NEMZETBIZTONSÁGI SZEMLE
7. évfolyam (2019) 1. szám 31–41. • DOI: 10.32561/nsz.2019.1.3

Csizner Zoltán[1]

A tömeges adatgyűjtés kérdései

The Questions of Mass Surveillance

Az USA és egyes európai országok tömeges adatgyűjtésének kérdése évek óta a figyelem középpontjában áll. A technikai eszközök, az informatikai programok fejlődése és a telekommunikációs szolgáltatók támogatása olyan mértékűvé tette ezt a fajta megfigyelést, amely a jogvédők komoly aggodalmára adott okot. Ugyancsak aggályos az a tervezet, melyet technikai eszközökkel végzett megfigyelésekkel a kínai kormány tervez bevezetni a közeljövőben.

Kulcsszavak: tömeges adatgyűjtés, Snowden, NSA, Kína, térfigyelő kamera

The mass data collection of the United States and some European countries is in the focus of attention for years. Technology, the development of the IT programs and the support of the telecommunication service providers have developed this monitoring to a level which cause a serious concern within the defenders of the law. That plan is also solicitous, which is intended to be introduced by the Chinese Government regarding the technical monitoring in the near future.

Keywords: mass surveillance, Snowden, NSA, China, CCTV cameras

A tömeges adatgyűjtés

Tavaly ősszel a híradásokban vezető helyet kapott a Belügyminisztérium azon törvényjavaslata,[2] amely szerint a kormány által kijelölt, egységes tárhelyen kerülnének tárolásra a közterületen, illetve tömegközlekedési eszközökön működő kamerák felvételei. A kezdeményezés nem új keletű. Sok esetben nyert bizonyosságot már, hogy a különböző rendszerek, eltérő tárolási módok és technikai megoldások miatt értékelhetetlen és pár nap múlva már hozzáférhetetlen felvételek készültek egy-egy

[1] Csizner Zoltán r. ezredes, doktorandusz, Nemzeti Közszolgálati Egyetem Rendészettudományi Doktori Iskola; Terrorelhárítási Információs és Bűnügyi Elemző Központ. ORCID-azonosító: 0000-0002-1867-8560.

[2] T/2930. számú törvényjavaslat.

bűncselekmény helyszínén vagy az elkövető menekülési útvonalán. Természetesen a rögzített felvételek tárolásának és hozzáférésének részletes szabályozása elengedhetetlen, amely nélkül joggal lenne támadható az elképzelés.

De ez a kérdés nemcsak hazánkban aktuális. Gyakorlatilag Snowden óta mindenki előtt világos, hogy az orwelli „1984" sokkal közelebb lehet, mint azt valaha gondoltuk; a színes fantázia valóságközelivé vált. Az informatika fejlődése, a telekommunikációs eszközök elterjedése, a hírközlés robbanásszerű átalakulásának eredményeként kijelenthető, hogy a totális megfigyelés rémképe már rég nem technikai kérdés.

A hírszerzéssel – akár bűnügyi, akár titkosszolgálati szakterületről beszélünk – foglalkozó szakemberek szerint két esetben van baj: amikor nincs információ, vagy amikor túl sok az információ. A technikai fejlődés által elért információrobbanás ráébresztett mindenkit arra, hogy bármennyire is hatalom az információ, annak előzetes szűrése, értékelése nélkül elveszünk a tengerben.

Egy amerikai tanulmány szerint[3] már 2012-ben is naponta 2,5 billió gigabyte (GB) adat keletkezett. Az információ keletkezése soha nem látott módon gyorsul; 2020-ra az előjelzések szerint minden másodpercben személyenként 1,7 megabyte adatmennyiséget állítunk majd elő a Földön.

A titkosszolgálatok hamar felismerték ennek a hasznát, és elkezdték konkrét cél nélkül begyűjteni az adatokat. Addig, amíg ez az adatgyűjtés a mindenki számára elérhető nyílt forrásokat érintette, egyszerű OSINT-tevékenységről[4] beszélhettünk, de amint a magánszférát érintő adatokat, kommunikációt vonták megfigyelés alá, ennek jogszerűsége már erőteljesen megkérdőjeleződött. Az pedig tényszerű, hogy a megfigyelések, ellenőrzések és adatgyűjtések sok esetben túlléptek a célirányos, konkrét felderítéseken, mint ahogy ezt Edward Snowden, az NSA[5] és a CIA[6] egykori munkatársa 2013-ban nyilvánosságra hozta.

Edward Snowden és az NSA-szivárogtatás

Edward Snowden Észak-Karolinában született 1983-ban, és 30 évesen olyan ismertté vált a világon, hogy ilyen hírnevet kevesen érnek el. Édesanyja Baltimore-ban a szövetségi bíróságon dolgozott mint az informatikai hálózat vezetője, édesapja a Parti Őrség állományában teljesített szolgálatot.[7]

Iskolái után 2004-től az NSA biztonsági őreként dolgozott, majd 2006-ban felvették a CIA-hez informatikai területre. Később Hawaiira költözött a munkája miatt, de már ekkor elkezdte másolni és gyűjteni azokat az általa elérhető titkos dokumentumokat, amelyek később az angol *The Guardian* újságban jelentek meg 2013 júniusában. *Az elsők között nyilvánosságra hozott és az NSA által PRISM fedőnéven*[8] folytatott

[3] Arora 2019.
[4] Open Sourche Intelligance, nyílt forrású hírszerzés.
[5] NSA: National Security Agency, Nemzetbiztonsági Ügynökség.
[6] CIA: Central Intelligence Agency, Központi Hírszerző Ügynökség.
[7] Biography.com: *Edward Snowden* címszó.
[8] PRISM: Planning tool for Resource Integration, Synchronization, and Management, erőforrás-integráció, az összehangolás és management tervezési eszköze.

adatgyűjtési program feltárása olyan lavinát indított el a titkosszolgálatok tömeges adatgyűjtésével kapcsolatban, amely alapjaiban megváltoztatta ezt a fajta hírszerzést.

Snowden a titkos adatokat szisztematikusan gyűjtötte, azokról másolatokat készített. Mikor elérkezettnek látta az időt, titkosított csatornákon felvette a kapcsolatot Glenn Greenwalddal, a *The Guardian* brit lap újságírójával, valamint Laura Poitras dokumentumfilmessel. 2013 májusában egy hongkongi hotelben találkoztak, ahol több napot töltöttek el. Közben a *The Guardian*ben részletekben jelentek meg a leleplező cikkek, majd később a *The Washington Post*ban, illetve más elektronikus és nyomtatott sajtótermékben is egyre több részlet jelent meg.

A kiszivárogtatás miatt Snowdent az amerikai igazságügyi szervek több törvénysértéssel, közte az 1917-es kémtörvény[9] megsértésével vádolják. Egyes vélemények szerint hazájában 30 éves börtönbüntetés várna rá, és nem sok reményt fűznek az általa benyújtott – jogvédők, civil szervezetek, művészek által is támogatott – kegyelmi kérvényhez.

Snowden az újságokban több részletben mutatta be az NSA, illetve a társszervek által végzett, valójában konkrét cél nélküli adatgyűjtés folyamatait, eszközeit és viszszásságait. A leleplezés újdonsága nem abban állt, hogy a távközlési szolgáltatók együttműködtek a titkosszolgálatokkal, és lehetőséget biztosítottak az adatok megszerzésére, hanem abban, hogy ez a megfigyelés minden konkrét ok és cél nélkül zajlott, és gyakorlatilag minden elérhető adatot érintett.

A cikksorozat első részében ismertetett PRISM-program az egyik legnagyobb visszhangot váltotta ki. A programban az NSA bírósági végzés alapján felhatalmazást kapott a távközlési szolgáltatók által kezelt metaadatok begyűjtésére. A dokumentumok között szerepelt az a bírósági végzés is, amely az amerikai Verzion telekommunikációs céget kötelezte az adatok átadására és a titoktartásra. Ugyan a közzétett végzés csak ezt a céget nevesítette, de a többi dokumentum szerint a másik két legnagyobb amerikai telekommunikációs cég, az AT&T és a Sprint Nextel is érintett volt.

A végzés értelmében mind az USA-n belüli, mind az azon kívüli hívások adatait (hívó és hívott szám, cellainformációk, IMSI-adatok, hívás időtartama) át kell adnia, és így ezzel a három céggel az NSA az amerikai telefonforgalom jelentős részét megismerte. A telefonszolgáltatókon kívül az általa kezelt metaadatok megismeréséhez közvetlen hozzáférést biztosított többek között a Facebook, a Google, a Microsoft, a Yahoo, az AOL, a Skype vagy a YouTube is, akik a felhasználók adatain túl e-mailek adatait vagy a böngészési előzményeket is megosztották.

A második közzétett terület az NSA-vel szorosan együttműködő brit szervezet, a GCHQ[10] által végzett Tempora program volt. Eszerint a brit ügynökség a transzatlanti száloptikás kábel megcsapolásával gyűjtött információkat e-mailekről, hívásokról, üzenetekről vagy böngészési előzményekről. A begyűjtött adatokat a GCHQ megosztotta az NSA-vel. A botrány kirobbanása előtti évben, 2012-ben napi 600 millió hívást kezelt az ellenőrzött 200 kábelen, ami mintegy 21 petabyte[11] napi adatmennyiségnek felel

9 Espionage Act of 1917, az USA törvényhozása által 1917. június 15-én elfogadott jogszabály.
10 GCHQ: Government Communications Headquarters, technikai hírszerzést végző brit ügynökség.
11 1 petabyte = 10^{15} = 10000^{5} byte.

meg. Ezzel a teljesítménnyel a GCHQ a *Five Eyes koalíció*[12] egyik legeredményesebb tagja lett.

A harmadik rész a TAO-ról[13] szólt, *ami egy NSA-n kívüli, elit hackercsapat tevékenységét takarja. Ennek bevetésére akkor került sor, amikor az NSA nem volt képes feltörni egy titkosítási kódot. Az informatikai rendszerek védelmének feltörése, vírusok bejuttatása vagy a tárolt adatok megszerzése ennek a specialistákból álló csoportnak nem jelentett gondot.*

A Dishfire program az összes, az NSA által hozzáférhető szöveges üzenetet begyűjtötte a világ minden tájáról, és értékelte. Egyes becslések szerint közel 200 millió üzenet került az adatbázisba. Így erre természetesen nem kizárólag a célszemélyek vonatkozásában került sor, hanem vétlen, törvénysértés gyanúja nélküli személyekkel szemben is. A begyűjtött adatok (hitelkártyaadatok, kapcsolati hálók, tartózkodási adatok) alapján többek között tervezett utazásokról, pénzügyi tranzakciókról, érdeklődési körről vagy akár az aktuális tartózkodási helyről nyerhettek értékes információkat. Ebben nyújtott segítséget a Prefer nevű elemző program, amely mintegy 1,6 millió határátlépési és 800 ezer pénzügyi tranzakciós adatot szűrt ki.[14]

A következő részletezett technológia, a SOMALGET – amely része az NSA 2009-ben indított MYSTIC-programjának – a világ több országában (Fülöp-szigetek, Mexikó, Kenya és a Bahama-szigetek kerültek nevesítésre) a telefonforgalmak metaadatainak, továbbá egyes országok tekintetében a forgalmazások tartalmának megismerését biztosította. Az adatok és a tartalmak szinte már valós időtől rendelkezésre álltak, és 30 napig voltak elérhetők.[15]

Egy újabb fejezet volt a Xkeyscore program bemutatása, amelyet az NSA egyik legátfogóbb internetes ellenőrző rendszereként jellemeztek. Kiterjedt minden olyan lényeges mozzanatra, amit egy hétköznapi felhasználó a világhálón végez. Képes volt adatot gyűjteni e-mailekről, online csevegésekről vagy a böngészési előzményekről.[16] Az NSA ugyan elismerte a program létezését, de állításuk szerint az a külföldi jelek elfogását végző és jogszerűen működő rendszer része, továbbá korlátozott a hozzáféréssel rendelkező személyek köre.

Voltak olyan programok is, amelyekkel kapcsolatban az NSA nem adott választ, sőt a snowdeni információk birtokában lévő *The Guardian, The New York Times* és a *ProPublica* újságokat állítólag arra akarták rávenni, hogy ne is közöljék le az azokról szóló cikkeket. Ezek közé tartozott például a Bullrun, ami a hírek szerint egy olyan dekódoló program, amelynek célja, hogy feltörjön egyes elterjedten használt titkosító programokat. Ezután az NSA már a titkosítás kikerülésével férhetett hozzá online tranzakciókhoz és e-mailekhez.[17]

Joggal gondolhatnánk, hogy a sajtóban megjelent hírek valóságtartalma csekély, és valójában sem az amerikai, sem más országok titkosszolgálata nem sértette

12 Az NSA vezetése alatt álló, 1941-ben alapított közösség. Tagjai: USA, Egyesült Királyság, Új-Zéland, Ausztrália és Kanada, amely biztosítja a jelhírszerzés (SIGINT) során begyűjtött adatok közös felhasználását, átadását.

13 TAO: Tailored Access Operations, Speciális Hozzáférést Biztosító Művelet.

14 Ball 2014.

15 Gellman–Soltani 2014.

16 Greenwald 2013.

17 Perlroth–Larson–Shane 2013.

oly mértékben az alapvető jogokat. Azonban figyelemre méltó körülmény, hogy a szivárogtatást követően az Európai Unió Állampolgári Jogi, Bel- és Igazságügyi Bizottsága (LIBE)[18] *Az egyesült államokbeli NSA megfigyelési programjáról, a különféle tagállamokban megfigyelést végző szervekről és az uniós polgárok alapvető jogaira gyakorolt hatásukról, valamint a transzatlanti bel- és igazságügyi együttműködésről* címen egy vizsgálatot folytatott le, amelynek eredményét 2014 tavaszán ismertették.

A végleges jelentést[19] 2014. február 12-én fogadta el az EU Parlament. A jelentés – az újságírói információkkal, a vizsgálat során szerzett szakértői bizonyítékokkal és az egyes hatóságok beismerésével alátámasztva – az újságokban megjelenteket bizonyítottnak értékelte. Emellett olyan további tömeges megfigyelésekre is felhívta a figyelmet, amelyeket európai országok folytattak. Így adatok merültek fel a német, a francia és svéd titkosszolgálatok ilyen irányú tevékenységére vonatkozóan is.

A LIBE-jelentésben foglalt megállapítás a tömeges megfigyelés jogszerűségével kapcsolatban egyértelmű: „A nem célirányos, tömeges megfigyelés és az EU polgáraira vonatkozó adatok tömeges gyűjtése legalábbis az igazságosság alapelvének megsértése veszélyével járhat, különösen a büntetőeljárások során, az »ártatlanság vélelme« tekintetében, amely szintén mindenkire vonatkozik, nemzetiségre való tekintet nélkül.[20]

A tömeges megfigyelés szerepe azt eredményezi, hogy a büntetőjog, amelynek eredeti szerepe az egyedi cselekmények személyes felelősség alapján történő szankcionálása, eltolódik a kockázatcsökkentés és a lehetséges bűnözők azonosítása irányába, és ez ahhoz vezethet, hogy minden állampolgárt folyamatos megfigyelés alatt tartanak, és gyanús személyként kezelnek."[21]

Snowden megítélése és a következmények

Már a szivárogtatást megelőzően Snowden tisztában volt azzal, hogy az Egyesült Államokba nem térhet vissza, ezért egy olyan országot keresett menedékként, amelynek értékrendje hasonlított az általa preferálthoz. A választása Írországra esett, de az ottani menekülttörvény miatt a kérelme elutasításra került. Ezután több országban keresett menedéket, szóba került Venezuela is, de végül Moszkvától kapott segítséget.

Snowden tette ellentmondásos véleményeket eredményezett. Míg a jogvédők, a civilek egyértelműen üdvözítik a tevékenységét, addig az USA kormányzata és a titkosszolgálatok az amerikai nemzet történelmének legnagyobb és legkárosabb árulóját látják benne, és bűnözőnek tekintik.

Ugyan a Fehér Ház vizsgálata azt állapította meg, hogy a tömeges megfigyelésnek nincs érzékelhető haszna a terrorizmus elleni fellépésben, a CIA mégis azzal vádolta meg, hogy Iszlám Állam tagjai a kiszivárogtatásnak köszönhetően tudták

18 LIBE: Civil Liberties, Justice and Home Affairs, Európai Unió Állampolgári Jogi, Bel- és Igazságügyi Bizottsága.
19 A7-0139/2014. számú jelentés.
20 Az ártatlanság vélelme a büntetőjog alapelvének tekintendő, és azt mind az Emberi Jogok Európai Egyezménye, mind pedig az Európai Unió Alapjogi Chartája elismeri.
21 A7-0139/2014. számú jelentés.

észrevétlenül megszervezni a 2015-ös párizsi mészárlást, míg az NSA állítása szerint közel 1000 célszemélyük tűnt el az ellenőrzött felületekről.

Ennek ellenére a tömeges megfigyelésre felhatalmazást adó és 2015-ben lejáró – 9/11 okán elfogadott – *USA Patriot Act*[22] 215-ös cikkelyének alkalmazását a kongresszus nem hosszabbította meg. Helyette megkezdődött az *úgynevezett Freedom Act* tervezése[23], amelyet 2015. június 2-án fogadtak el. Az új törvény véget vetett a tömeges adatgyűjtésnek, egészen pontosan a végrehajtás jogi felhatalmazásának. A távközlési kommunikáció megfigyelésének lehetősége nyitott maradt, de a kormányzati szervek számára tiltott lett a hosszú távú adatbázis cél nélküli építése, továbbá a szolgáltatók által maximum másfél évig őrzött adatok csak szövetségi bíró engedélyével kérhetők ki.

Míg az USA-ban szigorítást eredményezett a kiszivárogtatás, addig Nagy-Britanniában a korábbi törvény módosítása inkább bővítette a hatóságok jogosítványait. A 2016. november 29-én elfogadott *Investigatory Powers Act 2016*[24] (közismerten a *Snoopers' Charter*) 48 szervezetnek, közte a GCHQ-nak adott felhatalmazást a távközlési szolgáltatók által kezelt adatok tömeges begyűjtésére, tárolására. A törvény egyes rendelkezései ellen a National Council for Civil Liberties[25] (NCCL) civil jogvédő szervezet keresetet nyújtott be, amelynek eredményeként az Egyesült Királyság Legfelsőbb Bírósága megállapította, hogy a törvény sérti az Egyesült Királyság állampolgárainak magánélethez való jogát, továbbá összeegyeztethetetlen az Emberi Jogok Európai Egyezményével. Ennek alapján 2018. november elsejéig a kormányzatnak törvénymódosítást kellett eszközölnie.[26]

Mindezt annak ellenére állapította meg a brit legfelsőbb bíróság, hogy a kifogásolt törvény végrehajtásának külső kontrollját egy 2000-ben létrehozott független bírói testület, az IPT[27] biztosítja, amely a vélt vagy valós titkos felderítésekkel kapcsolatos panaszok kivizsgálására hivatott. A szervezet független a többi bírói testülettől, döntéséhez előzetesen semmilyen jóváhagyást vagy engedélyt nem kell kérnie. A működés alapelvei között kiemelt helyen szerepel, hogy nem sértheti, veszélyeztetheti az Egyesült Királyság köz- vagy nemzetbiztonsági érdekeit. Amennyiben a vizsgálatuk nem állapít meg visszaélést, és a panaszt alaptalannak találják, a panaszos csak arról kap tájékoztatást, hogy nem történt jogsértés. A vizsgálat részleteiről, a megállapított körülményekről (így sem arról, hogy folyt-e ténylegesen titkos felderítés, sem arról, hogy az milyen részletekben felelt meg a jogi szabályozásnak) nem kap adatot.

Amennyiben az eljárás a panaszt megalapozottnak találja, úgy elrendelheti a jogsértő ellenőrzés, megfigyelés azonnali megszüntetését, a keletkezett adatok megsemmisítését, és kártérítést is megítélhet a panaszos számára. Ebben az esetben az adott ügytől függ, hogy a kap-e részletesebb tájékoztatást a körülményekről.

---

22 Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001; 2012. október 26-án Bush elnök által aláírt törvény.

23 H.R.2048 – USA FREEDOM Act of 2015.

24 A nyomozó (beleértve a felderítő és hírszerző) hatóságok eljárását szabályozó törvény.

25 NCCL: National Council for Civil Liberties, Polgári Szabadságjogok Nemzeti Tanácsa.

26 Zorz 2018.

27 IPT: Investigatory Powers Tribunal, Nyomozati Hatóságok Bírósága.

Az IPT mind a nemzetbiztonsági szolgálatok (SIS,[28] MI5[29], GCHQ), mind a rendőrség, a vámőrség vagy a fegyveres erők tevékenységét jogosult vizsgálni, sőt a skót bűnügyi és kábítószer-ellenes ügynökség[30] tevékenységére is hatáskörrel bír.

A sors fintora, hogy a Snowdennek menedéket nyújtó Oroszországban 2016. júliusban Vlagyimir Putyin orosz elnök is aláírta azt a törvényt, amely felhatalmazza a titkosszolgálatokat a tömeges megfigyelésekre és lehallgatásokra.[31] Az orosz törvény szerint a szolgáltatóknak a hívások metaadatait 3 évig, míg a közlemények, üzenetek tartalmát (beleértve a videókat is) fél évig kötelesek megőrizni. Ugyancsak kötelesek lesznek átadni az esetleges titkosítás esetén a „hátsó ajtóhoz" való kulcsot is, azaz biztosítani a hozzáférést.

Az úgynevezett „hátsó ajtó" máshol is visszatérő kérdés. A techcégek álláspontja szerint nem garantálható, hogy a nyitva hagyott hátsó bejárat és az ahhoz kiadott „kulcs" mindig jó kezekbe kerül, vagy mindvégig ottmarad. E félelem mellett óvatosságra inti a cégeket maga a snowdeni kiszivárogtatás is, hiszen ezzel mind az együttműködés titkossága, mind az átadott adatok védelme jelentősen sérült. Sokkal inkább felvállalják a harcot a hatalom ellen, ha garantálják a kommunikáció védelmét az általuk kifejlesztett titkosítással, speciális appokkal. Nem mellesleg ez az üzleti politikájukat is jobban szolgálja. A Snowden által nyilvánosságra hozott legnagyobb együttműködő cégek, mint a Facebook, a Google vagy a Yahoo például az „end-to-end"-szolgáltatást hirdetik, amely gyakorlatilag a két végfelhasználó közötti teljes titkosítást jelenti. De a bizalom már megtört, így a teljes biztonságra vágyó felhasználók egyre inkább a még makulátlan szolgáltatásokhoz fordulnak, mint amilyen a Signal vagy a Telegram. Utóbbinak sajátos reklámot jelent, hogy a titkosszolgálati jelentések szerint a dzsihadisták is előszeretettel használják a megbízhatósága és ellenőrizhetetlensége miatt.

A hatalommal vívott küzdelem egyik ismertté vált példája a FBI[32] vs. Apple vita, amely a San Bernardinóban elkövetett terrorcselekmény elkövetőjének mobiltelefonját érintette. 2015. december 2-án Syed Farook és Tashfeen Malik az iszlám nevében lövöldözni kezdett az Inland Regional Center szociális intézményben, amely során 14 személy meghalt, és további 21 megsebesült. A helyszínre érkező rendőrök a menekülő elkövetőkkel tűzpárbajt vívtak, amelyben mindkettőt lelőtték. A náluk talált IPhone5 telefon adatai az esetleges terrorista kapcsolataik felderítése érdekében nélkülözhetetlenek voltak, de a titkosítás feltörése sem az FBI-nak, sem az NSA-nek nem sikerült. Az Apple a kérést azzal tagadta meg, hogy ha biztosítaná a „hátsó kaput" az IPhone-hoz, nem látna garanciát arra nézve, hogy azt csak ebben az ügyben és csak a kérdéses mobilkészülékre alkalmaznák. Az elhúzódó jogi vita végén az FBI végül az izraeli Cellebration céget bízta meg a telefon tartalmának kinyerésével. Egy 2018-as hír szerint a telefonban a terrorcselekménnyel kapcsolatban releváns adat nem volt.

28 SIS/MI6: Secret Intelligence Service, Hírszerző Szolgálat, kormányügynökség.
29 MI5: Security Service, Biztonsági Szolgálat, kormányügynökség.
30 SCDEA: Scottish Crime and Drug Enforcement Agency, skót bűnügyi és kábítószer-ellenes ügynökség.
31 *Putyin rábólintott: indul a tömeges lehallgatás Oroszországban* 2016.
32 FBI: Federal Bureau of Investigation, Szövetségi Nyomozó Iroda.

Kína-szindróma

A kínai ipart a legtöbb ember a silány, jellemzően hamisított termékek legnagyobb kibocsátójaként azonosítja. Hihetetlen, de ugyanez az ipar a világ egyik legfejlettebb informatikai rendszerét építette fel, és az elkövetkező években ezt további dollármilliárdokkal igyekeznek bővíteni. A tervek szerint 2030-ig 150 milliárdos piacot fejlesztenek ki.

Ugyanakkor ehhez egy olyan felhasználási környezet csatlakozik, amely az alapvető jogokat, a polgárok magánéletének sérthetetlenségét szinte semmibe veszi. Ezt a nemzetközi politikai közvélemény kifogásolása mellett erőteljesen támadja több civil jogvédő szervezet is, mint például az *ACLU*[33] vagy a *HRW*.[34]

Kínában jelenleg 176 millió térfigyelő kamera pásztázza a közterületek, boltok, közintézmények területét, de az óvodák, iskolák, hotelek sem maradnak ki. Az egyik legszélsőségesebb példa szerint még a nyilvános vécékben sem lehet elrejtőzni; a pekingi Ég Temploma *(Temple of Heaven)* mosdóiban be kell szkennelni az arcot, hogy a gép kidobja a vécépapírt.[35]

Az utóbbi évek fejlesztéseinek eredményeként 2017 szeptemberében indult útjára Kínában egy olyan, 20 millió okoskamerából álló hálózat,[36] ami az AI-rendszerének[37] köszönhetően nemcsak megfigyel és rögzít, hanem egy központi adattárhoz kapcsolva elemez, kiértékel és jelzéseket ad.

A videoadatokat kiegészíti a tervek szerint egy, az azonosítást is elősegítő hangadatbázis is, amelybe eddig közel 70 000 minta került már felöltésre. De ez a pár tízezer minta eltörpül az ország összes (!) állampolgáráról rögzített DNS- és daktiloszkópiai nyom, illetve a nyilvántartások fotóadatai mellett.

Az elemző szoftvert gyártó CloudWalk nevű helyi cég egy olyan programot is tesztel, amely a megfigyelt adatokból (mozgás, viselkedés) végzett elemzéssel meghatározza, reális-e az esélye bűncselekmény elkövetésének.

Ez fontos eleme a 2014-ben bejelentett, elképzelések szerint 2020-ig bevezetésre kerülő értékelési rendszernek *(Social Credit System),*[38] amely a kamerák és más tömegesen begyűjtött adatok feldolgozására alapozva a polgárok megbízhatóságát, antiszociális viselkedésüket vagy a kormányellenes, kritikus megnyilvánulásaikat vizsgálja. De természetesen a hivatalos közleményekben a felhasználás elsődleges céljaként a bűnmegelőzés és a bűncselekmények felderítése szerepel.[39]

A kínai kormány által közzétett tervezetet Rogier Creemers[40] fordította le angolra és publikálta. Eszerint a kormány négy fő fókuszterületen értékelné a polgárokat:

– őszinteség a kormányzati ügyekben,
– üzleti becsületesség,

33 ACLU: American Civil Liberties Union, Amerikai Polgári Szabadságjogokért Szövetség.
34 HRW: Human Rights Watch, Emberi Jogok Felügyelete. *China: Voice Biometric Collection Threatens Privacy* 2017.
35 Tan 2017.
36 Lo 2017.
37 AI: artificial intelligence, mesterséges intelligencia.
38 Social Credit System: tervkörvonalazás egy társadalmi kreditrendszer kivitelezésére.
39 *Planning Outline for the Construction of a Social Credit System (2014–2020)* 2014.
40 Rogier Creemers holland születésű (Susteren, 1972), Hollandiában élő internet- és médiakutató, kiemelten kezeli Kína kérdését.

– társadalmi becsületesség,
– igazságügyi hitelesség.

Minden polgár egy középszintű pontértékről indul, és a tevékenysége alapján ehhez gyűjt, vagy ebből veszít. A tervek szerint a pontérték 350 és 950 között mozogna, és a személyi azonosítóhoz rendelnék hozzá. Mivel az egyes egyének besorolása, pontértéke mindenki számára megismerhető lesz, az sem meglepő, hogy a tervek szerint az is negatív értékelést eredményez, ha valaki alacsony pontszámú személlyel tart kapcsolatot, ami már önmagában megbélyegzést és szegregációt jelent majd.[41]

A rendszer a modern kor minden lehetséges eszközét (a már említett kamerafelvételeket, az elektronikus fizetési adatokat, a közösségi hálókat, az algoritmikus szűréseket, állami adatbázisokat) felhasználná ahhoz, hogy teljesüljön a totális kontroll. Figyelemmel kísérik többek között a hobbit, az érdeklődési kört, a vásárolt árukat és azok mennyiségét, a felkeresett helyeket, intézményeket, a munkahelyre érkezés-távozás adatait.

És ugyan a rendszer a kínai állampolgárokra vonatkozna elsősorban, azonban a külföldiek sem maradnak ki teljesen. Az országban működő összes külföldi céget kötelezik arra, hogy a kínai felhasználók adatait olyan helyi szerveren (is) tárolniuk kell, amelyhez hozzáférést kell biztosítaniuk. Mindemellett pedig a kínai kormány szeretné az értékelési rendszert minden Kínában működő üzletre is kiterjeszteni.[42]

Összegzés

Tény, hogy nagyon csábító az az adathalmaz, amely szerte a világban körülvesz minket, mint ahogy különösen nehéz elfogadni azt a körülményt, amikor ez az adat elveszik a szükséges felhasználást megelőzően. De ez nem eredményezheti azt, hogy azok a jog korlátait átlépve kerüljenek felhasználásra. Ahogy Finszter Géza fogalmazott: „A jogsértések ellen nem lehet jogsértő módon felvenni a küzdelmet, az esetleges eredménytelenség következményeit pedig az államnak magának kell viselnie, mert a történelmi tapasztalatok szerint ez kevesebb kárt okoz a közösségnek, mintha maga az állam kezdene el bűnöző módjára cselekedni."[43]

Ugyanakkor szükséges lenne megtalálni azt a technikai és normatív megoldást, amely az adatok személytelenné tétele mellett hosszabb időn át biztosítaná az elérhetőségüket, akár az idő múlásával arányos fokozott jogi garanciák beépítése mellett. Hiszen nem az adat megőrzése sérti igazán az alapvető jogokat, hanem a nem megfelelő felhasználás. Ezzel szemben az elveszett adat már megismételhetetlen, az esetek többségében már egy vissza nem fordítható folyamat vége.

Véleményem szerint egy ilyen megoldás mellett a hazai központi tárhely kialakítása is úgy lehet hasznos eleme a bűnüldözésnek és a nemzet biztonságáért felelős szervezetek munkájának, hogy azt az adatvédelem területéről sem kérdőjelezhetik meg.

41 Stanley 2015.
42 Meissner 2017.
43 Finszter 2007, 12.

Felhasznált irodalom

A7-0139/2014. számú LIBI-jelentés. Elérhető: www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A7-2014-0139+0+DOC+XML+V0//EN (A letöltés dátuma: 2019. 03. 29.)

Ball, James (2014): *NSA collects millions of text messages daily in 'untargeted' global sweep.* Elérhető: www.webcitation.org/6OHZxSmLT?url=https://www.theguardian.com/world/2014/jan/16/nsa-collects-millions-text-messages-daily-untargeted-global-sweep (A letöltés dátuma: 2019. 03. 29.)

Biography.com: *Edward Snowden* címszó. Elérhető: www.biography.com/people/edward-snowden-21262897 (A letöltés dátuma: 2019. 03. 29.)

Finszter Géza (2007): Rendvédelemről szóló alkotmánybírósági határozatok elemzése. In Virág György szerk.: *Kriminológiai Tanulmányok*, 44. kötet. Budapest, OKRI.

Gellman, Barton – Soltani, Ashkan (2014): *NSA surveillance program reaches 'into the past' to retrieve, replay phone calls.* Elérhető: www.washingtonpost.com/world/national-security/nsa-surveillance-program-reaches-into-the-past-to-retrieve-replay-phone-calls/2014/03/18/226d2646-ade9-11e3-a49e-76adc9210f19_story.html?noredirect=on&utm_term=.1171a30bb2d5 (A letöltés dátuma: 2019. 03. 29.)

Greenwald, Glenn (2013): *XKeyscore. NSA tool collects 'nearly everything a user does on the internet'.* Elérhető: www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data (A letöltés dátuma: 2019. 03. 29.)

H.R.2048 – USA FREEDOM Act of 2015, 114th Congress (2015–2016). Elérhető: www.congress.gov/bill/114th-congress/house-bill/2048 (A letöltés dátuma: 2019. 03. 29.)

Lo, Tiffany (2017): *Big brother is watching you! China installs 'the world's most advanced video surveillance system' with over 20 million AI-equipped street cameras.* Elérhető: www.dailymail.co.uk/news/article-4918342/China-installs-20-million-AI-equipped-street-cameras.html (A letöltés dátuma: 2019. 03. 29.)

Meissner, Mirjam (2017): *China's Social Credit System: A big-data enabled approach to market regulation with broad implications for doing business in China.* Elérhető: www.merics.org/sites/default/files/2017-09/China%20Monitor_39_SOCS_EN.pdf (A letöltés dátuma: 2019. 03. 29.)

Perlroth, Nicole – Larson, Jeff – Shane, Scott (2013): *N.S.A. Able to Foil Basic Safeguards of Privacy on Web.* Elérhető: www.nytimes.com/2013/09/06/us/nsa-foils-much-internet-encryption.html?_r=0 (A letöltés dátuma: 2019. 03. 29.)

Planning Outline for the Construction of a Social Credit System (2014–2020) (2014). Elérhető: https://chinacopyrightandmedia.wordpress.com/2014/06/14/planning-outline-for-the-construction-of-a-social-credit-system-2014-2020/ (A letöltés dátuma: 2019. 03. 29.)

Arora, Shivam (2019): *Data Science vs. Big Data vs. Data Analytics.* Elérhető: www.simplilearn.com/data-science-vs-big-data-vs-data-analytics-article (A letöltés dátuma: 2019. 03. 29.)

Stanley, Jay (2015): *China's Nightmarish Citizen Scores Are a Warning For Americans.* Elérhető: www.aclu.org/blog/privacy-technology/consumer-privacy/chinas-nightmarish-citizen-scores-are-warning-americans (A letöltés dátuma: 2019. 03. 29.)

Tan, Kenneth (2017): *Face recognition scanners installed at Temple of Heaven bathrooms to wipe out toilet paper theft.* Elérhető: http://shanghaiist.com/2017/03/20/toilet_paper_theft_cameras/ (A letöltés dátuma: 2019. 03. 29.)
Zorz, Zeljka (2018): *UK High Court rules part of Snoopers' Charter incompatible with EU law.* Elérhető: www.helpnetsecurity.com/2018/04/30/snoopers-charter-eu-law/ (A letöltés dátuma: 2019. 03. 29.)