Szénay Márta

SurPRISE – rendhagyó közvélemény-kutatás a biztonságról, a megfigyelésről és a magánszféráról[1]

A SurPRISE projekt keretében szervezett állampolgári konzultációkon (lásd a keretes írást) e tanulmány olvasója is részt vehetett volna. Olvashatott volna, sőt ismeretterjesztő filmeket is megnézhetett volna a megfigyelésen alapuló biztonsági technológiákról, amelyek fő célja, hogy felhívják a figyelmet valamilyen biztonságot veszélyeztető eseményre, ami ezáltal kivédhetővé, megelőzhetővé válik. Mivel nem tudható, ki, mikor, milyen terror- vagy bűncselekményre készül, de az igen, hogy a jövőbeli elkövetők közöttünk járnak, hozzánk hasonlóan vásárolnak, utaznak, használják az internetet és a mobiltelefonjukat, ezért ezek a biztonsági technológiák mindenkiről – így rólunk is – folyamatosan gyűjtik az adatokat és elemzik annak érdekében, hogy egy esetleges fenyegetést időben leleplezzenek. A New York-i ikertornyok ellen 2001. szeptember 11-én végrehajtott terrortámadást követően a mindenkire kiterjedő megfigyelés soha nem látott ütemben kezdett terjedni. A változás nem csak mennyiségi volt: a biztonsági ipar ezen ágazatának felpörgése azóta is szinte hónapról hónapra produkálja az egyre szofisztikáltabb technológiai megoldásokat.

Ezeken az állampolgári konzultációkon a résztvevők arról beszélgettek, hogy mit gondolnak erről a megfigyelésről: örülnek-e neki, mert ettől valóban nagyobb biztonságban érzik magukat, vagy éppen zavarja őket, és nem is igazán tartják e technológiákat hatékony megoldásnak a bűnelkövetők megfékezésére. Milyen igényeik, elvárásaik lennének azokkal szemben, akik a megfigyeléseket végzik, akik az emberekről – rólunk – a rengeteg adatot

1 A tanulmány a SurPRISE projekt honlapján elérhető (http://surprise-project.eu/dissemination/research-results/) következő kutatási jelentések megállapításaira épített: D2.4. Pavone, V., Degli-Esposti, S. and Santiago, E. (2015): Key factors affecting public acceptance and acceptability of SOSTs D6.4. Körmöczi, A., Szénay, M. and Venczel, T. (2014): Country report – Hungary D6.10. Strauss, S. (2015): Synthesis report of the large scale events D7.2. Szénay, M. (2015): Comparative report of the small scale events.

összegyűjtik, tárolják és elemzik. Egyáltalán: lehet-e tudni, kik a megfigyelők és mi történik az összegyűjtött információkkal.[2]

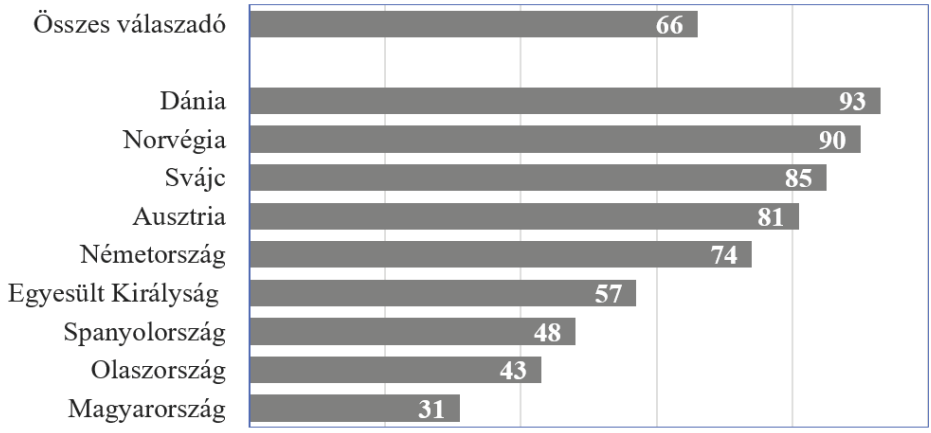
Tanulmányunkban ismertetjük a kutatás legfontosabb eredményeit, az állampolgári konzultációk résztvevőinek véleményét és az abból kirajzolódó igényeket, amelyek tanulságosak lehetnek a döntéshozók számára.

Biztonságérzet az európai országokban

Az ország békéjének, a lakosság biztonságának garantálása minden politikai hatalom számára kiemelt prioritású feladat. Azonban az, hogy az emberek mennyire érzik magukat biztonságban egy adott országban, sok mindentől függ, sokszor nem is csak az objektív biztonsági helyzettől, hanem például attól is, hogy milyen az ország kultúrája, polgárai mennyire szeretnék „bebiztosítani" a jövőjüket.

Először nézzük meg, hogy a kilenc európai országban3 hogyan válaszoltak az állampolgári konzultációk résztvevői arra a kérdésre, hogy országukban biztonságban lehet-e élni:

1. ábra. „Úgy érzem, ebben az országban biztonságban lehet élni" – az állítással egyetértők aránya százalékban; N=1780



(Saját szerkesztés)

2 Aki úgy érzi, hogy – hasonlóan azok nagy részéhez, akik az állampolgári konzultációkon részt vettek – nem eléggé tájékozott, nem tudja, pontosan miről is van szó, melyek ezek a technológiák és mire valók, tekintse meg a konzultációk résztvevői számára készült, magyar nyelvre is lefordított információs magazinokat és szinkronizált ismeretterjesztő filmeket a kutatás nemzetközi honlapján: http://surprise-project.eu/dissemination/information-material-from-the-participatory-events.

3 A kutatásban részt vevő országok: Ausztria, Dánia, Egyesült Királyság, Magyarország, Németország, Norvégia, Olaszország, Spanyolország, Svájc.

2014-ben, amikor a konzultációkra sor került, a kutatásban részt vevő kilenc ország lakosságának pontosan a kétharmada (66%) érezte úgy, hogy hazájában biztonságban lehet élni *(1. ábra).* Azonban a biztonságérzet országonként jelentős eltéréseket mutatott. A két skandináv országban, Norvégiában és Dániában szinte alig akadt olyan, akik ne érezte volna országát biztonságos helynek. Nem ingatta meg ezt a biztonságba vetett bizalmat az sem, hogy 2011-ben – tehát alig három évvel a kutatást megelőzően – Norvégiát az ország történetének legsúlyosabb terrortámadása érte, amely közel 80 halálos áldozatot követelt, és amit egy szélsőjobboldali nacionalista, Anders Behring Breivik követett el. A dán résztvevőkben szavak szintjén felmerült, hogy Dánia aktív katonai részvétele a terrorizmus elleni harcban esetleg biztonsági kockázati tényező lehet, de ez csak halvány aggodalomnak bizonyult, ami szintén nem jelent meg a biztonsággal kapcsolatban feltett kérdésre adott válaszokban: az állampolgári konzultáción részt vevő dánok 93 százaléka volt azon az álláspontón, hogy országában biztonságban lehet élni.

A magyarok között volt a legalacsonyabb azok aránya, akik szerint az országban biztonságban lehet élni: csupán minden harmadik résztvevő vélte Magyarországot biztonságos helynek *(1. ábra).* Miért ilyen kedvezőtlen a magyarok véleménye a biztonságról? Mitől félnek? A beszélgetésekből kiderült, hogy nem a terrorizmustól. A negatív vélemények hátterében többek között a közbiztonság sokak szerint nem megfelelő állapota, egzisztenciális félelmek, szociális problémák, mint például az egészségügy állapota, illetve a hatalomtól való félelem állt. Ez utóbbi a jogbiztonság, jogegyenlőség területén érzékelt vagy megtapasztalt hiányosságok miatt fennálló félelemként merült fel, illetve volt, aki fehérgalléros bűnözést említett, mint ami ellene hat a biztonságérzetnek.

A hangsúlyok minden országban másra helyeződtek és a félelmek szintje is eltérő volt, azonban a terrorizmustól való félelem, a nagyobb bűntények és nemzetbiztonsági kockázatok miatti aggodalmak, amelyek a nagy, központosított megfigyelési rendszerek kiépítéséhez hivatkozási alapként szoktak szolgálni, szinte egyáltalán nem merültek fel a konzultációk során.

Magyarországon kevésbé volt jellemző, de a többi országban gyakran előjött a félelmek és aggodalmak között magától a biztonsági technológiák általi megfigyeléstől való félelem is, pedig annak paradox módon éppen a biztonság növelése lenne a célja. A kutatás egy olyan összefüggésre is rávilágított, amely szerint sok esetben éppen azok tartanak jobban a biztonsági célú általános megfigyeléstől, akik egyébként is jobban aggódnak a biztonság miatt. A kutatás nem találta igazolhatónak azt az előzetes hipotézist, hogy *minél inkább aggódnak az állampolgárok a biztonságukat érintő fenyegetések miatt, annál nagyobb valószínűséggel találják elfogadhatónak a megfigyelésen alapuló biztonsági technológiákat.* Mindez erősen felveti a lakosság egészét figyelő biztonsági technológiák hatékonyságának kérdését, illetve ezeknek a magánszférára és az állampolgári szabadságjogokra gyakorolt negatív hatását.

Öt biztonsági technológia megítélése

A biztonságtechnológiák hatékonyságának és tolakodó voltának megítélése technológiánként változott. A konzultációk résztvevői az alábbi öt technológiáról beszélgettek:

Intelligens/okos térfigyelő kamerák (CCTV): olyan térfigyelő rendszerek, amelyek többet nyújtanak a közterületek puszta megfigyelésénél. Az intelligens vagy más néven okos térfigyelő rendszerek képesek az arcok felismerésére, az emberek viselkedésének elemzésére és tárgyak azonosítására.

„Civil" drónok: nem katonai célra használt pilóta nélküli, tehát távirányított repülő szerkezetek, melyeket a megfigyelési tevékenységek széles körében lehet bevetni. Felszerelhetők kamerával és más érzékelő technológiákkal, így akár repkedő térfigyelő kameráknak is tekinthetők.

Okos- és mobiltelefonos követés: a mobiltelefonból származó helymeghatározási adatok elemzésével információ nyerhető ki a telefon használójának tartózkodási helyéről és mozgásáról egy adott időszakban. Az adatokat szoftverekkel vizsgálva a mobilszolgáltató, illetve az adatokhoz hozzáférő hatóságok részletes képet kaphatnak a telefon gazdájának mozgásmintázatairól. A telefonkészülék helyét azon mobiltelefon-tornyokból származó adatokkal lehet bemérni, amelyekhez a telefon kapcsolódott. A globális helymeghatározó rendszer (GPS) vagy a vezeték nélküli adatforgalom (wifi) az okostelefonok esetében még pontosabb helymeghatározást tesz lehetővé.

Internetes megfigyelés (DPI): hardvereszközök és speciális, úgynevezett mély csomagvizsgálatot (Deep Packet Inspection) végző szoftverek segítségével lehetőség van az interneten átmenő összes üzenet és információ elolvasására, elemzésére de akár manipulatív célú megváltoztatására is. Ez a módszer segíthet kiszűrni az internetre feltöltött illegális tartalmakat, szerepet játszhat a szervezett bűnözés leleplezésében, az internetes vírusok terjedése elleni küzdelemben, elősegítheti a szerzői jogok tiszteletben tartását. Kormányok használhatják bizonyos tartalmak cenzúrázására is. Az Európai Unió országaitól eltérően az USA-ban jogszerűen lehet használni célzott reklámozásra.

Biometria: a kifejezés az emberek fizikai vagy viselkedési jellegzetességeinek mérésén alapuló automatikus azonosságfelismerő rendszerekre utal. A biometrikus azonosítás kontrollálhatja, hogy bizonyos helyekre kik léphetnek be. Leggyakrabban a biometrikus útleveleknél használják arc-, ujjlenyomat- és/vagy íriszazonosításra. Hétköznapi használata is terjed, például egyre több okostelefon kap ujjlenyomat-olvasót, megvédve ezzel a telefont az illetéktelen használattól. Egyre több területen kezdi felváltani a jelszavas azonosítást valamilyen biometrikus megoldás.

A konzultációk résztvevői jelentős különbségeket láttak az egyes technológiákban abból a szempontból, hogy azok mennyire képesek választ adni a biztonsági kihívásokra, tehát mennyire hatékonyak, mennyire növelik az ország biztonságát és az emberek biztonságérzetét, illetve alkalmazásuk mennyire sértő a magánszférára és az állampolgári szabadságjogokra nézve.

Az öt technológia közül az intelligens/okos kamerák bizonyultak a legelfogadhatóbbnak. Különösen nagy volt a szimpátia irántuk az Egyesült Királyságban, ami nem meglepő, mivel ez a technológia talán ebben az országban a legelterjedtebb. Azonban a térfigyelő kamerák és az üzemeltetésük igen költséges, ezért – bár Magyarországon is terjed ez a technológia – 2014-ben, az állampolgári konzultációk szervezésének évében hazánk gazdasági hátránya okán is jelentősen le volt maradva e téren nem csak az Egyesült Királyságtól, de a kutatásban részt vevő összes európai országtól is. Ennek ellenére a technológia elfogadottsága Magyarországon még az Egyesült Királyságénál is nagyobb volt. Míg a teljes mintában 38 százalék tartotta az intelligens kamerákat hasznosnak és egyben a privát szférát nem igazán sértőnek, ez az arány az Egyesült Királyságban 50 százalék, Magyarországon pedig még ennél is több, 62 százalék volt.

Talán részben azért is ez a technológia volt minden országban a legelfogadottabbak között, mert a *térfigyelő kamerák* intelligens funkciói csak kevéssé voltak ismertek, és a konzultációk résztvevői sok esetben a hagyományos térfigyelő kamerákról alkotott véleményüket terjesztették ki az intelligens kamerákra. A hagyományos térfigyelő kamerákról azért gondolták a résztvevők, hogy viszonylag kevésbé sértik a privát szférát, mivel azok nem az egyes embereket célozzák, és az összegyűjtött információk sem egyénekhez kötöttek. Azonban az okos, tehát például arcfelismerő szoftverrel felszerelt kamerák esetében már más a helyzet, kiváltképp akkor, ha például a kamerához kapcsolt adatbázisban nemcsak a potenciális bűnözők arcának biometrikus adatai találhatók meg, hanem a teljes lakosságé. Ekkor már beazonosíthatók a kamera látóterébe kerülő személyek. Másik példa lehet, ha az intelligens kamerák rendszámleolvasó szoftverrel felszerelt változata autópályát figyel vagy a városi buszsávot ellenőrzi, a rendszámok alapján szintén összekapcsolható a kamera előtt elhaladt autó a tulajdonossal.

A térfigyelő kamerákat, akár intelligensek, akár hagyományosak, elsősorban elrettentő hatásuk miatt tartották alkalmasnak a konzultációk résztvevői a közbiztonság javítására és személyes biztonságérzetük növelésére, annak ellenére, hogy elsősorban az azokat legjobban elfogadó, sőt a terjedésüket sokszor kifejezetten szorgalmazó magyar résztvevők gyakran említettek olyan konkrét eseteket, amikor a térfigyelő kamera ott volt, a bűncselekmény mégis megtörtént. Számukra az intelligens kamerák a sokszor nem megfelelően működő hagyományos készülékek javított változatát képviselték, ezért is voltak annyira népszerűek.

A kamerával felszerelt *drónok* megítélése már nem volt annyira pozitív, mint a térfigyelő kameráké, mivel a drón olyan „intim" területekre is beláthat, mint például valakinek a kertje. Ezért úgy gondolták, hogy ha bűnmegelőzésre, általános megfigyelésre használják, az erősen sértheti a magánszférát. Mivel a drón alkalmas lehet például arra, hogy egy tüntetésen végigfényképezze a résztvevőket, sértheti a demokratikus szabadságjogokat is. Önmagában is veszélyesnek tartották a drónok használatát, mert például *„le tudnak zuhanni"* vagy *„terroristák is használhatják őket robbanóanyag célba juttatására"*. A konzultációkon részt vevők csak speciális helyzetekben engednék a drónok bevetését. Ilyen lehet például egy tűzeset, valamilyen természeti katasztrófa, terrortámadás vagy nagyobb baleset. Keresésnél,

mentésnél is hasznos lehet, mert kiválthatja a veszélyes terepen mentést végzők felderítési munkáját. Úgy vélték, hogy súlyos bűneseteknél alkalmas lehet az elkövetők üldözésére vagy a közbiztonság javítására például tömegeseményeken, mint amilyen a londoni olimpia volt. A konzultációk résztvevői nem engednék viszont a drónok lakossági használatát, illetve azt a fegyverbirtoklásához hasonlóan szabályoznák, az üzemeltetést még hatósági személyek esetén is vizsgához kötnék.

Az *okostelefonos helymeghatározásra* a konzultációk résztvevői elsősorban mint kényelmi megoldásra tekintettek, ami csak korlátozott mértékben alkalmas bűnesetek megelőzésére vagy felderítésére. A személyes biztonságérzetet sem azért növeli ez a technológia, mert segít megakadályozni bűneseteket, hanem a mindennapi életben felhasználható kényelmi szolgáltatásai miatt. Például segít elkerülni az autópályán a dugókat; vagy ha valaki veszélybe kerül vagy eltéved, s a tartózkodási helye bemérhető, hamarabb érkezhet a segítség; vagy lehetővé teszi például a ránk bízott kiskorúak vagy idősödő szülők követését. Ugyanakkor voltak, akik szerint ez a fajta biztonságérzet inkább egy társadalmilag konstruált érzetként értelmezhető; az emberek, amikor még nem voltak mobiltelefonok, sem érezték magukat kevésbé biztonságban, de amióta megszoktuk, hogy az életünk részei, nélkülük kissé kiszolgáltatottnak érezzük magunkat, csökken a biztonságérzetünk.

A konzultációk résztvevői úgy érezték, hogy e technológia biztonsági célú hatósági használat esetén jelentősen betolakszik a magánszférába, veszélyt jelenthet a demokratikus szabadságjogokra, és az is probléma, hogy az egyénnek nincs kontrollja a helymeghatározási adatokból levont következtetések felett. A résztvevők közül többen is beszámoltak arról, hogy bizonyos helyekre nem visznek mobiltelefont, hogy ezt a fajta követést úgymond „lerázzák".

Az *internetes megfigyelést* nemzetbiztonsági, bűnmegelőzési szempontból elsősorban akkor tartották hasznosnak a kutatásban részt vevők, ha azt a digitális infrastruktúra fenntartásához vagy súlyos bűncselekmények gyanúsítottjainak megfigyelésére használják. Azonban úgy vélték, ha általános, mindenkire kiterjedő megfigyelésre használják, akkor a megbeszélt öt technológia közül az internetes megfigyelés sérti a magánszférát a legjobban, mert a kommunikáció tartalmát is érinti. Ráadásul az adatok manipulálhatók, módosíthatók, tehát visszaélésre is lehetőséget teremtenek, illetve kontextusukból kiragadva esetleg a kinyert információk félreértelmezhetők, ami súlyos következményekkel járhat az egyénre nézve. Úgy vélték, hasznos eszköz lehet viszont akkor, ha törvényes, bírósági felhatalmazás alapján alkalmazzák. Ez a technológia titkossága, teljes láthatatlansága miatt kelt félelmet az emberekben. Sokan úgy vélték, az elfogadhatósága erősen kontextusfüggő, és azon múlik, hogy a kormányzat mennyire korrekt és az érvényben lévő szabályozás mennyire tisztességes.

A *biometrikus azonosításnak* az ujjlenyomatvételen kívüli lehetőségei kevéssé voltak ismertek 2014-ben. A résztvevők megbízhatónak és biztonságosnak gondolták alkalmazását. Úgy vélték, a biometrikus azonosítás valóban garantálja a biztonságot például a munkahelyi beléptetésnél vagy repülőtereken, és nem sérti a privát szférát. Egyedül a biometrikus adatok tárolásának biztonságossága keltett némi aggodalmat, mivel az illetéktelen behatolás az adatbázisba olyan súlyos bűncselekményt is elősegíthet, mint a személyazonosság-lopás.

A *2. ábra* azt mutatja, hogy mely technológiákat mennyire tartottak hasznosnak, illetve a magánszférára nézve tolakodónak az állampolgári találkozók résztvevői. A magyarok véleménye egyedül az okos térfigyelő kamerák megítélése esetében különbözött nagymértékben a többi ország polgárainak véleményétől: a nyíl mutatja, hova kerülne ez a technológia az ábrában a magyarok véleménye alapján.

2. ábra. A biztonsági technológiák megítélése hasznosság és tolakodásuk mértéke szerint

(Saját szerkesztés)

Ezen öt technológia kialakulásának körülményeiről, fejlődéséről és az alkalmazásukhoz kapcsolódó dilemmákról bővebbet is meg lehet tudni a korábban már említett SurPRISE projekt honlapján magyarul is hozzáférhető információs magazinokból és ismeretterjesztő filmekből.

Magánszféra – hol a határ?

A konzultációkon folytatott beszélgetések rávilágítottak arra, hogy a biztonság értelmezése több dimenzió mentén történik. Része például a nemzetbiztonság, a közbiztonság, a szociális biztonság, az internetbiztonság, de a legfontosabb a személyes biztonságérzet. A megfigyelésen alapuló biztonsági technológiáknak akkor nagyobb az elfogadottságuk, ha növelik ezt a személyes biztonságérzetet. Ha nem képesek erre, ha nem a lakosság személyes biztonságérzetét kikezdő kihívásokra válaszolnak, akkor elutasításra találnak. További probléma, hogy sokakat aggaszt a mindenkire kiterjedő általános megfigyelés, tehát maguknak a biztonságtechnológiáknak a használata csökkentheti a személyes biztonságérzetet. Mindezek ellenére a konzultációk résztvevői sok pozitívumot is láttak ezekben az új biztonsági technológiákban, és sok példát is tudtak hozni arra, amikor a megfigyelés helyénvaló és szükséges volt. Egyöntetű vélemény volt azonban, hogy az általános, mindenkire kiterjedő megfigyelést túlzónak, aránytalannak és szükségtelennek tartják, különösen akkor, ha a megfigyelés behatol a privát szférának egy olyan területére is, amit a magánszféra magjaként lehetne jellemezni.

Bár az angol „privacy" szó fordításának kissé eltérő jelentése van a különböző nyelvekben, a magánszféra fogalmának értelmezése hasonló volt a kutatásban részt vevő országokban. Az

állampolgárok különféle megközelítéseket használva próbálták megmagyarázni, mit jelent számukra a magánszféra fogalma. A véleményeket két fő irány jellemezte. Az egyik szerint a magánszféra egy jól körülhatárolható valóságos, lelki vagy digitális tér vagy szféra, amit gyakran tényleges vagy virtuális határ vesz körül. A másik megközelítés szerint a magánszféra egy lehetőség, szabadság, képesség vagy jog arra, hogy valaki eldöntse, mi az, ami számára privát. Tulajdonképpen nincs nagy ellentmondás a két megközelítés között, mivel ez utóbbi az első megközelítésben meghatározott határvonalak kijelölésének a szabadságára utal.

Sokan úgy vélték, hogy a magánszféra folyamatos változásban van, tulajdonképpen egyre szűkül az elektronikus kommunikáció növekedésével. Az emberek beletörődnek, hogy bizonyos internetes aktivitással életük egy része visszavonhatatlanul láthatóvá válik, és a nyilvánosság egyre inkább behatol a magánszférába. Azonban általános vélekedés volt, hogy a magánszférának létezik egy olyan magja, amelyet mindenáron védelmezni kell.

A konzultációk résztvevői leggyakrabban az otthont, a családi környezetet sorolták a magánszféra magjához. Ehhez sokan hozzávették még a személyes kapcsolatokat, a személyes gondolatokat, a személyes kommunikáció minden formáját, tehát a szóbeli és írott kommunikációt is, illetve a cselekvés szabadságát. Többek számára az adatvédelem is a magánszféra része, és a védelmezendő „maghoz" sorolták a személyes adatokat, elsősorban az úgynevezett érzékeny adatokat, mint a politikai és vallási nézetek, szexuális orientáció, az egészségügyi információk, a banki és pénzügyi adatok, de voltak, akik a telefonszámot és az e-mail-címet is. Volt olyan résztvevő, aki így összegezte, mit jelent számára a magánszféra sérthetetlen, mindenképpen védelmezendő magja: „*Mindenféle adat, amelyen keresztül egy személy elérhető vagy valamilyen módon megkárosítható.*" Vagy: „*Minden olyan információ, amivel kárt, veszteséget lehet valakinek okozni vagy valakit zaklatni lehet.*"

Együttélés a megfigyeléssel

Mivel a megfigyelés ritkán látható vagy érezhető, többnyire nincs közvetlen hatással az emberek mindennapi életére, ezért nem is vagyunk tudatában, hogy ezek a technológiák folyamatosan információkat rögzítenek rólunk. Talán ezért is, a konzultációk résztvevőinek csak kisebb hányadát jellemezte, hogy a megfigyelés miatt megváltoztatná a viselkedését vagy próbálná időnként elkerülni a megfigyelést. Azt azonban többen kifejezésre juttatták, hogy jó lenne tenni valamit, de többek közt a tájékozottság és a tudás általános hiánya passzivitást eredményez.

Az általunk megvásárolt technológiákon keresztül – mint amilyen például az internet- és mobilszolgáltatás, vagy amikor bekamerázott autópályákon utazunk, átlépjük az országhatárt, vagy csak sétálgatunk térfigyelő kamerával megfigyelt köztereken – folyamatos megfigyelés alatt állunk, ezzel ma már együtt kell élnünk, akár akarjuk, akár nem. Tehát a konzultációkon elhangzott alábbi vélemények, hozzáállások közül képviselnünk kell valamelyiket, amivel, ha nem is feltétlenül elvi szinten, de a mindennapi gyakorlatban egyetértünk és elfogadjuk ezt a fajta megfigyelést:

- Bár volt néhány résztvevő, aki szinte a paranoia határát súroló félelemmel tartott a megfigyeléstől, a leggyakoribb a *racionális viselkedés* volt, amikor valaki elfogadja ugyan a megfigyelést, de azért, amennyire lehet, megpróbálja védeni a magánszféráját. Ez a viselkedés gyakran nem is tudatos védekezés, hanem általános elővigyáza-

tosság, ami már szokássá vált. Például valaki alaposan meggondolja, mire használja az internetet; jól meggondolja, milyen oldalakon regisztrál; nem mindig ugyanazt a böngészőt használja; nem mindig visz magával mobiltelefont; meggondolja, kit hív a telefonon; van pár téma, amiről telefonon nem beszélget.

- Voltak, akik úgy vélték, egyáltalán nem kell foglalkozniuk a megfigyeléssel. Gyakori érvük volt a *„nekem nincs rejtegetnivalóm”,* illetve az, hogy *„csak a bűnözőknek vagy azoknak kell félni*ük *a megfigyeléstől, akiknek vaj van a fejükön”*.
- Voltak, akik azzal nyugtatták meg magukat, hogy ők mások számára érdektelen kisemberek, mondván: *„mi olyan kicsik,* érdektelenek vagyunk*”,* vagy *„m*ásokat akarnak megfigyelni, nem minket”.
- A tehetetlenség, kiszolgáltatottság érzése is megnyilvánult a magyarázatokban: *„Túl kicsik vagyunk ahhoz, hogy tehetnénk ellene.*” Ez az attitűd különösen erős volt a magyar résztvevők körében. Talán a kiszolgáltatottság érzésének a fő oka a nem túl távoli korszak kulturális hatása, amikor az emberek hozzászoktak vagy arra lettek szocializálva, hogy erős állami megfigyelés alatt éljenek. Az is szerepet játszhat, hogy a civil szféra, amelyik megvédhetné a polgárokat vagy támogathatná őket a dolgok alulról jövő megváltoztatásában, Magyarországon gyenge.
- Volt, akit a beletörődés jellemzett: a mai világban „ú*gyis mindenki tud mindenkiről mindent,* úgyse *tudunk semmit tenni a megfigyelés ellen”,* nemcsak azért, mert nem vagyunk képesek képviselni az érdekeinket, hanem azért is, mert minden hiábavaló.
- És voltak, akik úgy érezték, azért nem tesznek semmit a megfigyelés ellen, mert a kényelem számukra fontosabb, hiszen ezek az eszközök, amelyeken keresztül megfigyelhetőkké váltak, már rengeteg módon beépültek az életükbe, amin nem szeretnének változtatni.

A biztonságtechnológiák elfogadása – ambivalens hozzáállás

Az állampolgári konzultációk résztvevőinek nagy része nem utasította vissza önmagukban a megfigyelésen alapuló biztonsági megoldásokat, és bár a beszélgetésekből kiderült, hogy a nemzetbiztonság érdeke számukra távoli, nehezen értelmezhető fogalom, 59 százalékuk támogatta a megfigyelésen alapuló technológiák használatát a nemzetbiztonság érdekében. Azonban a véleményeknek másik oldala is van. A kilenc országban megrendezett konzultációk közel 2000 résztvevőjének:

- 72%-a aggódott amiatt, hogy a megfigyelésen alapuló biztonsági technológiák használata sérti a magánszférát;
- 70%-a vélte úgy, hogy túl sok információt gyűjtenek róla ezek a biztonsági megoldások;
- 70%-a azt gyanította, hogy amint ezeket a technológiákat üzembe helyezik, valószínűleg visszaélnek velük;
- csupán 34%-a vélte úgy, hogy ha valaki nem tett semmi rosszat, nem kell aggódnia a megfigyelés miatt;
- 69%-a aggódott, hogy a róla gyűjtött adatokat felhasználhatják ellene;
- 66%-a követelt olyan alternatív megoldásokat a biztonság növelésére, amelyek nem alkalmazzák a megfigyelésen alapuló biztonsági technológiákat.

Mit is akarnak tehát az európai állampolgárok? – tehetnénk fel a kérdést, mert a vélemények némileg ellentmondanak egymásnak. Az ellentmondás feloldása egyszerű: *nem szeretnének félelemben élni, de szeretnék megőrizni a magánszférájukat és demokratikus szabadságjogaikat is.* A konzultációk résztvevői olyan hatékony biztonsági megoldásokat szorgalmaztak, amelyek összhangban vannak a magánszféra tényleges védelmével. Tehát abba az esetben elfogadható számukra ezeknek a technológiáknak a használata, ha a megfigyelés nem általános, mindenkire kiterjedő és folyamatos, hanem célzott; ha hozzájárul a személyes biztonságérzet növeléséhez; vagy aktívan képes életeket menteni; figyelembe veszi a magánszféra védelmének szempontjait is; a technológia bevezetése és alkalmazása jól szabályozott, ellenőrzött és átlátható. A technológiák elfogadása kapcsán a kutatás a következő további összefüggéseket tárta fel:

- A megfigyelésen alapuló biztonságtechnológiák elfogadásának legfontosabb tényezője a biztonsági szervekbe és politikai intézményekbe vetett bizalom.
- Az elfogadás jóval nagyobb, ha a technológia csak a gyanúsítottakat figyeli meg.
- Minél jobban sérti egy technológia a magánszférát, annál kevésbé tartják hatékonynak, szemben azzal az elképzeléssel, amelyet az alkumodell is képvisel, hogy a biztonság csak a magánszféra megsértése árán növelhető.
- Az érzékelt fenyegetettség mértéke csak korlátozottan hat a biztonságtechnológiák elfogadására, mivel más szempontok is fontosak, és a biztonság, megfigyelés és magánszféra közötti összefüggések is komplexebbek, mint azt a biztonságért felelős döntéshozók általában feltételezik.
- A kutatás azt az összefüggést támogatta, hogy – ha eltekintünk a 30 év alattiaktól – minél idősebb valaki, annál jobban elfogadja e technológiákat. Tehát nem támasztja alá azt a sokak által igaznak vélt elképzelést, hogy éppen a fiatalok azok, akik kevésbé aggónak amiatt, hogy e technológiák egyre jobban behatolnak a magánszférájukba. A legfiatalabbak eltérő attitűdjét azzal lehet magyarázni, hogy a kérdés felelősségteljes átgondolásához kell valamennyi élettapasztalat. Emiatt is fontos, amit a találkozókon sokan szorgalmaztak, hogy a konzultációkon felvetett témákról a lakosság minél szélesebb rétegeit tájékoztatni kell; a felvilágosító, ismeretterjesztő munkát már az iskolában el kellene kezdeni.

Azok a technológiák a jobban elfogadottabbak:

- amelyek olyan bűntényekre koncentrálnak, amelyek a lakosság körében is prioritást élveznek;
- amelyeket jól körülírt céllal alkalmaznak;
- amelyek haszna közvetlenül is érzékelhető; illetve
- amelyek működését az emberek – tehát azok az „ártatlanok", akiket megfigyelnek – ellenőrizni tudják, vagyis rálátásuk van arra, hogy ki, mikor és milyen információkat gyűjt róluk, mi történik ezekkel az adatokkal, hogyan van az egész folyamat szabályozva.

Azok a technológiák kevésbé elfogadhatók:

- amelyeknél nagy a veszély, hogy nem arra fogják használni, amire eredetileg szánták azokat;

- amelyek elősegítik az intoleranciát és a szegregációt, tehát például a szoftverek úgy vannak programozva, hogy eltérően kezelik a társadalom különféle szegmenseit esetleg nemzetiségi, etnikai vagy más alapon;
- amelyek kiszorítják az emberi tényezőt; illetve;
- amelyek bevonják a magánszektort vagy más országok nemzetbiztonsági szerveit.

Mit lehet tenni?

Az egyik lehetőség, hogy amikor úgy érezzük, a megfigyelés túlságosan beavatkozik a privát szféránkba, megváltoztatjuk, jobban kontrolláljuk a viselkedésünket. Jeremy Bentham 18. századi angol filozófus *Panoptikon*ja (vö. Foucault 1990 [1975]: 3. fejezet) – egy börtönökre kidolgozott épületdizájn – jól példázza ezt. A kör alakú épület közepén elhelyezett megfigyelőtoronyból minden rabot látni lehet, miközben a rabok nem láthatják az őröket a toronyban, tehát nem tudják, mikor figyelik őket, ezért mindig úgy viselkednek, mintha épp figyelnék őket, azaz hatékonyan kontrollálják saját viselkedésüket. A rabok esetében ez fontos fegyelmezőerőként működött a korábbi fizikai erőszak helyett.

A konzultációk résztvevői közül azok, akik addig még nem gondolkodtak el a megfigyelésen alapuló biztonsági technológiákról, sokszor az állampolgári találkozón döbbentek rá, hogy ezek a technológiák mennyire alkalmasak lehetnek a demokratikus szabadságjogok gyakorlásának megnyirbálására pusztán a folyamatos megfigyeléstől való félelem, aggodalom által kiváltott önkontrollon keresztül. Lehetségesnek tartották, hogy valaki e megfigyelés miatt korlátozza, miket posztol az interneten, vagy esetleg kifejezetten emiatt nem megy el egy tüntetésre.

A konzultációkon arra a kérdésre, hogy megpróbálnák-e valahogy aktívan elkerülni e biztonsági technológiáknak az előzőekben leírt „figyelő szemeit", vagy esetleg miattuk megváltoztatnák-e a viselkedésüket, az okos térfigyelő kamerák esetén a résztvevők 20 százaléka, a mobiltelefonos helymeghatározás esetén 30 százaléka és az internetes megfigyelés esetén 36 százaléka válaszolt igennel.

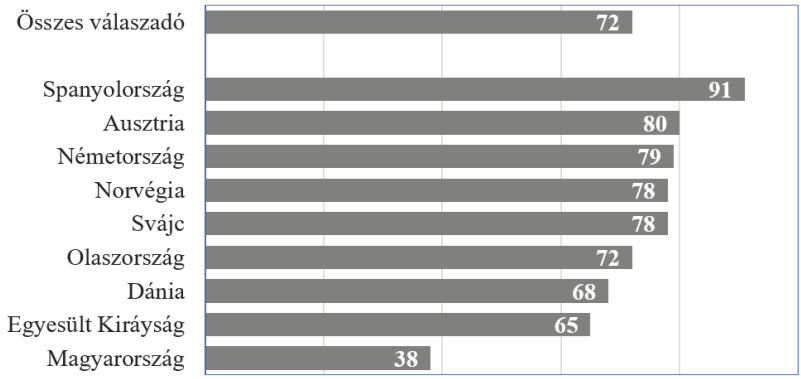
Egy másik lehetőség a tiltakozás. Technológiától függően a konzultációk résztvevőinek 15–20 százaléka szívesen tenne valamit aktívan, például kampányolna az állampolgárokat folyamatosan megfigyelő biztonsági technológiák ellen, és további 10 százalék, ha maga aktívan nem is tenne semmit, elvben támogatná ezeket a tiltakozókat. Tiltakozás helyett nagyjából minden második résztvevő inkább többet szeretett volna tudni arról, hogyan védhetné meg a magánszféráját, a demokratikus jogait, tehát tiltakozás helyett inkább a védekezés lehetőségében látta a megoldást. Az internetes megfigyelés és a mobiltelefonos követés esetében jelentős kisebbségben (11 és 16 százalék) voltak azok, akiknek nem voltak averzióik a technológia alkalmazásával szemben. A térfigyelő kamerák nagyobb elfogadottságát mutatja, hogy a válaszadók 28 százaléka egyáltalán nem ellenezte alkalmazásukat.

A tiltakozók, az elkerülők és a viselkedésüket megváltoztatók gyakran azok közül kerültek ki, akiknek nagyobb előzetes tudása volt a konzultációkon megvitatott témákról, és feltételezhetően jobban tisztában voltak ezeknek a technológiáknak az árnyoldalaival, következésképpen jobban aggódtak az alkalmazásuk negatív társadalmi következményei miatt.

A magyarok véleménye

A magyar résztvevők az átlagnál valamivel jobban hajlottak rá, hogy elfogadják a megfigyelésen alapuló biztonsági technológiákat, és jóval kevesebben aggódtak amiatt, hogy ezek a biztonságtechnológiák negatív hatással lehetnek a magánszférára *(3. ábra)*. Egybevág ezzel a kutatási megállapítással az a tény is, hogy Magyarországon a magánszférához, adatvédelemhez kapcsolódó közéleti viták is szinte teljesen hiányoznak.

3. ábra. „Aggódom, hogy a megfigyelésen alapuló biztonsági technológiák használata sérti a magánszférát" – az állítással egyetértők aránya százalékban; N=1780



(Saját szerkesztés)

Ez a különbség részben azzal a történelmi-kulturális ténnyel magyarázható, hogy Magyarországon a demokratikus fejlődés nem hosszú, organikus folyamatként ment végbe, mint a kutatásba bevont nyugat-európai országokban, hanem az átmenet a diktatórikus rendszerből a demokráciába „felülről" indult és rendkívül gyorsan történt. A demokratikus gyökerek nem hatolnak le mélyre a társadalom szövetébe, nem itatják át a kultúrát, nincs hagyománya a magánszféra és a személyiségi jogok védelmének, a társadalmi mozgalmaknak csekély a tömegbázisa. Csupán néhány civil szervezet foglalkozik adatvédelemmel[4] és személyiségi jogokkal, és ezeknek a szervezeteknek sincs megfelelő társadalmi támogatottsága.

További magyarázat lehet, hogy bár Magyarországon az 1990 előtti totalitárius egypártrendszer a lakosság széles körű megfigyelésével próbálta bebiztosítani a hatalmát, az ellenvéleményeket elhallgattatni, az elnyomó politikai rendszer eltörlésével az emberek mintha átestek volna a ló túlsó oldalára, és a személyes adataik és a magánszférájuk vonatkozásában egyfajta érdektelenség és nemtörődömség alakult ki. Biztonságban is érezhették magukat, mivel a kommunista hatalom elsöprését követően az információszabadság és a magánszféra védelme kitüntetett szerepet kapott az immár demokratikus Magyarországon, és az 1992-ben elfogadott igen haladó szemléletű adatvédelmi törvénnyel az ország Európa élvonalába került. Igaz, húsz évvel később, a 2012-ben hatályba lépő új adatvédelmi törvény ehhez képest visszalépésnek tekinthető, mert megszüntette az adatvédelemért és informá-

4 A három legjelentősebb szervezet az Eötvös Károly Intézet, a Társaság a Szabadságjogokért (TASZ) és a Magyar Helsinki Bizottság.

ciószabadságért felelős független ombudsmani hivatalt, és helyette egy adatvédelmi hatóságot (NAIH) állított fel, amely, noha formálisan független, az adminisztratív hierarchiába tagozódik. A témába vágó további fejlemény, hogy az ország alacsony terrorfenyegetettsége ellenére 2010-ben egy nagy terrorelhárítási központ létesült, a TEK, amely bírói engedély nélkül is jogosult állampolgárok titkos megfigyelésére.[5] De éppen a kutatásban is megfigyelt érdektelenség miatt ezek a témák nem kerültek be az állampolgárok érdeklődési szférájába, a konzultáción is csak elvétve és nagyon keveset tudott egy-egy résztvevő ezekről a dolgokról. Az idősebb generációk pedig még az előző rendszerben hozzászoktak a megfigyeléshez, megtanultak együtt élni vele. Többször is elhangzott a beszélgetések során: „*Ez ugyanaz a megfigyelés, ami régen volt, csak gépekkel.*"

Mivel a magyarok kevésbé aggódtak e technológiák miatt, jóval kevesebben is voltak közöttük, akik tiltakoznának az alkalmazásuk ellen vagy próbálnák elkerülni azokat, netán a viselkedésüket változtatnák meg. Az aggodalom alacsonyabb szintje mögött feltehetően többek közt a nyugat-európai polgártársakhoz képest jelentősebb ismerethiány állt. Bár a találkozók résztvevői közül mind a kilenc országban sokan érezték úgy, hogy több információra lenne szükségük, a magyar résztvevők között az ismeretek iránti igény még erőteljesebb volt, és a konzultációkon a politikusok felé megfogalmazott javaslataikban, igényeikben is nagyobb hangsúlyt kapott a témáról szóló ismeretterjesztés.

Ismeretek a megfigyelésről, a jogi szabályozásról

Az állampolgári konzultáció mint kutatási módszer a résztvevők involválásával és a kutatási folyamat során átadott információkkal maga is gerjesztette a résztvevőkben a hiteles és releváns információk iránti igényt, azonban az egyértelműen megállapítható volt, hogy az átlagemberek kevés információval rendelkeznek a felvetett témákról, vagy a tudásuk felszínes és esetenként téves. Amikor megfogalmazták, mi mindenről szeretnének tudni, voltak, akik úgy érezték, túl sok erőfeszítésbe kerül, és túl sok erőforrás fordítódik ezeknek a technológiáknak a fejlesztésére és túl kevés a megfelelő felvilágosító kampányokra arról, hogy miképpen működnek, hogyan szabályozzák és ellenőrzik őket, melyek a hatóságok jogai és kötelezettségei és melyek az állampolgárok jogai és kötelezettségei e téren.

Az egyik leggyakoribb kérdés az volt, hogy valójában kik is azok az „ők", akik kitalálják az egész rendszert, akiknek hozzáférésük van a technológia által generált megfigyelési adatokhoz. A konzultációk résztvevői nem igazán voltak tisztában azzal, hogy ki ellenőrizheti az adataikat és azok hova futnak be. A beszélgetések során időnként a nem nevesített többes szám harmadik személy egyes számba váltott, amivel a résztvevők általában egy számukra rejtélyes, nagy hatalommal bíró egyénre utaltak, aki a rendszer tetején foglal helyet valahol a háttérben, aki irányítja ezt az egészet. De hogy ki is ez az „ő", az nagy kérdés maradt.

Másik kérdés, hogy milyen folyamatok működnek az egyes megfigyelésen alapuló biztonsági technológiák esetében. Hogyan és mikor kapnak „ők", tehát az összegyűjtött adatokat felhasználók hozzáférést a személyes adatokhoz? Hogyan gyűjtik, tárolják és használják a személyes információkat, hogyan elemzik a lakosságról a „gépekkel" összegyűjtött infor-

5 Az ebben az ügyben született elmarasztaló strasbourgi bírósági ítéletről és annak lehetséges következményeiről lásd Pásztor Emese tanulmányát az *Információs Társadalom* e lapszámunkkal egy időben megjelenő 2017/1. számában.

mációkat? Egyáltalán: milyenfajta információkat gyűjtenek és konkrétan milyen célra? Mik a megfigyelésen alapuló biztonsági technológiák hatásai a magánszférára és az egyének és a társadalom biztonságára? Többen feltették a kérdést: „Én saját magam hogyan vagyok érintve?" És: „*Hogyan tarthatok meg bizonyos információkat bizalmasnak?"* Melyek általában a hatóságokra és az állampolgárokra vonatkozó szabályozások, jogszabályok és jogok? A „titokzatos ők" kivel osztják meg az információkat? Hogyan lehet egy átlagpolgárt megvédeni, ha tévesen értelmezik a róla gyűjtött információkat, vagy olyan információkat gyűjtenek róla, amelyek a magánszférájának ahhoz a bizonyos magjához tartoznak, amelyet semmiképpen nem szeretne illetéktelenekkel megosztani?

Azok, akik jobban tisztában voltak a megfigyelésen alapuló biztonsági technológiák szabályozásával, többet akartak megtudni a nemzeti és EU-s szabályozásról. Azok, akik kevesebbet tudtak, több közérthető nyelven írt alapinformációt igényeltek, például az adott ország adatvédelmi törvényének tartalmáról. Voltak, akiket az érdekelt volna, hogyan alakultak ki a jelenlegi szabályozások, és milyen célok, szándékok állnak a szabályozások mögött? Kik vesznek részt a szabályzások kialakításának folyamatában, kiknek van ebbe beleszólásuk, például vannak-e a háttérben politikai vagy gazdasági lobbicsoportok? Az állampolgárok hogyan találhatják meg vagy érhetik el a témában releváns információkat és dokumentumokat, és kinek a felelőssége, hogy tájékoztassa a nyilvánosságot?

Az állampolgári találkozók résztvevői számára készített ismeretterjesztő magazinok és filmek betöltötték funkciójukat, az ismeretátadás mellett involválták a résztvevőket, felkeltették érdeklődésüket. Hozzájött ehhez, hogy az állampolgári konzultáció, mint kutatási módszer, felelősséggel ruházza fel a résztvevőket, mivel a találkozó végén megfogalmazott állampolgári javaslatok és igények valóban eljutnak az illetékesekhez, a lakosság is „szót kap" a döntési folyamatban. A résztvevők ezt átérezve döbbentek rá, hogy véleményük felelősségteljes képviseléséhez alapvető a megfelelő tájékozódás.

Bizalom az üzemeltetőkben, a jogi szabályozásban – az aktuális politikai hatalomban

A biztonsági technológiák üzemeltetői részben mint intézmények, részben mint a technológiát közvetlenül működtető operátorok jelentek meg a beszélgetésekben. A konzultációk résztvevői gyakran jobban tartottak attól, hogy az adatokhoz hozzáférő operátorok élnek vissza az információkkal, mint attól, hogy az intézmények működésével lennének gondok. Úgy vélték, visszaélésekre egyrészt azért kerülhet sor, mert az operátorok is csak *„esendő emberek"*, másrészt, mert nem kellő mértékben felügyelik őket vagy nincsenek jól kiképezve, illetve azok, akiket ilyen pozíciókban alkalmaznak, nem a legalkalmasabbak a feladatok elvégzésére, nem kellőképpen megbízhatóak.

A kezelők láthatósága vagy láthatatlansága befolyásolta, hogy az állampolgárok hogyan értékelik a megbízhatóságukat. Amikor az operátorok „láthatóbbak", mint például a térfigyelő kamerarendszerek esetében, amikor belátni a megfigyelőszobába, vagy csak látni lehet, ahogy ki-be járnak a biztonsági emberek, a megbízhatóság (pozitív vagy negatív) megítélése az egyénekből indul ki. Amikor azonban az operátorok rejtve vannak (pl. internetes megfigyelés), akkor többnyire a hatóságokat értékelik, és értékelésük a hatóságok általános megítélése szerint változik.

A megfigyelésen alapuló biztonsági technológiákat üzembe helyező és működtető hatóságokkal és rendvédelmi szervekkel szembeni bizalom az egyik legfontosabb tényező, ami befolyásolja e technológiák elfogadását. Azonban a bizalom összetett fogalom, és fontos vonása, hogy feltételezi a kölcsönösséget. Továbbá, ha valami kikezdi a bizalmat, az azonnal képes megroggyanni, míg visszaállítása fáradságos, sok esetben időigényes folyamat.

A hatóságok és rendvédelmi szervek iránti attitűdökben és a megfigyeléssel összegyűjtött adatok felhasználása miatti aggodalomban az tükröződik, hogy sok esetben probléma van ezzel a bizalommal. Bár a válaszadók nagyjából kétötöde szerint a hatóságok megbízhatóak, amikor ezeket a technológiákat használják, jelentős volt azok aránya, akik tartottak tőle, hogy a hatóságok visszaélnek a hatalmukkal: az intelligens/okos kamerák esetében 46 százalékuk, a mobiltelefonos helymeghatározás esetében 34 százalékuk, valamint az internetes megfigyelésről vitatkozók 52 százaléka képviselte ezt a véleményt.[6]

A bizalom hiányában az is szerepet játszhatott, hogy sokan nem rendelkeztek elégséges ismeretekkel arról, hogy a technológiát hogyan helyezik üzembe, az adatfeldolgozás folyamatait hogyan szabályozzák és ellenőrzik, és milyen jogi biztosítékok védik az állampolgárokat a visszaélések ellen. Ennek tükrében a biztonsági és rendvédelmi szervek, illetve az állami intézmények iránti bizalomtól függően pozitív és negatív attitűdöket fogalmaztak meg a résztvevők. Elsősorban azokban az országokban, például Spanyolországban, Olaszországban és Magyarországon, ahol a hatóságok iránti bizalom nem kifejezetten volt erős, a konzultációk résztvevői gyakran voltak azon az állásponton, hogy a megfigyelésen alapuló biztonsági technológiák használata nem eléggé szabályozott, és ha még az is lenne, a biztonsági és rendvédelmi szervek nem tartanák be a szabályokat.

A többi országban a hiányos ténybeli tudás ellenére sokan voltak, akik pozitív hozzáállást fogalmaztak meg, feltételezve, hogy ha ők nincsenek is tisztában a szabályozással, attól az még bizonyára létezik. Azonban többen aggódtak, hogy ha vannak is szabályozások, a laikus embereknek nehéz megérteniük ezeket a dolgokat. Mások azt hiányolták, hogy miért nem hozzák nyilvánosságra az információkat ezekről a témákról. Azok, akik azt állították magukról, hogy jobb ismereteik vannak a témáról, úgy vélték, a mostani technológiai fejlődéshez képest a vonatkozó törvények idejétmúltak.

Az állampolgárok többsége nem szeretne közvetlen beleszólást a megfigyelésen alapuló biztonsági technológiák szabályozásába, és szakértőkre bízná ezt a munkát azzal a feltétellel, hogy az eredményeket közérthetően kommunikálják a nyilvánosság felé. Ugyanakkor megfogalmaztak néhány általános igényt:

- Szükség van a megfigyelésen alapuló biztonsági technológiákat használó biztonsági szervek aktív, állandó külső ellenőrzésére, amelyeket a megfigyelést végző szervtől, politikától és gazdasági vagy kereskedelmi érdekektől mentes testületnek vagy szervezetnek kellene működtetnie, hogy biztosítani tudja az elszámoltathatóságot, és megakadályozza a biztonsági szerv hatáskörének túlzott növekedését.
- Az állampolgárok számára lehetővé kell tenni, hogy kérésükre hozzáférhessenek a megfigyelésen alapuló biztonsági technológiák által gyűjtött személyes adataikhoz.
- Fel kell mérni a megfigyelésen alapuló biztonsági technológiák használatának szükségességét, megfelelő és arányos voltát.

6 Strauss, S. (2015): Citizen Summits on Privacy, Security and Surveillance: Synthesis Report, http://surprise-project.eu/dissemination/research-results/.

- Az állampolgárokat tájékoztatni kell a törvényes adatgyűjtésről, az adatfeldolgozásról és a létező jogi biztosítékokról.
- A jogi biztosítékoknak akkor is könnyen hozzáférhetőeknek kell lenniük, amikor magáncégek használnak megfigyelésen alapuló biztonsági technológiákat.

Amellett, hogy az állampolgári találkozókon résztvevők zöme átlátható és szigorú ellenőrzési mechanizmusokat igényelt, egy további szempont is felmerült: a biztosítékok nem lehetnek annyira bürokratikusak, hogy megnehezítsék a biztonságért felelős szervek munkáját. Emellett a szabályozásnak technológiánként differenciáltan kell lennie. Az olyan technológiák esetében, mint a térfigyelő kamerák, kevesebb biztosíték is elég lehet, mint például a jogok megsértésére nagymértékben alkalmasnak vélt DPI, tehát az adatforgalom tartalmának pásztázásán alapuló internetes megfigyelés esetében.

A technológiákat működtetőkkel szembeni bizalom hiánya szorosan összefüggött a biztonsági szervek elszámoltathatóságának, átláthatóságának és ellenőrzésének vélt hiányával. Az emberek szeretnének bízni, de érzékelik a hiányát annak a közös alapnak, amire ezt a bizalmat építeni lehetne. Ezt súlyosbítja az a felfogás, hogy e biztonsági és megfigyelési intézkedések éppen e hatóságoknak az állampolgárok iránti bizalmatlanságán alapulnak, hiszen a mindenkire kiterjedő megfigyelés elvi alapja az, hogy mindenki potenciális bűnelkövető.

Az állampolgárok javaslatai

A konzultációk résztvevői 6–8 fős csoportokban osztották meg a gondolataikat, sokszor kiegészítve egymás tudását vagy vitatkozva egymással. Már a megbeszélések során is sokféle állampolgári igény, javaslat felmerült, de a konzultáció végén minden csoport közös javaslatot dolgozott ki az európai és hazai politikusok, döntéshozók számára. A közel 300 állampolgári javaslatot ötvözve a független szakértői véleményekkel és az empirikus kutatás egészének eredményeivel készültek el a SurPRISE projekt ajánlásai az Európai Bizottság részére (Čas 2015), hogy az állampolgárok igényeit is figyelembe lehessen venni az új uniós szabályozásban.

Az alábbiakban összefoglaljuk a konzultációkon részt vevő állampolgárok közel 300 üzenetének a lényegét.

A használatra vonatkozó stratégiák

A megfigyelésen alapuló biztonsági technológiák arányos és célzott használatát kell biztosítani a széles körű megfigyelés helyett, és e technológiákat csak akkor szabad alkalmazni, amikor valóban szükség van rájuk. A megfigyelésbe bevont állampolgárok körét korlátozni kell, hogy minél kevesebb „ártatlant" figyeljenek meg. Az összegyűjtött adatok lehetséges felhasználásának időtartamát korlátozni kell, tehát azokat egy idő után törölni kell az adatbázisból. A megfigyelésen alapuló biztonsági technológiákat mindig törvényesen és felelősségteljesen kell használni. Fontos a „gépek" használatának emberi ellenőrzése is.

Szabályozás és ellenőrzés

A javaslatok jelentős része vonatkozott a megfigyelésen alapuló biztonsági technológiák szabályozására és ellenőrzésére. Általános igényként merült fel e technológiák bevezetésének és alkalmazásának szigorú szabályozása és ellenőrzése. Néhány specifikus javaslat is megfogalmazódott:

- Uniós szabályozásnak kell megalapoznia a nemzeti szabályozást.
- Globális szabályozás szükséges elsősorban az internetes megfigyelés vonatkozásában.
- A technológiákat működtető intézmények belső ellenőrzési folyamatain kívül fontos a külső, független felügyelet a bizalom megteremtéséhez.
- A személyekhez köthető megfigyeléshez, mint amilyen a mobiltelefonos helymeghatározással végzett követés vagy az internetes megfigyelés (DPI), bírósági felhatalmazás és ellenőrzés szükséges.
- A szabályozásnak az állampolgárok számára is világosnak és érthetőnek kell lennie.
- Átláthatóságra van szükség azt illetően, hogy:
- a személyes adatokat hogyan használják,
- hogyan dolgozzák fel az adatokat, és
- melyek a technológia alkalmazásának pozitív és negatív oldalai.
- A biztonságpolitika kialakításába az átláthatóság és tájékoztatás elősegítése érdekében civil és emberi jogi szervezeteket kell bevonni.
- A szabályozásnak tartalmaznia kell az elfelejtéshez való jogot is, tehát ha valakit megfigyeltek, de nem bizonyosodott rá semmi, az adatait törölni kelljen a rendszerből.

Az alternatívák szerepe

Bár a konzultációk résztvevői sokféle aggodalmat fogalmaztak meg, nem utasították el eleve a megfigyelésen alapuló biztonsági technológiák használatát, azonban kifejezték azon félelmüket, hogy a technológia esetleg átveheti az irányítást az emberektől, ami a hagyományos biztonsági megoldások visszaszorítását eredményezheti.

A résztvevők hangsúlyozták, hogy bár a megfigyelési technológiák kiegészítő használatára szükség lehet rövid távon, de hosszú távon azokat a társadalmi problémákat kellene kezelni, amelyek közvetetten felelősek a bűnözésért, a terrorizmusért. Fontosnak tartották a társadalmi összetartás, a gazdasági igazságosság, valamint az egyén és az intézmények társadalmi felelősségvállalásának előmozdítását a biztonsági stratégia részeként.

A megfigyelésnek tiszteletben kell tartania a magánszférát és az állampolgári jogokat

Voltak olyan javaslatok, amelyek elutasították a megfigyelést, és elvetették az alkumodellt, mint a biztonság és a magánszféra között fennálló összefüggést. Ugyanakkor néhányan elégedettek lettek volna a megfigyelés korlátozásával és a magánszféra „magjának" a védelmével. Konszenzus volt a résztvevők között abban, hogy a demokratikus szabadságjogokat, tehát a szólásszabadságot és az állampolgári jogok gyakorlását is védelmezni kell.

Igény a tájékoztatásra

A résztvevők úgy érezték, hogy a hatóságok és a lakosság által birtokolt információk aszimmetrikusak. Ezen megfelelő tájékoztatással, ismeretterjesztő kampányokkal kellene változtatni.

Bizalom és bizalmatlanság a biztonsági és rendvédelmi szervek iránt

Gyakori vélemény volt, hogy azoknak, akiknek hatáskörében áll mások megfigyelése, ahhoz is megvan a hatalmuk, hogy visszaéljenek a helyzetükkel. Azt is sokan gondolták, hogy a megfigyelésen alapuló biztonsági technológiák kiterjesztett használata már önmagában növeli a visszaélés kockázatát.

A megfigyelésért felelős biztonsági és rendvédelmi szervek (és más állami hatóságok is) az alábbi esetekben lesznek megbízhatóak:

- az embereknek pozitív személyes tapasztalataik vannak velük kapcsolatban;
- az intézményekhez nem társítanak visszaéléseket;
- tájékoztatnak vagy közzétesznek információkat az adatgyűjtésről, -tárolásról és -használatról;
- átlátható a tevékenységük és a működésük;
- nincs korlátlan hatáskörük;
- ellenőrzik a tevékenységüket;
- az intézmények dolgozói, akik hozzáférnek az adatokhoz, jól képzettek, nem élnek vissza a hatalmukkal, nem korruptak, és jól meg vannak fizetve, így kevésbé megvesztegethetők.

Az az igény is megfogalmazódott, hogy a biztonsági szervek által gyűjtött adatokat a hatóságok szervezetükön belül tárolják, és korlátozzák a biztonsági megfigyelésben közreműködő magáncégek – például internet- és mobilszolgáltatók – szerepét az adatgyűjtésben.

Az állampolgárok bevonása

A résztvevők az állampolgári találkozóhoz hasonló nyilvános megbeszéléseket és nyílt vitákat igényelnének ezeknek a technológiáknak az alkalmazásáról, és azt, hogy beleszólásuk legyen abba, milyen esetekben, mikor és hogyan alkalmazzák e technológiákat.

Igényelnék annak lehetőségét, hogy valamiképpen ellenőrizhessék azokat az adatokat, információkat, amelyeket ezekkel a biztonsági technológiákkal gyűjtenek róluk. Az ezzel kapcsolatos minimális elvárásuk az volt, hogy a hatóságok részletesen tájékoztassák az állampolgárokat az adatgyűjtésről, meghatározva a megfigyelésben érintettek körét. Ugyanakkor az embereket már iskoláskortól oktatni kellene, hogy felelősségteljesebben használják ezeket az új technológiákat.

A technológia fejlesztése a magánszféra védelme érdekében

A megfigyelésen alapuló biztonsági technológiákat nemcsak a biztonsági kockázatok elhárítása érdekében kellene továbbfejleszteni, hanem abba az irányba is, hogy azok működésük közben minél jobban védjék a magánszférát, és automatikusan megakadályozzák a visszaéléseket.

Van-e más lehetőség, mint az alku?

A SurPRISE projekt egyik fontos célkitűzése az volt, hogy megvizsgálja az alkumodell létjogosultságát, tehát azt, hogy igaz-e az az elterjedt nézet, miszerint a biztonság csak a magánszféra megsértése árán növelhető, és így zéróösszegű játszmát feltételez: amennyivel többet szánunk az egyik érvényesítésére, annyit kell elvennünk a másikéból. Az állampolgári konzultációk során többféle véleménnyel találkoztunk, amelyek jól tükrözik, hogy a kérdés ilyenfajta leegyszerűsítése semmiképpen sem elfogadható.

Az alkumodellt *elfogadók* hajlamosak voltak kizárólag a megfigyelésen alapuló biztonsági technológiák kontextusában értelmezni a kérdést, tehát amikor a magánszféra és a biztonság kapcsolatát értékelték, kizárólag a megfigyelésre épülő biztonsági megoldásokra tudtak gondolni, és úgy vélték, ebben a kontextusban a modell érvényes, mert a megfigyelés önmagában sérti a magánszférát. Számukra a legnagyobb kihívás az volt, hogy hogyan lehet megtalálni az egyensúlyt a kettő között. Ugyanakkor még azok is, akik elfogadták a modellt, úgy vélték, fontos gondoskodni a technológiákkal összegyűjtött személyes adatok védelméről.

A *bizonytalanok* azt a nézetet vallották, hogy a biztonság és a magánszféra közti alkura sok esetben nincs szükség, például:

- ha a szabályozás világos és tisztességes, ugyanis a magánszférát a technológia puszta bevezetése nem veszélyezteti, csak annak alkalmazása, vagyis hogy kik jutnak hozzá az összegyűjtött adatokhoz, és azokat hogyan használják fel;
- ha a megfigyelésen alapuló konkrét biztonsági technológia alapvetően nem tekinthető magánszférát sértőnek (pl. a biometrikus azonosítást sokan a magánszférára nézve ártalmatlan technológiának tartották, és sokan a térfigyelő kamerákat sem tartották a magánszférára veszélyesnek);
- különleges helyzetekben, amikor a technológia aktívan életet menthet (pl. természeti katasztrófa esetén senki nem aggódna, hogy őt is megfigyelheti a mentésnél bevetett drón);
- ha a megfigyelésen alapuló biztonsági technológiákat nem megelőzésre, hanem egy már megtörtént esemény után használják (mert az első esetben rengeteg adatot gyűjtenek általában feleslegesen rengeteg ártatlan emberről is);
- hosszú távon, mert például a jobb életminőség nagyobb biztonsághoz vezethet a magánszféra veszélyeztetése nélkül, és akkor már nem lenne szükség az emberek megfigyelésére a biztonság garantálása érdekében, még ha rövid távon szükséges is lehet feladni a biztonság érdekében a magánszféra egy kis szeletét.

Az *alkumodell elutasítóinak* fő érvei a következők voltak:

- A leggyakoribb vélemény az volt, hogy a biztonság olyan módszerekkel is javítható, amelyek nem a megfigyelési technológiákon alapulnak (pl. több rendőr, jobb közvilágítás vagy mozgásérzékelő lámpa, szomszédok, lakóközösségek vagy kisebb települések, városrészek lakói odafigyelnek egymásra, egymás javait is tudatosan vagy önszerveződő csoporttal védik stb.).
- Mások úgy érezték, a társadalom lehet biztonságos úgy is, hogy egyúttal megvédi az emberek magánszférához való jogát. Úgy vélték, hogy a biztonsági technológiák fejlesztésénél figyelembe kell venni a magánszféra tiszteletét és az adatvédelmi jogsza-

bályokat. Egy technológia nemcsak abban lehet előremutató, hogy fokozza a biztonságot, hanem abban is, hogy jobban védelmezi az „ártatlan" tömegek magánszféráját.

- Néhányan azzal az érvvel utasították e el a modellt, hogy a félelem és a bizonytalanság nem valós, hanem szított, és a hatóságoknak akár érdekük is fűződhet ahhoz, hogy félelmet generáljanak az emberekben, mert ezzel tudják rávenni őket arra, hogy feladják bizonyos jogaikat, például a magánszférához való jogot és a demokratikus szabadságjogokat.

Állampolgári konzultáció – kutatási módszer, ami egyben lehetőség is arra, hogy az állampolgárok is hallassák szavukat

A SurPRISE projekt középpontjában egy széles körű állampolgári részvételen alapuló empirikus kutatás állt. Az Európai Unió FP7 keretprogramja által támogatott kutatás első szakaszában kilenc országban közel kétezren vehettek részt egész napos állampolgári konzultációkon. A második szakaszban öt országban félnapos konzultációkon közel kétszázan vettek részt.* A találkozókon a résztvevők 6–8 fős asztaltársaságokban osztották meg egymással véleményüket a megfigyelésen alapuló biztonsági technológiákról. Bár a kutatás mintája nem tekinthető klasszikus véletlen mintának, mivel a különféle csatornákon hirdetett találkozókra bárki önként jelentkezhetett, a találkozókra meghívottak kiválasztásának fő szempontja az volt, hogy a résztvevők demográfiai összetétele tükrözze az országra jellemző megoszlásokat nem, életkor, iskolai végzettség, a lakóhely településének jellege szerint, és az adott országban élő bevándorlók vagy kisebbségek is arányosan képviselve legyenek a találkozókon. A módszertan szempontjából fontos megjegyezni, hogy a részvételhez nem volt szükség semmilyen előzetes tudásra. A résztvevők a találkozókat megelőzően információs anyagokat kaptak. Az empirikus kutatás első szakaszában a tájékozódást vitaindító filmek is segítették, amelyekben szakértők mondtak el érveket és ellenérveket a megvitatásra kerülő technológiákról. A résztvevők kérdőíves kérdésekre válaszoltak, javaslatokat fogalmaztak meg a döntéshozók számára, illetve a beszélgetésekről jegyzetek is készültek, tehát nagy mennyiségű kvantitatív és kvalitatív „adat" keletkezett a konzultációk során.

Az állampolgári konzultáció, mint kutatási módszer, számos területen nyújt többletet a hagyományos közvélemény-kutatásokhoz képest, mivel segít meghaladni e kutatások korlátait. Az egyik ilyen korlát az idő- és információhiány. Ez a korlát különösen nyilvánvaló, amikor a kutatás témája új vagy összetett, ami új technológiák esetében szinte mindig fennáll. A klasszikus módszerek általában nem engedik, hogy a válaszadók elmagyarázzák, miért gondolkodnak egy bizonyos módon, és általában arra sincs lehetőség, hogy elmondják, ők mit változtatnának vagy tennének azért, hogy valami megváltozzon, fejlődjön, jobbá váljon. Az állampolgári konzultáció során lehetőség van az emberek mélyebb megértésére. A különféle dilemmákkal szembesített résztvevőknek van idejük kifejteni és egymással is megbeszélni véleményüket, és arra is van idő, hogy új ötletek szülessenek. Az információkat saját értékrendjükkel, világnézetükkel és élettapasztalataikkal ötvözve a résztvevők tudáson alapuló véleményeket és jól átgondolt javaslatokat képesek megfogalmazni. A megfontoláson és kellő mérlegelésen alapuló kutatási eredmények szembesíthetők a témában érintett, különféle érdekeket képviselő csoportok véleményével, akik mind arra hivatkoznak, hogy az állampolgárok, tehát a lakosság érdekeit képviselik. Az állampolgári találkozó lehetőség a döntéshozók számára, hogy meghallgassák az állampolgárok véleményét is – a témától függően – helyi, országos vagy nemzetközi szinten.

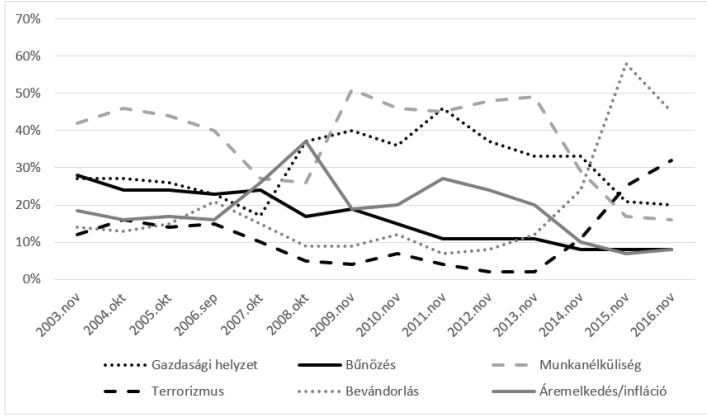
* Az első szakaszban konzultációt szervező országok: Ausztria, Dánia, Egyesült Királyság, Magyarország, Németország, Norvégia, Olaszország, Spanyolország, Svájc; a második szakaszban konzultációt szervező országok: Dánia, Magyarország, Norvégia, Olaszország, Spanyolország. Magyarországot a kutatásban a Medián Közvélemény- és Piackutató Intézet képviselte a cikk szerzője, Szénay Márta vezetésével.

Kitekintés

A SurPRISE projekt állampolgári konzultációira 2014 első felében került sor; az elemző munka 2015 januárjában lezárult. A kutatás témája szempontjából fontos esemény volt az állampolgári konzultációkat megelőző évben, 2013-ban kirobbant Snowden-ügy, amely titkos dokumentumok kiszivárogtatásával bizonyította, hogy az amerikai titkosszolgálatok széles körben figyelik az emberek mobiltelefon-hívásait és internetes tevékenységét az Egyesült Államokban és világszerte.

Párizsban a *Charlie Hebdo* szerkesztősége ellen elkövetett terrortámadást, amellyel a terrorizmus új európai szakasza vette kezdetét, 2015 januárjában, a kutatás lezárásának hónapjában hajtották végre, és bár a menekülthullám már megindult Európa felé, 2014 első felében, amikor a találkozókra sor került, még nem beszélt senki európai migrációs válságról, és a téma még az akkor már jelentősebben érintett Olaszországban rendezett találkozókon sem kapott figyelmet. Az EU-tagállamok polgárainak két legfőbb problémája még mindig a gazdasági válság és annak legfőbb következménye, a munkanélküliség volt. A SurPRISE projekt keretében rendezett állampolgári konzultációk óta sokat változott a világ, és mára a terrorizmus és a bevándorlás aggasztja legjobban az uniós polgárokat *(4. ábra)*. Vajon e változások hatására jelentősen megváltozott az emberek véleménye a biztonságról, a megfigyelésről és a magánszféráról?

4. ábra. Az EU lakossága számára legfontosabb problémák, amelyekkel hazájának szembe kell néznie (28 ország átlaga)[7]



A biztonsági intézkedések részben az elmúlt két évben európai célpontok ellen végrehajtott terrortámadásokra hivatkozva megszaporodtak, és bár nem tudunk róla, vélelmezni lehet, hogy fokozódott a lakosság megfigyelése. A híradások beszámolnak olyan esetekről, amikor letartóztatnak merényletre készülőket, mégis jó néhány terrortámadást sikeresen hajtottak végre a sokszor korábban már a hatóságok látóterébe került, tehát célzottan is megfigyelt terroristák.

7 A grafikon a következő kérdésre adott válaszok eredményeit mutatja: „Mi jelenleg az a két legfontosabb probléma, amivel (ORSZÁGUNKNAK) szembe kell néznie?", Eurobarometer Interaktív, http://ec.europa.eu/COMMFrontOffice/publicopinion/index.cfm/Chart/getChart/chartType/lineChart/themeKy/31/groupKy/188/savFile/5.

A 2016 karácsonyát közvetlenül megelőző berlini terrortámadást a város polgármestere a „szabadság ellen elkövetett merényletként" értékelte. Berlin a szabadság szimbóluma, ami azt is jelenti, hogy mentes az állami megfigyeléstől. Bár vannak Németországban térfigyelő kamerák, Berlinben azok nem engedélyezettek a közterületeken. Vajon változni fog-e ez a jövőben? Meg lehet-e állítani, illetve egyáltalán szeretnék-e megállítani az európai emberek a mindent és mindenkit egyre jobban kontrolláló biztonsági technológiák fokozódó terjedését, amelyek alkalmazói a közelmúlt terrortámadásai miatt immár a korábbinál jóval nagyobb hitelességgel hivatkozhatnak a terrorveszélyre?

Az EU-csatlakozásra pályázó török kormány digitális cenzúrával próbálja megakadályozni a hírek áramlását. Az emberek elszigetelése a hírek egy részétől és a közösségi oldalaktól a szolgáltatókra kifejtett nyomáson keresztül érhető el – például az internet lassításával vagy bizonyos hírportálok teljes „elnémításával" –, de az információk torzítására, meghamisítására is lehetőség nyílik az internetes megfigyelés részeként alkalmazott mély csomagvizsgálattal (DPI). Hogy ez megtörténik vagy sem, nem tudhatjuk. Vannak országok, ahol ezeknek a technológiáknak az alkalmazása a hatalom egyoldalú döntése, és nincsenek meg a megfelelő „fékek és ellensúlyok", amelyek legalább részben védelmezhetnék az állampolgárok jogait a hatalommal szemben.

Bár nem európai példa, de idetartozik, mert a megfigyelésen alapuló biztonsági technológiák erre is lehetőséget teremtenek: a kínai hatalom a digitális totalitárius állam[8] kiépítésével szeretné megerősíteni pozícióit, és egy „társadalmi kreditrendszer" bevezetését tervezi. A rendszernek dióhéjban az a lényege, hogy az új technológiák bevetésével az állam tökélyre vinné állampolgárai megfigyelését, és életük minden területéről adatokat gyűjtene, amelyekből folyamatosan értékelné, pontozná viselkedésüket, tehát azt, hogy mennyiben felelnek meg a hatalom szempontjából eszményinek számító állampolgár ideájának. Ha a hatalom által elvárt módon viselkedik valaki, jutalompontokat kap, ha valamit másképp tesz, pontokat veszít. Mindenki ismerhetné a pontszámát, aminek mértéke alapján juthatna esetleg előnyökhöz vagy érhetnék hátrányok a mindennapi életben. A párt a technológián keresztül folyamatosan szemmel tartja valamennyi állampolgárát, akik a megfigyelés következménye miatti aggódás hatására önként mondanak le magánszférájuk és szabadságjogaik egy részéről, és válnak olyan „alattvalókká", amilyennek a párt látni szeretné őket. Ez a rendszer még nincs bevezetve, és még nem is készült el teljesen. Elképzelhető, hogy a jövőben ilyen rendszerek biztosítják majd a világban a rend fenntartását, a rendét és a biztonságét, amire végső soron mindannyian vágyunk?

Hivatkozott irodalom

Čas, Johann (szerk.) (2015): *Policy Paper and Manual.* (Kutatási jelentés D 6.13.) Interneten: http://surprise-project.eu/wp-content/uploads/2015/03/SurPRISE-D6.13-Policy-paper-and-manual.pdf.

Creating a Digital Totalitarian State. *The Economist* (2016 december 17–23.): 20–22.

Foucault, Michel (1990 [1975]): *Felügyelet és büntetés.* Budapest: Gondolat.

Körmöczi Andrea, Szénay Márta és Venczel Tímea (2014): *Country Report – Hungary.* (Kutatási jelentés D 6.4.) Interneten: http://surprise-project.eu/wp-content/uploads/2014/10/D6.4_Country_report_Hungary_final_30.9.pdf.

Nielsen, Jacob Skjødt és Szénay Márta (2014): Involving Citizens in Security Policy Making. (konferencia-előadás: Joint Conference of SurPRISE, PRISMS and PACT, 2014. 11. 13–14., Bécs, Ausztria.) Interneten: http://surprise-project.eu/wp-content/uploads/2014/11/Nielsen_Szenay_Involving-Citizens-in-security-policy-making.pptx.pdf.

8 Creating a Digital Totalitarian State. *The Economist* (2016 december 17–23.): 20–22.

Pavone, Vincenczo, Sara Degli-Esposti és Elvira Santiago (2015): *Key Factors Affecting Public Acceptance and Acceptability of SOSTs.* (Kutatási jelentés D 2.4.) Interneten: http://surprise-project.eu/wp-content/uploads/2015/02/SurPRISE-D24-Key-Factors-affecting-public-acceptance-and-acceptability-of-SOSTs-c.pdf.

Standard Eurobarometer 86 (2016): *Public Opinion in the European Union* (2016 ősze). Interneten: http://ec.europa.eu/COMMFrontOffice/publicopinion/index.cfm/Survey/getSurveyDetail/instruments/STANDARD/yearFrom/1974/yearTo/2016/surveyKy/2137.

Strauss, Stefan (2015): *Synthesis Report of the Large Scale Events.* (Kutatási jelentés D 6.10.) Interneten: http://surprise-project.eu/wp-content/uploads/2015/02/SurPRISE-D6.10-Synthesis-report.pdf .

Szénay Márta (2015): *Comparative Report of the Small Scale Events.* (Kutatási jelentés D 7.2.) Interneten: http://surprise-project.eu/wp-content/uploads/2015/01/SurPRISE-D7.2-Comparative-report-Citizen-Meetings.pdf.