

Megfigyelés, magánszféra és biztonság

MI AZ ÖN VÉLEMÉNYE?

surprise
surveillance
privacy
security



Ez a projekt az Európai Unió Kutatási és Technológiafejlesztési Hetedik Keretprogramjának a támogatásában részesült. A támogatási szerződés száma: 285492.

Tartalom

1	Üdvözljük a SurPRISE projektben	5
2	Összefoglalás	6
3	Megfigyelés, magánszféra és biztonság	9
3.1	Megfigyelés	9
3.2	Magánszféra és adatvédelem: valóban fontos ügyek?	9
3.3	Biztonság	10
4	Öt új biztonsági technológia	12
5	Intelligens térfigyelő kamerák	13
5.1	Miért fejlesztették ki az intelligens térfigyelő kamerákat?	13
5.2	Hogyan használják az intelligens kamerákat?	14
5.3	Hogyan növeli biztonságunkat	15
5.4	Milyen problémákat vet fel?	15
6	Drónok	17
6.1	Miért fejlesztették ki a drónokat?	17
6.2	Mire használják a drónokat?	18
6.3	Hogyan növelik biztonságunkat?	19
6.4	Milyen problémákat vetnek fel?	19
7	Internetes megfigyelés mély csomagvizsgálattal	21
7.1	Mi célból fejlesztették ki a mély csomagvizsgálatot?	22
7.2	Hogyan használják a mély csomagvizsgálatot?	22
7.2.1	Kereskedelmi célú felhasználás	23
7.2.2	Közbiztonsági és nemzetbiztonsági használat	23
7.3	Hogyan növeli biztonságunkat?	24
7.4	Milyen problémákat vet fel?	24
8	Okostelefonos helymeghatározás	25
8.1	Miért fejlesztették ki az okostelefonos helymeghatározást?	25
8.2	Hogyan használják az okostelefonos helymeghatározást?	27
8.2.1	Kereskedelmi használat	27
8.2.2	Polgári- és nemzetbiztonsági használat	27
8.3	Hogyan növeli biztonságunkat?	28
8.4	Milyen problémákat vet fel?	28
9	Biometria	29
9.1	Milyen céllal fejlesztették ki az első biometrikus azonosítórendszereket?	29
9.2	Mire használják a biometrikus rendszereket?	29
9.3	Milyen előnyökkel jár?	31
9.4	Milyen problémákat vet fel?	31
10	A megfigyelésre alapuló technológia az egyetlen lehetőség?	33
10.1	Alternatív biztonsági intézkedések: a globális szint	33
10.2	Alternatív biztonsági intézkedések: a helyi szint	34
11	És most Önön a sor	36
	Az ismertetőről	37
	A projektben résztvevő intézmények	38

1 Üdvözöljük a SurPRISE projektben

Üdvözöljük európai kutatásunkban, a SurPRISE kutatási projektben. Az elnevezés az angol kutatási cím rövidítése: "Surveillance, Privacy and Security", magyarul "Megfigyelés, Privátszféra, Biztonság". A SurPRISE projekt legfőbb célja, hogy összegyűjtse az európai polgárok véleményét az új biztonsági technológiákról. E technológiák jelentős része azon alapszik, hogy megfigyeli az embereket, és kifürkészi, mit csinálnak, mivel foglalkoznak. A rendőrség és a biztonsági emberek arra használják ezeket az információkat, hogy ellenőrizzék, mi történik, észrevegyék és elhárítsák a biztonsági problémákat. Amikor az Ön csomagjait szkennerekkel vizsgálják át a repülőtéren, vagy térfigyelő kamerák (CCTV) rögzítik minden mozdulatát, miközben az utcán sétál, Ön is szembe találja magát a megfigyelésen alapuló biztonsági technológiákkal. A SurPRISE projekt szeretne hozzájárulni ahhoz, hogy ezek a technológiák hatékonyak, biztonságosak legyenek, és tiszteletben tartsák az emberi jogokat. Ehhez szükségünk van az Ön segítségére.

Azért hívtuk meg Önt a SurPRISE projektbe, mert az Európai Bizottság szeretné megkérdezni az Unió lakosaitól, milyen lépésekre lenne szükség ahhoz, hogy mindannyian, minden szempontból nagyobb biztonságban érezhessük magunkat. A SurPRISE állampolgári találkozón Ön megoszthatja a többiekkel az új biztonsági technológiákkal kapcsolatos

véleményét, gondolatait. A SurPRISE projekt pedig összegyűjti a résztvevők véleményét, és eljuttatja az Európai Bizottsághoz.

A SurPRISE project kilenc európai országban gyűjti össze az emberek véleményét az új biztonsági technológiákról: Magyarország mellett Angliában, Ausztriában, Dániában, Németországban, Olaszországban, Spanyolországban, Svájcban és Norvégiában.

Ez az ismertető alapvető információkat nyújt azokról a kérdésekről, amelyeket a magyarországi találkozón fogunk megvitatni 2014 júniusában. Tájékoztatást ad azokról az új biztonsági technológiákról, amelyek a SurPRISE-kutatás középpontjában állnak. Az ismertető emellett háttérinformációkat is tartalmaz a megfigyelés, a magánszféra és a biztonság európai helyzetéről.

A részvétele pontosan azért fontos a számunkra, mert Ön nem a téma szakértője. Azért kértük fel a részvételre, mert Ön egy az európai polgárok közül, akiknek az életére közvetlen hatással vannak az európai és hazai politikusok döntései.

A politikusaink döntenek a biztonságpolitikáról, de Ön és a többi állampolgár lesznek kénytelenek együtt élni e döntések következményeivel. Éppen ezért nagyon fontos az Ön véleménye.

A tudomány ismereteket nyújt, de nem mondja meg, mit kell tennünk. A döntés a miénk. Mondja el Ön is véleményét!

2 Összefoglalás

Sokan már el sem tudnák képzelni az életüket okostelefonok, bankkártyák vagy internet nélkül. Abba azonban nem gondolnak bele, mert talán nem is tudják, hogy e technológiák használata során számtalan elektronikus feljegyzés keletkezik rólunk. Ezekből a feljegyzésekből ugyanis kiolvasható, mikor hol tartózkodunk, és esetenként még az is, hogy mit csinálunk éppen. Például a banki tranzakciók, tehát a bankkártyás fizetés is, adatokkal szolgálhatnak az általunk vásárolt termékekről és arról, hogy ezeket honnan szereztük be. Ezeket az adatokat azután a bankok saját adatbázisaikban tárolják, és általában mi magunk is láthatjuk őket a banki számlakivonatokon.

A légitársaságoknál tárolt utazási foglalásokra vonatkozó adatokból kiolvasható, hogy éppen a világ valamely veszélyesebb régiójába tartunk-e, vagy onnan térünk-e haza. A mobiltelefon adatai mutatják, mikor hol tartózkodunk, kivel telefonálunk és milyen gyakran. Ezeket az adatokat a mobiltelefon szolgáltatók és az internetszolgáltatók raktározzák adatbázisaikban. Az európai szabályozás kötelezővé teszi ezen adatok tárolását legalább hat hónapig, de legfeljebb két évig. Ez lehetővé teszi a legtöbb ember azonosítását és nyomon követését élete egye pillanataiban.

Ezekből a technológiákból, illetve az ezekkel gyűjtött információkból mi is és mások is profitálhatnak. Az Európában és másutt elkövetett, sok áldozatot követelő terrortámadások nyomán a kormányok elkezdtek befektetni olyan fejlett biztonsági technológiákba, amelyek az ilyen információkat használják. Emellett több meglévő törvényt is módosítottak, illetve újakat hoztak annak érdekében, hogy az ilyen adatokhoz biztonsági célból könnyebben hozzá lehessen férni. Habár léteznek „hagyományos” hírszerzési források, a kormányok rájöttek, hogy a potenciális terroristák és bűnelkövetők az új módszerekkel sokkal egyszerűbben leleplezhetők. A hétköznapi emberekhez hasonlóan, a bűnözők és a terroristák is rendelkeznek bankszámlával, személyazonosságuk igazolására alkalmas dokumentumokkal, használják az internetet és van mobiltelefonjuk. Ők is utaznak tömegközlekedési eszközökkel, megfordulnak közterüle-

teken, és vásárolnak termékeket, szolgáltatásokat. Talán ha többet lehetne megtudni ezekről a tevékenységeikről, könnyebb lenne a bűnözők és terroristák nyomára bukkanni. Sok kormány biztos abban, hogy az új biztonsági technológiáknak köszönhetően nem csupán a bűnelkövetők elfogása válik lehetővé, hanem a potenciális bűnözők azonosítása is már azt megelőzően, hogy valamit elkövetnének. Mivel ezek a technológiák a fentebb leírt módon használják az információkat, a SurPRISE projektben úgy emlegetjük ezeket, mint ‘megfigyelésen alapuló biztonsági technológiák’.

A megfigyelésen alapú biztonsági technológia tehát:

olyan technológia, amely a legkülönbözőbb összefüggésekben gyűjt információkat a lakosságról egy biztonsági probléma kezelésére.

Ezek a technológiák elemzik az emberek mindennapjairól keletkezett információkat. Olyan adatokat dolgoznak fel, amelyek többek közt mobiltelefonokból, az internetről, vagy ‘intelligens’ technológiákból nyerhetők ki, mint amilyenek például a digitális térfigyelő rendszerek. A cél a bűnözők és terroristák azonosítása, lehetőleg még mielőtt elkövetnének valamit.

Ebben az információs füzetben öt ilyen biztonsági technológiát fogunk részletesebben megvizsgálni:

- **Intelligens térfigyelő kamerák (CCTV):** Olyan térfigyelő rendszerek, amelyek továbbmennek a közterületek pusztá megfigyelésénél. Az intelligens térfigyelő rendszerek digitális kamerái képesek az arcok felismerésére, az emberek viselkedésének elemzésére, és tárgyak azonosítására.
- **‘Civil’ drónok:** nem katonai célra használt pilóta nélküli légi járművek (UAV). A megfigyelési tevékenységek széles körében lehet bevetni a drónokat. Fel lehet őket szerelni kamerával és más érzékelő technológiákkal, és akár úgy is lehet őket tekinteni, mint egy repülő térfigyelő kamera.

- **Internetes megfigyelés mély csomagvizsgálattal:** Hardver eszközök és speciális szoftverek segítségével lehetőség van az interneten átmenő össze üzenet és információ elolvasására, elemzésére és manipulatív célú megváltoztatására is.
- **Okostelefonos helymeghatározás:** A mobiltelefonból származó helymeghatározási adatok elemzésével információ nyerhető ki a telefon használojának tartózkodási helyéről és mozgásáról egy adott időszakban. A telefonkészülék helyét a mobiltelefon-tornyokból származó adatokkal lehet bemérni, amelyekhez a telefon kapcsolódott. Még pontosabb helymeghatározást tesz lehetővé a globális helymeghatározó rendszer (GPS), vagy a vezeték nélküli adatforgalom.
- **Biometria:** A biometria az emberek fizikai vagy viselkedési jellegzetességeinek mérésén alapuló automatikus azonosságfelismerő rendszerekre utal. Leggyakoribb használata a biometrikus útleveél, amely arc-, ujjlenyomat- és/vagy íriszazonosításon alapszik.

Mind az öt technológia hozzájárulhat biztonságunk növeléséhez azáltal, hogy beazonosítja a gyanús személyeket, a bűncselekményeket és más illegális tevékenységeket. Vannak, akik azt gondolják, hogy hozzájárulhatnak életünk kényelmesebbé tételéhez is. Mindegyik technológia azonban egy sor hátránnyal is jár. Az intelligens térfigyelő kamera-rendszerek vagy a kamerával felszerelt drónok például csak bizonyos körülmények között működnek, és sok „téves riasztást” produkálnak. A mély csomagvizsgálat teljesen ellehetetleníti a diszkréciót az internetes kommunikációban. Az okostelefonos helymeghatározást nehéz kontroll alatt tartani, mivel sok mobiltelefonos alkalmazás továbbít információkat a telefonból a használó tudta nélkül. A biometrikus adatokat tartalmazó adatbázisokból kiszivárgó adatok a személyazonosság ellopásához vezethetnek. Az információgyűjtés és az információk felhasználása feletti kontroll hiánya problémákat vet fel mindegyik általunk vizsgált technológia kapcsán.

Ezeknek a technológiáknak a használata azonban kérdéseket vet fel az emberi jogok, a magánszféra, a szabályozás és a bizalom vonatkozásában. Ezek a technológiák ugyanis általában az emberek tudta nélkül gyűjtenek és továbbítanak róluk adatokat. Így aztán elkerülhetetlen, hogy ártatlan emberekről is gyűjtsenek adatokat, és elemezzék azokat, bizonyos technológiák esetében szándékosan. Megvan tehát a lehetőség, hogy behatoljanak a magánszféránkba, amelynek védelme Európában alapvető emberi jog. Az is előfordulhat, hogy egy ártatlan embert tévesen azonosítanak veszélyes személyként, aminek súlyos következményei lehetnek az illető életére.

A technológiák által kínált biztonsági előnyök ellenére egyesekben kétségeket ébreszt a róluk származó információk biztonsági célra való felhasználása. Ha e technológiáknak köszönhetően mindenkinek a biztonsága nő, talán rendben is van ez így. Azonban, ha az alapvető emberi jogok is sérülnek, talán soha nem mondhatjuk, hogy ez rendben van. Az emberek sokféle véleményt képviselhetnek attól függően, hogy mit gondolnak egy csomó más kérdésről, például ezekről:

- Valóban hatásosak ezek a technológiák?
- Mennyire tolaakodnak be a magánszféránkba?
- Van-e megfelelő jogi szabályozás?
- Az új technológiákat vajon mindig a törvények betartása mellett alkalmazzák?
- Megbízhatóak-e azok az intézmények, amelyek alkalmazzák őket?
- Törvényileg mennyire jól szabályozott az ilyen intézmények működése?
- Átláthatóak-e ezek az intézmények és elszámoltathatóak-e minden esetben, amikor biztonsági okokra hivatkozva megsértik a magánszférát?
- Ki ellenőrzi a megfigyelést végzőket?
- Milyen alternatív megoldások léteznek, és ezek mennyire célravezetők?

Ez néhány kérdés azok közül, amelyeket megvizsgálunk majd az állampolgári találkozón.

A tudományos ismeretterjesztés, a tudatos fogyasztóvá váláshoz szükséges ismeretek átadása és különösképpen a tudományos és technológiai fejlődés ellentmondásainak megismertetése alapvető fontosságúak ahhoz, hogy az emberek részt tudjanak venni nyilvános vitákban, és gyakorolni tudják demokratikus jogaikat.

A következő néhány bekezdésben bevezetünk néhány fontos fogalmat, amelyek témánkhoz kapcsolódnak, mielőtt részletesebben bemutatnánk az öt kiválasztott technológiát.

Kérjük, folytassa az olvasást, hogy még többet megtudjon ezekről a témákról!

3 Megfigyelés, magánszféra és biztonság

3.1 Megfigyelés

A megfigyelés szó hallatán elsőként talán a „Nagy Testvér” ugrik be legtöbbünknek, akár a közkeletű valóságshow-kból, akár George Orwell 1984 című könyvéből. E kép miatt könnyen társítjuk a megfigyeléshez azt a háborzongató érzést, hogy egy nagyhatalmú, de számunkra ismeretlen szervezet vagy személy figyel bennünket.

A SurPRISE projektben a megfigyelésről olyan értelemben beszélünk, hogy ez „az emberek ellenőrzése, hogy viselkedésük szabályozható és irányítható legyen”. Ez több okból is történhet. Például a rendőrség térfigyelő kamerákat vagy kamerával felszerelt drónokat használhat, hogy beazonosíthassa vagy kövesse az utcai bűnelkövetőket. Vagy például egy keresőmotor szolgáltató elemezheti a felhasználók szörfölési viselkedését internetes módszerekkel azért, hogy javítsa a kereső szoftvert. A megfigyelés használható tehát bűnmegelőzésre és bűnözők elfogására, de arra is használják, hogy termékeket, szolgáltatásokat adjanak el.

De ha a megfigyelés valóban teljesen hétköznapi dolog, Ön joggal tűnődhet el azon, hogy akkor vajon mi is a baj vele? A „megfigyelt társadalomról” vagy „kukkoló társadalomról” szóló híradások valahogy mindig vészjóslóan hangzanak. A helyzet ugyanis az, hogy a megfigyeléshez szükséges technológia birtoklása komoly hatalommal ruház fel. Éppen ezért fontos, hogy mindazok, akik e hatalom birtokában vannak – mint például a bűnüldöző és rendvédelmi szervek, adatbrókerek vagy kiskereskedők – hatalmukkal becsületesen bánjanak, kellően tiszteltetben tartva az állampolgári szabadságjogokat és a törvényeket.

Lehet, hogy Ön azt gondolja, nincs mit eltitkolnia és nincs semmi félnivalója. Ez a hozzáállás nagyban függhet attól, hogy ki és miért figyeli Önt, és hogyan értelmezi az Ön tetteit. Ha Ön ebbe nem látna bele, és szava se lehetne hozzá, és a szabályok egyszer csak Ön ellen fordulnának – tegyük fel, az Ön etnikai vagy vallási hovatartozása, szexuális beállítottsága, nemi hovatartozása vagy politikai nézetei miatt – ilyen esetben mit tenne? Egyebek mellett

ezért lehet a túlzott mértékű megfigyelés romboló hatással más emberi jogokra is, mint amilyen például a szabad véleménynyilvánításhoz való jog. Ilyen körülmények között a megfigyelés sokat árt hat a társadalmi bizalomnak, ami ahhoz vezethet, hogy az emberek végül félnek vállalni saját magukat, nézeteiket. Ezért azután nagy tétje van annak, amikor a megfigyelésből származó különféle adatokat biztonsági célokra használják.

3.2 Magánszféra és adatvédelem: valóban fontos ügyek?

Az egyik fő aggály a magánszférához és az új biztonsági technológiák által előállított és felhasznált adatok védelméhez köthető. Bár a magánszféra sokunk számára mást és mást jelenthet, abban mindenki egyetért, hogy fontos része a mindennapi életnek. Sok dolog van, amit esetenként talán Ön is szívesebben kezel magánügyként. Például a következőket:

- azt, amit csinál, gondol vagy érez
- információkat az intim kapcsolatairól, hol tartózkodik, mit ír másoknak levélben vagy emailben, milyen jellegzetes tulajdonságai vannak, hogy néz ki
- az Ön testét: hogy mennyit kíván felfedni belőle, vagy hogy el tudja-e hárítani a nem kívánt érintést vagy motozást, és ellenőrizni tudja-e, mi történik az Öntől származó DNS-mintával, ujjlenyomattal, és más, a testéből/testéről származó úgynevezett biometrikus adattal

Gondoljon csak bele, örülne-e, ha egy biztosítótársaság korlátlan hozzáféréssel rendelkezne az Ön összes egészségügyi leletéhez? Vagy ha a rendőrség meghallgathatná az Ön összes telefonbeszélgetését? Vannak függőyei az otthonában? Még ha az első és a második kérdésre „nemmel” válaszolt, és csak a harmadikra mondana „igen”, Önről akkor is elmondható, hogy törődik a magánszférájával. És ezzel egyáltalán nincs egyedül! A közösségi médiát használó fiatalokról készült kutatások rámutattak, hogy a privát szférájuk féltése miatt többségük igen komolyan megválogatja, hogy milyen tartalmakat oszt meg magáról az interneten. Sokan szeretnek információkat megosztani magukról, de

csak bizonyos határok között. Az egyének számára minden, ami e határok mögött található, életük azon területéhez tartozik, amelyet védeni akarnak a külső hatásoktól: ez a magánszférájuk.

A SurPRISE projektben úgy definiáljuk a magánszférát, hogy az:

az egyének az a képessége, hogy magában, a nyilvánosság látókörén kívül tudjon maradni, és a rá vonatkozó adatokat, információkat kontrollálni tudja.

A magánszférához és a személyes adatok védelméhez fűződő jog alapvető emberi jog az Európai Unióban. Mindenkinek szüksége van a magánszférához való jogra: hogy szabadon cselekedhessen, hogy kedvére találkozhasson és vitathasson meg dolgokat másokkal egy demokratikus társadalomban. Az emberek nem élhetnek demokratikus szabadságjogaikkal igazán, hogyha valaki ismerheti minden gondolatukat, szándékukat és cselekedetüket.

Az új európai adatvédelmi törvények ezért hangsúlyt fognak fektetni rá, hogy e modern technológiákba beletervezzék a privátszféra védelmét, hogy azok már eleve kevésbé sértsék a magánszférát. Ösztönözni fogják a vállalatokat, amelyek az új biztonsági technológiákat gyártják, hogy a fejlesztés és tervezés minden fázisába kalkulálják bele a magánszféra védelmét. Ezt az új megközelítést nevezik 'beépített adatvédelemnek'.

3.3 Biztonság

A SurPRISE projektben a következő módon definiáljuk a biztonságot:

a biztonság az az állapot, amelyben nem vagyunk kitéve veszélynek, vagy a veszélyekkel szemben megfelelő védelem áll rendelkezésünkre; amikor tehát biztonságban érezhetjük magunkat, nincs veszélyérzetünk.

A biztonság fogalma nemcsak az olyan kézzel fogható dolgok kapcsán értelmezhető, mint amilyen például egy épület, egy információs rendszer, vagy éppen az országhatárok. A biztonság fogalmának éppúgy fontos eleme az emberek biztonságérzete is. Egy ideális világban a hatékony biztonsági in-

tézkedések az emberek biztonságérzetét is növelik, de a valóságban ez nem mindig van így.

Furcsának tűnhet, de amiatt, hogy az új biztonsági technológiák veszélyt jelenthetnek a magánszféránkra, előfordulhat, hogy *nem javítják*, hanem *rontják* biztonságérzetünket. Ez nem feltétlenül igaz mindenkire. A magánszférához hasonlóan a biztonság is mást és mást jelenthet a különböző embereknek. Mindannyiunknak megvan a maga elképzelése arról, hogy mi fenyegeti a biztonságunkat, illetve hogy mire lennének hajlandóak, hogy megvédjük mindazt, ami számunkra fontos.

Ez igaz azokra is, akik felelősek a biztonságért. Be kell azonosítaniuk és le kell küzdeniük a főbb fenyegetéseket. Minden kormányról elmondható, hogy csak korlátozottan állnak rendelkezésére azok a gazdasági, emberi és technikai erőforrások, amelyeket a biztonság szavatolása érdekében fel tud használni. Éppen ezért rangsorolniuk kell, hogy mire milyen mértékben összpontosítanak. Az Európai Unióban a következő ügyek élveznek elsőbbséget:

- a kiberbiztonság fokozása az Európai Unióban mind az állampolgárok, mind a cégek számára
- a nemzetközi bűnügyi hálózatok felszámolása
- a terrorelhárítás
- Európa erősítése, hogy képes legyen kilábalni bármilyen válságból és katasztrófából

Mivel Európa eldöntötte, hogy mostantól a válságokból és katasztrófákból való kilábalásra is komolyan összpontosít, a biztonság értelmezése mára túlmutat a terrorelhárítás és a bűnmegelőzés fogalmain. Európa figyelmet fordít a környezet és természeti kincseink, az infrastruktúra, a gazdaság, valamint egészségünk védelmére is. A politikai döntéshozók számára a biztonság fogalma ily módon kiterjed a polgárok életének csaknem minden területére. Ez a szemlélet sok Európai országban meghatározóvá vált. De vajon beválthatóak-e a biztonsággal kapcsolatos ígérek az élet minden területén? A biztonsági ipar, amelynek célja, hogy kielégítse ezt az igényt, mára nagyra nőtt Európában. A nagyvállalatok mellett számtalan kisebb cég is helyet kap benne. A megfigyelésen alapuló leg-

újabb fejlesztésű biztonsági technológiák között olyanokat találunk, mint például:

- intelligens térfigyelő kamerák (CCTV), amelyek képesek azonosítani ismert elkövetőket, illetve érzékelni a gyanús viselkedést
- internetes megfigyelés, amely a vírusok, a hackerek, valamint a személyazonosság eltulajdonítására törekvők tevékenységének megakadályozására irányul
- biometrikus azonosító rendszerek, amelyek célja megakadályozni, hogy illetéktelenek juthassanak be egy adott területre, illetve meggyorsítani a beutazást egy országba azok számára, akiket az állam 'megbízható utasnak' tart
- légi térfigyelő drónok, amelyek képesek a levegőből észlelni veszélyes tevékenységeket, amelyek a földről nem láthatók. Az így megszerzett információk segítségével a biztonsági személyzet gyorsan eljuttatható a veszély helyszínére
- fejlett utasinformációs rendszerek, amelyek a veszélyt jelentő utasokat még utazásuk megkezdése előtt képesek azonosítani
- helymeghatározó- és követő technológiák, amelyek mozgó objektumok védelmét szolgálják (például értékes vagy veszélyes anyagok szállításakor), valamint lehetővé teszik a gyanús személyek pontos térbeli azonosítását

4 Öt új biztonsági technológia

A SurPRISE project a következő öt biztonsági technológiát vizsgálja:

- Intelligens térfigyelő kamerák
- (Civil) drónok
- Internetes megfigyelés mély csomagvizsgálattal
- (Okos-) telefonos helymeghatározás
- Biometrikus azonosítás

Ezeket a biztonsági technológiákat folyamatosan fejlesztik, és még sok kérdés nyitott ezekkel kapcsolatban.

A következő fejezetekben összefoglaljuk, hogy ezek a technológiák hogyan működnek, miért fejlesztet-

ték ki őket, kik és hogyan használják őket. Emellett bemutatjuk, hogyan növelik biztonságunkat, és a használatuk milyen problémákat vet fel.

A SurPRISE projekt és az Európai Unió számára egyaránt fontos, hogy kiderüljön, az emberek hogyan vélekednek ezekről az új biztonsági technológiákról, és mennyire tartják elfogadhatónak őket. Ezért nagyon fontos az Ön véleménye is. Talán Ön már ismeri és támogatja, vagy éppen kimondottan ellenzi egyik vagy másik új technológiát. A SurPRISE találkozó során sok lehetősége lesz hangot adni véleményének. Nagyon szeretnénk, ha mindenképpen elgondolkodna a következő kérdéseken.

Mitől lesz egy új biztonsági technológia jobban avagy kevésbé elfogadható az Ön számára?

Esetleg:

- Ha Ön jobban ismeri a technológiát és annak működését?
- Ha többet tud arról, hogy a különböző intézmények, állami szervek hogyan használják e technológiákat és a segítségükkel megszerzett információkat?
- Ha hatékony a kapcsolódó törvényi szabályozás és ellenőrzés?
- Ha több információval rendelkezik azokról az aktuális fenyegetésekről, amelyek leküzdése az adott technológia célja?

Vagy azon múlik, hogy Ön mennyire gondolja súlyosnak az adott technológia magánszférára gyakorolt hatását. Például:

- Lehet-e kínos az Ön számára?
- Sérti-e az Ön alapvető emberi jogait?
- Továbbít-e adatokat harmadik fél számára az Ön tudta és beleegyezése nélkül, vagy hatással van-e bármilyen más módon az ön magánszférájára?

Esetleg azon múlik, hogy mennyire hatékony az adott technológia:

- Kényelmesebbé teszi-e az Ön életét?
- Segítségével nagyobb biztonságban érezheti-e magát?
- Az Ön véleménye szerint valóban pontosan azonosítja-e a gyanúsítottakat?

Vagy talán csak akkor figyel fel az ilyen biztonsági technológiákra, amikor ezek jól láthatóan és kézzel foghatóan ott vannak Ön körül. Mint például egy repülőtéren, az utcán, egy mobiltelefon vagy az internet használata során. Más körülmények között esetleg nem is zavarják Önt. Vagy Ön most még elfogadja őket, de aggódik amiatt, hogy hogyan változik mindez a jövőben.

5 Intelligens térfigyelő kamerák

A hagyományos kamerák sokszor hozzátartoznak az utcaképhez, találkozunk velük a köztereken vagy a boltok bejáratánál. A kamerák televíziós kapcsolatban állnak a kontrollszobával, ahol sokszor több tucat képernyő közvetíti a szakképzett operátornak a kamerák által vett képet. A kamerák rögzítik, amit „látnak”, tehát a felvételek eltárolódnak, de egy bizonyos idő elteltével törlik őket. A rendszer zárt, ezért zárt láncú kamerarendszernek is nevezik, mivel a felvételek kizárólag a kontrollszoba képernyőin jelennek meg. Ha az operátor észrevesz valami gyanúsat, telefonon kapcsolatba lép a biztonsági őrkkel vagy a rendőrséggel, hogy azok közbeléphessenek.

5.1 Miért fejlesztették ki az intelligens térfigyelő kamerákat?

A térfigyelő kamerákat eredetileg a rakétatámadások leleplezésére és a kockázatot jelentő ipari folyamatok távolból történő irányítására fejlesztették ki a II. világháborúban. Biztonsági technológiaként először az USA-ban kezdték el árusítani őket az 50-es években. A rendőrség a 60-as évektől használja őket. 2013-ban a térfigyelő kamerák szerepe döntő volt a bostoni maratonton történt robbantás elkövetőinek a leleplezésében.



A térfigyelő kamerák intelligens változatainak kifejlesztésekor azokra a problémákra koncentráltak, amelyekkel a térfigyelő kamerák a kezdetektől küszködtek. A lényeg, hogy túl sok a kamera ahhoz képest, hogy mennyi a képernyőket figyelő szem-pár. A hagyományos kamerarendszerrel szemben az intelligens térfigyelő rendszer digitális kamerák hálózatából áll, ezekhez egy számítógépes rendszer

is kapcsolódik, amely képes elemezni a digitális képeket. A szoftver a képek alapján elemzi, hogy mi történik. Ha valami szokatlant észlel, riasztó jelet ad ki, amivel felhívja az operátor figyelmét a gyanús képekre. A rendszer rögzíti a riasztást, és a számítógép elkülöníti a riasztáshoz kapcsolódó képeket, amelyek így könnyen megoszthatóvá, továbbküldhetővé válnak.

Az intelligens térfigyelő rendszerek sok mindenre alkalmasak. Leggyakrabban arra használják őket, hogy:

- azonosítsanak objektumokat, mint például járműveket a rendszámuk leolvasásával, amit összevetnek a betáplált adatbázissal
- személyeket azonosítsanak az arcuk alapján, amikor az arc egyszerű, világosan értelmezhető háttér előtt jelenik meg. Az azonosításhoz az adatbázisban tárolt, már ismert személyek fotójával vetik össze a képet.
- őrizetlen csomagokat azonosítsanak, de csak abban az esetben, ha a csomagot egy üres térben hagyták.

Bár az intelligens térfigyelő kamerák az alább felsoroltakat még nem tudják megbízhatóan produkálni, a szoftvereket folyamatosan fejlesztik, abból a célból, hogy:

- képesek legyenek tömegben, ruházatuk alapján azonosítani embereket
- gyanús viselkedéseket azonosítsanak, vagy a kamera által megfigyelt területen szokatlannak tűnő viselkedéseket észleljenek, mint például lézengő fiatalok. A lefilmezett viselkedést folyamatosan összevetik az adatbázisban tárolt, ismert viselkedésmintákkal.

Nem minden intelligens térfigyelő rendszer egyforma. Hogy mennyire „intelligens” a rendszer, az attól függ, hogy a hozzá kapcsolódó szoftver mennyire jól tudja elemezni a kapott képeket, és attól is, hogy a megosztás után mi történik a képekkel. A rendszereket különböző céllal helyezik üzembe, tehát lehet, hogy egy bizonyos rendszer nem mindenre képes abból, amit eddig felsoroltunk, mert a rendszer üzemeltetője nem feltétlenül igényli az összes funkciót.

5.2 Hogyan használják az intelligens kamerákat?

Az intelligens kamerarendszerek kereskedelmi forgalomban kapható termékek, amelyeket biztonsági- és védelmi-technológiai vállalatok árusítanak. Számtalan rendszer kapható már. Az intelligens térfigyelő kamerák legfőbb intézményi felhasználói jelenleg a közlekedési hatóságok, például autópályát, repteret vagy vasutat kezelő társaságok, a helyi önkormányzatok és a rendőrség.

Budapesten például a rendőrség 2012 végén kezdett el intelligens térfigyelő kamerákat használni a buszsávok ellenőrzésére. A rendőrség jogszerűen használhatja a képeket bírságolásra, ha valaki ráhajt a buszsávra.

Az Európai Unió 16 különböző projektet támogat, amelyek az intelligens térfigyelő rendszerek algoritmusait és funkcióit hivatottak továbbfejleszteni. Jelenleg olyan bonyolultabb célokra is fejlesztenek és folyamatosan javítanak algoritmusokat, mint a gyanús viselkedés felismerése vagy az arcok felismerése tömegben. Ezek használata még nem terjedt el, de folyamatosan tesztelik az új rendszereket. Például a római, londoni, párizsi, brüsszeli, milánói és prágai közlekedési hatóságok nemrégiben olyan rendszer kipróbálásában vettek részt, amely intelligens térfigyelő kamerákat használ a

gyalogosok megfigyelésére. A rendszer riasztja az operátorokat gyanús csomagok, a gyalogosok rendellenes mozgása vagy szokatlan viselkedése esetén. Ez a rendszer még nincs üzembe helyezve, a tesztelése még ennek az ismertetőnek a megírása idején is zajlott.

Az intelligens kamerák talán legelterjedtebb használata az automatikus rendszámfelismerés. A rendszám tábláról készült digitális kép segítségével a rendszámot össze lehet vetni az országos autótulajdonosi nyilvántartással, a biztosítási adatbázisokkal és a rendőrségi nyilvántartásokkal. Az gépkocsi tulajdonosa és a bejegyzett címe gyorsan megállapítható, és a rendszámfelismerő kamera máris megjelöl egy konkrét személyt adott időben és térben. A rendszer alkalmas a lopott járművek felismerésére, és kiszúrja, ha egy jármű az adó vagy a kötelező biztosítás befizetése nélkül fut, vagy gyorsabban halad, mint a szabályok szerint.

Kérdés, hogy a különböző típusú bűncselekmények vagy szabálysértések ugyanolyan mértékű megfigyelést tesznek-e indokolttá. Minden kihágás ellenbe kell-e vetni az intelligens kamerákat, vagy inkább csak a legveszélyesebb bűncselekmények leleplezésére alkalmazzuk őket? Németországban például 2008-ban az Alkotmánybíróság adatvédelmi okokból korlátozta a rendszámleolvasó ka-

Hogyan működik az intelligens térfigyelő kamera?

A térfigyelő kamerához kapcsolt „intelligens” algoritmusok megtanulják, hogy hogyan ismerjék fel a viselkedések bizonyos típusait. Ezeket „riasztásindító” eseményeknek hívják: például amikor valakinél fegyver van, vagy valaki mozdulatlan egy mozgó tömegben. Az algoritmus egy sor számításból áll, ami végigfut a digitális képekben tárolt adatokon. Az intelligens algoritmus képes megtanulni, mit kell keresnie, mivel egyre több adatot elemez.

A térfigyelő rendszerek intelligens algoritmusainak az a dolga, hogy lemásolják az emberi szem és agy működését. A szoftver apró egységekre, „pixelekre” bontja fel a képet. Ön találkozhatott már a „pixel” szóval, ha van digitális fényképezőgépe vagy okostelefonja. Ha a digitális fényképezőgép 8 megapixeles, akkor minden egyes kép, amit a fényképezőgép készít, 8 millió pixelből áll.

Az algoritmus képes kiszámolni a képen minden egyes pixel mozgásának az intenzitását. Így tudja a szoftver minden egyes jelenetben azonosítani az aktív területeket. Ebből tanulja meg felismerni a mozdulatokat a képen. A rendszer, a már megismert minták alapján, képes ezután azonosítani és osztályozni az eseményeket. Például a szoftver egy foci meccsen meg tudja különböztetni a passzív nézőket a fel-le ugráló rajongóktól.

merák használatát, ragaszkodva ahhoz, hogy a rendőrség csak akkor tárolhassa az adatokat, ha az adatbázis ellenőrzése azonnal megtörténik, és az eljárás azonnal megindul. A rendszámleolvasó kamerákat az autópályadíj behajtására is használják, de ez is kiváltott némi kritikát, mivel erre a célra rendelkezésre állnak olyan módszerek is, amelyek kevesebb megfigyeléssel járnak.

5.3 Hogyan növeli biztonságunkat

Az intelligens térfigyelő kamerák a következőképpen tudják javítani a biztonságot.

1. A biztonsági problémákat könnyebb észrevenni a keletkezés pillanatában:
 - A rendszer észreveszi, ha valami szokatlan történik, és riasztja az operátort. Ez megkönnyíti az operátor számára a képek értelmezését.
 - A riasztás megkönnyíti az operátor számára, hogy gyorsabban és hatékonyabban döntsön arról, kell-e lépéseket tennie a biztonsági probléma elhárítására.
 - Az algoritmusok olyan részleteket is észrevesznek, amin az operátor esetleg átsiklik. Ez azért lehetséges, mert a rendszer az információk igen nagy tömegét képes kezelni.
2. Mind a bűnözéstől mind a megfigyeléstől való félelem csökken:
 - Amikor egy biztonsági technológia hatékonyan működik, az emberek biztonságban érzik magukat, mert tudják, hogy ha bármi szokatlan történik körülöttük, azt gyorsan azonosítja a térfigyelő rendszer.
 - A digitális kamerák sokkal több részletet képesek megfigyelni, mint a hagyományos kamerák. Ez azt jelenti, hogy kevesebb kamera szükséges ugyanannak a területnek a megfigyelésére.
 - A privát szféra védelme növelhető, mivel a képek „érzékeny” részei, mint például magántulajdonba tartozó területek, elsötétíthetők, hogy a kezelő ne láthassa azokat.

5.4 Milyen problémákat vet fel?

Az intelligens térfigyelő kamerák hátrányairól sem szabad megfeledkezni.

1. A jelenleg használt intelligens algoritmusokkal számtalan probléma van. Például előfordulhat,

hogy téves riasztást adnak le, tehát az algoritmusok nem mindig értelmezik helyesen a biztonsági eseményt. Például összetévesztenek egy ártatlan embert egy gyanúsítottal. A leggyengébb pontok a következők:

- Megbízható módon csak bizonyos tárgyak, például rendszámtáblák vagy üres térben őrizetlenül hagyott csomagok azonosíthatók.
 - A kamerák kevésbé tudják felismerni, mi történik egy tömegben.
 - A leplezett bűncselekményeket, mint például a zsebtolvajlás vagy a bolti lopás, nehéz azonosítani.
 - Az algoritmus elfogult is lehet, mivel azt emberek programozzák, tehát emberek döntenek el, mit kell „abnormálisként” értelmezni. Megtörténhet, hogy a rendszereket, szándékosan vagy véletlenül, úgy programozzák, hogy azok diszkriminatív módon célozzanak meg kisebbségeket.
 - A jövőben, ha egy potenciális bűnöző tudja, hogy intelligens térfigyelő kamerákat használnak, egyszerűen a ruházata lecserélésével lerázhatja a követést, ha az algoritmusok a ruházat felismerése alapján dolgoznak.
 - A téves riasztások nagy aránya miatt az operátorok elveszíthetik a rendszerrel szembeni bizalmukat, és figyelmen kívül hagyhatják, amit a rendszer „mond” nekik.
2. Az intelligens térfigyelő kamerák hatékonyabban és ugyanakkor kisebbek, ezáltal:
 - Mivel jóval több információt képesek begyűjteni, ezért sokkal jobban sérthetik a magán-szféránkat. Ez annak következménye, hogy nagyobb valószínűséggel készülnek felvételek és elemzések ártatlan emberekről is.
 - Ezeket a kamerákat nehezebb észrevenni, tehát az emberek számára is nehezebb rájönni, hogy intelligens térfigyelő kamerák bámulják őket. Ennek következtében nehezebb az emberek számára elkerülni a megfigyelést vagy kifogást emelni ellene.
 - Hatással lehet a véleménynyilvánítás szabadságára, és az emberi méltóságra, ha valakinek a viselkedését az emberi és szoftveres megfigyelés ezen kombinációja segítségével a közterületeken és a nyilvános helyeken megfigyelik.

3. Az emberi tényező ezeknek a rendszereknek a működtetésében is jelen van, ami azt jelenti, hogy:
- Emberek kellene a képek értelmezéséhez, és a riasztás megerősítéséhez. Igaz, hogy a rendszer azonosíthat egy szokatlan viselkedést, de nem tudja megmondani, mi váltotta ki azt.
 - Nagyon szigorúan kell szabályozni, hogy milyen típusú keresésekre szabad programozni a kamerákat, és a szabályozásnak védelmet kell nyújtania az adatokkal való visszaélések ellen.

6 Drónok

A drón egy pilóta nélküli légijármű-rendszer repülő eleme. Vagy távirányítással, egy pilóta által kezelt földi vezérlőrendszerrel kívülről irányítják, vagy fedélzeti számítógép vezeti. Távirányított repülőgépek, távirányított járműnek, ember nélküli légi járműnek is nevezik a drónokat. Ezek az eszközök azt követően kaptak széles nyilvánosságot, hogy az Egyesült Államok a szeptember 11-i terrortámadás után fokozta bevetésüket a terrorizmus ellen Afganisztánban, Pakisztánban, Jemenben és Szomáliában. Napjainkban sok európai ország szereli fel fegyveres erőit drónokkal.

A drónokat azonban nemcsak a katonaság alkalmazza hadi jellegű helyzetben: az állampolgárok biztonsága érdekében a rendvédelmi szervek is használják őket felderítésre és megfigyelésre. Egyre gyakoribb a nem-katonai, „civil” drónok alkalmazása repülő térfigyelő kameraként biztonsági fenyegetések megelőzésére vagy felfedezésére. Nemcsak biztonsági célokra vetik be a civil drónokat: használják őket térképészeti céllal, ingatlanok fotózására vagy éppen játékokra is. További fontos szempont, hogy olyan helyeken is alkalmazhatók, amelyek megközelítése veszélyes lehet, például lavinák, földrengések vagy nukleáris balesetek helyszínén. A hírhedt fukusimai katasztrófa után is drónokat használtak az erőmű állapotának felmérésére és a sugárzási szint mérésére.



Mivel a SurPRISE projekt a meglévő és fejlesztés alatt álló, megfigyelést célzó technológiákra, mint a polgárok biztonságát védő eszközökre koncentrál,

az alábbiakban főleg a civil, biztonsági célokra használt drónokról fogunk beszélni.

6.1 Miért fejlesztették ki a drónokat?

A pilóta nélküli repülő szerkezeteket kezdetben katonai felderítésre, illetve célzott csapások végrehajtására fejlesztették ki. Az első távirányított repülőgépet még az első világháború idején vetették be. A szükséges technológiát 1916-ban A. M. Low brit professzor fejlesztette ki, célja a német zeppelinek elleni, a földről irányítva bevethető fegyver létrehozása volt, de felmerült egy olyan „repülő bomba” elkészítése is, amelyet egy, a közelben repülő, pilóta vezette gépről irányítanak.

Bár a drónokról manapság leginkább a katonai bevetésükre asszociálunk, pilóta nélküli repülő szerkezeteket egyre nagyobb számban használnak kormányzati szervek, vállalatok, valamint magán-személyek is.

Az Európai Unióban a „könnyű” drónok – azaz a 150 kilogrammnál könnyebb szerkezetek – és az összes biztonsági vagy katonai célú drón használatának szabályozása a tagállamok hatáskörébe tartozik. Magyarországon most készítik elő a teljesen elavult, 1995-ös helyett majdan életbe lépő új szabályozást – a mostani állapot szerint még egy kicsi, kamerával felszerelt játékszernek a hátsó kertben történő használatához is engedélyt kellene kérni a Nemzeti Közlekedési Hatóságtól. A nagyobb, kereskedelmi célú drónok szabályozásának kérdését jelenleg is vizsgálja az Európai Bizottság. A tervek szerint 2016-ban kezdődne meg integrálásuk az EU polgári légtérirányító rendszerébe, hogy aztán 2028-ra a drónok „teljes jogú” szereplőként repülhessenek az európai légtérben.

A kutatások fő iránya, hogy a jövő drónjai még inkább emberi felügyelet nélkül működhessenek, a fejlesztők ezzel a robotika, illetve a mesterséges intelligencia határait feszegetik. A drónok következő generációját már olyan érzékelőkkel igyekeznek felszerelni, amelyek lehetővé tennék, hogy teljesen önállóan repüljenek akár városi környezetben is. Előrelépések várhatók az apró mikrodrónok tömeges előállításában is. A drónokhoz kapcsolódó

technológiai lehetőségek gyors ütemben fejlődnek, mivel megépítésük és használatuk költsége egyre alacsonyabbá válik.

A drónokat változatos kiegészítő eszközökkel lehet felszerelni, amelyek a megfigyelés mellett akár a beavatkozásra is képessé tehetik a pilóta nélküli gépeket. Elsősorban az adott légi jármű mérete és terhelhetősége határozza meg, hogy milyen kiegészítőkkal lehet felszerelni.

6.2 Mire használják a drónokat?

A pilóta nélküli repülőket hatékonyan egészíthetik ki a közfeladatot ellátó szervezetek meglévő eszközei (hagyományos légi járművek vagy műholdak) például a válsághelyzetek kezelésében, a rendvédelem, a határvédelem, a közlekedésirányítás területén, vagy akár a tűzoltási műveletekben.

A közbiztonsággal összefüggésben a rendvédelmi szervek az EU-ban leginkább nagy embertömegek felügyelésére használják a drónokat a sok embert

megmozgató rendezvényeken, mint például zenei fesztiválok, tüntetések vagy sportesemények, hogy segítségükkel időben észleljenek bármilyen váratlan eseményt vagy a tömeg mozgásában bekövetkező hirtelen változást. Használhatóak ezen kívül bűnügyi helyszínelésre, a határvédelem területén történő nagyobb szabású alkalmazásuk lehetőségét pedig a közeljövőben egyre inkább ki fogják használni az EU tagállamai. Bevetettek már drónokat például kábítószer-ültetvények megtalálására, vagy rendőrségi üldözések támogatására is.

A közterületek megfigyelésére használt drónok óriási előnyökkel rendelkeznek a korábbi megoldásokhoz képest. Sokkal nagyobb területet képesek szemmel tartani, mozgékonyak, és az, hogy 50, vagy akár 200 méteres magasságban is repülhetnek, más perspektívát is lehetővé tesz, mint a rögzített kamerarendszerek képe.

A drónoknak számtalan kereskedelmi felhasználása lehetséges. Alkalmazhatók például mezőgazda-

Hogyan működnek a drónok?

Pilóta nélküli repülőgépek számtalan méretben és formában léteznek, és szinte bármilyen „rakománnyal”, azaz például kamerákkal, érzékelőkkel vagy éppen rakétákkal felszerelhetők. A drónokat általában egy földi központban dolgozó, kezelőszemélyzet vezérli, amely irányítja és megfigyeli a jármű és kiegészítőinek működését. Arra is van lehetőség, hogy drónokat okostelefon vagy táblagép segítségével vezéreljünk. Egyes esetekben a pilóta nélküli repülőket előre meghatározott repülési útvonalat programoznak, természetesen a hatótávolságukat figyelembe véve. Azonban a távirányítással összehasonlítva, a drónok ilyen, önálló tevékenységre történő programozása még gyerekcipőben jár, viszont a ma zajló kutatások egyik fő irányát képezi. A jármű és a kezelő közti kommunikáció számos formában megvalósulhat, ám nagyobb távolságok áthidalása ma még nehezen képzelhető el műholdas kapcsolat nélkül, amin keresztül a drón által gyűjtött adatok eljuthatnak a központba, a másik irányban pedig a kezelők utasításokat adhatnak a repülőnek.

A pilóta nélküli repülő rendszer általában a következő összetevőkből áll:

- A pilóta nélküli repülő szerkezet (drón)
- Földi irányítóközpont, sokszor maga sem helyhez kötött
- Összeköttetés a kettő között, általában műholdas kapcsolaton keresztül
- Kiegészítő felszerelések

A drónok mérete és felszerelése óriási változatosságot mutat attól függően, hogy milyen célra kívánják őket használni. Felszerelhetők például köztéri rendszerekhez kapcsolódó kamerákkal, érzékelőkkel, éjjellátó vagy infrakamerákkal, radarokkal, Wi-Fi sugárzásra képes, vagy bármilyen más kommunikációs technológiákkal, kémiai vagy nukleáris szennyeződést kimutató szenzorokkal, valamint fegyverzettel. Mivel a ma folyó kísérletek egyik fő iránya a madarak vagy rovarok mozgását utánozni képes mikro- és nanodrónok kifejlesztése, nem túlzás azt mondani, hogy a jövőben a drónok szinte korlátlanul lehetnek majd képesek bármit vagy bárkit, bárhol és bármikor megfigyelni, bár ma még az elképzelhető felhasználási területeket elvben legalábbis nagyban korlátozzák a kapcsolódó törvényi szabályozások.

sági vagy halászati tevékenység támogatására, elektromos vagy gázvezetékek felügyeletére, infrastruktúra ellenőrzésére, vezetékek nélküli kommunikáció biztosítására vagy műholdjelek felerősítésére, természeti erőforrások számba vételére, filmfelvételek készítésére, digitális feltérképezésre, földterületek vagy az élővilág megfigyelésére, vagy éppen a levegőminőség ellenőrzésére és kezelésére.

A lenyűgöző lehetőségek ellenére számos még megoldatlan technikai problémája is van a drónoknak. Ott van például repülési magasságuk, idejük és sebességük korlátozottsága, illetve a levegőben történő üzemanyag-feltöltésük kérdése. A drónok ezen felül igencsak érzékenyek a rossz időjárási körülményekre, a sűrű felhőzet, az erős szél vagy az eső is megnehezíti használatukat. Aztán ott van az is, hogy a drónokra telepített fejlett eszközök (például kamerák vagy érzékelők) által szolgáltatott adatok feldolgozása sávszélességi vagy kapacitási problémákba ütközhet. A kamerák képe már csak az eszköz mozgásából adódóan is elmosódott vagy homályos lehet.

6.3 Hogyan növelik biztonságunkat?

1. A pilóta nélküli repülőket segítségével könnyebben felfedezhető biztonsági problémák
 - A drónok ellenőrizhetnek óriási és/vagy nehezen elérhető területeket. Így keresési és mentési feladatok esetében a drónok kutathatnak olyan, nehezen járható területeken, mint például egy sűrű erdő. A drónok lehetővé teszik óriási határmenti övezetek megfigyelését is, felfedezve az illegális határátlépőket vagy leleplezve az embercsempészek tevékenységét.
 - A drónok képesek a mozgásra. Nem csak felfedezhetik és regisztrálhatják a gyanús tárgyakat vagy személyeket, hanem követni is tudják őket, amíg szabad területen haladnak. A követésre bevethető, emberek alkotta egységekkel ellentétben a drónok soha nem fáradnak el, és kevésbé felfedezhetők, így hosszú ideig egy tárgy vagy egy személy nyomában maradhatnak.

- A drónok kevésbé láthatóak, mint a rögzített kamerarendszerek egységei, így a potenciális bűnelkövetők is nehezebben veszik észre őket.

2. Csökken a bűncselekményektől és az illetéktelen behatolásoktól való félelem

- Ha az emberek tudják, hogy egy adott terület drónok megfigyelése alatt áll, feltehetően nő a biztonságérzetük, hiszen tudatában vannak, hogy a környezetükben történő bármilyen szokatlan eseményt gyorsan felfedeznek a fejük felett lebegő egységek.

6.4 Milyen problémákat vetnek fel?

1. A drónok kevésbé láthatóak, mint a közterületen elhelyezett kamerák vagy érzékelők, ez pedig még inkább lehetővé teszi, hogy a segítségükkel válogatás nélkül gyűjtsenek és tároljanak információt az állampolgárokról azok tudta nélkül, ezzel komoly potenciális veszélyt jelentve a magánéletükre.
 - A pilóta nélküli gépek lehetőségei messze túlszárnyalják a köztéri kamerarendszerekét, mivel a drónok olyan helyekről is képesek információt gyűjteni, amelyeket az emberek megpróbálnak védeni a kíváncsi tekintetektől, például falak, kerítések, vagy más tárgyak építésével. A levegőből olyan magánterületekre is belátás nyílhat, amelyek el vannak zárva a rögzített helyű kamerák elől.
 - A legtöbb megfigyelési technológiához hasonlóan a drónok is képesek arra, hogy válogatás nélkül rögzítsenek és tároljanak információkat, így aztán nagyobb valószínűséggel figyelik meg és elemzik ártatlan emberek tevékenységét. Ez a tudat nyugtalanító hatással lehet a társadalom tagjaira.
 - A köztéri kamerarendszerekhez képest a drónokat még nehezebb észrevenni, ez pedig azt is jelenti, hogy az emberek még kevésbé lehetnek tudatában, hogy éppen megfigyelik őket. Mivel mozgásban, ráadásul a levegőben dolgoznak, azt is nehéz kideríteni, hogy tulajdonképpen ki is irányítja őket. Így még nehezebben kerülhetik el az emberek a

megfigyelést, és tiltakozni is kevésbé tudnak ellene.

- Mindez egy állandó bizonytalansággal töltheti el a megfigyelt embereket, viselkedésükben is bizonyos változásokat idézve elő, amelyekkel igyekeznek elkerülni a nem kívánt és negatív figyelem felkeltését. Ez a fentebb is említett „dermesztő hatás” tovább erősödhet, ahogy a drónokat egyre inkább „intelligens” kamerarendszerekkel szerelik fel, amelyek képesek például viselkedési, vagy éppen a rendellenességre utaló sémákat kiszűrni, ezzel pedig immár komolyan befolyásolva az olyan alapvető jogok gyakorlásának lehetőségét, mint a szólás- vagy a gyülekezési szabadság.
 - A drónok köztéri kamerarendszerekkel és helymeghatározó eszközökkel kombinált használata az állampolgárok sokkal átfogóbb megfigyelését teszi lehetővé, beleértve mozgásuk, viselkedésük és társadalmi életük részletes adatai alapján felállított profilok készítését is.
2. Az adatrögzítő eszközökkel – például kamerákkal vagy érzékelőkkel – felszerelt drónok esetében fennáll a veszélye annak, hogy az adatokhoz illetéktelen személyek férhetnek hozzá a feltörhető (vagy nem is létező) titkosítás, illetve az irányítóközpont vagy a pilóta, illetve a repülő eszköz közti kommunikáció megzavarásával.
 3. Mindezek mellett felmerülnek azok a nyilvánvaló kockázatok is, amelyeket a drónok zsúfolt, városi környezetben történő üzemeltetése jelent.
 - A pilóta nélküli repülő baleseti rátája még mindig jóval magasabb, mint a hagyományos repülő eszközöké, mivel érzékenyebbek az időjárási körülményekre (szél, eső, köd), és nem vonatkoznak rájuk olyan szigorú biztonsági előírások. Ez veszélynek teheti ki az alattuk élő és dolguk után siető embereket.

7 Internetes megfigyelés mély csomagvizsgálattal

Az internet-, és telefonszolgáltatók, valamint a távközlési vállalatok mindig is képesek voltak hálózatauk felügyeletére, monitorozására. Az információt arról, hogy ki kivel kommunikál, milyen weboldalat látogat, és milyen szolgáltatásokat vesz

igénybe, a számlázáshoz, a hálózatrányításhoz és a vállalati marketinghez használták. Azonban a mély csomagvizsgálat (DPI) névre hallgató technológia az interneten zajló kommunikáció tartalmának az elérését is lehetővé teszi a szolgáltatók, a titkos-

Hogyan működik a mély csomagvizsgálat?

Az információ, amit Ön küld vagy fogad az interneten, igen összetett folyamaton megy keresztül, miközben jó pár számítógépen áthalad.

Az internet által összeköttetésben álló számítógépek feldarabolják az Ön által küldött üzenetet, és kisebb egységekre, úgynevezett „csomagokra” bontva továbbítják azt. Ennek köszönhetően az információ vagy üzenet könnyebben halad át az interneten. Amikor a csomagok megérkeznek célállomásukhoz, itt puzzle módjára összekapaszkodnak, hogy az üzenet ismét teljes legyen. Hasonlóan a postán feladott levelekhez, minden ilyen csomagon található egy címke, amit „címezésnek” hívnak. Ezen van feltüntetve, mi ez a csomag, mit tartalmaz, kitől származik és hova tart. A csomagban belül található a „rakomány”, ami tulajdonképpen az üzenet tartalma.

Minden csomagnak több rétege van, amelyek különböző információkat tartalmaznak az üzenetről. Ezek a rétegek az orosz matrjoska babához hasonlóan egymásba ágyazódnak. Az internetszolgáltatóknak ezek közül néhány réteget mindenképpen meg kell vizsgálni, hogy a csomagokat megfelelően továbbítani tudják. Az esetek többségében elég, ha csupán a címezést ellenőrzik (egy postai levél esetén ez lenne az, ami a borítékra van írva), és nem szükséges átnézniük az üzenet tartalmát, vagyis a mélyebb rétegeket. Ezt nevezzük felszíni csomagvizsgálatnak. Ezzel szemben a mély csomagvizsgálat alkalmazása során a címke mellett az üzenet összes többi rétegét, vagyis a teljes tartalmát átvizsgálják.

A csomagokat olyan számítógépes algoritmusokkal ellenőrzik, amelyek az üzeneteket pásztázva speciális adatfajtákra, információkra keresnek. Az okos térfigyelő kamerákról szóló részben már volt szó algoritmusokról, vagyis olyan számítások sorozatairól, amelyek rendezik és elemzik az adatokat. Ugyanilyen algoritmusokat használ a mély csomagvizsgálat is, csak más módon.

A mély csomagvizsgálat során az algoritmusok úgy vannak kialakítva, hogy bizonyos „kulcsszavak” után kutassanak, hasonlóan ahhoz, mint ahogy Ön is rákeres kulcsszavakra az internetes böngésző keresőjében. Az, hogy a mély csomagvizsgálat pontosan milyen adatok után kutat, azon múlik, hogy ki és milyen célból futtatja azt. A keresett kulcsszavak kapcsolatban állhatnak például bűncselekményekkel, vagy egyéb gyanús tevékenységekkel, esetleg egy új számítógépes vírussal, vagy akár azzal, hogy valaki egy adott terméket megvásárolt-e.



szolgálatok és a kormányok számára. Ez olyan, mintha a postán felbontanák és elolvasnák a leveleinket, esetenként akár változtatnának is a tartalmukon, vagy törölnének belőlük, esetleg szándékosan nem kézbesítenék ki őket.

A mély csomagvizsgálat képes figyelemmel kísérni minden internetes tevékenységünket és kommunikációnkat. Kezdve attól, hogy mit olvasunk el, milyen honlapokat látogatunk meg, milyen videókat nézünk meg, illetve, hogy milyen szavakra keresünk rá a böngészőben, egészen addig, hogy kikkel és mit kommunikálunk e-mailben, egyéb üzenetküldő rendszereken vagy a közösségi oldalakon. A mély csomagvizsgálatot végző alkalmazások megnyitják és átvizsgálják üzeneteket, hogy kiszűrjék közülük azokat, amelyek veszélyes tartalmakat hordoznak. Éppen ezért ahhoz, hogy a mély csomagvizsgálat az Ön internetes kommunikációját is érintse, nem szükséges, hogy Ön gyanúsított legyen. Ez a technológia képes ugyanis lehallgatni és elolvasni minden üzenetet, ami az internetszolgáltató hálózatán áthalad.



7.1 Mi célból fejlesztették ki a mély csomagvizsgálatot?

A mély csomagvizsgálatot eredetileg azért fejlesztették ki, hogy kiszűrjék a vírusokat, illetve az egyéb rosszindulatú szoftvereket (malware), ame-

lyek kárt okozhatnak a számítógépes hálózatban. Manapság a mély csomagvizsgálattal üzenet-elemzéssel már nemcsak a vírusokat lehet megfékezni, hanem az interneten kifejtett rossz szándékú, veszélyes vagy törvényellenes tevékenységek is leleplezhetők.

Az összes eszköz, ami a mély csomagvizsgálathoz szükséges, az internetszolgáltatók birtokában van. A szolgáltatók így ellenőrzésük alatt tudják tartani az internet teljes működését mind lokálisan, mind regionálisan, mind pedig országos-, illetve nemzetközi szinten. Ezek a vállalatok saját céljaikra szánták ezt a technológiát, azonban hamar ráébredtek, hogy komoly haszonra is szert tehetnek ennek eladásából. Idővel más vállalatok, például védelmi ipari cégek is bekapcsolódtak a módszer fejlesztésébe. Így mára a mély csomagvizsgálati technológiának komoly piaca lett.

7.2 Hogyan használják a mély csomagvizsgálatot?

Európában a mély csomagvizsgálatot legálisan csak nagyon korlátozottan lehet használni: a jelenleg hatályos jogszabályok szerint az internetes forgalom „szűrésére”, vírusok és rosszindulatú programok (malware-ek) elhárítására lehet hadba állítani. Ezenfelül segítheti az internetszolgáltatókat a hálózatukban zajló adatforgalom irányításában. Azonban a mély csomagvizsgálat arra is képes, hogy az internetes kommunikációk teljes tartalmát elemezze. Amikor erre használják, alkalmas olyan speciális bűncselekmények leleplezésére is, mint amilyen például a gyermek-pornográfia terjesztése. Ez azonban jogi szempontból meglehetősen ellentmondásos, mivel jelenleg nincs érvényben olyan jogszabály, ami a mélycsomagvizsgálatot megfelelő részletességgel szabályozná. Ennek az az oka, hogy amikor a kommunikációs technológiákra vonatkozó európai jogszabályokat megalkották, még nem létezett a mély-csomagvizsgálati technológia. Az Európai Bíróság és az Európai Adatvédelmi Biztos értelmezése szerint a meglévő törvények az on-line kommunikáció „szűrését” csak korlátozott mértékben teszik lehetővé. Új törvények kidolgozására van szükség, amelyek a mély csomagvizsgálat lehetőségeit részletesen leírják és megfelelően szabályozzák.

Emiatt jelenleg Európában legálisan még nem megengedett a mély csomagvizsgálat alkalmazása a kommunikációk általános figyelésére, a szerzői jogok internetes megsértésének felderítésére, a politikailag kényes tartalmak vagy a célzott reklám letiltására, bár maga a technológia már alkalmas lenne ezekre a dolgokra. Az európai törvények védik a bizalmas kommunikációt. A mély csomagvizsgálat sértené az emberi jogok európai egyezményét is, hiszen indokolatlan, tömeges, nem célzott megfigyelést jelent, mivel a komputeres közöti információforgalom minden kis bitjét képes leolvasni.

Más a helyzet az Egyesült Államokban, ahol ez a terület nincs szabályozva, és sok cég használja is ezt a módszert reklámok célzott terjesztéséhez. Amennyiben Ön például Gmail™ vagy Yahoo™ postafiókkal rendelkezik, az Ön üzenetei szinte biztosan áthaladnak az Egyesült Államokon, és átesnek mély csomagvizsgálaton. 2013 nyarán került nyilvánosságra, hogy minden bizonnyal az amerikai Nemzetbiztonsági Ügynökség (NSA), és a brit hírszerzés, a General Communications Headquarters (GCHQ) is tömeges megfigyelést végző programokat használt.

Egyelőre megválaszolatlan az a kérdés, hogy a mély csomagvizsgálatot milyen módon lehet észlelni, korlátozni vagy kontrollálni. Habár a szabályozás folyamatosan igyekszik felvenni a tempót a technológiai fejlődéssel, szinte lehetetlen felmérni, hogy milyen mértékben használják ezt a módszert. Bármelyik Ön által küldött üzenet megfordulhat a világ bármely pontján mielőtt célba ér, és eközben akár több országban is átvizsgálhatja annak tartalmát mély csomagvizsgálattal egy internetszolgáltató vagy egy kormány titkosszolgálat. Szinte lehetetlen megmondani, mi történik. A szabályozás hiányában az interneten „vadnyugati” állapotok uralkodnak, ahol a kormányok és vállalatok kedvükre használhatják ki a zavaros helyzetet.

Csupán annyit tudhatunk biztosan, hogy világszerte különféle intézmények használnak mély csomagvizsgálatot. Időnként internetszolgáltatók, marketingcégek, rendőri szervek, illetve állami titkosszolgálatok élnek ezzel a módszerrel. Az amerikai titkosszolgálatok Edward Snowden szá-

mítógépes szakember leleplezése nyomán, az elmúlt évben nyilvánosságra került tömeges állami megfigyeléseinek túl is ismert a mély csomagvizsgálat néhány felhasználása is: egy részük kereskedelmi felhasználás, más részük a közbiztonsági és nemzetbiztonsági területhez kapcsolódik.

7.2.1 Kereskedelmi célú felhasználás

- **Hálózati biztonság:** üzenetek átvizsgálása abból a célból, hogy kiderüljön, nem tartalmaznak-e vírusokat, illetve, hogy kiszűrjék a felhasználók közötti nagyméretű fájlmegosztást
- **Viselkedés alapú internetes reklám:** adatok gyűjtése az üzenetekből azzal kapcsolatban, hogy valaki milyen termékeket részesít előnyben. Európában ez nem engedélyezett, de az Egyesült Államokban sok vásárló kedveli, és ott szabad is. Lehetővé teszi a vásárlók számára, hogy egyszerűbben hozzájussanak a nekik megfelelő termékekhez és szolgáltatásokhoz
- **Digitális jogok védelme:** üzenetek átvizsgálása abból a célból, hogy leleplezzék az illegális fájlmegosztást, illetve a szerzői jogok megsértését

7.2.2 Közbiztonsági és nemzetbiztonsági használat

Bűncselekmények állami megfigyelése: a mély csomagvizsgálat alkalmas bizonyos bűncselekmények felderítésére, bár alkalmazása jogilag vitatott. Ilyen bűncselekmények például:

- a számítógéprendszerek ellen irányuló, vagy számítógéppel elkövetett jogsértések (pl. gyermekpornográfia terjesztése)
- rasszista tartalmak megosztása, rasszista indítatású fenyegetések
- felbujtás terrorcselekmények elkövetésére, vagy azok szervezése
- népiártást vagy emberiség elleni bűntetteket helyeslő tartalmak megosztása

Cenzúra: sokan gyanítják, hogy diktatórikus rezsimok világszerte használnak mély csomagvizsgálatot politikai ellenfeleik félrevezetésére, megfélemlítésére. Az egyik amerikai hadiipari vállalat, a NARUS, amely egyébként a Boeing leányvállalata, eladta a mélycsomagvizsgálati technológiát a líbiai kormánynak, amit az fel is használt az arab tavasz során, hogy megakadályozza az ellenzéki vélemé-

nyek terjesztését. Ezzel egy időben Anglia a kiviteli engedélyek visszavonásával korlátozta a mély csomagvizsgálat technológia exportját Egyiptomba, Bahrainba és Líbiába. Nem tudni, honnan, de Irán is hozzájutott a technológiához. Irán a mély csomagvizsgálattal nemcsak megfigyeli az állampolgárait és nemcsak cenzúrázza az internetes tartalmakat, hanem félrevezetés céljából meg is változtatja azokat. Kína hasonló módon alkalmazza ezt a technológiát. Felmerülhet tehát a kérdés, vajon Európában is alkalmaznak-e internetes cenzúrát.

7.3 Hogyan növeli biztonságunkat?

A mély csomagvizsgálat javíthatja az információbiztonságot és elősegíti a bűnözés elleni harcot azzal, hogy képes kiszűrni és blokkolni a 7.2.2 pontban felsorolt veszélyes, ártalmas vagy bűnözésre utaló üzeneteket.

Bár a mély csomagvizsgálat nem képes megelőzni a súlyos bűncselekményeket, amelyekre ezek az üzenetek utalhatnak, lehetővé teszi azok felderítését, és bizonyítékokat szolgáltathat egy nyomozásban. Megakadályozni is képes viszont a számítógépes vírusok terjedését és az internetes bűnözés más formáit.

7.4 Milyen problémákat vet fel?

A mély csomagvizsgálat a következő problémákat veti fel:

1. A mély csomagvizsgálat mindent lát.

- Képes minden üzenetet és bizalmas tartalmat elemezni, miközben azok áthaladnak a hálózaton, ami annyit jelent, hogy mély csomagvizsgálat mellett az elektronikus kommunikáció többé nem maradhat magánügy.
- Az a tudat, hogy a kommunikáció már nem bizalmas többé, erőteljes öncenzúrát válthat ki, ahol az emberek félnek nyíltan kommunikálni egymással, és feladják a szabad önkifejezést.
- Fontos lenne, hogy a mély csomagvizsgálat alkalmazása szigorúan legyen szabályozva, mivel az használója számára jelentős hatalmat biztosít.

2. A technológia gyorsabban fejlődik, mint a szabályozás.

- Nincsenek világos szabályok arra, hogy a mély csomagvizsgálatot mire szabad használni és mire nem.
- A gyakorlatban a mély csomagvizsgálat alkalmazásának a módja kizárólag a technikát használó tisztességén múlik. Ezt a technológiát bármire fel lehet használni, a számítógépes vírusok felderítésétől a politikai elnyomásig.
- Olyan országokban, ahol az állam és az internet szolgáltató vállalatok között szoros a kapcsolat, könnyen előfordulhat, hogy az állam hozzáfér a polgárok teljes elektronikus kommunikációjához.

3. Nehéz megállapítani, hogy pontosan ki és hol alkalmaz mély csomagvizsgálatot:

- Az egész világra kiterjedő egységes jogi szabályozásra lenne szükség. Adatvédelmi hatóságok már egy ideje világszerte felhívásokat fogalmaznak meg a privátszféra nemzetközileg elfogadott minimum követelményeinek a meghatározására.
- A mély csomagvizsgálat szabályozását egy olyan nemzetközi intézményre kellene bízni, amely ténylegesen képes megbüntetni azokat, akik visszaélnék vele.

4. A mély csomagvizsgálat hatékonysága megkérdőjelezhető.

- Miközben a mély csomagvizsgálatot végző számítógépek a potenciálisan veszélyt jelentő összes üzenetet kiszűrrik, nem képesek valódi szövegértelmezésre vagy rangsorolásra, így felvesztődik a téves értelmezés lehetősége, és az a probléma, hogy esetleg ártatlan emberekből is gyanúsítottak válhatnak.
- Több szakértő kétségbe vonja a mély csomagvizsgálat hatékonyságát az illegális tartalmak leleplezésében.

8 Okostelefonos helymeghatározás

Az okostelefon a svájci bicskához hasonlóan olyan eszköz, ami tökélyre fejlesztette a többfunkciósságot. Nagyjából 5 milliárd mobiltelefon-előfizetés van a világon. Európában egy főre átlagosan 1,3 előfizetés jut. Ez hatalmas mennyiség, különösen, ha figyelembe vesszük, hogy az 1990-es évek első feléig nem is léteztek zsebben hordozható telefonok.

8.1 Miért fejlesztették ki az okostelefonos helymeghatározást?

Az okostelefon viszonylag új fejlesztés. Azért annyira közkedvelt, mert amellett, hogy hagyományos mobiltelefonként is működik, sok minden másra is képes. Valójában az okostelefonok sokkal inkább tekinthetők kis zsebszámítógépeknek, amelyek telefonálásra is alkalmasak. A számítógépekhez hasonlóan, minden okostelefon rendelkezik egy úgynevezett operációs rendszerrel, ami lehetővé teszi az e-mailezést, a chatelést, és az internetes böngészést. Az okostelefonokon olyan alkalmazások is futtathatók, amelyekkel játszhatunk, térképet használhatunk, vagy éppen híreket olvashatunk. Jellemzőjük a nagy és színes érintőképernyő, valamint gyakran található rajtuk digitális kamera és média-lejátszó is.

A mobiltelefonok története egészen a második világháborúig nyúlik vissza. Az egyszerű mobiltelefon tulajdonképpen egy üzenetek küldésére és fogadására képes vezeték nélküli rádióvevő készülék volt. Az első vezeték nélküli rádióvevők az úgynevezett kézi adó-vevők walkie-talkie néven váltak ismertté, és a fronton szolgáló katonák közötti kapcsolattartást segítették. Az 1970-es és az 1980-as évek során komoly előrelépés történt a mikroprocesszorok terén, ami a kézi telefonok kifejlesztését eredményezte. A legelső ilyen mobiltelefon pont akkora és olyan nehéz volt, mint egy tégl, és az akkumulátora nagyjából 20 percig bírta. Mennyi minden megváltozott azóta! Az 1980-as évekkel kezdődően növekedni kezdett a mobiltelefon-tornyok száma, ami mind a helyi, mind pedig a nagy távolságú mobilkommunikációt jelentősen javította.

A mobiltelefon-tornyok nélkülözhetetlenek a mobiltelefon működéséhez. Minden torony egy bizonyos földrajzi terület lefedéséért felelős. Ahhoz, hogy a mobiltelefonok kapcsolódni tudjanak a hálózathoz, lehetővé téve ezáltal a telefonálást és az üzenetküldést, először is kapcsolódniuk kell a legközelebbi mobiltelefon-toronyhoz. A telefon helyét így mindig rögzíti az az torony, amelyikhez a készülék éppen kapcsolódik. Amikor a készülék használója átmegy egy másik mobiltelefon-torony körzetébe, a telefon automatikusan átkapcsolódik erre a toronyra. A készülék használatjának mozgása így a szolgáltató számára követhetővé válik. A jelenleg érvényben lévő európai uniós szabályozások szerint a szolgáltatók legalább 6, legfeljebb 24 hónapig őrzik meg az így nyert adatokat. Ugyan az Európai Unió Bírósága 2014 áprilisában megsemmisítette az erről szóló rendeletet, a tagállamokban egyelőre nem változtatták meg a vonatkozó rendelkezéseket.

Az okostelefonok emellett más módon is követhetők. Az okostelefon használója például be tudja állítani, hogy a készülék a saját helyzetét globális helymeghatározó műhellyel (GPS) vagy vezeték nélküli hálózat segítségével mérje be.



Mindez a helymeghatározáson alapuló okostelefonos szolgáltatások rohamos fejlődéséhez vezetett. Ezek többnyire mint alkalmazások (app) tölthetők le a telefonra. Az alkalmazás egy olyan

szoftver, ami a készülék számára plusz funkciót vagy szolgáltatást tesz elérhetővé. A helymeghatározáson alapuló alkalmazások például lehetővé tehetik használatuk számára, hogy tájékozódjanak a környékbeli éttermekről vagy üzletekről, vagy arról, hogy melyik ismerősük tartózkodik épp a közelben. Manapság már helymeghatározáson alapuló játékok is léteznek. A helymeghatározáson alapuló alkalmazások használata várhatóan növekedni fog az elkövetkező években.

A helymeghatározáson alapuló szolgáltatások igen hasznosak az okostelefon-használóknak. A magánszféra védelmét támogatók körében azonban mégis sokan aggódnak, hogy az okostelefonok túl sok személyes adatot szolgáltatnak. Például amikor Malte Spitz, hat hónapra visszamenőleg megszerzte telefonjának helymeghatározásból származó adatait, először csupán értelmetlennek tűnő számokat és betűket látott maga előtt. Ezért megnézte az adatokat egy szakemberrel, akinek az adatokból kirajzolódott Malte egész élete. Malte a Die Zeit nevű német újság segítségével egy animációt készített, ami részletesen bemutatja, hol járt az előző fél évben. Malte-t hamar nyugtalanítani kezdte, hogy életéről ennyi részlet kideríthető,

különösen, ha valaki összekapcsolja ezeket az adatokat az olyan közösségi médiákból származó információkkal, mint amilyen például a Twitter vagy a Facebook.

Az amerikai legfelsőbb bíróság által tárgyalt ügy során a bíró megállapította, hogy a GPS adatokból „vitathatatlanul kiolvashatók” a magánjellegű, bizalmas látogatások, mint például amikor „valaki felkeresi a pszichiáterét, plasztikai sebészét, az abortusz- vagy az AIDS-klinikát, a sztriptíz bárt, védőügyvédjét, egy motelt bizalmas találkozó céljából, egy szakszervezeti ülést, a mecsetet, a zsinagógát, a katolikus templomot, vagy éppen egy meleg bárt stb.”

Hogy működik az okostelefonos helymeghatározás?

A hagyományos mobiltelefonok és az okostelefonok egyaránt használhatók helymeghatározáshoz. Három módon lehet meghatározni egy mobiltelefon helyét: mobiltelefon tornyok segítségével, GPS-szel, illetve vezeték nélküli hálózatokon keresztül. Az első módszer minden mobiltelefonnál működik, míg a második és a harmadik kizárólag az okostelefonoknál.

Mobiltelefon-tornyok: Minden telefon csatlakozik a legközelebbi mobiltoronyhoz, hogy a hívásokat, az üzeneteket, valamint az e-maileket továbbítani tudja a mobil hálózatra. Minden telefon egyedi referenciaszámmal rendelkezik, amely a telefont összekapcsolja a hozzá tartozó előfizetési számlával, és így módon magával a telefonhasználóval. Ezzel válik lehetővé a telefonszámla elkészítése. Amennyiben a titkosszolgálatok vagy más bűnüldöző szervek követni akarják valaki mozgását, elkérhetik a szolgáltatóktól a mobiltornyokból származó adatokat. Ezekből az adatokból aztán kiolvasható, hogy a személy telefonja mikor mely mobiltelefon-tornyok körzetében fordult meg. Amikor minden toronyból összegyűjtik ezeket az adatokat – ahogy ezt az Unió országai teszik – a telefon követhetővé, tulajdonosának a mozgása megismerhetővé válik.

GPS: Az okostelefonok rendelkeznek térkép programmal, illetve olyan alkalmazásokkal, amelyek működése a globális helymeghatározáson alapszik. Amikor a készüléken a GPS funkció be van kapcsolva, a telefon úgy méri be saját helyzetét, hogy kiszámolja saját távolságát a legközelebbi GPS műholdaktól. Amikor a GPS funkció ki van kapcsolva, a készülék nem képes a helyét ezzel a módszerrel bemérni. Azonban ez a funkció aktiválható a távolból anélkül, hogy a telefon gazdája érzékelné azt, például ha olyan alkalmazás fut a telefonon, amelyik lehetővé teszi a telefon helyének meghatározását, ha az elveszett vagy ellopták. Az alkalmazások szolgáltatói begyűjtik a helymeghatározási adatokat, és előfordul, hogy továbbértékesítik azokat marketing célokra. Amikor a titkosszolgálatok és egyéb bűnüldöző szervek egy bizonyos személyt keresnek, bekérhetik a telefontársaságoktól a GPS adatokat is.

Vezeték nélküli hálózat (Wi-Fi): Az okostelefonok képesek kapcsolódni vezeték nélküli hálózatokhoz is. Ilyenkor bemérhetővé válik, hogy mely vezeték nélküli hálózat hatótávolságán belül használják az adott készüléket. Jelen esetben is igaz, hogy ha kikapcsoljuk ezt az alkalmazást, a készülék nem követhető ilyen módszerrel. Egy Wi-Fi modem hatótávolsága beltéren átlagosan 20 méter, de kültéren ennél több.

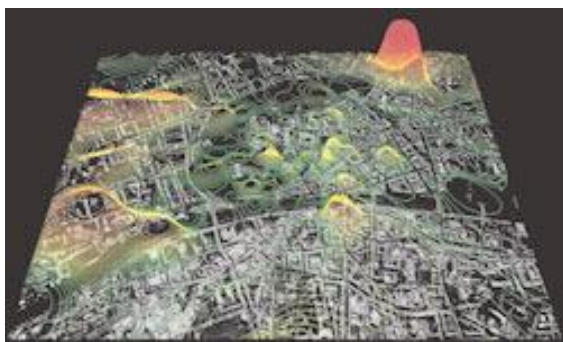
Hasonló módon követhető minden más 'okos' hordozható készülék is. Ilyenek például az iPad-ek, táblagépek, notebook-ok.

8.2 Hogyan használják az okostelefonos helymeghatározást?

Az okostelefonos helymeghatározást egyaránt használják kereskedelmi és biztonsági célokra.

8.2.1 Kereskedelmi használat

- **Telefonszámla ügyintézés:** A mobilcégeknek szükségük van a számlázáshoz a helymeghatározásból származó adatokra, valamint a telefon azonosítószámára.
- **Célzott értékesítés:** A szoftvercégek, amelyek olyan alkalmazásokat készítettek, mint például a Twitter, az Angry Birds vagy a FourSquare, begyűjtik a helymeghatározási és más elérhetőségi adatokat, és továbbértékesítik azokat reklámcégeknek, akik ezeket az adatokat hirdetéseik célzott terítéséhez használják, mégpedig úgy, hogy mindegyik ott legyen elhelyezve, ahova annak célközönsége leginkább ellátogat. Az Angry Birds játékprogramot világszerte egymilliárdan töltötték le. A program használóit meglepte a hír, hogy a finn gyártó, a Rovio Entertainment rutinszerűen gyűjti és adja el a programmal játszó helymeghatározásból származó adatait. A hasonló alkalmazások fele gyűjt ilyen adatokat még akkor is, ha azokra semmi szükség nincs a program működéséhez.
- **Várostervezés:** A helymeghatározási adatok felhasználhatók arra is, hogy feltérképezzék a város közterületeinek a használatát. Mivel a városokban jóval több mobiltelefon-torony van, mint vidéken, a telefonok mozgása itt sokkal pontosabban követhető. Ez a kissé kísérteties kép egy ausztriai város, Graz mobiltelefon-használati térképét ábrázolja. Az amerikai MIT egyetem kutatói Grazban, a telefontulajdonosok anonimitásának megtartása mellett, követték a mobiltelefonokat, hogy képet készíthessenek az emberek mozgásáról a városban. A cél az volt, hogy a város- és közlekedés-tervezők megismerjék, hogyan használják az emberek a várost.



8.2.2 Polgári- és nemzetbiztonsági használat

- **Eltűnt és sérült emberek felkutatása:** Az Egyesült Államokban és Kanadában az E-911 nevű szolgáltatás törvényben előírtan figyeli az összes mobilkészülék GPS-ét, hogy vészhelyzet esetén megtalálhassa azok használóit. Európában nagyjából 180 millió segélyhívást kezdeményeznek évente, ezek 60-70 százalékát mobiltelefonról. A mobilkészülékek automatikusan felfedik földrajzi helyzetüket az európai segélyhívószám, a 112 hívásakor is. Az amerikaiakkal és a kanadaiakkal ellentétben az európaiak számára azonban nincs előírva, hogy a GPS-t folyamatosan bekapcsolva kellene tartaniuk telefonjukon.
- **Bűnelkövetéssel gyanúsítottak mozgásának követése:** A titkosszolgálatok és a bűnüldöző szervek megkaphatják a helymeghatározásból származó adatokat, ha azokat külön kérvényezik a szolgáltatótól. Az ilyen jellegű kéréseket jelenleg Európában adatvédelmi törvények szabályozzák. A szolgáltatók ilyen megkeresések esetén minden rendelkezésükre álló adatot kiadnak a gyanúsítottal kapcsolatban. A titkosszolgálatok emellett más telefonkövető módszerekkel is rendelkeznek, amelyeket különösen fontos követések esetén alkalmazhatnak.
- **Családtagok nyomon követése:** Magánszemélyek is profitálhatnak a helymeghatározáson alapuló szolgáltatásokból. Például egyre több szülő ismeri az olyan mobiltelefon-követő szolgáltatásokat, amelyekkel folyamatosan ellenőrizhetik, gyermekük merre jár.

Ellentmondások az okostelefonos helymeghatározás körül

A New York-i Occupy-tüntetések során az USA kormányzati szervei kényszerítették a Twitter-t, hogy adjon át minden helymeghatározásból származó adatot, amivel a tüntetőket azonosítani lehet. Nemrégiben a Twitter „Kérlek, ne kövess” címmel új szolgáltatást indított. Ez lehetővé teszi, hogy a felhasználók hamis tartózkodási adatokat kapcsoljanak üzeneteikhez. A Google Maps segítségével a Föld bármely tetszőleges pontját megjelölhetik erre a célra. Más alkalmazások, mint például a „Hamis helymeghatározásom”, vagy a „Hamis GPS pozíció” és a „GPS-csaló” is hasonló elven működnek.

8.3 Hogyan növeli biztonságunkat?

Számos módja van annak, ahogy az okostelefonos helymeghatározás javítja a biztonságot:

- Lehetővé teszi, hogy megtalálják a bajba jutottakat és segítsenek rajtuk.
- Lehetővé teszi a családok számára, hogy felügyeljék a gyermekeket és a gondoskodásra szoruló családtagokat.
- A helymeghatározási adatokra támaszkodva a rendőrség és más bűnüldöző szervek ki tudják deríteni, hogy ki volt jelen egy bűntett helyszínén, és ki zárható ki a gyanúsítottak közül. Ugyanilyen módon be tudják mérni és nyomon tudják követni a gyanúsítottakat egy folyamatban lévő nyomozás során.

8.4 Milyen problémákat vet fel?

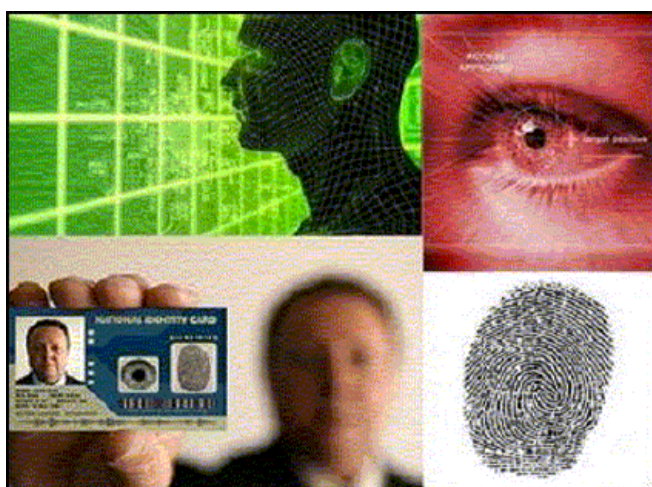
Az okostelefonos helymeghatározás a következő problémákat veti fel a magánszféra, a szabályozás és az emberi jogok kapcsán:

- A telefonhasználóknak nincs teljes kontrollja az okostelefon által kiadott adatok felett. Ez különösen nagy gondot okoz a veszélyeztetett felhasználóknak, mint amilyenek például a védett tanúk, akik nem akarnának adatokat kiadni tartózkodási helyükről, de azért szeretnék használni telefonjukat. Bizonyos készülékek, mint például az Apple iPhone, automatikusan tárolják a helymeghatározásból származó adatokat, és ez a funkció semmikor nem kapcsolható ki.
- Számos alkalmazás akkor is begyűjti a helymeghatározásból származó adatokat, ha ezekre valójában semmi szüksége nincs. A nyilvánosság erős nyomása nélkül pedig nem valószínű, hogy a cégek több kontrollt adnának e téren a felhasználók kezébe.
- Sok alkalmazásfejlesztő cég Európán kívül működik, ezért nem kötik őket az európai adatvédelmi szabályozások. Emiatt az EU-nak nehéz ragaszkodni ahhoz, hogy magánszféra-barát alkalmazásokat fejlesszenek. Az Európai Unió elektronikus adatvédelmi irányelvének (ePrivacy directive) egy újabb módosítása azonban kimondja, hogy a felhasználóktól beleegyezésüket kell kérni ahhoz, hogy az okostelefonos alkalmazások használhassák adataikat, függetlenül attól, hogy az alkalmazást nyújtó cég a világ mely pontjához kötődik.

- A mély csomagvizsgálathoz hasonlóan jelen esetben is igaz, hogy az olyan országokban, ahol a kormány és a szolgáltatók kapcsolata szoros, könnyebben előfordulhat, hogy az állam hozzájut a teljes lakosság helymeghatározásból származó adataihoz.
- Amikor ezeket az adatokat arra használják, hogy azonosítsák egy tüntetés résztvevőit, ez könnyen öncenzúrához vezethet, mivel az emberek jobban meggondolják, hogy egyáltalán elmenjenek-e tüntetni, vagyis hogy éljenek-e demokratikus jogaikkal.

9 Biometria

„Biometrikus” alatt vagy olyan rendszereket értünk, amelyek személyek mérhető fizikai jellemzőit – az ujjlenyomatot, a DNS-t, a retina véredénystruktúráját, az arcvonásokat vagy akár a test szagát – használják, vagy egyedi viselkedési jellegzetességeket vizsgálnak, mint mondjuk a testtartás, a hang, esetleg a billentyűleütési szokások. E rendszerek célja, hogy megállapítsák, ellenőrizzék a személyazonosságot, vagy kategorizálják az egyéneket.



Egyes országokban felveszik az állampolgárok ujjlenyomatait vagy más biometrikus azonosító adatait, és ezeket a személyazonosító igazolványokon vagy egy adatbázisban tárolják. Első lépésként tehát rögzítik az adott személy jellemzőit, majd egy biometrián alapuló rendszerben tárolják el. A későbbiekben aztán ezt az eredeti biometrikus információt veszik elő és használják arra, hogy azonosítsák a szóban forgó személyt. A számítástechnikai kapacitás fejlődése azt eredményezte, hogy mára léteznek automatikus biometrikus rendszerek, amelyek például egész tömegek másodpercek alatti azonosítását is lehetővé teszik.

9.1 Milyen céllal fejlesztették ki az első biometrikus azonosítórendszereket?

A 19. században az államok igazságügyi rendszereinek fejlődése szükségessé tette egy központosított, formalizált személyazonosítási módszer bevezetését. A jogrendek többsége a törvénnyel először összeütközőkkel elnézőbb volt, mint a visszaeső

bűnözőkkel szemben. Ezért is volt szükség olyan formalizált nyilvántartásra, amelyben az elkövetett bűncselekményeket és az elkövetők valamilyen egyedi jellemzőit rögzítették. Franciaországban Alphonse Bertillon dolgozta ki a „Bertillonage”-nak nevezett eljárást, amely az egyének részletesen rögzített testi jellemzőit, például magasságukat, karjuk hosszát, külsejük leírását, illetve fotókat használt személyazonosításra. Az 1890-es években aztán egy újabb, jobb eredményekkel kecsegtető rendszer született, miután Francis Galton kidolgozott egy módszert a bűnözők azonosítására ujjlenyomatuk alapján, amely sokkal egyedibb jellemzőnek bizonyult, mint a Bertillon használt adatok. A 20. században aztán újabb, a személyazonosításra alkalmas jellemzőket fedeztek fel. Frank Burch 1936-ban állt elő az ötlettel, hogy a retina mintázata pontos azonosítóként szolgálhatna, az 1960-as években pedig létrejöttek az arc- illetve hangfelismerést lehetővé tévő technológiák.

9.2 Mire használják a biometrikus rendszereket?

A biometrikus azonosítást hagyományosan a rendvédelmi szervek használják bűncselekmények ismertetésére vagy még ismeretlen elkövetőinek azonosítására, illetve annak megállapítására, hogy valaki jogosult-e belépni egy védett területre, például kormányhivatalokba, kutatólaborokba stb.

A 21. században a biometriát egyre elterjedtebben használják a határvédelem területén. Egyes országokban a vízumért folyamodók egyes biometrikus jellemzőit is rögzítik. Az országba belépéskor aztán ezeket az adatokat például arra használják, hogy megállapítsák, az illető személy belépését korábban már megtagadták, esetleg biztonsági kockázatot jelent, vagy előzőleg már a megengedett időnél tovább tartózkodott az országban. Az Európai Unióban például tíz ujjlenyomatot és egy digitális fotót rögzítenek azokról, akik EU-s vízumért folyamodnak. Ezeket az adatokat a VIS-adatbázisban (Visa Information System – Vízuminformációs Rendszer) tárolják. Az EU létrehozta a hasonlóan működő EUROADAC adatbázist is, amelyben a menedékjogokért folyamodók, illetve az EU területén felfede-

zett olyan bevándorlók adatait rögzítik, akik ellenőrzés nélkül jutottak át a határokon. Az adatbázis segít a menedékkérők és illegális bevándorlók kezelésének módszerét rögzítő, 2003-ban elfogadott dublini rendelet hatékony végrehajtásában.

A biometria katonai alkalmazási területei között megemlíthetjük, hogy az USA fegyveres erőinél hordozható készülékeket rendszeresítettek, amelyek az afganisztáni és iraki hadszíntereken lehetővé teszik, hogy rutinszerűen rögzítsék a katonákkal kapcsolatba kerülő személyek szívrághártya-mintázatát vagy más biometrikus azonosítóit. A gyanúsított nyilatkozott embereket aztán felveszik az „Engedélyezett Biometrikus Megfigyelési Listára”, amely lehetővé teszi a terepen szolgáló katonák számára, hogy azonosítsák a terrorista-gyanús egyéneket, vagy felfedezzék például, ha valaki ismert lázadócsoporthoz áll kapcsolatban, és ennek következményeként nem alkalmazható az amerikai hadsereg által fenntartott külföldi léte-

sítményekben. Az utolsó információk szerint a listán 209 ezer, a világ minden tájáról származó személy adatai szerepelnek.

Igaz, hogy a biometrikus azonosítási eljárásokat a 20. század elejétől eredetileg biztonsági célokra hozták létre és fejlesztették, közben azonban egyre inkább magáncégek is alkalmazták őket. Előnyük elsősorban abban rejlik, hogy a jelszavakkal, kulcsokkal vagy beléptetőkártyákkal ellentétben a személyes jellemzőket igencsak nehéz elfelejteni vagy elveszteni. Ezért aztán sokan biztonságosabbnak és nehezebben kizárhatóknak tartják ezeket, mint a hagyományos megoldásokat. Az utóbbi években számos területen terjednek robbanásszerűen a biometrikus azonosító módszerek, például egyre több csúcskategóriás okostelefonba építenek ujjlenyomat-olvasót. A Facebook arcfelismerő szoftvert használ, hogy a felhasználók felöltött fényképein automatikusan javaslatot tegyen felvételen szereplők azonosítására. A cég DeepFace

Hogyan működik a biometrikus azonosítás?

Az első lépés az illető személy biometrikus adatának, például ujjlenyomatának vagy szívrághártya-mintázatának rögzítése, általában egy kép formájában. Az információt képként, vagy egy, a biometrikus adatokból egy algoritmus segítségével létrehozott sablon formájában tárolják. A magánszféra védelmének érdekében a javasolt eljárás az, hogy csak a sablont őrzik meg, a képet pedig nyom nélkül törlik.

A biometrikus adat – akár a képről, akár a sablonról van szó – számos helyen tárolható, például a rögzítést végző központban – mondjuk a felvételt végző szerkezetben – várhatja a további felhasználást, vagy a személy által magánál hordott intelligens eszközön, például egy chippel ellátott személyazonosító kártyán. Az is elképzelhető, hogy elküldik egy központi adatbázisba, és ott tárolják el, ahol aztán több rendszer is hozzáférhet az adatokhoz.

Ha a biometrikus alapú „összevetés” sikerrel jár, akkor a rendszer felismeri az adott személyt. Amennyiben sikertelen az összevetés, akkor a személy ismeretlennek számít, és a rendszer „visszautasítja”. Az első rögzítéskor készített kép vagy sablon ritkán egyezik meg teljesen az azonosítás pillanatában felvett biometrikus jellemzővel. Az ilyen jellemzők ugyanis hajlamosak kis mértékben megváltozni, de a felvétel körülményei, vagy a használt berendezés is változhat. Elkerülhetetlen, hogy az azonosítás bizonyos hibaszázalékkal működjön.

A biometrikus rendszerek felhasználhatók bűnmegelőzési célokra is, különösen, ha a vizsgált személyek viselkedési jegyeinek vizsgálatának elemzésére használják őket, és a cél nem az azonosítás, hanem a megfigyelt emberek kategóriákba sorolása. Az intelligens megfigyelő kamerákba épített arcfelismerő és viselkedéselemző funkciók tulajdonképpen a térfigyelő kamerák biometrikus képességekkel történő kiegészítéseként működnek.

nevű, tesztelés alatt álló projektje állítólag 97,25 százalékos pontossággal megállapítja, hogy két képen ugyanaz a személy látható-e. A bankok megbízható hangazonosító rendszereket fejlesztenek, hogy az ügyfelek pusztán egy jelszó bemondásával a telefonba elérhessék bankszámlájukat vagy jóváhagyják tranzakcióikat. Számos vállalatnál használnak ujjlenyomat-olvasókkal felszerelt céges laptopokat, így elméletileg elzárva az illetéktelen személyeket a bizalmas információkhoz való hozzáféréstől. Egyes köztéri reklámfelületek más és más hirdetést mutatnak attól függően, milyen nemű vagy korú személy áll előttük.

A biometriás rendszereket azonban az azonosításnál túl egyre inkább viselkedéselemzésre is használják. Számos edzést segítő eszköz és alkalmazás használ valós idejű biometrikus adatokat, például a pulzus- vagy a légzésszámot, hogy személyre szabott tanácsokkal vagy feladatokkal lássa el a felhasználókat. Biztonsági területen pedig a biometrikus adatokkal dolgozó eszközöket meglévő rendszerekbe építik be (például a köztéri kamerák arcfelismerő képességgel történő felvértezése), ez pedig új távlatokat nyit a felügyeletben és megfigyelésben. Ebben az összefüggésben fontos megjegyezni, hogy az ilyen fejlett rendszerek távolról vagy mozgás közben, az alany tudta nélkül is képesek információkat gyűjteni. Adott esetben a rendszer például riasztást adhat le, ha mondjuk egy köztéri kamera ismert, és a rendőrségi adatbázisban szereplő bűnözőt azonosít.

9.3 Milyen előnyökkel jár?

A biometriás rendszerek a következő módokon javíthatják a közbiztonságot:

- A biometrikus adatokon alapuló azonosítókat immár több mint egy évszázada használják a rendvédelmi szervezetek ellenőrzésre és azonosításra. Az arcvonásokat rögzítő, vagy a DNS-t elemző rendszerek igen hatékonyan segíthetnek a bűnüldözésben és súlyos bűncselekmények elkövetőinek azonosításában.
- Az összegyűjtött biometrikus információk arra is használhatók, hogy növeljék a bizalmas adatok feldolgozásának biztonságát. Például segíthetnek abban, hogy mondjuk egy telefonszolgáltató cégnél kizárólag az arra felhatalmazott

emberek férjenek hozzá a kötelezően megőrzött helymeghatározási adatokhoz.

9.4 Milyen problémákat vet fel?

Több negatívum is van, amiket figyelembe kell venni:

1. A biometria nem tévedhetetlen.
 - Kimondható, hogy egy biometrikus jellemzőről készült két digitális „felvétel” soha nem lesz pontosan ugyanolyan. A használt felszerelés eltérése, vagy az olyan környezeti körülmények különbsége, mint mondjuk a hőmérséklet vagy a megvilágítás, téves igazolásokhoz és téves visszautasításokhoz vezethet. Bármely biometrikus rendszer bizonyos százalékban tévesen azonosíthat egy személyt, és hozzáférést engedélyezhet nem megfelelő embereknek, más esetekben pedig arra az eredményre juthat, hogy a jogosult személyek adatai nem egyeznek meg saját, korábban felvett biometrikus azonosítójukkal.
 - Ráadásul az emberek biometrikus jellemzői megváltozhatnak életük során, például a korral, esetleg egy műtét vagy egy baleset következményeként. Előfordulhat, hogy a biometrikus rendszerek ilyen esetben többé nem „ismerik fel” őket.
 - A biometrikus adatokat is meg lehet hamisítani, ez pedig fokozza a személyiségtolvajlás veszélyét.
 - A technológia mai szintje mellett még mindig túl könnyű átverni például egy arcfelismerő rendszert a megjelenés olyan egyszerű megváltoztatásával, mint a más hajviselet, arcszőrzet, smink, szemüveg vagy kontaktlencse viselése, stb.
2. A múltban a biometrikus azonosítás drága és időigényes volt. Ez korlátozta azt a hatást, amelyet az ilyen technológiák az emberek személyes adatainak védelméhez fűződő jogaira gyakoroltak. Mára ez megváltozott, ami például genetikai alapú diszkriminációhoz, illetve a magánszféra fokozatos leépüléséhez vezethet, ha nincsenek megfelelő biztosítékok. Például a megfigye-

lő rendszerek és az okostelefonok felszerelése a közösségi hálózatok adatbázisából építkező arcfelismerőkkel az egyének anonimitásának és szabad, ellenőrizetlen mozgásának a végét jelenthetik.

3. A legtöbb esetben a biometrikus adatok felvételéhez szükség van az adott személy együttműködésére. Ilyen például az ujjlenyomatok rögzítése, ahol az egyénnek lehetősége van hozzájárulást adni adatai rögzítéséhez, illetve meggyőződni azok biztonságos kezeléséről. Adatok felvétele lehetséges azonban a célszemélyek tudta és beleegyezése nélkül is, például egy arcfelismerővel felszerelt kamera felhasználásával. Ez súlyosan befolyásolja az egyének önkéntes beleegyezéshez fűződő jogait, vagy azt, hogy megtudják, pontosan ki és mire használja adataikat.
4. Ha a biometrikus jellemzőket úgy tekintjük, mintha megváltoztathatatlanok lennének, kellemetlen meglepetést okozhat, ha már a felvételnél hiba vagy nem kívánt beavatkozás történik, amely a személy téves megbejegyzéséhez vezethet.

10 A megfigyelésre alapuló technológia az egyetlen lehetőség?

Felmerülhet Önben a kérdés, hogy a biztonsági technológiák jelentik-e az egyetlen megoldást a biztonsági problémákra. Sokszor úgy tűnhet, hogy a biztonság csupán azon múlik, hogy ki tudjuk-e szűrni és követni tudjuk-e a bűnözőket és a fenyegetést jelentő személyeket. A megfigyelésen alapuló biztonsági technológiák arra a feltételezésre épülnek, hogy minél több ember minél pontosabb megfigyelése egy minél kiterjedtebb ellenőrző-rendszer segítségével a legjobb módja annak, hogy felismerjük a potenciális veszélyeket, megtaláljuk az elkövetőket, ha bűncselekmény történik – sőt akár még azelőtt, hogy egyáltalán sor kerülhetne rá. Ha már egy ilyen rendszer kiépült, a biztonságot szinte kizárólag a megfigyelés fokozásával igyekeznek erősíteni.

A teljes képhez azonban ez a megközelítés nem elegendő. Igaz, hogy ma főként ilyen biztonsági technológiákat használnak a bűnözők és terroristák kézre kerítéséhez és következő lépéseik előrejelzésére, léteznek azonban más módszerek is a biztonság javítására. Ebben a fejezetben olyan megközelítéseket mutatunk be, amelyeket a megfigyelésen alapuló biztonsági rendszerek alternatívájának tekinthetünk.

A „biztonság” sokféle módon értelmezhető kifejezés, így javításának kérdése is számos megközelítést tesz lehetővé. A társadalmi stabilitás, a szociális biztonságérzet, a társadalmi intézményekbe vetett bizalom csak néhány azok közül a tényezők közül, amelyek jelentősen befolyásolják az állampolgárok biztonságérzetét.

10.1 Alternatív biztonsági intézkedések: a globális szint

A korábban bemutatott, európai biztonsági prioritások alapján arra a következtetésre juthatunk, hogy a biztonság olyan kérdés, amely az élet minden területére kiterjed. Részt képezik persze a „klasszikus” biztonsági problémák, mint a bűnözés vagy a terrorizmus. Ahogy azt fentebb kifejtettük, az új biztonsági technológiák lehetőséget adnak arra, hogy megtaláljuk azokat az embereket, akik részt vesznek vagy részt akarnak venni ilyen cselekmények elkövetésében. Azonban az ilyen problémák

létrejötté mögött mélyebben fekvő okok vannak, mint például a szegénység, határokon belüli vagy országok közti konfliktusok, politikai vagy vallási különbségek. A biztonsági technológiák nem képesek megváltoztatni ezeket az alapvető tényezőket.

Az európai biztonsági prioritások a válsághelyzeteket és a katasztrófákat is biztonsági problémaként kezelik. Ilyen események lehetnek az élelmiszer- vagy a vízhiány, pénzügyi válságok, járványhelyzetek vagy természeti katasztrófák, amelyek mind az általános emberi létbiztonságot fenyegetik. Ha a biztonságra, mint az „általános emberi létbiztonság”-ra gondolunk, akkor érdemes egy gyors pillantást vetnünk néhány globális társadalmi kihívásra is.

A természeti vagy ember okozta katasztrófák következményeinek enyhítésére törekvő biztonságpolitikai kezdeményezéseket elő lehet terjesztetni és nyomukban be is lehet vezetni különféle intézkedéseket. Az ilyen kezdeményezések többsége hosszú távú, átfogó megközelítésből indul ki. A méltányos nemzetközi kereskedelmet, segítségnyújtást és adósságkezelést előmozdítani kívánó kezdeményezések nem csupán gazdasági, hanem olyan környezetvédelmi problémák megoldását is célozzák, mint a természeti erőforrások túlzott kiaknázása, a környezetszennyezés, illetve a természeti és éghajlati rendszerek felborulásával fenyegető változások. Mindezek végső soron egyben biztonsági problémák is. A másik oldalról pedig a válsághelyzetekben végrehajtott helyi és országos intézkedések hatékonyabbá tétele, vagy a kommunikációs és információs infrastruktúrák, illetve az élelmiszer- és ivóvízellátás fejlesztése mind javítják az életkörülményeket, és ezzel egyben az érintett területek biztonsági helyzetét is.

A biztonság más irányú megközelítései, és az ebből születő, a javítását célzó alternatív intézkedések nemcsak globális szinten vannak jelen. Ezért szeretnénk, ha ilyen szemmel megvizsgálná az Ön közelebbi környezetét, és számba venné azokat az intézkedéseket, amelyek látszólag más célok mellett egyben a biztonság javítását is előmozdíthatják.

Összegezve: az országos és a nemzetközi megoldások

- A globális kereskedelmi rendszerek igazságszábbá tétele, segélyek nyújtása és adósságcsökkentés.
- A jövedelmek és a munkalehetőségek egyenlőbb elosztását lehetővé tévő gazdasági és szociális intézkedések bevezetése.
- A katasztrófa-elhárítás infrastruktúrájának és erőforrásainak javítása.
- A fenntartható és alternatív energiaforrások egyre hatékonyabb kihasználása
- A kommunikációs és információs hálózatok fejlesztése, valamint az élelmiszer- és ivóvízellátás javítása a világnak erre rászoruló területein.

10.2 Alternatív biztonsági intézkedések: a helyi szint

A nagyobb biztonság megértéséhez és eléréséhez helyi szinten is számos út vezet. A biztonsági helyzet javításának egyik lehetséges módja például olyan technológiák bevezetése, amelyek nem a megfigyelésre épülnek. A fémdetektorok, a mozgásérzékelős lámpák, a hangra aktiválódó riasztók, a különböző veszélyekre figyelmeztető berendezések, sőt még a nyilvános segélyhívó telefonok is mind-mind olyan technológiák, amelyek megfigyelés vagy adatgyűjtés nélkül növelhetik a biztonságot. Ezek inkább az állampolgároknak igyekeznek lehetőséget adni arra, hogy reagáljanak és közbelépjenek, ha valamilyen veszély leselkedik rájuk vagy a tulajdonukra. Az olyan eszközök, mint a fémdetektorok, a veszély forrására (a fémtárgyra) fókuszálnak, ahelyett hogy a potenciálisan veszélyessé váló személyek jellemzőit vizsgálnák. Általában meglehetősen hatékonyan működnek ugyan, azonban csak egy bizonyos helyen és időben, illetve korlátozott számú veszélyforrás felfedezésére alkalmasak – viszont nem jelentenek veszélyt a magánszférára.

A bűnmegelőzés javítása, és ezzel a nagyobb biztonság városrendezési és –tervezési módszerekkel is elérhető. Az épített környezet strukturális átalakításai, például a „veszélyzónák” (nehezen ellenőrizhető utcák, terek és parkok) számának csökkentése segíthet a közterületeken tartózkodók biztonsá-

ságérzetének javításában, és ezzel együtt abban is, hogy az emberek tudatosabban felmérjék környezetüket, illetve a rájuk leselkedő veszélyeket.

Összegezve: a nem megfigyelésre és nem adatgyűjtésre épülő alternatív megközelítések

- Bűnmegelőzés várostervezés és a környezet átalakítása segítségével.
- Megfigyelést nem alkalmazó technológiák bevezetése.

Olyan, a biztonságot javító módszerek is lehetőségek, amelyek a megfigyelésre épülnek ugyan, és eközben nem gyűjtenek és nem tárolnak tömegesen adatokat. Egy tipikus példája ennek a rendőrség tevékenységének fokozása, például a sűrűbb járőrözés. A hagyományos rendőri jelenlét erősítése nem technológiai jellegű megfigyelés útján is javítja a biztonságot. Ezenkívül léteznek „szomszédok egymásért” típusú kezdeményezések, amelyekben a lakóközösség tagjai maguk között osztják fel a környék szemmel tartásának feladatát, és ha bármilyen gyanús tevékenységre lesznek figyelmesek, értesítik a rendőrséget. Egyes magán vagy közösségi terekbe a beléptetést előre összeállított vendéglisták alapján engedélyező portások vagy biztonsági őrk maguk is jó példái a megfigyelésen alapuló, ám fejlett technológiát és tömeges adatgyűjtést nem alkalmazó megoldásoknak.

Összegezve: Megfigyelésen alapuló, nem technológiai jellegű intézkedések

- A hagyományos rendőri tevékenység fokozása.
- Önkéntes alapú, a környéket ellenőrző civil szervezetek létrehozása.
- Biztonsági őrk, vagy más, bejáratokat és helyeket szemmel tartó személyek alkalmazása.

Végezetül pedig léteznek a nagyobb biztonságra törekvésnek olyan módjai is, amelyek nem annyira a bűnözők tevékenységének ellehetetlenítésére, illetve az elkövetők kézre kerítésére, tehát nem pusztán az elrettentésre épülnek. Ehelyett olyan hosszú távú, átfogó lépésekben gondolkoznak, amelyek képesek lehetnek az erőszak, bűnözés, vallási gyűlölet, fajgyűlölet vagy hátrányos megkülönböztetés mélyebb, gazdasági és társadalmi okain enyhíteni. A biztonsági technológiák az ilyen

bonyolult, alapvető emberi biztonsági problémák kezelésében is kevésbé hatékonyak.

A biztonság ilyen átfogó megértésére alapozva különböző intézkedések bevezetésére születtek javaslatok, mint például a helyi közösségek és a rendőrség kapcsolatának javítása, vallási, vagy más alapon szerveződő civil csoportok bevonása a helyi szintű problémák megoldásába, ezzel erősítve a társadalmi összefogást és felelősségvállalást. Az aktív foglalkoztatáspolitikai intézkedések, a bűnöző életmódba történő „becsúszás” veszélyének leginkább kitett embereknek biztosított tanulási és mentorálási programok végső soron mind a biztonságot javító intézkedések is. Az alkohol- vagy kábítószer-problémákkal küzdők rehabilitációjával foglalkozó önkéntes egyesületek, vagy a bevándorlók beilleszkedését segítő fogadóközpontok, esetleg a sokszor önszerveződő szociális központok létrehozása egytől egyig olyan helyi lehetőségekre kínálnak példát, amelyek a helyi társadalom kohéziójának javítása közben egyben az adott terület biztonsági helyzetére is jó hatással vannak.



Az ilyen megközelítések két irányból közelítenek a problémához. Egyrészt az érintettek (a lehetséges veszélyek miatt aggódó helyi polgárok) aktív részvételére építenek a konfliktusok enyhítésében, másrészt pedig a bajba került vagy már bűnt elkövető emberek (újra) integrálását célozzák közösségi munka, és nem fegyelmező büntetés révén.

Az olyan aktív oktatási programok, amelyek például az integrációra, a mindenféle másság elfogadására, illetve az önmenedzselés elsajátítására irányulnak, hozzájárulhatnak a társadalmi, kulturális és gazdasági feszültségek enyhítéséhez, illetve segíthetnek kialakítani egy helyi és országos kö-

zösséghez való tartozás érzését, amellyel áttételes módon e közösségek biztonságát is javítják.

Összegezve: megközelítések, amelyek hosszú távon a társadalmi viszonyok javítására, illetve a feszültségek enyhítésére irányulnak

- A szociális rendszerek anyagi eszközeinek, módszereinek fejlesztése, több és jobban képzett személyzet alkalmazása.
- Annak elősegítése, hogy a polgárok aktívan részt vegyenek a helyi problémák és konfliktusok megoldásában.
- A különböző érintett csoportok és szervezetek közti kommunikáció javítása.
- A foglalkoztatási, képzési és hasonló programok (anyagi) támogatása.
- Helyi közösségi színterek, illetve segítőközpontok létrehozása és támogatása.

Röviden bemutattunk alternatív megközelítéseket és elképzeléseket ebben a fejezetben, de Önben is felmerülhetnek ötletek, amelyek a biztonság növeléséhez vezethetnek. Az is lehet, hogy Ön úgy látja, az európai biztonságpolitikának nem a bűnözésre és a terrorizmusra kellene összpontosítania, hanem más prioritásokat kellene előtérbe helyeznie.

11 És most Önön a sor...

Reméljük, nem érzi úgy, hogy túl sok információt zúdítottunk Önre! A jó hír az, hogy Ön az ismertető végéhez ért. Így van most rá egy kis ideje, hogy átgondolja a kérdéseket és problémákat, amelyeket felvetettünk ebben a kiadványban.

Az előbbiekben áttekintettük azt az öt biztonsági technológiát, amelyekről az állampolgári találkozón szó lesz. Elmagyaráztuk, hogyan működnek, hogyan használják őket, hogyan növelik a biztonságunkat, és milyen problémákat vetnek fel. Bemutattuk kifejlesztésük hátterét egy olyan Európában, ahol komoly figyelmet szentelnek a biztonságnak, és ahol a biztonság a mindennapi élet része. A megfigyelésnek és a magánszférának azért tulajdonítottunk kiemelt fontosságot, mert a biztonság kapcsán mostanra igen általánossá vált személyes adataink összegyűjtése és felhasználása. Végezetül bemutattunk néhány alternatív, nem technológián alapuló megoldást is a biztonság előmozdítására.

Most Önön a sor, hogy mérlegeljen és átgondolja a véleményét a felvetett témákról. Ön szerint mennyire lennének elfogadhatóak ezek a technológiák, ha még inkább hétköznapivá válna használatuk? Lehet, hogy Ön úgy gondolja, hogy a maga módján mindegyik hozzájárul biztonságunk fokozásához, és segíthet a különböző, ránk leselkedő veszélyek megelőzéséhez, illetve hozzájárulhat a bűncselekmények számának csökkenéséhez. De az is lehet, hogy Ön az alternatív, nem technológián alapuló megoldásokat érzi célravezetőbbnek. Vagy úgy véli, inkább a képzett biztonsági személyzetre és rendőrségre támaszkodó hagyományosabb megoldásokat kellene előnyben részesíteni az általános megfigyelésen alapuló információgyűjtéssel szemben. Az is lehet, hogy Ön nem érzi, hogy biztonságunk igazán veszélyeztetve lenne, és nem lát túl

sok okot az aggodalomra.

Ugyancsak elképzelhető, hogy Ön meg van győződve arról, hogy ezek a technológiák jó kezekben vannak, mivel olyan állami szervek használják, amelyek elszámoltathatók. De az is lehet, hogy Önnek kétségei vannak, hogy vajon ezek a hatóságok képesek-e szakszerű és etikus módon használni ezeket a technológiákat, figyelembe véve az egész társadalom érdekeit.

Az is lehet, hogy Ön úgy érzi, e technológiák alkalmazása Önt nem igazán érinti, hiszen ezek olyanok ellen irányulnak, akik valamit elkövettek, illetve csak olyan helyeken alkalmazzák ezeket, ahol Ön nem fordul elő. De azt is gondolhatja, hogy mindenkinek foglalkoznia kellene ezekkel a problémákkal, mert a technológiák által begyűjtött adatok mennyisége óriási, és mert e technológiák „szemében” mindenki potenciális bűnöző. Az is lehet, hogy Ön semmi kivetnivalót nem lát abban, ahogy ezeket a technológiákat napjainkban alkalmazzák, de aggódik, hogyan változhat ez a jövőben.

Akármi is a véleménye, magánszféránkból áldozni a nagyobb biztonságért cserébe nem jelent mindenki számára könnyű döntést. A SurPRISE projekt célja, hogy megismerje azt a sokféle nézetet, ahogyan az emberek az új biztonsági technológiákról gondolkodnak.

Alig várjuk, hogy személyesen is találkozzunk Önnel az állampolgári találkozón! Amennyiben többen szeretne megtudni a projektről és a partnerintézményekről, kérjük, látogasson el a SurPRISE projekt nemzetközi honlapjára: <http://surprise-project.eu>.

“A magánszférát érintő kérdések legalább annyira politikai és stratégiai, mint jogi és technológiai problémák.”

Colin J. Bennett a kanadai Victoriái Egyetem professzora, biztonságpolitikai szakértő

Az ismertetőről

Ez az információs anyag a SurPRISE Projekt állampolgári találkozóinak résztvevői számára készült. Az ismertető kiadásáról az Osztrák Tudományos Akadémia Technológia Értékelő Intézete gondoskodott (Austrian Academy of Sciences, Strohgasse 45/5, A-1030 Bécs, Ausztria) a SurPRISE konzorcium minden partnerországára számára. Tudjon meg többet a projektről és a kutatás partnerintézményeiről a SurPRISE honlapon: <http://surprise-project.eu/>.

Az ismertetőben található információk a SurPRISE projekt partnerintézményei által készített tanulmányokból származnak, amelyek tudósok, politikusok és szakemberek kutatási eredményein és írásain alapulnak a világ minden részéből.

Ez a kiadvány annak az információs magazinnak a kiegészített és átszerkesztett változata, amelyet Dr. Kirstie Ball (The Open University) írt a 2014. első három hónapjában kilenc országban megrendezésre kerülő állampolgári találkozók résztvevői számára.

- Szerzők: Dr. Kirstie Ball, The Open University; Maria Grazia Porcedda and Mathias Vermeulen, EUI; Elvira Santiago and Vincenzo Pavone, CSIC; Regina Berglez, IRKS; Eva Schlehahn, ULD; Márta Szénay, Medián
- Tudományos Tanácsadó Testület: Dr. Monica Areñas Ramiro, Mr Robin Bayley, Professor Colin Bennett, Dr. Gloria González Fuster, Dr. Ben Hayes, Dr. Majtényi László, Mr Jean Marc Suchier, Ms Nina Tranø, Prof Ole Wæver
- Dizájn: Zsolt Bartha (Medián); készült az első magazin alapján, amelyet Mr. Peter Devine, Mr. David Winter készített (Corporate Media Team, Learning and Teaching Solutions, The Open University)
- Képek: Mr. David Winter, Corporate Media Team, Learning and Teaching Solutions, The Open University. 14. oldal: Vision Systems, <http://www.visionsystems.co.nz/assets/Video-Analytics1.jpg>
18. oldal: Mat Wellington, "Police Use QuadCopter – UK" March 23rd 2011, <http://multirotor-news.com/2011/03/23/police-use-quadcopter-uk>
26. oldal: © iStockPhoto.com / alexsl,
28. oldal: Senseable City Lab, Massachusetts Institute of Technology 30. oldal: © KIVI NIRIA DV, 2011
- Ez a projekt az Európai Unió Kutatási és Technológiafejlesztési Hetedik Keretprogramjának a támogatásában részesült. A támogatási szerződés száma: 285492.
- Ez az ismertető itt érhető el: <http://surprise-project.eu>

A projektben résztvevő intézmények

- Institut für Technikfolgen-Abschätzung/Osterreichische Akademie der Wissenschaften,
- Coordinator, Austria (ITA/OEAW)
- Agencia de Protección de Datos de la Comunidad de Madrid*, Spain (APDCM)
- Instituto de Políticas y Bienes Públicos/Agencia Estatal Consejo Superior de Investigaciones Científicas, Spain (CSIC)
- Teknologiradet - The Danish Board of Technology Foundation, Denmark (DBT)
- European University Institute, Italy (EUI)
- Verein für Rechts-und Kriminalsoziologie, Austria (IRKS)
- Medián Közvélemény- és Piackutató Intézet, Hungary (Medián)
- Teknologiradet - The Norwegian Board of Technology, Norway (NBT)
- The Open University, United Kingdom (OU)
- TA-SWISS/Akademien der Wissenschaften Schweiz, Switzerland (TA-SWISS)
- Unabhängiges Landeszentrum für Datenschutz, Schleswig-Holstein/Germany (ULD)

* APDCM, the Agencia de Protección de Datos de la Comunidad de Madrid (Data Protection Agency of the Community of Madrid) 2012. december 31-ig szintén tagja volt a SurPRISE projekt kutatási konzorciumának. A megszorító intézkedések részeként a spanyol kormány 2012 végén felszámolta az intézményt.

Ez a projekt az Európai Unió Kutatási és Technológiafejlesztési Hetedik Keretprogramjának a támogatásában részesült. A támogatási szerződés száma: 285492.

Megfigyelés, Privátszféra, Biztonság: Széleskörű állampolgári részvételen alapuló felmérés Európában a biztonsági technológiák elfogadhatóságát és elfogadását meghatározó tényezők feltárására.

