

Rév István
Vuhantól Nagyvenyimig
Rév István 2020.04.19 13:03

<https://magyarnarancs.hu/publicisztika/vuhantol-nagyvenyimig-127845>

A hivatalos Új Kína hírügynökség hírportálja, a XinhuaNet február 10-én adta hírül, hogy a kínai hatóságok és az állami tulajdonban lévő China Electronics Technology Group közös fejlesztésének eredményeként letölthetővé vált a „közeli kontaktus kereső” alkalmazás.

Miután megadta nevét, személyi és telefonszámát, a felhasználót ez a mobiltelefonra letölthető applikáció arról tájékoztatja, hogy az elmúlt hetekben hány olyan személlyel került közeli kapcsolatba – tartózkodott vele egy légtérben, ült a repülőn egyazon sorban, utazott vele ugyanabban a vasúti fülkében és a többi –, akinek koronavírustesztje pozitív eredményt mutatott. Az adatokat a légi- és vasúttársaságok, a helyi igazgatási szervek, a munkahelyek, a kórházak és az arcfelismerő szoftverrel rendelkező térfigyelő kamerák szolgáltatják. Ha az derül ki, hogy a felhasználó fertőzöttel került közeli kapcsolatba, az applikáció előírja a követendő rendszabályokat. Aki megszegi az elkülönítési tilalmat, nem jut messzire: az arcfelismerő szoftverrel felszerelt több mint százmillió közterületi biztonsági kamera egyike azonosítja őt, és automatikusan értesíti a rendőrséget és a munkahelyi főnökét. A bűnös nem csak karanténba kerül, de arra a listára is ráteszik a nevét, amely a kirótt büntetéseket teszi közzé. Az elérhető információk szerint az elmúlt hetekben több mint kétszázmillió kínai állampolgár töltötte le a detektort.

A kínai kormány 2014 júniusában jelentette be, hogy 2020-ra az egész országra kiterjedő, ún. „társadalmi kreditrendszert” hoz létre. Az állampolgárokat és a cégeket a politika iránti őszinteség, az üzleti és társadalmi tisztesség és a jogi hitelesség alapján pontozzák. Aki nem ér el bizonyos pontszámot, és kevésbé megbízhatónak mutatkozik, nehezen vagy sehogy sem jut bankkölcönhöz, nem vásárolhat hitelbe, nem vehet repülő- és vonatjegyet, nem utazhat külföldre, nem juthat bizonyos szolgáltatásokhoz, nem regisztrálhat társkereső oldalon. A magas pontszám ellenben jutalmakat és kiváltságokat ér. Az elmúlt években, többnyire a digitális fizetési rendszerhez kapcsolva, a legtöbb kínai tartományban bevezették a rendszer számos elemét, és a tervek szerint – a különböző változatok összekapcsolásával – az idén egységesítik, országossá teszik és centralizálják a pontrendszert. A „közeli kontaktus kereső” letöltése ugyan önkéntes, de a le nem töltés súlyos büntetőpontokat von maga után.

*

Ezek a rendszabályok mintegy szintetizálják a Michel Foucault francia filozófus által leírt két járványügyi modellt: a szegregálást és a folyamatos felügyeletet. A lepratelep szigorúan szegregáló logikájára ráépül a pestis teljes körű, folyamatos nyilvántartáson alapuló felügyeleti rendszere.

„A pestises város a világtól elvágott, mozdulatlan, merev tér” – írja Foucault *Felügyelet és büntetés* című művében. (Gondolat, 1990, ford. Fázsy Anikó.)
„Szüntelen a felügyelet. Mindenütt éber tekintet... hogy a nép azonnal engedelmessé váljon, s a magisztrátus hatalma abszolút legyen. Valamennyi ember a kalitkájába zárva, valamennyi az ablakában, nevét kiáltva s megmutatva magát, ha kéri – íme, élők és holtak nagy seregszemléje.

Ez a felügyelet állandó nyilvántartást kíván. A városban tartózkodó minden embert egyenként lajstromba vesznek: rávezetik a nevét, az életkorát, a nemét. A patológus nyilvántartás állandó és központosított. Valamennyi ember betegséghez és halálhoz való viszonyát a hatalom szervei nyilvántartásokon és határozatokon szűrik át. Ez a zárt, a világtól elvágott, minden pontján ellenőrzött tér, ahol az egyének kijelölt helyhez vannak szögezve, ahol a legkisebb mozdulatot is ellenőrzik, minden eseményt följegyeznek, ahol a hatalom megosztatlan, folyamatos, hierarchikus alakzatban működik, ahol minden egyént állandóan kijelölnek, megvizsgálják és besorolják az élők, a betegek és a halottak csoportjaiba – ebből áll össze a fegyelmező gépezet tömör modellje. Mindenkinek előírja, hol a helye, melyik a teste, milyen a betegsége és a halála, mi a java. A leprás száműzetése és a pestis helyhez kötése nem ugyanabból a politikai ábrándképből fakad. Az egyik az egynemű közösség, a másik a fegyelmezett társadalom álma.”

A járvány sújtotta, totálisan ellenőrzött tér a maga megrettent lakóival – épp ez „a demokrácián túli” hatalom ábrándja.

*

A leprát – hivatalos nevén a Hansen-kórt, magyarul a bélpoklot – évszázadok óta radikális elkülönítéssel tartják távol a normalitás világától, jóllehet ez az egyik legkevésbé fertőző betegség. Bár az Egészségügyi Világszervezetnek az évezredfordulóra sikerült a kórt gyakorlatilag megfékeznie, 2013-ban még mindig mintegy 200 ezer új esetet regisztráltak világszerte. A betegeket ma is elkülönített telepekre száműzik, mint amilyen az indiai Újdelhi melletti Tahirpur, „a Remény

falva”, vagy a „Nemzeti Szanatórium” Ooshimán, a Japán-tenger egyik távoli, viharoktól gyakran tépázott szigetén, vagy a romániai Tichilești elkülönítő Isacceában, a Duna deltájában.

A lepratelepen a gettóba zártak státusa, helyzete egynemű; nincsen folyamatos megfigyelés, belső felügyelet, személyre szabott regula – a lényeg az elzárás, a bezárás, a kizárás. A cigánytelepek fenntartása, a hajléktalanok kiszorítása, hajléktalanszállókba terelése is ezt a szegregációs logikát követi.

A karanténban – és ezt A londoni pestis, Daniel Defoe 1665-ös dokumentumregénye óta tudjuk – folyamatosan, minden pillanatban, mindenki számára érezhető módon van jelen a hatalom. Mindent és mindenkit megfigyel, számon tart és elkülönít. A hét hónapig tartó londoni bubópestis 200 ezer áldozatot követelt; a járványnak vélhetőleg csak az 1666. szeptemberi nagy tűzvész vetett véget, amely elpusztította a kórt terjesztő patkányok és egyéb kórokozók többségét. A 800 ezer lakosú Londonban a magiszterek, szindikusok, felügyelők éppúgy részletes ismeretekkel rendelkeztek a rájuk bízott városrész lakosságáról, mint ma a hatóságok a 11 millió lakosú Vuhanban, Kína kilencedik legnépesebb városában.

Nem könnyű egy 11 milliós óriás várost működtetni, vesztegzár idején fenntartani a rendet, betartatni a szigorú utasításokat. A Pentagon alá tartozó Joint Special Operations University 2016-ban videót készítettett Megavárosok: az urbánus jövő, a mind nagyobb komplexitás címmel. A 2030-ra elképzelt disztópikus jövőt, az elképzeltetlen vagyoni egyenlőtlenséget, nyomort, szeméthegeket, rettegő gazdagokat, elviselhetetlen lakósűrűséget, szétrohadt infrastruktúrát, erőszakot, digitális terrorizmust bemutató filmet a Terrorista fenyegetés című kurzus hallgatóinak mutatták be. A film szerint a hadsereg legmodernebb eszközökkel rendelkező elit egysége sincs felkészülve a megavárosokban fenyegető káoszra. Mégis, a terrorelhárító központ az egyetlen remény.

Kína azonban más eszközöket talált e társadalmi problémák kezelésére.

*

A kínai állam 1998-ban indította el az Arany Pajzs programot. Ekkor még az a naiv elképzelés élt a világban, hogy az internet az alulról jövő demokratikus kezdeményezések, a civil társadalom, az egyéni szabadság megvédésének eszköze lesz az autokratikus uralmi törekvésekkel szemben. Az Arany Pajzs eredetileg defenzív célokat szolgált: ez lett volna a „nagy kínai tűzfal”, amely megszüri az

interneten terjedő tartalmakat, és felállítja a digitális cenzúrát. De a rendszer arra is lehetőséget teremtett a közbiztonsági minisztérium számára, hogy végre ne csupán az informátorok jelentéseiből, hanem a legmodernebb technológia segítségével szerezzon információt a lakosságról. Ekkor kezdett kiépülni a ma már állítólag több mint százmillió köztéri kamerával működő, biometrikus adatok továbbítására, arc- és hangfelismerésre képes rendszer.

Kínában egy évtizeddel ezelőtt kezdett terjedni a mobiltelefonos fizetés. Az Alibaba, a Google kínai megfelelője bevezette az Alipay rendszert, a több százmillió felhasználóval rendelkező Tencent üzenetküldő megnyitotta WeChat Pay szolgáltatását. Ma már a fizetések többségét mobiltelefonnal bonyolítják le – évi több mint 3,5 billiónyi tranzakciót.

Az Alibaba pénzügyi leányvállalata a Szezám hitel(pont) rendszert működteti. (Ez a név is az Ali baba mesére utal.) A Szezám nem csupán pénzügyi szolgáltatás. Az applikációt letöltő minden ügyfél – ma már sok százmilliónyian – „megbízhatósági pontszámot” kap 350 és 950 pont közt. Az ezt kiszámoló algoritmus figyelembe veszi a felhasználó hitel-visszafizetési történetét, anyagi és társadalmi helyzetét, családi állapotát (házasok és gyerekesek előnyben), vásárlási szokásait, rokonainak, ismerőseinek társadalmi, anyagi helyzetét, közüzemi díjfizetési megbízhatóságát és politikai megbízhatóságát. A Szezám a pénzügyintézeteken és az üzleteken, taxivállalatokon, szállodaláncokon, utazási szolgáltatókon kívül nem csak a Tinder résztulajdonában lévő Zhenai.com társskereső portállal áll kapcsolatban, de az állami közműszolgáltatókkal és a rendőrségi és bírósági adatbázisokkal is. Nem csupán kereskedelmi szolgáltatás ez, hanem olyan komplex rendszer, amely a magáncégeket állami intézményekkel és rendvédelmi szervekkel köti össze, és összekapcsolja a kereskedelmi, adminisztratív és állambiztonsági adatbázisokat. Az Alibaba és Tencent vezetője tagja a kínai internetet felügyelő állami bizottság igazgatótanácsának.

Az ügyfél hiteltörlesztési, díjfizetési késlekedése a hitelpontszám csökkentését vonja maga után. Alacsony pontszámmal nem lehet hitelhez jutni, vonatjegyet vásárolni, szállodai szobát foglalni, autót bérelni – de még biciklit sem. Hétszáz pont felett viszont nem szükséges a letét az autóbérléshez, soron kívül lehet kórházi vizsgálatokhoz jutni, engedélyt szerezni a schengeni vízum igényléséhez, és jár a VIP-folyosó is a repülőtéri biztonsági kapuhoz. (Ez utóbbi luxust Magyarországon is igénybe vehetik bizonyos bankok fekete, „platina” hitelkártyával rendelkező ügyfelei.) Az adatbázis összeköttetésben áll az ügyfél mobilszámával, így telefonos szolgáltatások esetén a rendszer a magas pontszámmal rendelkező ügyfelet

automatikusan előresorolja, a többieket pedig várakoztatja: „türelmét kérjük, minden munkatársunk foglalt”. Az Alibaba 2016-ban Körök néven új alkalmazást kínált társat kereső nők számára – mely kizárólag 750 feletti Szezám-ponttal rendelkező férfiak számára volt elérhető. A szolgáltatás, a prostitúció nemkívánatos növekedését megakadályozandó, rövid idő múltán elérhetetlenné vált.

A Szezám-pontoknak kialakult feketepiacra van, sőt hamis Szezám-identitást is lehet vásárolni. Amiképpen Amerikában, Kínában is megjelentek a „reputáció tanácsadók”, akik nemcsak az Instagram-, YouTube-, Facebook- és TikTok-fiókok kezelésében igazítják el ügyfeleiket, hanem a Szezám-pontok feltornászásának leghatékonyabb eszközeibe is beavatják őket. A pontszámokat nem csupán a felhasználó viselkedése alakítja. Számít, hogy mit mondanak, hogyan vélekednek róla ismerősei az interneten, hogy kikkel, milyen státuszú, mennyire megbízható emberekkel áll kapcsolatban. Ezért a felhasználó jobban teszi, ha megválogatja a barátait; ha kell, lecseréli vagy letiltja a régi ismerősöket, netán új életet kezd.

A koronavírus-járvány kitörésekor az Alipay rendszer új szolgáltatást dobott piacra. Az Egészség Kód először a kelet-kínai Hangcsouban vált elérhetővé, de a „kontakt mátrix” ma már a legtöbb kínai városban letölthető. A pénzügyi tranzakciókhoz kapcsolódó alkalmazás tudatja a felhasználóval, hogy az elmúlt időszakban regisztrált mozgása, érintkezései alapján piros, sárga vagy zöld csoportba tartozik-e – azaz a fertőzöttek, a veszélyeztetettek vagy az ártalmatlanok közé. Amint az ügyfél letölti a szoftvert, a háttérben futó „reportInfoÉshelymeghatározásARendőrségnek” nevű program – a felhasználó értesítése nélkül – elküldi telefon- és személyi számát a hatóságoknak. A besorolás alapján azután a rendszer közli a betartandó előírásokat. Hasonló, bár kétségtelenül kevésbé szofisztikált rendszer működött a 18. század végén Poroszországban, Medizinische Policey néven.

A 2014-ben bejelentett „társadalmi kreditrendszernek” ez évtől kellene országosan működnie. A világjárvány bizonyára meggyorsítja és könnyebben elfogadhatóvá teszi bevezetését. A történelmi tapasztalat azt sugallja, hogy a nagy válságok – és a koronavírus-pandémia kétségtelenül ilyen – az autokratikus rendszerek megerősödésének kedveznek. Mindazonáltal érdemes elgondolkodni az élelmiszerimportra szoruló Nagy-Britannia példáján, amely a napóleoni háborúkat követő válságos időkben kényszerintézkedések nélkül, demokratikus úton is képes volt megoldani a lakosság ellátását; s így működött a II. világháborúban, a Blitz idején is.

*

A digitális ellenőrzés és felügyelet magyarországi állapotáról a laikus állampolgár igen kevés információval rendelkezhet. Magyarországon ma vészhelyzet van, miközben pár megyében még a „tömeges bevándorlás okozta válsághelyzet” is érvényben van; ezt legutóbb 2019. szeptember elején hosszabbította meg újabb fél évvel a kormány. Az pedig 2018 októberében, az Egyes belügyi tárgyú és más kapcsolódó törvények módosításáról, azaz egy újabb salátatörvényről folyó parlamenti vita során vált nyilvánvalóvá, hogy a kormány az ún. **Szitakötő rendszer** bevezetésére készül. Az ártatlannak hangzó program keretében összekapcsolnák a térfelügyelő kamerákat, sőt a közterületi hangfelvételeket is, a felvételeket pedig egységes tárhelyen őriznék, ahonnan az adatokat az erre felhatalmazott hatóságok bűnüldözési, nemzetbiztonsági, bűnmegelőzési, illetve közlekedésszervezési célokra kérhetik majd ki. (Erről lásd korábbi cikkünket: A NER-testvér szemmel tart, Magyar Narancs, 2019. február 14.) A tervezet olyannyira ellentétes volt az Alaptörvény szövegével, hogy még Péterfalvi Attila, a Nemzeti Adatvédelmi és Információszabadság Hatóság elnöke is arra kényszerült, hogy 2018. október 1-jén levélben tudassa súlyos aggályait Felkai Lászlóval, a Belügyminisztérium államtitkárával. A NAIH szerint a Szitakötő projekt „egy az ország valamennyi településén jelen lévő, egységes központosított rendszerbe szervezett, a közterületeken tartózkodók, a közlekedők és a tömegközlekedési eszközökön utazók intenzív és tömeges megfigyelését lehetővé tevő képi megfigyelőrendszer létrehozására vonatkozik. A következő adatok érzékeltetik a tervezett megfigyelőrendszer nagyságrendjét: **35 000 kamera képfolyamainak folyamatos gyűjtése a Kormányzati Adatközpontban, 25 000 TByte megfigyelési adat folyamatos kezelése** és (a településeknél megjelenő további költségeket leszámítva) központi szinten legalább 50 milliárd forint közpénz elköltése mindennek megvalósítása érdekében. A normaszöveg a lehető legáltalánosabb módon a gyűjtött adatok »felhasználására« ad lehetőséget, amibe a mindenkori technikai lehetőségek függvényében bármely felhasználási mód beleérthető a képfolyam egyidejű, ember általi megfigyelésétől kezdve a képállományok lementésén vagy más rendszerbe való áttöltésén keresztül akár a megfigyelt személyek automatikus biometrikus azonosításáig, mozgásának követéséig, továbbá viselkedési, valamint kapcsolati profiljának feltérképezéséig.”

Nincs hozzáférhető információ a tervezett rendszer állapotáról, de a Nemzeti Infokommunikációs Zrt. által 2019. február 18-án közzétett „Közbeszerzési terv” tartalmazza a „Szitakötő projekt országos kiterjesztését megalapozó tanulmány” elkészítésére vonatkozó szándékot, valamint a Szitakötő rendszer fejlesztését szolgáló, Az Integrált Közlekedésszervezési és Szabályozási Rendszer közbiztonsági,

közlekedésbiztonsági, rendvédelmi célú informatikai fejlesztése című dokumentumot.

<https://magyarnarancs.hu/belpol/a-ner-testver-szemmel-tart-117270>

A Szitakötő-projekt és csatolt részei

A NER-testvér szemmel tart: jön a totális megfigyelés?

Szalai Anna 2019.03.24 19:10

A személyes és vagyoni adatokon túl központi tárhelyre gyűjtik az egészségügyi állapotra és a szálláshelybérlésre vonatkozó információkat is. A Szitakötő-rendszer bevezetése után majdnem minden lépésünkről tudni fog az állam.

Kormányzati kémszoftverként működik a két évvel ezelőtt létrehozott Elektronikus Egészségügyi Szolgáltatási Tér (EESZT) – fogalmaz meglehetősen sarkosan Alexin Zoltán adatvédelmi szakértő.

Advertisement

Állítja, a magyar rendőrségnek, az ügyészségnek, a bíróságnak és több más állami hatóságnak lényegében korlátlan hozzáférése van a rendszerbe feltöltött egészségügyi adatokhoz. A 2017-es bevezetés óta minden állami, sőt a múlt évtől bizonyos magánegészségügyi intézményben tett látogatásunkat naplózzák, beleértve a kért vizsgálatokat, azok eredményeit, a kezelést és a recepteket is.

Így egy helyen megtalálható a teljes egészségügyi profilunk, kórtörténetünk, jól kiolvashatóak belőle orvoslátogatási szokásaink, gyengeségeink (például a cigarettázás), krónikus betegségeink, a terméketlenség, a fogyatékoság, a korábbi műtétek, balesetek. Sőt még az is, hogy a felírt gyógyszert kiváltottuk-e. Szabó Bálint, az Állami Egészségügyi Ellátó Központ fejlesztésért felelős főosztályvezetőjének közlése szerint tavaly októberben már több mint 500 millió egészségügyi dokumentum volt elérhető az EESZT-ben.

A rendszer alapbeállításaként kezelőorvosunk, háziorvosunk, sőt üzemorvosunk is szinte minden adatunkhoz hozzáfér. (Néhány kivétel van csupán: a HIV/AIDS

státusra, a szexuális úton terjedő megbetegedésekre, a pszichiátriai, addiktológiai kezelésekre vonatkozó adatokat csak a szakorvos ismerheti.)

Bár az ügyfélkapun keresztül elérhető elektronikus felületen bizonyos hozzáféréseket letilthatunk, ehhez olyan fokú adatvédelmi tudatosságra van szükség, amely nálunk nem jellemző. Másrészt az orvosoknak van egy „sürgősség gombja”, amellyel valamennyi korlátozás felülírható – mondja Alexin Zoltán, bár azt ő sem tagadja, hogy az EESZT egészségügyi krízishelyzetekben igen jó szolgálatot tehet. Az is a rendszer javára írandó, hogy nem kell minden korábbi zárójelentést és ambulánslapot megőrizni, hiszen ezt megteszi az EESZT. A rendszer ugyanakkor nem küld e-mail-értesítést arról, hogy ki és milyen adatokat kért le rólunk.

Az Orbán-kormány 2015-ben teljes hozzáférést biztosított a nyomozó hatóságoknak a Nemzeti Egészségbiztosítási Alapkezelő (NEAK) elődjénél, az OEP-nél tárolt egészségügyi adatokhoz. A jogszabályi felhatalmazás alapján a rendőrség hamar rákapott arra, hogy a központi adatállományból lekérje egy-egy állampolgár egészségügyi adatait. Alexin tavaly nyár végén közérdekű adatigénylés formájában kikérte a NEAK-tól az ilyesfajta lekérések számát; a válaszból kiderült, hogy a törvény elfogadásának évében 4800 alkalommal éltek a lehetőséggel a nyomozó hatóságok, 2017-ben pedig 13 ezernél is többször.

Az Európai Unió általános adatvédelmi rendelete (GDPR) lehetővé tette az adatok törlésének kezdeményezését, és a bírósági jogorvoslatot az állami adatkezelésekkel szemben, de Alexin szerint ennek egyelőre nincs nyoma Magyarországon. A tavaly májusi bevezetés óta csak az adatvédelmi törvényt módosították, holott a GDPR előírásaival nem teljesen megfelelő adatkezelés további, nagyjából 700 jogszabályban, rendeletben szerepel. Ezek közül 50-et most egy csokorba szedtek, az erről szóló salátatörvényt várhatóan tavasszal tárgyalja az Országgyűlés.

Az EESZT haladó és előremutató fejlesztés, amely adott esetben akár életmentő is lehet – érvel Asbóth Márton, a Társaság a Szabadságjogokért (TASZ) magánszféraprojektjének vezetője, mondván, a rendszer törvényi felhatalmazáson alapul. Igaz, a rendszer szerinte sem kellően titkosított, sokkal megnyugtatóbb lenne, ha az adatokhoz csak az állampolgár hozzájárulása után férhetne hozzá akár a háziorvosa is.

Erre kiválóan alkalmas lenne az e-személyi, amely már tartalmazza a tájszámot is – az adatok így csak az egyedi PIN-kód megadásával lennének elérhetőek. Péterfalvi Attila, a Nemzeti Adatvédelmi és Információszabadság Hivatal (NAIH) elnöke

szerint az esetenkénti engedélyezés tényleg jobban szolgálná a személyes adatok védelmét, de adott esetben jelentős egészségügyi kockázattal is járhatna. A GDPR egyébként számos felhatalmazást ad a tagállamoknak a kötelező adatkezelés előírására.

Hol, mikor, kivel

Az érzékeny adataink esetleges laza kezelése miatti aggodalom az e-személyi bevezetések befurakodott sokakba, és ezt csak táplálta az elektronikus személyi igazolványok utazási kártyaként való bevetésének ötlete.

A rendszer pilotprogramja már fut Debrecenben; az e-személyi a használó azonosítását szolgálja, az utazás díját pedig a kártya mögé rendelt virtuális számláról emelik le. A megoldás jelentősen leegyszerűsíti a közlekedők életét, hiszen nem kell külön bérletet, jegyet váltani. De az orwelli örökös megfigyeléstől tartó állampolgárok gyomra könnyen összerándulhat emiatt.

A kártyafunkció bővítésével ugyanis nemcsak a használó személyes adatairól, adóazonosítója révén a vagyoni helyzetéről, a tajszáma alapján pedig a betegségeiről kaphat képet a mindenkori hatalom, hanem arról is könnyen térképet rajzolhat, hogy merre jár. Asbóth szerint az e-személyi alkalmas arra, hogy az utazási jogosultság megvásárlásakor egyedi azonosító képződjön, ami csak az e-személyi felhasználásával együtt teszi lehetővé a személyazonosítást. Az ombudsmannak – bár tett erre ajánlást – nincs tudomása arról, hogy az elektronikus jegyrendszer lehetővé teszi-e majd az anonim kártyahasználatot.

Az egységes, személyi számon nyugvó állami adatbázisok szétválasztása a rendszerváltás egyik vívmánya volt. Később az adó- és a tajszámot is tartalmazó azonosító kártya bevezetésére a Medgyessy-kormány kísérletet tett, de a terv már a kabinetben belül elbukott. Az Orbán-kormány azonban végigvitte ezt: a 2015-ös javaslat nem mellékesen arra is vonatkozott, hogy egy adott személy különböző (idegenrendészeti, lakcímnnyilvántartó, adóhivatali, társadalombiztosítási, közlekedésrendészeti, rendőrségi) nyilvántartásokban szereplő adatait „az azonosítóhoz tartozó titkosított kapcsolati kódon keresztül” a korábbinál egyszerűbben összekapcsolhatóvá kell tenni.

Az adatvédelmi aggályokra az a hivatalos válasz, hogy a kártyán szereplő azonosítók segítségével elérhető összes adathoz senki nem férhet hozzá egyben. Mindenre külön kapcsolati kódokat hoznak létre, amelyek sehol sem érnek össze; csakhogy ezeket az adott hatóság képezi a saját szoftverével.

Mi arra a biztosíték – teszi fel a kérdést Alexin Zoltán –, hogy nem fejtí azt vissza, amikor arra szüksége van? Ráadásul bármilyen elektronikus rendszert fel lehet törni, napjaink tömeges adatlopásai ékes bizonyosságul szolgálnak erre. Másrészt az Országgyűlés bármikor adhat törvényi felhatalmazást a három azonosító együttes eléréséhez, még ha ez ellentétes lenne is az Alkotmánybíróság korábbi határozatával. Az állampolgár viszont nem választhat: akinek lejár a személyije, az automatikusan e-személyit kap. A Belügyminisztérium (BM) tájékoztatása szerint január végéig valamivel több mint 4 millió plastiklapot adtak ki, míg a régi típusú személyiből még 4,8 millió darab van érvényben.

Abszolút biztonságot egyetlen elektronikus információs rendszer sem tesz lehetővé. A „megfigyelési társadalom” kialakulását elsősorban nem a technológiai innováció, hanem a társadalmak demokratikus fejlődése, az adatbiztonsági garanciákra kiterjedő jogi szabályozás akadályozhatja meg – magyarázza Péterfalvi Attila, aki szerint a GDPR köti a tagállami jogalkotókat. Aki pedig valamely adatkezelést sérelmesnek talál, a NAIH-hoz és a bírósághoz fordulhat.

A NER-testvér mindenesetre egyre kíváncsibb. A módosított turizmustörvény idén januártól lépcsőzetesen kötelezővé teszi a szállásadóknak, hogy a náluk tartózkodó vendégek személyes adatait (nevét, születési idejét és úti okmánya adatait) továbbítsák a Nemzeti Turisztikai Adatszolgáltató Központ (NTAK) tárhelyére, ahol ahhoz hozzáférhetnek az önkormányzatok, a NAV, a rendőrség, az idegenrendészet és a KSH.

Az NTAK létrehozását idegenrendészeti okokkal, az adminisztrációs terhek csökkentésének és a szürkegazdaság fehérítésének céljával is indokolták. Guller Zoltán, a Magyar Turisztikai Ügynökség (MTÜ) vezérigazgatója mindenesetre tagadta a Magyar Időknek, hogy a vendégekkel kapcsolatos bármilyen személyes adatot tárolnának vagy kezelnének. Állítása szerint csak statisztikákat állítanak össze.

Ám az NTAK csupán az egyik célpontja az adatok továbbításának. Az érintett törvény másik módosítása szerint a szállásadó rögzítette adatait az NTAK-hoz is használt szoftver automatikusan feltölti egy olyan tárhelyre, ahol nemcsak a szállásadó, hanem a rendőrség is közvetlenül hozzáfér az információkhoz – hívja fel a figyelmet a balatontipp.hu. Amennyiben a rendőrség részletes adatokra lenne kíváncsi, a cél megjelölésével adatszolgáltatást kérhet.

A NAIH Magyar Narancsnak küldött válasza szerint az NTAK-nál valóban csak

deperszonalizált adatokat gyűjtene, míg a rendőrség kétlépcsős adatigényléssel juthat információhoz. A központi nyilvántartás csupán arra ad választ, hogy a keresett személy hol szállt meg; viszont további adatok kérhetők a szállásadótól, s ő erre kérésre köteles válaszolni.

Tavaly novemberben ennél jóval nagyobb vihart kavart egy elsőre ártalmatlannak tűnő salátatörvény. Az egyes belügyi tárgyú és más kapcsolódó törvények módosításáról szóló jogszabályban sok minden mellett egy közterületi kamerarendszer kiépítéséről, illetve az azzal gyűjtött adatok központi tárhelyre való felöltéséről is rendelkeztek.

Felröppen

Az ellenzéki vezérszónokok egymást túllicítálva sorolták aggályaikat. Vadai Ágnes (DK) szerint ezzel a törvénnyel a hatalom egyetlen dolgot szeretne elérni: azt, hogy minél többeket ellenőrizhessenek, „nyomon követhessék, hogy a rendszerrel, az Orbán-rezsimmel szemben állók milyen módon, kivel beszélgetnek, kivel találkoznak. Mára ott tartunk, hogy lényegében a magánlakás lesz az egyetlen olyan hely, ahol önökkel szemben szerveződni lehet”. Vadai arra is emlékeztette a kormánypárti képviselőket, hogy 2014-ben a rendészeti bizottság vitájában éppen a Fidesz két képviselője ágált a legjobban a józsefvárosi kamerarendszer kiépítése és a kamerák összekapcsolása ellen. Kósa Lajos és Bíró Márk akkor úgy vélte, hogy ez „nagy mértékben érinti a magyar polgárok adatvédelmi igényeit”. Ehhez képest a gyakorlatot most nem egy kerületre, hanem a fővárosra, majd az egész országra kiterjesztenék.

Konrád Károly, a BM államtitkára válaszában lényegében elismerte, hogy a kamerarendszer kapcsán nem készült előzetes hatástanulmány, de ezt azzal üttötte el, hogy az önkormányzatok már eddig is működtettek térfigyelőket. Szerinte annyi változik, hogy ezentúl nem a helyhatóságok, hanem a rendőrség dönt a kamerák felhelyezéséről, az adatkezelés törvényességi garanciáját pedig a NAIH jelenti.

Ehhez képest Péterfalvi Attila NAIH-elnöknek a HVG által megszellőztetett leveléből az derült ki, hogy a hivatalnak eleinte fogalma sem volt arról, mekkora rendszert hozna létre a BM. Az egyeztetések során aztán kirajzolódott, hogy „az ún. Szitakötő-projekt egy, az ország valamennyi településén jelen lévő, egységes központosított rendszerbe szervezett, a közterületeken tartózkodók, a közlekedők és a tömegközlekedési eszközökön utazók intenzív és tömeges megfigyelését lehetővé tévő képi megfigyelő rendszer létrehozását” célozza. A tervezethez csatolt

költségvetési mellékletből pedig az is tudható, hogy „35 ezer kamera képfolyamainak folyamatos gyűjtése valósulna meg a Kormányzati Adatközpontban.

A 25 ezer terabájt megfigyelési adat folyamatos kezelése központi szinten 50 milliárd forint közpénz elköltését jelentené, és erre még rájönne a településeknél megjelenő, megsaccolhatatlan összegű további költség”. A cikk megjelenése után Péterfalvi gyorsan kiadott egy közleményt, miszerint megállapításai egy korábbi tervezetre vonatkoztak, észrevételeit azóta a BM beépítette a szövegbe. Így bekerült az a kitétel is, miszerint a felvételek hozzáférhetővé tételéről továbbra is a kameraképeket feltöltő dönthet. A Magyar Narancsnak még azt is hozzátette, sajnálatosnak tartja ugyanakkor, hogy „a megfigyeléshez kapcsolódó »hallgatóság« újraszabályozására nem került sor, mint ahogy az adatfelhasználás lehetséges módozatainak differenciált szabályozására sem”.

Érdeemes beleolvasni Péterfalvi egy másik levelébe is, amelyben az okosváros központi platformszolgáltatás létrehozásáról és működtetéséről szóló kormányrendelet tervezetére reagált tavaly november 16-án (kormányrendeletként ez nem került a parlament elé, így az ellenzéki képviselők nem is akadékoskodhattak). A NAIH elnöke ebben arról ír, hogy a Szitakötő-projektről szóló előterjesztésben még nem volt szó arról, hogy az „országos léptékű, folyamatosan működő megfigyelőrendszer biometrikus technológiát fog alkalmazni. Csak a monori okosváros projektről szóló előterjesztésben jelent meg az az utalás, hogy a központi megfigyelőrendszerbe esetleg automatikus arcaazonosítási képesség lesz integrálva”. Péterfalvi felhívja a figyelmet, hogy a közterületen közlekedők nem képesek arról dönteni, hogy biometrikus adataikat kezeljék-e, valós időben őket felismerjék-e. Hiányoznak ehhez az alkotmányos garanciák, és a tervezet a GDPR szabályainak sem felelne meg.

Behálózás

A Belügyminisztérium lapunk érdeklődésére azt válaszolta, hogy „nem jön létre egyetlen »közös« kamerarendszer, minden érintett szerv felvételeit külön tárolja a tárhelyszolgáltató, amely a tárolt adatokat nem ismerheti meg, azokon semmiféle műveletet (gyűjtés, rendszerezés, lekérdezés, továbbítás, nyilvánosságra hozatal, összekapcsolás, törlés stb.) nem végezhet. A jogszabály csak az egyedi informatikai alkalmazást biztosító adatkezelést teszi lehetővé, amelynek révén egyszerűsödik, gyorsul, hatékonyabbá válik az adatmegismerés”. Ezek szerint tehát a kamerarendszereket külön működtetik, de az adatokat egy közös kormányzati tárhelyre töltik fel.

A felvételeket a korábbi 5–15 nap helyett 30 napig őrzik a BM szerint a „nyomozáseredményesség” növelése érdekében, de a kameraképek csak az adatgazda engedélyével válnak hozzáférhetővé a nyomozó szervek részére. Az adatgazda pedig minden esetben az érintett kamerákat üzemeltető szervezet. Csakhogy a felvételeket immár nem csupán nyomozáshoz kérhetik ki, hanem bűnmegelőzési célból is. „Ebbe pedig nagyon sok minden beletartozhat” – hangsúlyozza Asbóth Márton, aki szerint az adatok készletezése semmiképpen nem elfogadható. A megelőzéshez előben kellene követni az eseményeket, hogy azonnal reagálhassanak rá – ez viszont aligha kivitelezhető.

A BM által a Narancsnak küldött válaszban felhívta a figyelmet, hogy a törvény semmilyen rendelkezést nem tartalmaz a jelenleg üzemelő térfigyelő kamerák bővítéséről, felszerelésének üteméről. Tényleg nem – ám van néhány árulkodó szerződés és közbeszerzés, ami erre utal. Mint arról korábban beszámoltunk (lásd: Csak belépővel!, Magyar Narancs, 2018. november 15.), a Budapest Közút Zrt. 2015-ben uniós forrásokból fejlesztette ki az Integrált Közlekedésszervezési és Szabályozási Rendszerét (IKSZR), ennek keretében 400 térfigyelő kamerát helyezett el, amelyek közül 110 rendszámleolvasásra is alkalmas. (Londonban 197 kamera van, Milánóban 43.)

A Fővárosi Közgyűlés adatvédelmi okokra hivatkozva a Fővárosi Önkormányzati Rendészeti Igazgatóságra (FÖRI) testálta a rendszer működtetését. 2017 decemberében a Budapest Közút, a FÖRI és az állami Nemzeti Infokommunikációs Szolgáltató (NISZ) Zrt. (ezt az állami céget jelölte ki tavaly a BM a térfigyelő kamerák központi tárhelyének is) szerződést kötött az IKSZR-nek a NISZ rendszerébe illesztéséről. 2017 márciusában az IKSZR szoftverfejlesztője, a GVSX Szolgáltató Kft., illetve a FÖRI és a Budapesti Rendőr-főkapitányság (BRFK) megállapodott a szoftver használati jogainak átadásáról, majd júliusban a BRFK hirdetmény nélküli tárgyalásos eljárás keretében a GVSX-et bízta meg az IKSZR-nek a Szitakötő-rendszerbe, illetve a Központi Adatközpont (KAK) felhőjébe illesztésével.

A cél az, hogy a közterületeken lévő kamerák adatai egyetlen központi adattárba fussanak be, és a rendszer alkalmassá váljon a célzott keresésre: mikor és melyik mérőpont alatt haladt el a meghatározott rendszámú autó, és a rendszer természetesen megadja a rendszámhoz kötődő adatokat is.

A Pintér Sándor miniszter által szorgalmazott rendszer a 24.hu információi szerint az

önkormányzatoknál használtaknál sokkal nagyobb felbontású, **minimum 16 megapixeles kamerákat használ majd,** amelyek felvételei rendszám- és arcfelismerő programok futtatására is alkalmasak. A rendszer magába foglalja majd a közútfenntartók, az önkormányzatok, a közlekedési vállalatok és a pénzügyintézetek utakon, állomásokon, köztereken, intézményekben kihelyezett kameráit. A Szitakötő-rendszert több lépcsőben valósítanák meg.

Az első a fent említett fővárosi IKSZR beépítése a rendszerbe; ezt követné Budapest, majd a megyei jogú városok és végül az ország többi településének bekamerázása. A teljes hálózat két év alatt épülne ki. Ezután elég lesz a különböző, már most meglévő, külön futó adatgyűjtő rendszereket összekapcsolni a teljes profilképzéshez.