



Megfigyelés, magánszféra és biztonság

MI AZ ÖN VÉLEMÉNYE?



surprise

surveillance
privacy
security



Contents

1	Üdvözljük a SurPRISE projektben	5
1.1	Hogyan olvassuk ezt az ismertetőt?	6
2	Összefoglalás	7
3	Csak egy átlagos hétköznapi...	9
3.1	Megfigyelés, magánszféra és biztonság	10
3.1.1	Megfigyelés	10
3.1.2	Magánszféra és adatvédelem: valóban fontos ügyek?	11
3.1.3	Biztonság	12
4	Három új biztonsági technológia	13
5	Intelligens térfigyelő kamera	15
5.1	Miért fejlesztették ki az intelligens térfigyelő kamerákat?	15
5.2	Hogyan használják az intelligens kamerákat	17
5.3	Hogyan növeli biztonságunkat	18
5.4	Milyen problémákat vet fel?	18
6	Internetes megfigyelés mély csomagvizsgálattal	21
6.1	Mi célból fejlesztették ki a mély csomagvizsgálattal	21
6.2	Hogyan használják a mély csomagvizsgálattal	22
6.2.1	Kereskedelmi célú használat	23
6.2.2	Közbiztonsági és nemzetbiztonsági használat	24
6.3	Hogyan növeli biztonságunkat?	24
6.4	Milyen problémákat vet fel?	25
7	Okostelefonos helymeghatározás	27
7.1	Miért fejlesztették ki az okostelefonos helymeghatározást	27
7.2	Hogyan használják az okostelefonos helymeghatározást	29
7.2.1	Kereskedelmi használat	29
7.2.2	Polgári- és nemzetbiztonsági használat	30
7.3	Hogyan növeli biztonságunkat	30
7.4	Milyen problémákat vet fel?	31
8	Tényleg a technológia az egyetlen megoldás?	33
8.1	Megoldások helyi szinten	33
8.2	Megoldások országos és nemzetközi szinten	33
9	Önön a sor...	35
	Az ismertetőről	36

1 Üdvözljük a SurPRISE projektben

Üdvözljük 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 mozgását, 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 érezzük 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.

Kilenc európai országban kerül sor állampolgári találkozókra: Magyarország mellett Angliában, Ausztriában, Dániában, Németországban, Olaszországban, Spanyolországban, Svájcban és Norvégiában. A találkozók eredményeit 2014 júniusában továbbítjuk az Európai Unióhoz, és ezt követően válnak majd nyilvánosan is elérhetővé a média, a kormányok illetve a közvélemény számára.

Ez az ismertető alapvető információkat nyújt azokról a kérdésekről, amelyeket a magyarországi SurPRISE találkozón fogunk megvitatni 2014 januárjában. 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.

Tisztában vagyunk vele, hogy ez az ismertető nem könnyű olvasmány, de nem fogjuk tesztelni a tudását, és nem akarunk Önből szakembert faragni! Az ismertető célja pusztán annyi, hogy képet adjon a találkozó témáiról, illetve hogy segítse Önt a megfigyelés, a magánszféra és a biztonság kérdésköreiről való gondolkodásban, saját véleményének kialakításában. 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 SurPRISE projekt az emberektől összegyűjtött véleményeket el fogja juttatni (természetesen névtelenül) a képviselőkhöz és más döntéshozókhoz. A biztonsági technológiák kérdése összefüggésben áll az emberi jogokkal, az igazságosságot és a méltányosságot érintő kérdésekkel, illetve az állami intézményrendszer megbízhatóságával és hatékonyságával. Emiatt fontos, hogy a téma megvitatásába a lakosság is bekapcsolódjon, ne csupán a döntéshozók, az üzleti élet szereplői és a szakértők. 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!

1.1 Hogyan olvassuk ezt az ismertetőt?

A következő fejezet az összefoglalás, ami után öt nagyobb egységet talál. Az első egy általános bevezetés a megfigyelés, a biztonság és a magánszféra témáihoz. A következő három fejezet azt a három biztonsági technológiát mutatja be, amelyeket az állampolgári találkozón is megvitatunk majd. Bár ez a füzet három technológiáról szól, a találkozón csak kettőt tudunk majd részletesen megbeszélni. Az Önnek postázott meghívóból tudhatja majd meg, melyik kettőt.

E fejezetek számba veszik, hogy az adott technológiákat miért fejlesztették ki, hogyan használják ezeket, hogyan növelik a biztonságunkat, és milyen problémákat vetnek fel. Mindegyik fejezetben keretes írás tartalmazza a technológia működésének részletesebb bemutatását, illetve szintén keretbe foglalva található egy kis írást a technológiát jellemző ellentmondásokról. Az utolsó fejezet röviden bemutat néhány alternatívát a biztonsági technológiák kiváltására.

Amennyiben nem szeretné végigolvasni a teljes ismertetőt, figyelmébe ajánljuk a leglényegesebb szempontokat bemutató Összefoglalást.

2 Összefoglalás

A SurPRISE projekt célja, hogy megismerje az európai polgárok nézeteit az új biztonsági technológiákról. Ahogy az európai kormányokat egyre inkább nyugtalanítani kezdték az új biztonsági kihívások, mint a terrorizmus, a szervezett bűnözés, vagy a kiberbűnözés, úgy fektettek egyre több pénzt és energiát az új biztonsági technológiák kifejlesztésébe.

Több ilyen új technológia az emberek mindennapjai során keletkezett információk elemzését végzi. 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.

Mivel ezek a technológiák személyes adatokat is feldolgoznak, megfigyelésen alapuló biztonsági technológiáknak nevezzük őket.

A megfigyelésen alapuló biztonsági technológia tehát:

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

A SurPRISE állampolgári találkozók során három 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.
- > **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 használatjának tartózkodási helyéről és mozgásáról egy adott időszakban. A telefonkészülék helyét a mobiltelefon-toronyokból származó adatokkal lehet bemér-

ni, amelyekhez a telefon kapcsolódott. Még pontosabb helymeghatározást tesz lehetővé a globális helymeghatározó rendszer (GPS), vagy a vezeték nélküli adatforgalom.

Mindhárom 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 kamerarendszerek 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 használat tudta nélkül. Az információgyűjtés és az információk felhasználása feletti kontroll hiánya problémákat vet fel mindegyik általunk vizsgált technológia kapcsán.

A technológiák által kínált biztonsági előnyök ellenére egyesekben kétségeket ébreszt a rólok 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 tolakodnak be a magánszféránkba?
- > Megbízhatóak-e azok az intézmények, amelyek alkalmazzák őket?
- > Van-e megfelelő jogi szabályozás?
- > Ki ellenőrzi a megfigyelést végzőket?
- > Milyen alternatív megoldások léteznek, és ezek mennyire célravezetőek?

Többek között ezek azok a kérdések, amelyeket az állampolgári találkozón is megvitattunk majd.

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

3 Csak egy átlagos hétköznapi...

Melinda, útban a repülőtérre, autójával ráhajt a Budapestet délről elérő M5-ös autópályára. Közben felidézi azt, amikor legutóbb ugyanezen az úton haladt végig. Akkoriban az autópálya matricát még személyesen, egy eladótól kellett megvennie, most viszont az útdíj már automatikusan vonódik le bankszámlájáról. Ehhez autójának rendszámtábláját automatikus rendszámfelismerő rendszerrel (ANPR) ellátott kamerák olvassák le, a munka többi részét pedig az elektronikus útdíj-rendszer végzi el. Korábban sohasem tűnt fel neki, hogy a magasban kamerák lennének elhelyezve. Most azonban egyszerre többet is lát, és elgondolkodik, vajon hogyan juttatják el ezek a kamerák az adatokat közvetlenül az ő bankjához.

A repülőtérhez érve Melinda leparkolja autóját és felszáll egy reptéri minibuszra, amivel közvetlenül termináljához juthat, majd bejelentkezik járatára az önkiszolgáló check-in automatánál. Ráhelyezi útlevelét a gépre, ami a nevét összeköti foglalási adataival. Miközben Melinda elveszi beszálló-kártyáját, ráébred, hogy bizonyos vele kapcsolatos információk mindeközben valahol itt is tárolódtak.

Miután túl van az ellenőrzésen, Melinda ledobja maga mellé a kézipoggyászát a reptéri kávézóban, és rendel egy kávét. Egy pillanatra ismét gondolkodóba esik, mielőtt átnyújtja bankkártyáját a pincérnek: „nagyon kényelmes dolog ez a kártya” – gondolja, „de vajon ki és pontosan miért veszi nyilvántartásba most ezt a tranzakciót is?”

Miközben Melinda azt várja, hogy kávéja kicsit lehűljön, előveszi okostelefonját, hogy megnézzé rajta üzeneteit. Ahogy a telefon képernyője kivilágosodik, a kijelzőn látható hely-értesítő nyomban átvált Kecskemétre – Melinda jelenlegi lakóhelyéről – Liszt Ferenc Nemzetközi Repülőtérre. „Honnan tudja a telefonom? Kell, hogy legyen erre egy ésszerű magyarázat, de nem jut eszembe semmi megoldás” – tűnődik.

Melindának még épp jut ideje küldeni egy e-mailt egyik kollégájának, mielőtt elérkezik az idő a beszálláshoz. Miközben átállítja telefonját „repülés” üzemmódba, ismét eltűnődik: vajon mi fog történni az e-maillal, miközben az áthalad az interneten?

Ami Melindával történik, az egyáltalán nem különleges. A fent leírtak bármikor megtörténnek bármelyik utas életében. A technológiák számos előnyt nyújtanak Melinda számára, hiszen utazását kényelmesebbé és gyorsabbá teszi. Eközben azonban kétségeket is támasztanak benne: 'Vajon ki használja fel a személyes adataimat és pontosan mivel jár a számomra, hogy ezek bekerülnek a „rendszerbe”?’

Sok olyan technológia, amelyekkel Melinda utazása során találkozott, a repülőterek világán kívül is létezik. Sokan már el sem tudnák képzelni az életüket okostelefonok, bankkártyák vagy internet nélkül. Tény, hogy mindennapi tevékenységeink közben számtalan olyan elektronikus feljegyzés keletkezik rólunk, amelyekre Melinda is felfigyelt. Talán Melindához hasonlóan Önben is megfogalmazódtak már kérdések és kétségek ennek kapcsán. Ezekből a feljegyzésekből ugyanis kiolvasható, mikor hol tartózkodunk, és esetenként még az is, hogy mit csinálunk éppen. Például a banki tranzak-

ciók, 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 nyomonkövetését élete egyes pillanataiban. Feltehetőleg éppen ez az, ami Melindát nyugtalanítja, de egyben el is bizonytalanítja az a sok előny, amit ezek a technológiák nyújtanak.

Mások is profitálhatnak ezekből a technológiákból, illetve az ezekkel gyűjtött információkból. 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 közterületeken, 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.

Ha Melinda pontosan tudná, hogy személyes adatait erre is felhasználhatják, vajon továbbra is bizonytalan lenne? Ha ez nagyobb biztonságot jelent a számára és mindenki más számára is, ezt talán el tudná fogadni. 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.

Éppen ezért több kérdés is felmerül:

- > Megbízhatóak-e azok az intézmények, amelyek az így megszerzett adatokat használják?
- > Törvényileg mennyire jól szabályozott az ilyen intézmények működése?
- > Az új technológiákat vajon mindig a törvények betartása mellett alkalmazzák?
- > Átláthatóak-e ezek az intézmények és elszámoltathatóak-e minden esetben, amikor biztonsági okokra hivatkozva megsértik a magánszférát?
- > Valóban növelik-e ezek a technológiák a biztonságot?

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

Mielőtt rátérnénk annak a három technológiának a bemutatására, amelyekről a találkozón szó lesz, a következő néhány bekezdésben bevezetünk néhány fontos fogalmat, amelyek témánkhoz kapcsolódnak.

3.1 Megfigyelés, magánszféra és biztonság

3.1.1 Megfigyelés

A megfigyelés szó hallatán elsőként talán a „Nagy Testvér” ugrik be legtöbbünknek, akár a közkezdelt 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. A megfigyelésnek lehetnek például biztonsági okai, mint amikor például a rendőrség térfigyelő kamerákat használ, hogy azonosíthassa az utcai bűnelkövetőket. De megfigyelést alkalmazhatnak kereskedelmi céllal is. Ilyen lehet például, amikor egy szupermarket hűségkártya-programot használ, hogy felmérje, a különböző vásárlói csoportok milyen termékeket részesítenek előnyben. Ez aztán segít eldönteni, hogy milyen akciókkal célozzák meg az adott

csoportot a jövőben. 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 tiszteletben 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 árthat 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.

3.1.2 Magánszféraésadatvédelem: 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 függőnyei az otthonában? Még ha az első és a második kérdésre „nemmel” válaszolt, és csak a harmadikra mondana „igent”, Önről akkor is elmondható, hogy törődik a magánszféréjával. És ezzel egyáltalán nincs egyedül! A közösségi médiát használó fiatalokról készült kutatások rámutattak, hogy a privát szférjuk 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 egyénnek 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.

3.1.3 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 intézkedések 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 lennénk 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 így 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 legújabb 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 eltitulajdonítására 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 megbízhatónak 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 Három új biztonsági technológia

A SurPRISE projekt a következő három biztonsági technológiát vizsgálja:

- > **Intelligens térfigyelő kamerák**
- > **Internetes megfigyelés mély csomagvizsgálattal**
- > **(Okos-) telefonos helymeghatározás**

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

A következő fejezetekben összefoglaljuk, hogy ezek a technológiák hogyan működnek, miért fejlesztették ki őket, kik és hogyan használják őket. Emellett bemutatjuk, hogyan növelik biz-

tonságunkat, 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 kamera

Korábban már beszámoltunk róla, hogy Andrea, miközben a reptérre hajtott, kíváncsi volt, hogyan működnek a kamerák, amelyek tőle is beszedik az autópálya-használati díjat. Ezek a kamerák automatikus rendszámfelismerő programmal vannak ellátva. Az automatikus rendszámfelismerő kamera jó példa az „intelligens” térfigyelő kamerára.

A térfigyelő vagy más néven biztonsági kamerákat az Európában élők többsége már ismeri. 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 60-as években, az USA-ban és Angliában a rendőrség is elkezdett használni ilyeneket. A térfigyelő kamerák a 90-es években folyamatosan terjedtek Európában, elsősorban Angliában, de majdnem ilyen mértékben Franciaországban és Hollandiában is. 2013-ban a térfigyelő kamerák szerepe döntő volt a bostoni maratonton történt robbantás elkövetőinek a leleplezésében.

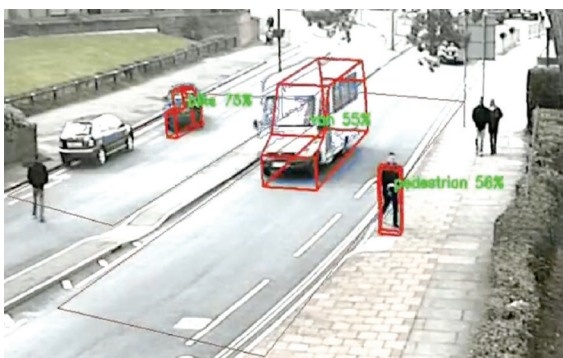
Az intelligens térfigyelő kamerák kifejlesztésekor azokra a problémákra koncentráltak, amelyekkel a térfigyelő kamerák a kezdetektől küszködtek. A lényeg, hogy túl sok a kamera ahhoz képest, hogy mennyi a képernyőket figyelő szempár. A hagyományos kamerarendszerrel szemben az intelligens térfigyelő rendszer 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.

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 focimeccsen meg tudja különböztetni a passzív nézőket a fel-le ugráló rajongóktól.

5.2 Hogyan használják az intelligens kamerákat

Az intelligens kamerarendszerek kereskedelmi forgalomban kapható termékek, amelyeket biztonsági- és védelmi-technológiai vállalatok árúsítanak. 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 a rendőrség 2012 végén kezdett el intelligens térfigyelő kamerákat használni a buszsávok ellenőrzésére. A rendőrség jogszerűen használhatja a képeket bűnszolgálatra, de az autóban ülő utasokról nem készülhet felvétel, és a nagyközönséget teljes körűen tájékoztatni kell a kamerák használatáról. A zürichi repülőtérén 2003 óta működnek arcfelismerő kamerák. Akkoriban ez úttörő felhasználás volt a korszerű határ-ellenőrzésre, amit azóta rendszeresítettek.

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 rendszámleolvasó készült digitális kép segítsé-



gével 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 gyorshajtásban vétke.

Kérdés, hogy a különböző típusú bűncselekmények vagy szabálysértések ugyanolyan mértékű megfigyelést tesznek-e indokoltá. Minden bűncselekmény vagy szabálysértés ellen be 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 kamerák 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. Londonban már korábban is használták a rendszámleolvasó kamerákat az útdíj behajtására, de mára ez már mind az országos, mind a helyi rendészeti stratégia része lett. 2010 óta 5000 rendszámleolvasó kamerát helyeztek üzembe Nagy-Britanniában, és az országos rendőrségi adatközpontban naponta 10-14 millió rendszámot olvasnak le.

Botrányok az intelligens kamerák körül: rendszámleolvasás az angliai Birmingham-ben

2011-ben a brit rendőrségnek le kellett szerelnie a rendszámleolvasó kamerákat az angliai Birmingham város három körzetében, ahol a muszlim népesség aránya magas. A kamerák felállítását egy terrorizmusellenes program finanszírozta, de a nyilvánosság előtt biztonsági okokra hivatkoztak. A közösségi vezetők és a helyi parlamenti képviselők határozottan ellenezték a kamerákat. Az ügy ártott a hatóságokkal szembeni bizalomnak is. Kétszáz kamerát szereltek fel, amelyből 64 titkos kamera volt, és a nyilvánosság teljes kizárásával kerültek a helyükre, de végül egy sem kezdte meg működését. A kamerákat vagy megsemmisítették, vagy máshol kezdték el használni. A projekt kudarca és a kamerák elvesztése 300.000 fontjába (kb. 100 millió forint) került a rendőrségnek.

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 algoritmus olyan részleteket is észrevesz, 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, elcsövéthetők, 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 rendszámok 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 hatékonyabbak és ugyanakkor kisebbek:
 - > Mivel jóval több információt képesek begyűjteni, ezért sokkal jobban sérthetik a magánszféránkat. 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 működtetéséhez is szükséges, 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.



Átláthatóvá kell tenni, miért vannak felszerelve az intelligens térfigyelő kamerák. Meg kell teremteni a lehetőséget, hogy az állampolgárok felkereshessék a rendszert üzemeltető vezetőt, hogy megkérdezzék, mire használják a kamerákat. Érezniük kell, jó oka van annak, hogy ott vannak a kamerák, és bízniuk kell használatukban.

Chris Tomlinson, biztonsági szakértő

6 Internetes megfigyelés mély csomagvizsgálattal

Mialatt Melinda a reptéri kávézóban ült, arra gondolt, vajon mi történhetett a kollégájának küldött email-lel miközben az keresztülhaladt az interneten. Könnyen lehet, hogy útközben „találkozott” az egyik netes megfigyelési módszerrel, az úgynevezett mély csomagvizsgálattal.

Az internet-, és telefonszolgáltatók, valamint a távközlési vállalatok mindig is képesek voltak hálózatuk felügyeletére, monitorozására. Az információt arról, hogy ki kivel kommunikál, milyen weboldalakat látogat, és milyen szolgáltatásokat vesz igénybe, a számlázáshoz, a hálózati irányításhoz és a vállalati marketinghez használták. Azonban a mély csomagvizsgálat (DPI) névre hallgató technológia az interneten zajló kommunikáció tartalmának a megismerését is lehetővé teszi a szolgáltatók, a titkosszolgálatok 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 működésük során észlelik és alakítják az üzenetek áthaladását a hálózaton. Megnyitják és átvizsgálják üzeneteinket, 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.



6.1 Micélbőlfejlesztették ki a mély csomagvizsgálatot

A mély csomagvizsgálatot eredetileg azért fejlesztették ki, hogy kiszűrjék a vírusokat, illetve az egyéb rosszindulatú szoftvereket (malware), amelyek kárt okozhatnak a számítógépes hálózatban. Manapság a mély csomagvizsgálatos üzenet-elemzéssel már nemcsak a vírusokat lehet megfékezni, hanem az interneten kifejtett rossz szándékú, veszélyes vagy törvényellenes tevékenységek is leleplezhetők.

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 „címzésnek” 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 címzést 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.

A mély csomagvizsgálat az úgynevezett routerekben (útvonalválasztó) történik. A router tulajdonképpen egy komputer, ami az üzeneteket irányítja az internetet alkotó különféle hálózatokban. Éppen ezért 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. És pontosan ezek a vállalatok azok, amelyek a mély csomagvizsgálat kifejlesztésében is úttörő szerepet játszottak. Alapvetően 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.

6.2 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 mély csomagvizsgálatot 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. És még ahol mindez megengedett, ott sem lehet korlátlanul használni. Az európai törvények, az adatvédelmi törvény és az Európai Unió Alapjogi Chartája védi a bizalmas kommunikációt. A mély csomagvizsgálat sértené az emberi jogok európai egyezményét is, hiszen indokolatlan, tömeges, nem célzott megfigyelést jelent, mivel a komputeres közötti információforgalom minden kis bitjét képes leolvasni. Egészen 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 bizonynyal az amerikai Nemzetbiztonsági Ügynökség (NSA), és a brit hírszerzés, a General Communications Headquarters (GCHQ) is tömeges megfigyelést végző programokat használt: az előbbi az Upstream nevű programot, az utóbbi a Temporát.

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 közben akár több országban is átvizsgálhatja annak tartalmát mély csomagvizsgálattal egy internetszolgáltató vagy egy kormány titkosszolgálat. Szinte lehetetlen megmondani, mi történik. Ez az eljárás ráadásul maga is generál információkat az üzenetekről, amelyeket meg lehet osztani

internetszolgáltatókkal vagy állami szervekkel, amiről szintén nehéz bármit is megtudni. 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 elmúlt évben nyilvánosságra került tömeges állami megfigyeléseinek túl ismert a mély csomagvizsgálat néhány más felhasználása is: egy részük kereskedelmi felhasználás, más részük a közbiztonsági és nemzetbiztonsági területhez kapcsolódik.

6.2.1 Kereskedelmi célú használat

- > **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

6.2.2 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 indíttatású fenyegetések
 - > felbujtás terrorcselekmények elkövetésére, vagy azok szervezése
 - > népirtást vagy emberiség elleni bűntetteket helyeslő tartalmak megosztása
- > **Cenzúra:** sokan gyanítják, hogy diktatórikus rezsimek világszerte használnak mély csomagvizsgálatot politikai ellenfelek félrevezetésére, megfélemlítésére. Az egyik amerikai hadiipari vállalat, a NARUS, amely egyébként a Boeing leányvállalata, eladta a mélycsomagvizsgáló technológiát a líbiai kormánynak, amit az fel is használt az arab tavasz során, hogy megakadályozza az ellenzéki vélemények 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.

A mély csomagvizsgálat ellentmondásai: a Phorm és a fogyasztók adatai Nagy-Britanniában

2008-ban egy amerikai vállalat, a Phorm megpróbált bevezetni egy rendszert Angliában a British Telecom, a Virgin Media és a TalkTalk telekommunikációs cégekkel együttműködve, ami mély csomagvizsgálattal tapogatta a cégek szolgáltatásait igénybe vevő felhasználók szörfölési szokásait. Az így nyert adatokat elemezték, és hirdetőknak adták el. A szolgáltatók azt mondták a felhasználóknak, hogy az alkalmazás az internetes bűnözést hivatott megelőzni, és nem árulták el, hogy valójában hirdetések elhelyezésére használják az adataikat. A British Telecom titokban tesztelte a rendszert, és több mint 18 millió adatfogást végzett. A brit fogyasztók tudomást szereztek a dologról, és tiltakoztak amiatt, hogy adataikat a cég a beleegyezésük nélkül használta fel. Végül a szolgáltatók megváltak a Phorm technológiától, és az Európai Bizottság jogi lépéseket kezdeményezett a brit kormány ellen, mert engedélyezte a szolgáltatás működtetését. Az ügy 2012. januárjában zárult le, miután Nagy-Britannia a törvények módosításával szankciókat vezetett be a kommunikációk törvénytelen lehallgatásáért, megfigyeléséért.

6.3 Hogyan növeli biztonságunkat?

A mély csomagvizsgálat javíthatja az információbiztonságot és elősegíti a bűnözés elleni harcot azzal, hogy képes kiszűrni és blokkolni a 6.2.2 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 szolgáltat egy nyomozásban. Megakadályozni is képes viszont a számítógépes vírusok terjedését és az internetes bűnözés más formáit.

6.4 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.
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 visszaélnak vele.
4. A mély csomagvizsgálat hatékonysága megkérdőjelezhető.
 - > Mivel a mély csomagvizsgálatot végző számítógépek csak a feltehetően problematikus üzeneteket azonosítják, felvetődik 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.



Jó pár mély csomagvizsgálatot alkalmazó vállalat Európán kívül működik, de az európai emberek adatait is elemzi. Emiatt nem lehet egyszerűen utasítani őket, hogy hagyjanak fel ezzel.

Eva Schlehan, Független Adatvédelmi Hatóság, Schleswig Holstein

7 Okostelefonos helymeghatározás

Amikor a repülő leszállt, Melinda bekapcsolta az okostelefonját, és meglepetten tapasztalta, hogy a tartózkodási hely átváltott a kijelzőn. Biztos volt benne, hogy van erre ésszerű magyarázat. Valójában minden mobilkészüléknek tisztában kell lennie pontos helyével, hogy működni tudjon. Az okostelefonokkal ezt a képességet sikerült teljesen új szintre fejleszteni.

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.

7.1 Miért fejlesztették ki az okostelefonos helymeghatározást

Az okostelefon viszonylag új fejlesztés. Azért annyira közkedvelt, mert amellet, 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. Talán Ön is emlékszik még rá, hogy az 1990-es években gombamód kezdtek szaporodni a mobil-tornyok. Sok vita kísérte akkoriban a nem túl esztétikus tornyok építését, és sokan aggódni kezdtek, hogy sugárzásuk káros lehet az egészségre.



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 használójának mozgása így a szolgáltató számára követhetővé válik. Az okostelefonok emellett más módon is követhetők. Az okostelefon használója például be tudja állítani, hogy a készülék a saját helyzetét globális helymeghatározó műhoddal (GPS) vagy vezeték nélküli hálózat segítségével mérje be.

Mindez a helymeghatározáson alapuló okostelefonos szolgáltatások rohamos fejlődéséhez vezetett. Ezek többnyire mint alkalmazások (apps) 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 használojuk

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.

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 országaitól megkövetelik – 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 helye is. Ilyenek például az iPad-ek, táblagépek, notebook-ok.

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, egy németországi zöld politikus hat hónapra visszamenőleg meg akarta szerezni telefonjának helymeghatározásból származó adatait, először bíróság elé kellett vinnie az ügyét, hogy ezekbe az adatokba egyáltalán betekinthessen. Amikor aztán kezébe vehette a kimutatást, csupán értelmetlennek tűnő számokat és betűket látott maga előtt. Ezért megnézte a papírokat egy statisztikussal, 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 a közel-múltban tárgyalt Egyesült Államok kontra Jones ügy során a bíró megállapította, hogy a GPS adatokból 'vitathatatlanul kiolvashatók' a magánjellegű, bizalmas látogatások, mint például amikor 'valaki felkeresi a pszichiátert, plasztikai sebészét, az abortusz- vagy az AIDS-klinikát, a sztriptíz bár, védőügyvédjét, egy motelt bizalmas találkozó céljából, egy szakszervezeti ülést, a mecsetet, a zsinagógát, a katolikus templomot, vagy éppen egy meleg bár stb.'

7.2 Hogyan használják az okostelefonos helymeghatározást

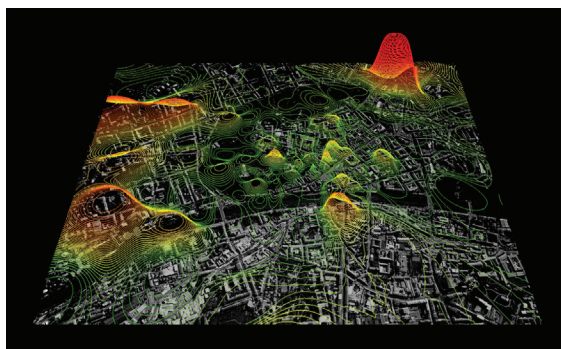
Az okostelefonos helymeghatározást egyaránt használják kereskedelmi és biztonsági célokra.

7.2.1 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 használoit 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.



7.2.2 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:** Magán-személyek 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.

7.3 Hogyan növeli biztonságunkat

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

1. Lehetővé teszi, hogy megtalálják a bajba jutottakat és segítsenek rajtuk.
2. Lehetővé teszi a családok számára, hogy felügyeljék a gyermekeket és a gondoskodásra szoruló családtagokat.
3. 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.

7.4 Milyen problémákat vet fel?

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

1. 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.
2. Bizonyos alkalmazások akkor is begyűjtik a helymeghatározásból származó adatokat, ha ezekre valójában semmi szükségük nincs. A nyilvánosság erős nyomása nélkül pedig nem valószínű, hogy a cégek több kontrollt adnának e téren a felhasználók kezébe.
3. 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.
4. 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.
5. 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.



Az okostelefonos helymeghatározás ugyanannyira hasznos az emberek számára, mint amennyire alkalmas a megfigyelésükre. Az okostelefon sok szolgáltatást tesz elérhetővé, és elősegíti a közösségi kapcsolatépítést ..., de nem mindig könnyű eldönteni és befolyásolni, hogy eközben kivel és hogyan osztjuk meg az adatainkat.

Gus Hosein, Privacy International

8 Tényleg a technológia az egyetlen megoldás?

Talán Ön is elgondolkodott már azon, hogy vajon tényleg a biztonsági technológiák jelentik-e az egyetlen megoldást a biztonsági problémákra? Gyakran úgy tűnhet, hogy biztonságunk szavatolása kizárólag a gyanús emberek kiszűrésén és elfogásán múlik. Ez azonban csak részben igaz.

Ahogy arról korábban már szó volt, az európai biztonsági prioritások szerint úgy tűnik, a biztonság életünk minden területén szerepet játszik. Ez vonatkozik az olyan „klasszikus” kihívásokra is, mint a bűnözés és a terrorizmus. Ahogy az előző oldalakon már szó volt róla, az új biztonsági technológiák felhasználhatók arra, hogy megtalálják azokat az embereket, akik részt vesznek ilyen tevékenységekben. A biztonsági problémák hátterében azonban gyakran húzódnak meg olyan okok, mint a szegénység, helyi-, illetve nemzetközi konfliktusok, vagy politikai, esetleg vallási ellentétek. A biztonsági technológiák azonban ezekre a bűnözést kiváltó okokra nem tudnak megoldást kínálni.

Az európai felfogásban a válság és a katasztrófák is a fontosabb biztonsági kihívások közé tartoznak. Itt olyan problémákra kell gondolni, mint a víz- és élelmiszerhiány, a pénzügyi válságok, a járványok terjedése, vagy a természeti katasztrófák. Ezeknek az igazán összetett és hosszú távú gondoknak a kezelése megint csak nem lehetséges a biztonsági technológiákra támaszkodva.

Éppen ezért, a biztonsági technológiák mellett, amelyeket a bűnözők és terroristák megtalálásához, illetve az elkövetni kívánt bűncselekmények felderítésére használnak, léteznek más megoldások is. Alább felsorolunk néhányat közülük. Lehet, hogy Önnek is vannak elgondolásai, hogyan lehetne a biztonságot növelni. Az is lehet, hogy Ön úgy látja, az európai biztonságpolitika középpontjában álló bűnözésről és terrorizmusról más területek felé kellene eltolni a hangsúlyt.

8.1 Megoldások helyi szinten

- > Biztonságosabb környezet kialakítása a közvilágítás fejlesztése, segélyhívó telefonok kiépítése és megnövelt rendőri jelenlét által
- > Jó kapcsolat előmozdítása a helyi közösségek és a rendőrség között közösségi bűnmegelőzési programok által
- > A vallási és egyéb csoportok problémáinak kezelése helyi szinten oly módon, hogy az növelje a társadalmi bizalmat
- > A helyi vezetés és rendfenntartás átláthatóvá és elszámoltathatóvá tétele
- > Több munka-, képzési-, és tanácsadási lehetőség biztosítása azok számára, akik nagyobb eséllyel válhatnak bűnelkövetővé.

8.2 Megoldások országos és nemzetközi szinten

- > A globális kereskedelmi rendszerek igazságosabbá tétele, segélyek nyújtása és adósságcsökkentés
- > A katasztrófa-elhárítás infrastruktúrájának és erőforrásainak javítása
- > Víz-, kommunikációs-, és információs infrastruktúrák fejlesztése, valamint az élelmiszerellátás javítása a világ arra rászoruló térségeiben
- > A fenntartható és alternatív energiaforrások hatékonyabb kihasználása
- > A társadalmi egyenlőtlenség és diszkrimináció problémáinak leküzdése

9 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 az ismertetőben felvetettünk.

Az előbbiekben áttekintettük azt a három biztonsági technológiát, amelyekről az állampolgári találkozók 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 nagy méreteket öltött személyes adataink felhasználása. Végezetül bemutattunk néhány alternatív, nem technológián alapuló megoldást is a biztonság előmozdítására.

Most Önön a sor, hogy mérlegeljen és átgondolja a véleményét a felsorakoztatott témákról. Ön szerint mennyire lennének elfogadhatóak ezek a technológiák, ha mindennapossá válna a használatuk? Lehet, hogy Ön úgy gondolja, hogy a maga módján mindegyik hozzájárul biztonságunk fokozásához, és képes csökkenteni a bűnözést. 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 törődnie kellene ezzel a problémával, mert a technológiák által begyűjtött adatok mennyisége igen nagy, 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 aggodik, 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 többet szeretne megtudni a projektről és a partnerintézményekről, kérjük, látogasson el a SurPRISE projekt nemzetközi honlapjára: <http://surprise-project.eu>.

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 partnerországa 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.

- > Szerző: Dr Kirstie Ball, The Open University
- > 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: Mr. Peter Devine, Mr. David Winter, Corporate Media Team, Learning and Teaching Solutions, The Open University
- > Képek: Mr. David Winter, Corporate Media Team, Learning and Teaching Solutions, The Open University.
- > A SurPRISE projekt szponzora: az Európai Bizottság 7. Keretprogramja
- > Ez az ismertető itt érhető el: <http://surprise-project.eu>
- > Hogyan készült az ismertető: Az ismertetőt Dr. Kristie Ball írta szoros együttműködésben a Dán Technológiai Tanács Alapítvánnyal (Danish Board of Technology), valamint a SurPRISE konzorciummal és annak Tanácsadó Testületével. Az ismertető négyfordulós belső ellenőrzésen esett át amit egy külső szakértői ellenőrzés követett, majd a kutatási pilot keretében fókuszcsoportok tesztelték Dániában, Magyarországon, és Nagy-Britanniában.

A projektben résztvevő intézmények

- > Institut für Technikfolgen-Abschätzung/Österreichische 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)
- > Teknologirådet - The Danish Board of Technology Foundation, Denmark (DBT)
- > European University Institute, Italy (EUI)
- > Verein für Rechts-und Kriminalsoziologie, Austria (IRKS)
- > Median Opinion and Market Research Limited Company, Hungary (Median)
- > Teknologirådet - 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 .

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

surprise
surveillance
privacy
security



