az algoritmikus diszkrimináció problémakörével, ami a programbizottság és a panelbeszélgetések szervezői közötti szakmai együttműködés eredménye. Ugyancsak népszerű téma volt az európai adatvédelmi reform; az EU új általános adatvédelmi rendeletének, a GDPR-nek az értelmezése, végrehajtása – és természetesen vannak visszatérő témák, mint az Internet of Things adatvédelmi vonatkozásai, az EU-USA viszony, az egészségügyi személyes adatok kezelése, vagy az adatvédelmi hatóságok lépéstartása a jogi és technológiai fejleményekkel.

3. ábra: A 76 oldalas programfüzet címlapja

[12] A panel témája 2016-ban az adatvédelmi hatóságok és az információs technológia viszonya volt; a szervezők a panelbeszélgetés kedvéért előzetesen az EU összes nemzeti és tagállami hatóságát megkeresték és empirikus vizsgálatot végeztek körükben, amelynek eredményei alapján strukturálták a beszélgetést. (A panelbeszélgetés videofelvétele – a többi panelbeszélgetéshez hasonlóan – megnézhető a https://www.youtube.com/watch?v=nwiXB0w5Mss címen.)

[13] https://www.youtube.com/watch?v=d1WkRGjAFO4

A főprogram három napja alatt 78 panelben 383 előadó, vitavezető, moderátor szerepelt. A fő helyszín most is a Les Halles de Scharbeek volt, de a Maison des Art ezúttal egy más rendezvény miatt foglalt volt, ezért a negyedik és ötödik programfolyam egy külső helyszínen, egy sajátos műemlék épületben, a Maison Autrique-ben zajlott, amelynek megközelítése 6-8 perces gyaloglást igényelt. Az épület ugyan igen érdekes[14], de konferenciák tartására csak korlátozottan alkalmas, és az oda-vissza gyaloglás is megnehezítette az idősávok betartását. Ezzel együtt néhány panel zsúfolásig (sőt, a később érkezők kényszerű elküldéséig) megtöltötte a ház – egyébként kis méretű – tereit; ráadásul arra is vigyázni kellett, hogy a földre tett és esetleg felrúgott kávés és üdítős poharak ne okozzanak kárt a szőnyegekben és az egyedi falfestésben.

Ebből a kínálatból természetszerűleg csak néhány előadást, panelt, illetve csatlakozó programot tudunk itt kiemelni. Először is a konferencia előrendezvényét, a Privacy Camp-et kell megemlítenünk: a legérdekesebb panelbeszélgetés és vita itt a közösségi megosztott szolgáltatásokról (Uber, Airbnb és társai) folyt. E szolgáltatásoknak általában csak az előnyös tulajdonságairól, gyorsaságáról és olcsóságáról hallunk, itt viszont a munkaerő etikátlan alkalmazásáról, a felhasználók személyes adatainak eladásáról is – de ami ennél fontosabb: arról, hogy miként lehetne egy fair online gazdaságot kiépíteni, más üzleti modell, a kooperatizmus alapján. Ennek vonzó technológiai megoldása lehet a blokklánc-alapú hálózat, amit eddig csak a Bitcoin-nal kapcsolatban ismert a felhasználók többsége. A vitát Seda Gürses, a Leuven-i Egyetem ismert informatikus kutatója vezette, a résztvevők: Ela Kagel, a „Supermarkt – platform for digital culture and alternative economies" szervezet képviselője, Shermin Voshmgir, a bécsi BlockchainHub-tól, és Tim Jordan a Sussex-i Egyetemről.[15] Kifejezetten szórakozató – ugyanakkor meghökkentő – volt Finn Myrstad, a Norvég Fogyasztóvédelmi Tanács képviselőjének prezentációja, aki a két divatos, beszélő „internet-baba", Cayla és I-Que képességeit és rejtett tulajdonságait illusztrálta, nevezetesen azt, hogy a baba a szülők tudta nélkül befolyásolja a gyerek ízlését, szokásait, tevékenységeit, sőt még a szülők beszélgetéseit is lehallgatja és egy amerikai céghez továbbítja.[16]

Emlékezetes élményt nyújtott a CPDP hivatalos megnyitóeseménye, a konferencia előestéjén tartott nyilvános vita Belgium állandó EU-képviseletén, amely a repülőgépes utaslisták bűnmegelőzési célú felhasználásáról folyt.[17] A bűnüldözés és bűnmegelőzés európai érdekeit Christiane Höhn (Council of the EU) képviselte – kulturáltan, egy olyan közegben, ahol az általa képviselt nézetek érezhetően kisebbségben voltak –, a szabadságjogokat pedig Sophie in't Veld, Európai Parlamenti képviselő, aki vehemens hangvételéről, kérlelhetetlen vitastílusáról ismert. A harmadik résztvevő Marc Rotenberg, az Electronic Privacy Information Center (EPIC) elnöke volt, aki amerikai oldalról szólt a vitához, az általa megszokott nyugodt, választékos, de megalkuvást nem ismerő stílusban. Sophie in't Veld kritizálta azokat a politikusokat és ipari szövetségeseiket, akik újabb pénztömegeket akar-

[14] Victor Horta, a szecesszió neves építésze utolsó, még nem szecessziósnak minősített, de az „új művészet" jegyeit már magán viselő épülete, amelyet egy brüsszeli család számára tervezett.
[15] A vita felvétele megtekinthető a https://www.youtube.com/watch?v=Z9Z9ewyhI0A&t=19s címen.
[16] Lásd a *#toyfail* című videót Finn Myrstad közreműködésével,
https://www.youtube.com/watch?v=lAOj0H5c6Yc
[17] https://www.youtube.com/watch?v=i1pf1GTFLPA

nak felhasználni az EU költségvetéséből személyesadat-gyűjtési és -elemzési rendszerek kiépítésére – ahelyett, hogy a tagállamok hajlandók lennének megosztani egymással azokat a bűnüldözési és bűnmegelőzési jelentőségű személyes adataikat, amelyeket már eddig is vitatható mértékben gyűjtenek és használnak.

A konferencia első napjának illusztris panelbeszélgetése az algoritmikus döntéshozatal magánéletre gyakorolt hatásaival és perspektíváival foglalkozott.[18] A felvetett főbb kérdések: kell-e vagy lehet-e jogilag szabályozni az algoritmusokat, és ha igen, hogyan? Milyen szintű átláthatóságot követelhetünk meg az emberek életét befolyásoló döntéseket hozó algoritmusoktól, és ezt a gyakorlatban hogyan lehet megvalósítani? Hogyan egyeztethető össze egyfelől az üzleti szféra jogos igénye az üzleti titkot képviselő és versenyelőnyt nyújtó információinak megőrzésére, másfelől az érintett személyek igénye arra, hogy átlássák az életüket befolyásoló döntések logikáját? A panel moderátora Antoinette Rouvroy volt, aki az algoritmikus kormányzás filozófiai problémáit kutatja, és az Európa Tanács megbízásából nemrég megírta átfogó tanulmányát Adatok és Emberek címmel[19], amelyben egyenesen egy új társadalmi szerződés szimbolikus megkötését tartotta szükségesnek az információs társadalom közegében – azonban a beszélgetés kifutott a rendelkezésre álló időből, és így a nézőnek hiányérzete maradt a panel kényszerű befejezésekor.

Érdekes panel szólt a de-identifikálás (közismertebb nevén anonimizálás vagy pszeudonimizálás) jogi és informatikai problémáiról: a beszélgetés ütköztette a GDPR elvárásait és jogi kategóriáit a mai és jövőbeli technológiai lehetőségekkel.[20] A vitapartnerek között egy adatintenzív szolgáltató cég, a navigációs adatokat gyűjtő és felhasználó TomTom képviselője is részt vett, így a vita nemcsak elvi síkon zajlott.

A kiválasztott fiatal kutatók számára szervezett academic session-ök résztvevői korszerű és egyáltalán nem elcsépelt témákról írták tanulmányaikat, bírálóik pedig érdemben szóltak hozzá a prezentációkhoz. Martina Klausner és Sebastian J. Golla (Humboldt Egyetem) a telerehabilitáció magánszféra-védelmi aspektusairól, közelebbről az intelligens tartásjavító fűzők használatáról tartott prezentációt; tanulmányuk tizenéves páciensekkel folytatott empirikus vizsgálatot is magában foglalt.[21]

Érdekes és nyilvánvalóan önreflektív panelbeszélgetés szólt a privacy konferenciák céges támogatásáról, annak etikájáról és implikációiról. Polarizált nézetek csaptak össze a beszélgetésben: egyesek szerint a céges támogatások eleve kizárják az ilyen konferenciák függetlenségét és kompromittálják szervezőit és előadóit. Mások szerint céges szponzorok nélkül nem lehetne megfelelő színvonalon ilyen konferenciákat rendezni. A vita ugyan nem a CPDP-ről szólt, de elhangzott, hogy a CPDP milyen korlátokat szab az ilyen támogatásoknak, és hogy mire fordítja az így bejövő összeget (főképp fiatal kutatók és civil szervezetek meghívására).

Nem túl feltűnő című, de annál élénkebb vitát kiváltó panel szólt a privacy típusairól. Ennek apropója egy nemrég megjelent tanulmány volt (Koops et al. 2016), amely egységes rendszerbe foglalta a személyes magánszféra dimenzióit. A privacy-tipológiáknak, csoportosításoknak hosszú előtörténete van, de ez a tipológia minden oldalról éles kritikát

[18] https://www.youtube.com/watch?v=1lclXyLPLPg
[19] „Of Data and Men: Fundamental Rights and Freedoms in a World of Big Data" (Rouvroy 2016).
[20] https://www.youtube.com/watch?v=v5OkiBSY1_Q
[21] https://www.youtube.com/watch?v=whJdeONAuC8

váltott ki – feltehetőleg pszichológiai és nem elméleti indíttatásból.[22] Roger Clarke, az egyik korai tipológia megalkotója például külön publikációvá fejlesztette kritikai észrevételeit (Clarke 2017).

Idén is volt surveillance art kiállítás a De Markten kiállítótermeiben, *Privacytopia Binary: Search Machine by the Museum and Webcam Venus & Brbxoxo* címmel (alkotók: Addie Wagenknecht és Pablo Garcia), de ezúttal halványabb volt a kiállítás, mind kivitelezésében, mind a kiállított művek vonatkozásában a korábbi évek kiállításainál. A Webcam Venus projekt például a webkamerás pornográfia modelljeit vette rá arra, hogy szegényes környezetükben vegyék fel híres festmények modelljeinek, szépségideáljainak közismert pózait, és így mintegy elemelte a modelleket a teljes kiszolgáltatottság és megfigyeltség állapotából.

A konferencia logisztikája gördülékenyebb volt az előző évekénél (természetesen a hatalmas létszám és a fizikai keretek korlátai között), például több diák önkéntes állt rendelkezésre a ruhatárnál, és több terminálnál lehetett regisztrálni a helyszínen. Proaktívabb volt a technikai szolgáltatás: a Grande Halle színpadán beszélgetők fejmikrofonokat használhattak, az operatőrök jobban követték a közönség soraiban történő eseményeket (szavazások, hozzászólások), és a panelbeszélgetések felvételét néhány már nap múlva a YouTube-on láthatta az, aki nem volt jelen a helyszínen, vagy ismét meg akarta nézni. Ezzel együtt a CPDP egy hét állandó intenzív jelenlétet igényel (bár vannak egy-egy napra érkezők és közben lazítók is); ez nemcsak az előadások meghallgatását jelenti, hanem a beszélgetéseket, komoly szakmai és üzleti tárgyalásokat, a csatlakozó rendezvények látogatását, és természetesen a késő estébe nyúló privát programokat, amelyek között vannak elegáns üzleti vacsorák és informális sörözések is. Ez utóbbiak jelentőségét nem szabad alábecsülni és elfogadni azok véleményét, akik szerint az ilyen konferenciák látogatása csak a bulizásról és a bevásárlóturizmusról szól, mivel éppen az ilyen levezető alkalmakkor születnek a legjobb ötletek közös publikációkra vagy kutatási projektekre.

Közismert, hogy a szervezeteknek van életciklusa, jól meghatározható fázisokkal – lehetséges, hogy a rendezvénysorozatoknak is van: a CPDP mindenképpen érett fázisba jutott fennállásának tíz éve alatt. El is hangzott a Scientific Committee zárt ülésén az egyik alapító tagtól, hogy változtatni kellene a bejáratott sablonokon, és a jövőben legyenek eltérő típusú, időtartamú és műfajú panelek. Ez a javaslat egylőre kisebbségben maradt, a többség értéknek tekintette a kialakult rendszert, de nem kizárt, hogy a közeljövőben ilyen irányban fejlődik tovább a CPDP konferenciasorozat.

Irodalom

Bauman, Zygmunt and David Lyon, *Liquid Surveillance – A Conversation,* Polity Press, Cambridge, 2013.

Clarke, Roger, "An Instrumentalist's View of Koops et al.'s Typology of Privacy", http://www.rogerclarke.com/DV/PTyp-1701.html (2017).

Gutwirth, Serge, Yves Poullet, Paul De Hert, Cécile de Terwangne and Sjaak Nouwt (eds.), *Reinventing Data Protection?,* Springer Science+Business Media B.V., 2009.

[22] https://www.youtube.com/watch?v=XvdZ-9eD0tQ

Koops, Bert-Jaap, Bryce Clayton Newell, Tjerk Timan, Ivan Škorvánek, Tomislav Chokrevski and Maša Galič, A Typology of Privacy", *University of Pennsylvania Journal of International Law*, Vol. 38. (2016) No. 2., pp. 483-575.

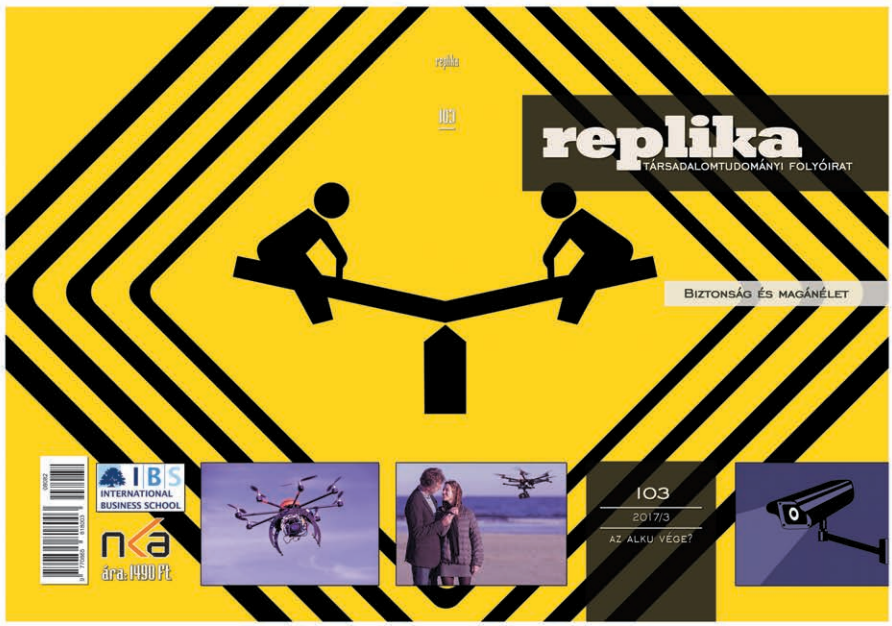
Norris, Clive, Paul De Hert, Xavier L'Hoiry, Antonella Galetta (eds.*), The unaccountable state of surveillance: Exercising access rights in Europe*, Springer International Publishing AG, Cham, 2017.

Rouvroy, Antoinette, *Of Data and Men: Fundamental Rights and Freedoms in a World of Big Data*, Report prepared for the Directorate General of Human Rights and Rule of Law, Council of Europe, Strasbourg, 2016.

Today we have unprecedented access to datasets bearing huge potential in regard to both business and research. However, beside their unquestionable utility, privacy breaches pose a significant risk to the release of these datasets (e.g., datasets originating from healthcare are good examples), thus service providers must use anonymization techniques to minimize the risk of unwanted disclosure. In this study, we focus on de-anonymization attacks, algorithms that are designed to "reverse" the anonymization process. In particular, we focus on a novel segment of these attacks that involve machine learning to improve robustness and efficiency. Furthermore, we highlight and discuss the similarity between de-anonymization and authentication: how can these algorithms, which are generally perceived as unethical, be used legitimately for security reasons under special constraints.

Keywords: anonymity, de-anonymization, machine learning, private sphere protection

CONFERENCE REPORT



Az Információs Társadalom jelen tematikus lapszámával egy időben jelenik meg a Replika folyóirat 103. száma, amelyben a két szerkesztőség együttműködésének eredményeképpen a „Biztonság és Magánélet" tematikus blokk tanulmányai olvashatók.

A Replika tematikus blokkjának tartalmából:

Székely Iván, Somody Bernadette és Szabó Máté Dániel: *Biztonság és magánélet: az alku-modell megkérdőjelezése és meghaladása. I. rész: Társadalomelméleti és szociológiai megközelítések*

Szénay Márta: *SurPRISE – rendhagyó közvélemény-kutatás a biztonságról, a megfigyelésről és a magánszféráról*

Ságvári Bence: *Diszkrimináció, átláthatóság és ellenőrizhetőség. Bevezetés az algoritmus-etikába*

Charles D. Raab: *A magánszféra mint biztonsági érték*