Összefoglaló
a LiSS WG4 3. találkozójáról
(Ljubljana, 2010. szept. 29-30.)

A Living in Surveillance Societies (a továbbiakban LiSS) elnevezésű, European Cooperation in Science and Technology (COST) finanszírozású projekt[1] 2009 áprilisában indult. A LiSS negyedik munkacsoportjába (WG4), amelynek témája a megfigyelés szabályozása és a közrend, 2009 júniusában kaptam meghívást mint az internet-bűnözés kutatója. A munkacsoport első ülése 2009. szeptember 23-24-én, Brüsszelben volt, amelyen meghatároztuk a munkacsoport céljait, a kidolgozandó témákat és a szervezők ismertették a COST finanszírozási mechanizmusát és a kutatásoknál felhasználható anyagi eszközöket. A második ülésre 2010. február 3-4-én, a svédországi Göteborgban, a harmadik ülésre 2010. szeptember 29-30-án, a szlovéniai Ljubljanában került sor.

Az ülésen William Webster projektvezető beszámolt a LiSS többi három munkacsoportjának tevékenységéről. A LiSS-nek összesen 155 résztvevője van, 26 országból. A LiSS már most elérte a célját, mert eleget tett a COST céljának: összeismertette a különböző Európai országokban azonos területen tevékenykedő szakembereket, akiknek részvételével új kutatócsoportok alakultak.

Az ülésen a WG4 tagjai prezentációkat tartottak közösen indított kutatásaikról. Az alábbiakban ezekből emelek ki néhányat.

*

1. William Webster (University of Stirling) & Eric Töpfler (University of Berlin): CCTV

Az utcai kamerák bűnmegelőzési hatása vitatott, ezzel szemben kiváló kommunikációs eszköz a politika kezében, amely így kipipálhatja a bűnmegelőzés és az állampolgári biztonság követelményének teljesítését. A kamerák azonban hamis biztonságérzetet nyújthatnak, mivel nem születnek hatástanulmányok alkalmazásukkal kapcsolatban. A kamerák az 1990-es években terjedtek el az Egyesült Királyságban, azóta közösségi és magánélet területein is előszeretettel alkalmazzák őket. Az előadók rámutattak az előrehozott büntetőjogi felelősség problematikájára, amikor például az Egyesült Királyságban a terrortámadás előkészítésének számít az is, ha valaki a kamerákról felvételt készít.

A másik kritikus kérdés, hogy ki kontrollálja és ki figyeli ezeket a kamerákat. Van-e operátor vagy csak felveszik az eseményeket? Az egyes bűncselekmények előkészületeinek felismerésében kritikus pont lehet, hogy a kamera-figyelő személyzet hogyan értelmezi a kamerák előtt zajló eseményeket. Ugyanakkor az adatvédelmi szempontok sem elhanyagolhatók az adatok gyűjtésének, tárolásának, kezelési módszereinek meghatározásánál.

Az előadók vizsgálták a kamerák társadalmi beágyazottságát is. Hol helyezik el, mit írnak a kamerák alá (alapvetően ez határozza meg, hogy a kamera az állampolgári védelem vagy a megfigyelés eszköze-e).

Az említett kritikus pontok mentén szükség lenne hatásvizsgálatok és összehasonlító elemzések elvégzésére a résztvevő országok között.

[1] A projektről bővebben lásd: http://www.cost.esf.org/domains_actions/isch/Actions/IS0807-Living-in-Surveillance-Societies-LiSS-End-date-April-2013; valamint: http://www.liss-cost.eu/

2. Charles Raab (University of Edinburgh): A „szabályozás" kritikus kérdései

Raab a szabályozás kérdését általánosan vizsgálja. A szabályozás szintjei lehetnek:
- nemzetközi szabályozás (pl. OECD)
- nemzeti szabályozásra vonatkozó jogszabályok (pl. az adatáramlás megfigyelése)
- önszabályozás (pl. internetes önszabályozó közösségek etikai kódexei)
- önálló, egyéni szabályozás („self-help")

A szabályozási problémák alapvetően a következő területeken, a következőképpen jelentkeznek:

1. Széttöredezés: akkor lép fel, ha a szabályozás eszközei és szintjei nem integráltak, ha nincs szinergia.
2. A szintek és szempontok sokasága következtében a szabályozási területek nem vagy csak kevéssé képesek integrálódni (pl. Európa Unió szabályozási dokumentumai, az OECD szabálykönyvei, az Európa Tanács egyezményei egymással nem képesek integrált rendszert létrehozni)
3. A szabályozást könnyen idejét múlttá tehetik a technikai fejlődés következében előálló új megoldások.
4. A szabályozást mindig korlátozzák a magánélet védelméhez/adatvédelemhez kapcsolódó követelmények.

A továbbiakban Raab azt vizsgálta, hogy a Gary T. Marx által a '90-es évek végén megfogalmazott adatvédelmi elvek közül[2] melyek implementálódtak mára az adatáramlással kapcsolatos szabályozásba. Ezek:

1. A sérelmi elv (harm principle), amelynek értelmében mindig vizsgálni kell, hogy az adott technológia vagy megoldás okoz-e előre nem látható fizikai vagy lellki sérelmet.

2. A másik a tudatosság (awareness), amelynek értelmében csak akkor alkalmazható az adatkezelési technológia, ha annak az állampolgárok tudatában vannak ill. ahhoz hozzájárultak.

3. A harmadik a minimum-elv (minimization principle), amelynek értelmében csak azok az adatok kezelhetők, amelyek feltételül szükségesek az adott szolgáltatás nyújtásához.

4. A negyedik pedig az emberi munka ellenőrzésének elve (human review, redress and sanction) azaz a kezelt adatok körét rendszeresen felül kell vizsgálni (adequate data stewardship and protection), biztosítani kell a panaszjogot és megfelelő szankciórendszert kell kiépíteni.

Azt is megállapítja ugyanakkor, hogy ezeket az elveket csak felismertük eddig, de nem építettük be a gyakorlatba.

Ennek ismeretében Raab a következő feladatokat fogalmazza meg a jövőre nézve:

1. fel kell mérni, milyen hatása van az adatkezelésnek (ezt szélesebb körben értelmezve a „megfigyelésnek") a magánéletre, és az adatkezelési szabályokat ennek megfelelően kell adaptálni (privacy impact assessment).
2. felül kell vizsgálni a szabályozó hatóságok szerepét: szükség van-e egyre több és szélesebb körű jogosultságra; körültekintően kell megvonni a szabályozó hatóságok kormányzati és üzleti befolyásának körét, nagyobb közösségi rálátást kell biztosítani a szabályozó hatóságok létére, elérhetőségére és működésére (az emberek nem

[2] Gary T. Marx: Ethics for the new surveillance (1998) The Information Society, 14(3): 174

tudják, hová fordulhatnak panasszal, ha sérülni érzik adatvédelemhez fűződő jogaikat), valamint integrálni kell az adatkezelési szinteket és módszereket.

3. Végül az adatkezelési elképzeléseket a technikai lehetőségekkel összhangban kell alakítani.

3. Székely Iván: BROAD (Broadening the Range of Awareness in Data Protection)[3]

Székely Iván (CEU, BME, Eötvös Károly Közpolitikai Intézet) a magyar Eötvös Károly Közpolitikai Intézet által megvalósított nemzetközi kutatásról számolt be a megfigyelés szabályozása keretében.

A kutatás alaptétele szerint meg kell ismernünk az információs technológia (IT) fejlesztőinek megfigyeléshez (adatgyűjtéshez, adatkezeléshez) való hozzáállását, hiszen az adatvédelem területén gyakorlatilag ők „alkotják" a szabályokat. Lawrence Lessig szavaival élve, ha a kód a jog, akkor a kód alkotói egyben a jogalkotók *(„if the code is the law … then the coders are the legislators"*). Ha pedig a kódok fejlesztői a jogalkotók, akkor meg kell ismernünk a szemléletüket, a gondolkodáukat ahhoz, hogy megértessük velük, milyen szabályoknak szeretnénk, hogy megfeleljenek az adatbázisok és az adatkezelés.

A kutatás hipotézisei:

1. Az európai IT szakemberek úgy szocializálódtak, hogy a fogyasztók helyett az erősebb felet (a megrendelőket) szolgálják ki (ellentétben például az Egyesült Államok IT fejlesztőmérnökeivel, akik leginkább saját, fogyasztói érdekeiket érvényesítik, így a többi fogyasztó érdekei is jobban érvényesülnek).
2. A magánélet védelméhez való ragaszkodás szintjét az állampolgárok aktuális viselkedése és attitűdjei tükrözik.

A kutatás keretében egyfelől 12-12 interjút vettek fel IT személyzettel Magyarországon és Hollandiában. Ezen túl online kérdőívet juttattak el nagyvállalatokhoz és egy random módszerrel kiválasztott mintához. Összesen 1800 kérdőívet töltöttek ki, amelyek közül 1076 volt értékelhető, megbízhatatlansági okok miatt. A kitöltők 91%-a férfi volt, és 77,9%-a magyar. Ezt figyelembe vették a minta súlyozásánál.
Az elsődleges elemzés szerint[4] az IT szakemberek túlnyomó része nem rendelkezik sem szakképzettséggel, sem pedig bármilyen felsőfokú végzettséggel. Adatvédelmi tudásuk hiányos. 99%-uk nem gondolja, hogy aggódnia kellene amiatt, mert nem megfelelően kezelik személyes adatait. Saját munkájuk megfigyeléséről elutasítóan gondolkodnak, míg ők maguk – bár ennek nincsenek tudatában – éppen hogy mások személyes adatainak megfigyelésére (gyűjtésére, tárolására: kezelésére) vállaltak munkaköri kötelezettséget. A kutatás azt találta, hogy a magánélettel kapcsolatos szenzitivitás minden faktortól független.

4. Székely Iván (EKI) & Charles Raab (University of Edinburgh): A megfigyelésről készült közvéleménykutatások metaanalízise

A kutatás valójában a meglévő kutatások adatainak metaanalízise. A kutatás kidolgozási fázisban van. Szeretnének egy olyan független elemzést készíteni, amelyben összesítik a meglévő kutatások eredményeit, adatait, anélkül, hogy megismételnék a kutatásokat.

[3] http://www.broad-project.eu
[4] A kutatás beszámolója 2011 januárjától elérhető az Eötvös Károly Intézet honlapján: http://www.ekint.org/

Fázisok

1. A meglévő kutatások összegyűjtése: közös halmazok, összefüggések, nézőpontok, elemzési szempontok, célok, módszerek feltérképezése. (Jelenleg ebben a fázisban van a kutatás.)
2. Etalon-kutatások kinevezése (a „legjobb gyakorlatok" mintájára a „legjobb kutatások")
3. Eredmények ismertetése és a kutatás/metaanalízis metodikájának elismertetése: hogyan lehet elemezni már meglévő kutatásokat.

5.Parti Katalin:

5.1. A kormányzati szintű internet-blokkolási megoldások technikai és alkotmányjogi elemzése és kritikája

Az utóbbi években egyre-másra látnak napvilágot az interneten megjelenő illegális tartalmak központi blokkolására, filterezésére irányuló megoldások. Amellett, hogy a blokkolás eszközei nem túl hatékonyak, még jelentős erőfeszítést is igényelnek és az állampolgári jogok csorbításával is járnak. Az internet kormányzati szintű ellenőrzését általában az online gyermekpornográfia elleni küzdelem égisze alatt vezetik be, de alapja lehet számos más ön- és közveszélyesnek tartott cselekmény is. Azonban minél kisebb kárt okozna a tartalommal való szembesülés a felhasználó oldalán, illetve minél távolabbi az ok-okozati láncolat az elszenvedett kár és az adott tartalommal való szembesülés között, annál kevésbé indokolt a tartalom blokkolása. A megvalósíthatóság technikai, alkotmányos, emberi jogi aggályait a német internet-blokkolási törvénnyel (2009) kapcsolatban ismertettem.[5]

5.2. A VR közösségek szabályozása – önszabályozás vagy rendőri jelenlét?

A rendőri szervek jelenléte a magasan szervezett[6] virtuális közösségekben () lehetőséget ad egyfelől a virtuális „állampolgárok" biztonságérzetének növelésére, másfelől pedig fedett nyomozati cselekmények útján a virtuális alteregók életének megfigyelésére, és így a bűncselekmények korai stádiumban való leleplezésére.

Számos ország tart fenn rendőri egységet virtuális közösségekben. Így pl. a londoni illetőségű Child Exploitation and Online Protection Centre, amely fedett nyomozásokat folytat a Second Life-ban folytatott gyermekpornográfia és gyermekprostitúció felgöngyölítésére. Kérdés azonban, milyen cselekmények üldözendők, mely rendőri szerv, milyen illetékességi szabály szerint jogosult eljárni és hogy a virtuális fórum (virtual space) üzemeltetőjének kötelessége-e az együttműködés, illetve jogában áll-e a felhasználói adatok kiadásának megtagadása adatvédelmi rendelkezésekre vagy üzleti célú megfontolásokra hivatkozva?

A virtuális közösségek szabályok közé szorítása elsősorban maguknak a közösségeknek a feladata (önszabályozás). Az internet decentralizált technikai struktúrája nem teszi lehetővé, hogy valamely külső entitás alakítsa ki a követendő szabályokat. Próbálkozni persze lehet, és nem vitatható el az állam büntetőjog-érvényesítésre való törekvése sem, amelyet a nemzetbiztonság és az állampolgárok védelme érdekében tesz.

---

[5] Erről l. még: Parti K.: „10 dolog, amit utálok benned", avagy a kormányzati szintű internet-blokkolás kritikája a német törvény kapcsán, In: Infokommunikáció és Jog, 38. szám (2010. június) pp. 97-104 Online elérhető: http://www.infojog.hu/sites/infojog.hu/files/Parti_tiz_dolog.pdf

[6] Ilyen közösségek a nem játékszabályok köré építkező, hanem a való élet normáit leképező virtuális szerveződések, pl. a Second Life (Második Valóság).

Figyelni kell azonban három fontos elvárásra:
Az első, hogy a jogszabályok átláthatók és követhetők legyenek. A virtuális közösségekben bizonyos tevékenységek nem ugyanúgy valósulnak meg, mint a valós térben, a hozzájuk kapcsolt veszély, illetve ártalom nem a valós veszély és ártalom egyértelmű leképeződése, éppen ezért ezeknek a cselekményeknek a virtuálisban való üldözése is kérdéses.
A második követelmény, hogy a büntetőjog maradjon meg hagyományos szerepében, azaz ultima ratioként. Ne a büntetőjogi legyen az elsődleges reakció a virtuális devianciák visszaszorítására. A jogi szabályozást egészítsék ki kormányzati szintű prevenciós intézkedések, mint amilyen a közösségi veszélytudatosítás (awareness raising), az iskolai oktatás, az állampolgári felvilágosítás. Ehhez a rendőrségnek és a civil szervezeteknek (INHOPE) megfelelő, interaktív bejelentőhelyeket kell létrehozni.
A harmadik nagyon fontos kritérium a jogalkalmazói gondolkodás virtuális térhez való hangolása. Ez nemcsak a jogalkalmazók folyamatos technikai képzését jelenti, hanem olyan, analitikus gondolkodás elsajátítását, amelynek segítségével a jogalkalmazó megérti a virtuális közösségek történéseit: ki, mit, miért tesz a virtuálisban. A virtuális közösség ismerete megtanít felismerni a tényleges veszélyhelyzeteket és a tényleges bűncselekmények előkészületi magatartásait.

*

A találkozón a résztvevők megállapodtak a közös kutatási témák publikálásában. A megjelenés helye lehet: Information Policy, Computer Law and Security Review, Journal of Contemporary European Research. A cél, hogy minél több ország képviseltesse magát egy-egy összehasonlító elemzésben. Elemzési szempontjaink: jogszabályok, iránymutatások, önszabályozó testületek etikai kódexei, nemzeti és nemzetközi diskurzusok, a magánélet és a biztonság érvényesülését vizsgáló tanulmányok, közvélemény-kutatások elemzése.

A COST munkacsoportok célja a nemzetközi kapcsolatok kiépítése, bővítése a hasonló témában kutató/publikáló szakemberek „egymásra találása", másfelől a választott téma körének meghatározása, definiálása, valamint a releváns közös kutatási/publikálási témák meghatározása. Ennek megfelelően felmerült a LiSS-munkacsoportok találkozásának igénye,[7] amelyre a következő ülés alkalmával kerülhet sor.

A munkacsoportunk következő ülése egybeesik az adatvédelmi nappal, azaz 2011. január 26-ával. A munkacsoport-ülés 2011. január 24-25-én lesz, majd január 26-án, a Computers, Technology and Data Protection adatavédelmi konferencia[8] „LiSS panelje" keretében bemutatjuk kutatási témáinkat, ezzel lehetőséget adva más munkacsoportok bekapcsolódására is.

Budapest, 2010. szeptember 29-30.

Dr. Parti Katalin
tud. fmts.
Bűnözéskutatási Osztály

[7] A LiSS WG-k munkájáról lásd bővebben: http://www.liss-cost.eu/working-groups/
[8] A konferencia weboldala: www.cpdpconference(s).org