Dr. Pap András László *az MTA doktora,*
egyetemi tanár, Nemzeti Közszolgálati Egyetem Rendészettudományi Kar,
Eötvös Loránd Tudományegyetem Gazdálkodástudományi Kar

Biztonság és hatékonyság: a rendészeti (állam) hatalom alkotmányos és társadalmi felfogásának átalakulása a digitális társadalomban[1]

A 2011. szeptember 11-ét követően kialakult, a rendészeti eljárások jogpolitikai környezetét alapvetően átrajzoló „új világrend" sajátosságát az adja, hogy a nyugati társadalmakban a választópolgárok és a jogalkotók között egyaránt széles körben elfogadottá vált az a nézet, hogy a hagyományos bűnüldözési, nemzetbiztonsági és hírszerzési technológia, vagy éppen az államok közti hadviselésre épülő konvenciós hadijog (és például a hadifoglyok vallathatóságának szabálya) nem alkalmas az öngyilkos merénylők és a terroristaszervezetek sajátos hadviselésének kezelésére. A tragikus eseményektől (vagy a félelemtől) sokkolt társadalom hangulatváltozásait a politikai elit, a jogalkotó és a jogalkalmazó sikeresen használja fel arra, hogy olyan mértékben terjessze ki közhatalmi jogosítványait, amilyenről korábban csak álmodni mert. A „terrorizmus elleni háború" égisze alatt például elfogadtathatók olyan, a bankszférát vagy a légiutas-forgalmat lebonyolító szállítóvállalatokat érintő (ám a költségviselés és a jogkorlátozás végpontján az ügyfeleket terhelő) előírások és korlátozások, amelyek a kábítószer vagy a szervezett bűnözés elleni fellépés során is a hatóságok „régi vágyai" közé tartozhattak, de alkotmányos aggályok miatt még csak fel sem merték vetni.

Az ezredforduló talán legjelentősebb változása ugyanis a rendészeti eljárások során alkalmazott vagy elvárt hatékonysági szempontok szerepének átalakulása. A terrorizmus elleni harc különleges retorikai és pszichológiai környezetében az alapjogi és a jogpolitikai vizsgálatok többsége nem jut túl a „szabadság kontra biztonság" elméleti (és meglehetősen doktríner) vitáján. Az elemzők többsége adottnak veszi, hogy a „szabadság" és a „biztonság" zéróösszegű játszma, a „biztonság" fogalmát pedig kritika nélkül azonosítja a kormányzat vagy a szakpolitika által javasolt különböző biztonsági intézkedésekkel, azok valós hatásának és társadalmi költségeinek vizsgálata nélkül. Annak ellenére van ez így, hogy az egyes intézkedések alkotmányosságának megállapításához hagyományosan alkalmazott szüksé-

[1] Az alább közölt írás az eredetileg a Tanulmányok „A BIZTONSÁG RENDÉSZETTUDOMÁNYI DIMENZIÓI – VÁLTOZÁSOK ÉS HATÁSOK" című tudományos konferenciáról, Pécsi Határőr Tudományos Közlemények XIII. Pécs, 2012, 29-39. oldalakon „Biztonság és hatékonyság: a rendészeti (állam)hatalom alkotmányos és társadalmi felfogásának átalakulása a digitális társadalomban" címen publikált tanulmány eredeti változata.

gesség-arányosság alapjogi tesztjéhez egyébként a költségvizsgálat logikailag elengedhetetlen lenne. Az alapjog-korlátozás arányosságára vonatkozó követelmény alapján ugyanis az alapvető jog korlátozásakor a legitim cél elérése alkalmas legenyhébb eszközt kell választani, és az elérni kívánt cél fontosságának arányban kell állnia az alapjog-korlátozás súlyával.[2]
További tendencia, hogy az eredetileg kivételesnek tekintett szemlélet és eljárásrend a „terrorizmus elleni harc" után általában a „bűnözés elleni harc" valamennyi területére alkalmazható válik. Mindemellett, a bűnüldözés helyett egyre inkább a bűnmegelőzés válik hangsúlyos területté, mégpedig oly módon, hogy egyre bővül azoknak a kényszerintézkedéseknek a köre, amelyeknek a bűnelkövetés megelőzését szolgáló társadalmi ellenőrzés szolgál alapjául: a hatékonysági szempontok sajátosan lazán értelmezett szempontjai és a digitális technológia kínálta adatelemzés, adatbányászat lehetőségeinek figyelembevételével.[3]

A hatásvizsgálat az alkotmányossági kívánalmakon túlmenően alapvető jogpolitikai követelmény is. Gondoljunk csak a büntetőpolitikai vitákra: a zérótolerancia elve, illetve az újabban Magyarországon is bevezetett „három csapás"-szabály kapcsán magától értetődő, hogy egy intézkedés bevezetés-ének mérlegelésekor vizsgálni kell annak széles körben értelmezett társadalmi hatásait is.[4] Egy szigorú büntetőpolitika az igazságszolgáltatási rendszert nyilvánvalóan terhelő költségeken túlmenően további terheket is ró a társadalomra: érinti például a fogvatartottak családját (így a gyermekek szociális helyzetét), növeli a gazdaságilag inaktív lakosságot stb. Becslések szerint például Amerikában a kábítószer elleni harc 1980-ban évi 10 milliárd dollárba került, és 31 000 fős börtönlakosságot jelentett; 2005-ben a küzdelem már 35 milliárd dollárnyi költséggel és 400 000 személy fogva tartásával járt. Miközben a terrorizmus elleni védekezés céljából életbe léptetett banki adatkezelési, adatszolgáltatási kötelezettségek elképesztő költségekkel járnak, közismert tény, hogy a terrorizmus nem feltétlenül drága: az FBI például pontosan feltérképezte a szeptember 11-i merényletek költségét, 303 672 dollárban állapítva azt meg.[5] Azt is kimutatták, hogy ennek az összegnek mintegy 47%-a készpénzként jutott el a megfelelő helyekre, ráadásul kis összegekben és legális

[2] Lásd pl. 20/1990. (X. 4.) AB határozat, ABH 1990.
[3] Az új kriminálpolitikai trend és a profilalkotás kapcsolatáról lásd Borbíró Andrea: Kriminálpolitikai és bűnmegelőzés a késő-modernitásban. A veszélyességi szemlélet feltámadása: a kockázati logika, Eötvös Loránd Tudományegyetem, Állam- és Jogtudományi Kar, Budapest, 2011. 64-68. o.
[4] Lásd pl. Fábián Erika: „Három csapás" szakmai szemmel – Kerekasztal-beszélgetés a Btk. szigorításáról (http://www.jogiforum.hu/hirek/23374), valamint Borbíró Andrea: „Three Strikes and You're Out!" Magyarországon – kriminálpolitikai racionalitás vagy szimbolikus jogalkotás? Acta Facultatis Politico-Juridicae Universitatis Budapestiensis 45. 2008
[5] Gouvin, Eric: Bringing Out the Big Guns: The USA Patriot Act, Money Laundering, and the War on Terrorism, Baylor Law Review, Fall 2003. 975. o.

kereskedelemi tevékenység (például mézeladás) formájában, tehát még a legprecízebb adat bejelentési szabályok mellett sem tűnt volna fel senkinek.[6].

A „biztonság" ténye és érzete

A szakembereknek – elsősorban a kriminológusoknak – széles körű ismereteik vannak a lakosság bűnözéssel kapcsolatos attitűdjeinek egyik legfontosabbikáról, a bűnözéstől való félelemről. Ez voltaképpen két érzés, a szűkebb értelemben vett félelem és a szorongás egyfajta keveréke.[7] A „terrorizmus elleni harc" sajátossága abból is fakad, hogy a társadalom biztonságérzete nem objektíven, a bűnözésre vagy terrorizmusra vonatkozó statisztikák függvényében alakul, hanem számos szociálpszichológiai együttható – és nem utolsósorban a polgárokhoz eljutó információk – nyomán változik. A veszély pedig hálás téma. A média, ha arra nem is képes, hogy megmondja az embereknek azt, hogy mit gondoljanak, mindenképpen erősen befolyásolja, hogy miről gondolkodjanak. Egy angol felmérés kimutatta, hogy noha az elmúlt években a bűnözés mértéke csökkent, a politikai napilapok olvasóihoz képest a bulvársajtót olvasók közül majdnem kétszer annyian (43%, szemben a 26%-kal) voltak azon az álláspontón, hogy emelkedett a bűnözés.[8]

Az életünket fenyegető veszélyeket tehát nem objektív szempontok alapján mérjük fel. Amerikában 1960 óta (2001. szeptember 11-évl együtt) ugyannyi áldozatot szedett a terrorizmus, mint ahányan villámcsapástól vagy szarvasgázolás következtében haltak meg: a hivatalos adatok szerint 4000 körüli a szám. Ehhez képest az influenza és tüdőgyulladás évi 60 000, az autóbalesetek pedig 40 000 ember halálát okozzák.[9] A terrorizmus elleni, „háborúvá" emelt intézkedéssorozat sajátossága éppen abban áll, hogy a háború (hasonlóan a „bűnözés"-hez) egy nyílt végű folyamat: soha nem lesz vége, és azt sem tudhatjuk, hogy az intézkedések valójában mennyire hatékonyak. Ha nem kerül sor terrortámadásra, azt a hatékony preventív eszközrendszernek tulajdoníthatjuk, ha mégis: az éppen hogy további intézkedések és eszközök bevetését teszi indokolttá. Ráadásul, a folyamatosan fenntartott félelem fontos identitás- és közösségképző erő, ami kifejezetten erősítheti az állami rendvédelmi apparátus érdekérvényesítő képességét, illetve retorikai eszköztárát. Végső soron azt is mondhatjuk: ha a bűnözés (pontosabban, az attól való félelem) a fejünkben, az érzéseinkben, szorongásainkban létezik elsősorban, akkor tulajdonképpen helyesen jár el az állam, ha lélektani placebókkal kezel bennünket,

[6] Uo.
[7] Lásd. pl. Korinek László: Félelem a bűnözéstől, Budapest: KJK, 1995.; Korinek László: A büntetőpolitika irányelvei Magyarországon, in Jakab András, Takács Péter (szerk.): A magyar jogrendszer átalakulása, 1985/1990–2005. Gondolat Könyvkiadó, Budapest, 2007. 473-496. o.
[8] Green, David A.: Public opinion versus public judgment about crime. Correcting the 'Comedy of Errors'. British Journal of Criminology, January 2006. 138–139. o.
[9] Solove, Daniel J.: Data mining and the security-liberty debate, Univeristy of Chicago Law Review, Winter 2008

és fölösleges lenne bajlódnia az egyes biztonsági intézkedések gyakorlati hatásvizsgálatával. Noha a jog közgazdasági elemzésével foglalkozó, angol nyelvterületen 'law and economics' néven művelt, többek között a bűnmegelőzés társadalmi költségeivel is foglalkozó diszciplína módszertana és tudományos eredményei évtizedek óta ismertek; úgy tűnik, hogy életbe léptetett különböző jogkorlátozások széles társadalmi támogatottsággal bírnak, az a terrorizmus megelőzésére intézmények tényleges hatékonyságának vizsgálata nélkül is.

Tudjuk, hogy az áldozattá válástól való félelemmel kapcsolatban például a költségek felmerülhetnek az emberek egészségromlását jelentő stressz, illetve az ehhez kapcsolódó egészségügyi kiadások formájában, de azáltal is, hogy a félelem magatartás-változást okoz. Ilyen például az, ha az emberek taxival vagy kocsival mennek bűnügyileg fertőzöttnek tekintett helyekre.[10] A költségek lehetnek közvetlenek, de közvetettek is: az előbbire példának a riasztóberendezések beszerzése vagy a biztosításra fordított összegek szolgálhatnak, utóbbira az, hogy az emberek korábban elindulnak a munkahelyükről, hogy ne egyedül, sötétben érjenek haza, és nem jelentéktelen az az időmennyiség sem, amelyet a véletlenül megszólaló riasztók elhallgattatásával töltenek. Az Egyesült Államok egy-egy felnőtt polgára például naponta két percet tölt különböző zárak kinyitásával és bezárásával, és ennél valamivel többet a kulcsai keresésével – ez az idő évi 437 dollárt jelent személyenként, össztársadalmi költségként pedig 90 milliárd dollárt.[11] Egyes elemzések szerint a biztonsági zárakra, riasztókra, őrökre stb. fordított évi 160–300 milliárdos tétellel a bűnmegelőzésre fordított privát kiadások a teljes igazságszolgáltatási és rendvédelmi szervezetrendszer működtetésével vetekedő kiadást jelentenek – részben egyébként azért, mert az előbbi kiadások jelentős része össztársadalmi következményét tekintve hatástalan, például amikor olyan bűnmegelőzési technológiára költünk, amely nem csökkenti a bűnözés mértékét, csak áthelyezi.[12]

„In God we trust, the rest we monitor"[13] Adatbányászat a rendészetben

A különböző területen dolgozó rendvédelmi szervek mindig is érdekeltek voltak olyan ellenőrzési módszerek kialakításában – illetve adaptálásában –, amelyek minimalizálja az emberi tényezőt, és optimalizálják például a repülőtéri vagy közúti igazoltatások találati arányait. Az információs technológia fejlődésével a piaci

[10] Dolan, Paul – Peasgood, Tessa: Estimating the Economic and Social Costs of the Fear of Crime, British Journal of Criminology, January, 2007. 123–124. o.
[11] Anderson, David A.: The Aggregate Burden of Crime, Journal of Law & Economic 42, 1999. 2/623–624. o.
[12] Mikos, Robert A.: "Eggshell" Victims, Private precautions, and the societal benefits of shifting crime, Michigan Law Review, November 2006, 308, 309, 315, 319. o.
[13] „Istenben bízunk, mindeki mást megfigyelünk", az amerikai haditengerészeti hírszerzés nem hivatalos mottója.

szektorban jelentős fejlődésnek indult ez az üzletág. Az ügyfélprofil ugyanis kulcsfontosságú a gazdasági életben: a tömeges marketing helyét egyre inkább átveszi a reklámok személyre szabása, amelynek során például a kábeltelevízió nézőjének csatornaválasztási szokásait abból a célból elemzi ki egy program, hogy pontosan a néző (vélt) igényére és érdeklődésére szabott reklámokat tudjon sugározni; a Google kereső pedig úgy követi a felhasználó „kattintásfolyamát", hogy marketingstratgiai célú ügyfélprofilt tudjon nyújtani róla az érdeklődő piaci szereplőknek; a Google levelezőrendstere, a népszerű és ingyenes Gmail pedig automatikusan végigszkenneli a felhasználó üzeneteit, és egy szöveg elemzőprogram segítségével olyan linkeket, szöveges hirdetéseket jelenít meg, amelyek feltehetően érdeklik a felhasználót.[14]

Nem meglepő tehát, hogy az adatbányászati-profilkészítő technológia iránt egyre nagyobb a kormányzati érdeklődés a rendészeti szférában. Az alapelv szerint minél több adat birtokába kerülnek a különböző rendészeti szervek (nemzetbiztonság, bevándorlási hatóság, rendőrség, adóhatóság), annál nagyobb az esély arra, hogy megfelelő szűrő- és feldolgozóprogram segítségével olyan összefüggésekre derül fény, amelyek nemcsak a jogsértések felderítésében, de megelőzésében is fontos szerepet játszhatnak. Az információs technológia gyors fejlődése pedig beláthatatlan távlatokat nyit meg – jelentős profitot és erős piacot teremtve, illetve ígérve az IT-cégek számára.

Gondoljunk bele, egy digitalizált utas-nyilvántartási rendszer mellett, ha egy valamilyen okból korábban gyanúsnak minősített utas belépésre jelentkezik egy légitársaság termináljánál, a rendszer az összes korábbi határátkelését, a korábbi járatokon vele együtt utazó személyek adatait, a jegyvásárlással kapcsolatos információkat is megmutathatja – sőt, egyéb rendszerekkel összekapcsolva esetleg telefonbeszélgetéseit, televíziócsatorna-preferenciáit, könyvtári kölcsönzéseit, az általa látogatott honlapokat is. A nemzetbiztonsági adatbányászat jelenlegi gyakorlata arra épül, hogy az adatok − főleg a könnyen beszerezhető adatok − gyűjtése önmagában hasznos cél, és éppen a banálisnak tűnő információk vezethetnek el a terroristákhoz, hiszen a privacy a terroristák legjobb barátja: hiszen, ha tudják, hogy figyelik az internethasználatukat és a telefonbeszélgetéseket, akkor nem fognak azokon a csatornákon kommunikálni.[15] Megállapíthatjuk tehát, hogy már nem is csak a klasszikus szabadságjogainkat, hanem a magánszféra háborítatlanságához (privacy) való jogunkat is feláldozzuk a „biztonságért".

Hírszerzésre tehát kitűnő partner a privátszektor: könnyebben, nagyobb mennyiségben szerez a rendészeti szervek számára használható információt, hiszen az adatszolgáltatás nem kötelező, pusztán járulékos eleme a szolgáltatás igénybevételének. Ráadásul így, a privát szektor szereplőinek közvetítésével olyan adatok bir-

[14] Lásd Google: FAQ about Gmail, Security & Privacy.
[15] Lásd például Posner, Richard A.: Privacy, surveillance, and law, Univeristy of Chicago Law Review, Winter 2008.

tokába is juthatnak a nyomozóhatóságok vagy a nemzet-biztonsági szervek, amelyeket bírósági engedély nélkül akár meg sem szerezhetnének, így viszont az állampolgárok öntudatlanul ugyan, ám önkéntesen rendelkezésre bocsátják azokat. A hatóságok ilyen jellegű érdeklődésének ugyanis az a sajátossága, hogy az adatbázisokat sok esetben nem legális csatornákon keresztül – bírósági engedély vagy hivatalos felszólítás alapján – szerzik meg; a potenciális adatforrásként azonosított és megkörnyékezett cégek ugyanis nincsenek abban a jogi és üzleti helyzetben, hogy ellenálljanak a hatóságok kérésének. A rendészeti szervek gyakran élnek az információs aszimmetria eszközével is: gyakran előfordul, hogy minden jogalap nélkül emlegetnek együttműködési, ügyfelekre vonatkozó adatszolgáltatási kötelezettséget, kihasználva, hogy a cégek számára kevés az anyagi és erkölcsi incentíva arra, hogy szakembert foglalkoztassanak a jogi háttér feltérképezésére, esetleg egy formális eljárás megindítására. Nagyon sok esetben mindez nemcsak a jog, de a politikai nyilvánosság ellenőrzésén kívül is zajlik. Az érvek mindig ugyanazok: fontos a titkosság, hogy ne dekonspirálódjon a hírszerzés, és ráadásul egy privát vállalat többet veszíthet, ha ellenáll. A lényeg: a hatóságok az ügyfelekre vonatkozó adatok sokaságát szerzik meg a privát szektortól – hol a jogi szabályozás hiányára, máskor a cégvezetők hiúságára vagy éppen hazafiságára építve, esetleg a közvetlen zsarolás eszközeivel.[16]

A technologizált hatékonyság mítosza

Úgy tűnik, hogy a biometrikus adatrögzítés és az összekapcsolható adatbázisok mezmerizáló lehetőségei elkápráztatják a politikai döntéshozókat – és a közvéleményt is.[17] Kevesen hallják meg ugyanis azokat a hangokat, amelyek a rendészeti célra igénybe vett információs technológia kockázataira hívják fel a figyelmet. Kevés szó esik például a technológia hiányosságairól: a biometrikus adatok felismerése során sok a hamis pozitív és a hamis negatív; nem világos, hogy ki viseli a felelősséget a rendszer meghibásodásáért; nem ismert az IT-rendszerek teherbírása és időtállósága; gyakori az adatokkal való visszaélés, például a „személyiséglopás" ('identity theft'), nehezen ítélhető meg a hálózatok biztonsága, a rendszerek összekapcsolásának veszélye stb. Amerikában egy 2004-es jelentés szerint 42 szövetségi szerv összesen 122 adatbányászati rendszert alkalmazott; ebből 36-ot a privát szféra adatszolgáltatása alapján működtetett. A rendszerek közül 46 volt átjárható egyéb szövetségi szervek számára; ebből 14 terroristák felkutatását szolgálta, 15 pedig egyéb bűnüldözési céllal működött. Ami a számokat illeti: 2008-ban például az ujjnyomatokat tartalmazó Automated Fingerprint Identification Service (AFIS)

[16] Lásd Michaels, Jon D.: All the resident spies: private-public intelligence partnerships in the war on terror, California Law Review 90, August 2008. 927–929. o.
[17] Bővebben lásd Lodge, Juliet: Trends in Biometrics, Directorate-General Internal Policies, Policy Department C. Citizens Rights and Constitutional Affairs. Briefing Paper, December 4, 2006

51 millió adatot tartalmazott,[18] a társadalombiztosítási rendszer (Social Security Administration) pedig 441 millió személy adatait tárolta.[19] Egy valamivel korábbi (2006-os) vizsgálat szerint azonban például az utóbbi rendszerben szereplő tételek 4,1%-a (7,8 millió tételt) hibás volt a név, születési idő vagy az állampolgárság tekintetében.[20] Az ok sokszor igen egyszerű: sokan vannak, akiket ugyanúgy hívnak, illetve, és az emberek például családjogi okokból meg is változtathatják a nevüket: 2010-ben például több mint 2 millió házasságot kötöttek, és 872,000-en váltak el. Olyan is előfordul, hogy egy embernek több (állandó, ideiglenes stb.) lakcíme is van, és Amerikában 2010-ben 35 millióan (a lakosság 11,6%-a) változtatott lakhelyet.[21] Mennyire lehet tehát hatékony egy ilyen rendszer? Egy 2007-es felmérés szerint a piacvezető marketingcégek esetében 2,24%-ban, illetve 2,15%-ban jeleznek vissza a célzott, illetve névre szólóan postázott hirdetésekre:[22] mindössze ilyen kis arányban a sokmillió potenciális ügyfél közül, akik – ellenétben a terroristákkal – nem rejtőzködnek, könnyen elérhetők. Ráadásul egy adatbányászati rendszer hatékony működtetéséhez sok ismert eset (a kereskedelmi marketing esetén: sok ismert ügyfél) kellene; szerencsére a terrorizmus esetében erről sem beszélhetünk.

Jeff Jonas, az IBM vezető kutatója szerint az adatbányászat technikailag nem hatékony a terrorizmus elleni harcban,[23] ugyanis nem csak több, hanem több *hasznos* információra lenne szükség. A terrorristavadászat egyébként is olyan, mint tűt keresni a szénakazalban, és a sok-sok adat talán csak a széna mennyiségét növeli. A telefonbeszélgetések formáját, időtartamát, helyét vizsgáló programok eredményeit például több száz, ily módon más tevékenységtől elvont FBI-ügynök vizsgálja – egyelőre igencsak kétséges eredménnyel.[24]

Az eredetileg piaci, kereskedelmi célra gyűjtött adatok rendészeti felhasználhatóságáról sem részletes vizsgálatok, sem viták nem folynak. Amikor egy mobilszolgáltató vagy más piaci szereplő nyilvántartást vezet az ügyfélről, és rögzít valamilyen adatot, a saját szempontjaira figyelemmel teszi azt, és egyáltalán nem biztos, hogy az adatot rendészeti célokra megfelelő lesz. Például egy, az ügyféllel telefonon vagy e-mailen kapcsolatot tartó cég számára nem jelent gondot, ha a rendszerben például egy elírás miatt hibásan szerepel az illető neve vagy személyi

[18] Cate, Fred H.: Government data mining: the need for a legal framework, Harvard Civil Rights-Civil Liberties Law Review 43, Summer 2008. 443. o.
[19] Uo. 439. o.
[20] Uo. 469. o.
[21] Forrás: U.S. Census Bureau.
[22] Uo. 473. o.
[23] Uo. 476. o.
[24] Kreykes, Bryan D.: Data mining and counter-terrorism: the use of telephone records as an investigatory tool in the „war on terror", A Journal for Law and Policy for the Information Society, Summer, 2008. 449-450. o.

száma; viszont súlyos következményei lehetnek azonban, ha mindez egy nemzetbiztonsági eljárás során jelentkezik.

New Yorkban a hatóságok elég hosszú időn keresztül minden ok nélkül igazoltathattak a napi négy-ötmillió utast szállító metróhálózat területén.[25] Az egyenruhások látványának nyilván van visszatartó ereje, de kérdés, hogy mekkora: arányos, hasznos-e az intézkedés? A napi 1,8 millió amerikai légiutas alapul véve,[26] ha csak 1%-uk is hibásan, ok nélkül szerepel a repülési tiltólistán vagy a kellemetlen, zaklató biztonsági intézkedéseket jelentő gyanúsítotti listán, az napi 18 ezer utast jelent; ez vajon nem túl magas ár a biztonsági rendszerért? Összehasonlításul: egy amerikai felmérés szerint a biztosítótársaságok és a bankok ügyfélminősítésének 25%-ában van olyan hiba, amelynek alapján végül (az ügyfélnek és a biztosítótársaságnak egyaránt kárt okozva) elutasítják a hitelkérelmet.[27] Talán nem is meglepő tehát, hogy amikor a Columbia Broadcasting System (CBS) 2006-ban megszerezte az 540 oldalas, 44 000 nevet tartalmazó repülési tilalmi ('no fly') listát, valamint a 75.000 nevet tartalmazó gyanúsítotti listát, az újságírók megállapították, hogy az hemzseg a hibáktól, illetve számos halott vagy éppen életfogytig tartó szabadságvesztés-büntetését töltő elítélt szerepel rajta.

Michael Chertoff amerikai belbiztonsági miniszterként azt nyilatkozta, hogy a nagy légitársaságok napi 9.000 téves találatot regisztrálnak a terroristagyanús személyeket tartalmazó listákon; nemegyszer az egyik legismertebb politikus, Edward Kennedy szenátor is áldozatul esett. Gyakran a szeptember 11-i terrortámadás miatt rendszeresített légimarsallok sem juthattak fel a gépekre, de a Nobel-békedíjas Nelson Mandela is szerepelt már ilyen listán. Ennek ellenére a 900 000 nevet tartalmazó amerikai lista folyamatosan bővül, nagyjából havi 20 000 névvel. (Összehasonlításképpen: 2001 előtt mindössze 16 név szerepelt a listán.)[28] Ráadásul, az amerikai kormány közlése szerint számos azonosított terrorista neve nem is szerepel a listán, mert az ő adataikat titkosan kezelik.

A digitális információs technológia emellett korántsem annyira megbízható, mint gondolnánk. A személyiséglopás pénzügyi (és érzelmi) költségeiről egyre többet olvashatunk. 2006-ban Amerikában a digitális személyiséglopások kivizsgálásra létrehozott Identity Theft Data Clearinghouse 246 035 beadványt kapott, és az összesen 1,6 millió panasszal a legnagyobb forgalmú fogyasztóvédelmi panaszhivatallá vált.[29] Például, a számítógépes kém-szoftverek, az úgynevezett spyware-ek ellen

[25] Solove, Daniel J.: Data mining and the security-liberty debate, Univeristy of Chicago Law Review, Winter 2008, 347-348. o.
[26] Uo. 353. o.
[27] Slobogin, Christopher: Government data mining and the fourth amendment, Univeristy of Chicago Law Review (Symposium: Surveillance), 2008. Winter, 324. o.
[28] Fisher, James: What price does society have to pay for security? A look at the aviation watch lists, Willamette Law Review, Spring 2008. 608. o.
[29] Cradduck, Lucy – Mccullagh, Adrian: Identifying the identity thief: Is it time for a (smart) Australia card? International Journal of Law and Information Technology, Summer 2008. 138. o.

szinte semmiféle védelme nincs a felhasználónak: ellophatják a banki kódjait, személyes adatait (így a gépben tárolt személyiigazolvány-számát, bankszámlaszámát); segítségével megcsapolhatók a bankszámlái, hamis leveleket küldhetnek a nevében stb.. Az Egyesült Államokban csak az egészségügy területén több mint félmillió olyan esetet regisztráltak, amikor valaki egy másik ember adatai kapott egészségügyi ellátást.[30] Nemcsak az fordul elő, hogy százezer dolláros kezelésekről kapnak emberek számlát, vagy hogy valaki, aki évek óta nem szült, egyszer csak értesítést kap arról, hogy drogpozitív újszülöttet hozott világra,[31] de akár emberéletekbe is kerülhetnek az eltérő vércsoportról vagy másokon elvégzett műtétekről szóló hamis, illetve meghamisított adatok.

Amellett, hogy az infokommunikációs területtel szoros kapcsolatban álló biometrikus technológiai piac Amerikában dinamikus fejlődést mutat,[32] sok kérdés merül fel az biometrikus megoldásokkal kapcsolatban. 2002-ben Tsutomu Matsumoto, a Yokohama Egyetem matematikusa például sikeresen bolonddá tett egy ujjnyomatolvasót egy gumicukorból készült hamis ujjal, a West Virginia University Biomedical Signal Analyis laboratóriumának kutatói pedig 40–94%-os eredményességgel ismételték meg ugyanezt gyurma, illetve halott emberek ujjának felhasználásával készült hamisítványokkal.[33] Kritikusok arra is felhívják a figyelmet, hogy a biometrikus adatokból a személyazonosság megállapításán túl egyéb következtetések is levonhatóak: az írisz-retina vizsgálatból például a magas vérnyomás, terhesség, AIDS; az ujjnyomatból pedig a Down-kór és a mellrák is kimutatható.[34]

Azt, hogy a technológiai fejlődés és hatékonyság nem feltétlenül jár kéz a kézben, jól mutatja a digitalizált egészségügy példája. Noha a RAND Intézet 80 milliárd dolláros évi megtakarítást jelzett előre Amerikában egy komplex egészségügyi rendszer bevezetésével, amelyen például interneten keresztül bonyolított orvosi konzultációt is lehetővé tesz. A bevezetést követően kiderült, hogy a megváltozott környezet következtében változás következett be az orvosok viselkedésében: megnőtt a viziteket követően elrendelt – további költségeket jelentő – vizsgálatok száma: például a korszerű, drága vizsgálatok (MRI, CT) esetében 70%-os a növekedés volt tapasztalható.[35]

Biztonság vagy privacy: a megfigyelés társadalma

A jelenkor rendészete tehát szorosan összefonódik a digitális és infokommunikációs technológiai ipar fejlődésével és a szférában aktív vállalatok szerepvállalá-

[30] Healthcare Registration: Medical identity theft, Healthcare Registration 17, No. 9, June 2008
[31] Uo.
[32] Thiessen, Patrick R.: The real ID Act and biometric technology: a nightmare for citizens and the states that have to implement it. Journal on Telecommunications and High Technology Law, Spring 2008, 494.
[33] Uo. 116. lj.
[34] Fisher, James: What price does society have to pay for security? A look at the aviation watch lists, Willamette Law Review, Spring 2008. 581-582. o.
[35] Lásd pl. Lohr, Steve: Digital records may not cut health costs, study cautions, The New York Times, March 5, 2012

sával. A személyes szabadság korlátozása kapcsán felmerülő klasszikus alapjogi kérdések mellett új elemként jelenik meg a privacy, a magánélet határainak átalakulását érintő problematika. Nemcsak a rendészetben – bár ott is –, hanem a fogyasztói társadalom szinte minden szegmensében jelen van, és áttekinthetetlenné válik az a folyamat, amely a polgárok személyes adatainak, szokásainak felhasználásához kapcsolódik. A mai kor társadalma „felügyelt világ": a „surveillance", a megfigyelésen alapuló irányítás társadalma, ahol minden infokommunikációs eszköz magában hordja a megfigyelési célú felhasználás lehetőségét. A társadalomtudományban meg is jelent egy új, a politikatudomány, a jog, az informatika, a szociológia és a filozófia megközelítéseit ötvöző diszciplína (egyesek szerint paradigma), a „surveillance studies", amely világunk valamennyi jelenségét a felügyelet és társadalmi irányítás prizmáján át vizsgálja. Az infokommunikációs társadalom esetében a surveillance már nem elsősorban olyasmit jelent, mint a 18 században Jeremy Bentham által felvázolt Panopticon-börtön, ahol őrök – vagy legalábbis potenciálisan jelen lévő őrök – figyelnek meg bennünket a fizikai valónkban, hanem a rólunk mesélő adatok összesítése és elemzése elvezet a „dataveillance"-hez, az adatok megfigyelése által megvalósuló társadalmi ellenőrzéshez. Ráadásul, a megfigyelési potenciált hordozó rendszereket adott esetben mi magunk üzemeltetjük – például a több mint egymilliárd felhasználó részvételével működő közösségi oldalak formájában –, így a surveillance „co-veillance"-é, közösen megvalósított ellenőrzéssé válik.

A surveillance studies[36] alapítójának tekinthető David Lyon már a kilencvenes évek első felében megjelentetett egy könyvet „The Electoronic Eye – The Rise of Surveillance Society"[37]címmel, amelyben surveillance alatt minden olyan személyes adatgyűjtést értett – függetlenül attól, hogy az érintett személy beazonosítására alkalmas-e – amely azután alkalmas a személy befolyásolására vagy irányítására. A megfigyelés társadalma – ahol mindenki potenciális terrorista vagy bűnelkövető – mint jelenség azonban igazából csak 2001. szeptember 11-e után bontakozott ki: a kötelező személyi igazolványok bevezetésével, a zártláncú térfigyelőrendszerek és a vezeték nélküli interneten alapuló lehallgatási technológiák elterjedésével; illetve a félelem, az ellenőrzés, a gyanú és a rejtőzködés hívószavainak megjelenésével. A modernkori terrorizmus ugyanis újfajta biztonsági intézkedéseket – és ellenőrzést – követel, mivel rugalmas, transznacionális, decentralizált hálózatok működésén alapul. A bűnüldözés- és megelőzés, valamint a terrorizmus elleni harc jegyében a felügyeleti technológiák használatában nemcsak mennyiségi, hanem minőségi változás is történt, és a felügyelet-megfigyelés-ellenőrzés új formában vált az emberek

[36] Lásd pl. Ball, Kirsite – Kevin Haggerty – David Lyon: Routledge handbook of surveillance studies, Abingdon, Oxon, New York: Routledge, 2012

[37] Lyon, David: The Electoronic Eye. The Rise of Surveillance society.,Minneapolis: University of Minnesota Press, 1994. (A cím magyar fordítása: „Az elektronikus szem – A megfigyelés társadalmának felemelkedése".)

életének részévé a totalitárius diktatúrákat már csak hírből ismerő nyugati társadalmakban. (Az új demokráciákban vagy a félautoriter rezsimekben élők számára legfeljebb a technológiai fejlődés jelentett újdonságot.)

Úgy tűnik, hogy a „félelem kultúrájában" a bizalom helyét átveszi az ellenőrzés, és az ezzel kapcsolatos morális fenntartások elenyésznek – legalábbis sokan látnak ebben üzleti lehetőséget. Jól példázza a tendenciákat a surveillance studies egyik másik kedvelt témája, a zárt láncú kamerákra ('closed-circuit television' – CCTV) alapozott, rövid időn belül világszerte elterjedt térfigyelőrendszerek vizsgálata. Ezek elsőként a privát szektorban jelentek meg, félig nyilvános helyeken: bankokban és bevásárlóközpontokban; ezt követte az ún. „elsődleges közterek": emlékművek, iskolák, tömegközlekedési eszközök, állami intézmények bekamerázása; majd a „másodlagos közterek": a kisebb forgalmú, központtól távolabb eső területek, a nagyobb bűnözési arányt mutató külvárosi területek; végül a jövő: a mindenütt jelen lévő megfigyelés. A folyamat sikerét több tényező is elősegítette: a térfigyelő rendszereket sikeres eszköznek tekintették a belvárosok újraélesztésére; arra, hogy vonzó üzleti közeget varázsoljanak azoknak a vállalkozóknak, akik a külvárosba költöztek. A tapasztalatok szerint a megfigyelőrendszerek ugyanis alkalmasak lehetnek arra, hogy a deviáns elemeket (és a szegényeket) távol tartsák például a bevásárlóközpontokból, és így azok a középosztály tiszta és biztonságos közegei lehessenek. Ráadásul, bár rendkívül költséges ezeknek a rendszereknek a felépítése, mégis – főleg 2011. szeptember 11. óta – a mindenkori kormányok sem sajnálják rá a pénzt, már csak azért sem, mert noha a térfigyelőrendszerek hatékonyságának az ellenőrizhetősége igen kérdéses, telepítésük úgy hat, mintha a politikusok hatásos eszközökkel lépnének fel a bűnözés ellen, vagyis az ilyen beruházások kampánycélokra tökéletesen hatékonyak lehetnek.[38] Így lassan a társadalom – vagy legalábbis a középosztály – élettere hasonlóvá válik a bevásárlóközpontokhoz: az ellenőrzés alig látható, de tudjuk, hogy folyamatos; a magáncégek által alkalmazott biztonsági őrök mindent látnak, és az ellenőrzéshez, illetve rendteremtéshez csak ritkán van szükség fizikai ráhatásra.[39]

Az állami, rendészeti ellenőrzés újszerűsége említett módon nem választható el a technológiai fejlődéstől: egyre olcsóbb tárolási és adatfeldolgozási kapacitás mellett nyílik lehetőség a telefonbeszélgetések lehallgatására, sms-ek, emailek, blogok, közösségioldal-bejegyzések megfigyelésére, és technológiai értelemben már nem utópia a „teljes megfigyelés" sem. A rendészetben egyre inkább előtérbe kerül a prevenció és a megfigyelés; ami a konkrét emberi tevékenységek ellenőrzése mel-

[38] Lásd pl. Norris, Clive – Mike McCahill – David Wood: The Growth of CCTV: a global perspective on the international diffusion of video surveillance in publicly accessible space, Surveillance and Society 1, 2004/2–3. o.

[39] Wakefield, Alison: The public surveillance functions of private security, Surveillance and Society 1, 2004/4. o.

lett egyre nagyobb mértékben terjed ki a polgárok adatainak elemzésére is.[40] Nemcsak a különböző rendőri szervek technológiai felszereltsége, az operatív munka technologizáltsága alakul át, hanem ezzel egyidejűleg az emberek – különösen az infokommunikációs korszakban szocializálódott fiatalabb generációk – privacy-váromány is; azaz sok esetben eleve lejjebb kerül az a szint, amelyet a polgárok a magánszféra védelme kapcsán az államtól, illetve a privát szolgáltatóktól elvárnak.

A megfigyelés társadalmában a dataveillance lehetővé teszi, hogy az adatbányászat automatikusan, a humán tényező kiiktatásával történjen, hiszen a hangsúly egyébként is egyre inkább a kockázatra terelődik a tényleges „veszély" helyett; maga a megfigyelés pedig láthatatlan marad, hiszen gépek végzik, algoritmusok alapján.[41]

A technológiai fejlődés egyébként számos olyan kérdést vet fel, amelyek az alapjogok értelmezésében, egymáshoz képesti viszonyában is jelentkeznek. A privacy, a magánélet védett magjának kontúrjai például igencsak képlékenyek, és a generációs szakadék is nehezíti az eligazodást: a jogszabályokat sokszor olyanok alkotják, illetve a bírósági ítéleteket olyanok hozzák, akik – elsősorban idősebb életkorukból fakadóan – alapvetően eltérő módon és attitűddel használják például a közösségi oldalakat és egyéb internetes fórumokat, mint azok a fiatal polgárok, akiknek paternalista módon meg akarják védeni a magánszféráját; függetlenül attól, hogy az érintettek tartanak-e rá igényt (és ha igen, milyen mértékben).

Az internethez kapcsolható radikális technológiai- és életforma-változás során új életviszonyok jöttek létre (például a „Nagy Testvér" mellett megjelent sok, a privát szektorból érkezett „Kis Testvér", és a kereskedelem vagy éppen a politikai közbeszéd új fórumai nyíltak meg), és ezek változást igényelnek és hívnak életre nemcsak a jogrendszerben általánosságban és konkrét jogintézmények tekintetében, hanem az egyes alkotmányos alapjogok egymáshoz vett viszonyát illetően is. Kétségtelen, hogy a világ alapvetően megváltozott: a kérdés az, hogy ennek milyen alapjogi, alkotmányjogi következményei lesznek. Azt tudjuk, hogy az új világot a korábbinál összehasonlíthatatlanul nagyobb adatforgalom, valamint örökéletűnek tűnő, potenciálisan mindenki számára elérhető adatok felfoghatatlan mennyisége jellemzi. Az emberek védtelenek és kiszolgáltatottak nemcsak az érzékeny adataikhoz hozzáférő – és ezáltal adott esetben beláthatatlan károkat okozó – személyekkel és szervezetekkel szemben, illetve a személyiséglopással vagy a terhes, az emberi méltóságot sértő személyre szabott reklámmal, marketinggel szemben is. Korántsem evidens ugyanakkor az, hogy e radikálisan megváltozott világban egyfajta alkotmányos szuperklauzulaként a személyes adatok védelme tekinthető-e az origónak, és a konkuráló alapjogok közül minden esetben előnyben részesítendő-e. Elvi, jogfilozófiai és politikai vitát kell ugyanis arról folytatni, hogy a technológiai

[40] Bővebben lásd Bloss, William: Escalating U.S. police surveillance after 9/11: an Examination of causes and effects, Surveillance and Society, 2007/3.
[41] Uo. 119. o.

újításoknak megfelelően létrejött új életviszonyok hogyan és mennyiben alakítják – mert nem kérdés, hogy azt teszik – a fennálló alkotmányos alapértékrendszert. Meggyőződésem, hogy a politikai közvéleménynek: a jogalkotóknak, a jogalkalmazóknak és a választó-polgároknak közösen kell megválaszolni azokat az alapjogi kérdéseket, amelyeket a hagyományos, pl. a szükségesség-arányosság sémáját követő alkotmányértelmezési módszerrel önmagában nem, vagy csak nagyon nehezen lehet eldönteni.

A rendészet esetében különösen élesen megmutatkozik az adatelemzés-alapú megközelítés térhódítása. A bűnüldözésre, de főleg a bűnmegelőzésre alkalmazott profil elvileg minden eddiginél precízebb módszerrel, egy aktuárius paradigmában is kialakítható; a „Nagy Testvér" mellett sok „Kis Testvér" részvételével. A „biztonság" áraként viszont már nem is csak a személyes szabadságjogainkat, hanem a magánszféránkat is kéri és használja az állami, valamint a kiszervezett biztonsági ipar. Erről pedig már csak azért is hajlandóak vagyunk lemondani, mert a közösségi oldalak, az internetes vásárlás, a digitális televízió, azaz az infokommunikáció társadalmában a privacy fogalma egyébként is átalakul. A „szabadság kontra biztonság" retorika és dilemma így lassacskán „privacy kontra biztonság"-kérdéssé szelídül; méghozzá egy olyan technológiai és társadalmi környezetben, ahol például a milliárdnyi polgár közreműködésével fenntartott közösségi oldalak fogyasztói egyúttal maguk is termékek; értékesíthetőek az üzemeltető által – akár rendészeti célra is. Az „informatizáció", azaz a társadalom információalapúvá válásának folyamata során minden infokommunikációs technológia a társadalmi ellenőrzés, felügyelet és megfigyelés szolgálatába állítható.