JOGI FÓRUM PUBLIKÁCIÓ

www.jogiforum.hu

Dr. Galántai Zoltán

E-privacy olvasókönyv

2003

A kötet megjelenését a SOROS ALAPÍTVÁNY támogatása tette lehetővé.

Az e-privacy-val kapcsolatos kutatások elvégzéséhez a Magyar Tudományos Akadémia Bolyai Ösztöndíja és az OTKA F030551 kutatási ösztöndíja nyújtott támogatást.

Lektorálta: Mink András

Technikai szerkesztő: Németh Vilmos

ISBN 963 206 463 1
Arisztotelész Kiadó, Budapest 2003

A megfigyelők megfigyelése

A Szerző meséje: Pedofilchip

Nagy-Britanniában nemrégiben azt vetették fel, hogy a börtönből kiengedett pedofilok bőre alá - helyi érzéstelenítéssel persze - olyan chipet kellene beültetni, aminek a segítségével ugyanúgy nyomon lehet őket követni, mint a lopott autókat (és meg lehet állapítani, hogy mikor térnek vissza egy korábbi bűncselekményük helyszínére vagy mikor közelítenek meg egy iskolát).

A chip alkalmas lenne a szívverés meg a vérnyomás ellenőrzésére is, hogy - a terv támogatói szerint - így idejében következtetni lehessen rá, ha a pedofil éppen újabb gazság elkövetésére készül. Az illetékes brit minisztérium elektronikus megfigyelési csoportja egyébként már hosszabb ideje foglalkozik az ilyen szexuális bűnözők folyamatos ellenőrzésének problémáival, és a beültethető chip ötlete akkor tetszett meg nekik, amikor az áldozatok egy csoportja felhívta rá a figyelmet.

Talán mondanom sem kell, hogy a jogvédők nem értenek egyet az elképzeléssel: „Az, hogy ilyen implantátumot ültetünk az elkövetők bőre alá, igencsak riasztó képet fest a jövőről... vajon hol a megállás? - kérdezi John Wadham, a Liberty igazgatója. - Egyelőre csak a szexuális bűnözők ellen használnák, de a következő lépésben más, marginális csoportokra... is sor kerülhet" az elmegyógyintézetek lakóitól a piti bűnözőkön keresztül a nem megfelelő vagy szélsőséges politikai nézeteket vallókig bezárólag mindenkire.

Az áldozatokat tömörítő Phoenix Survivors szóvivője, Shy Keenan viszont azt mondja, hogy „Belehalok a gondolatba, hogy azért váltam a pedofilok martalékává, mert az ilyeneknek is vannak emberi jogaik. Ezek a törvényen kívül élnek és nem lehet őket ellenőrzés alá vonni, tehát mindig tudnunk kell, hogy éppen mit csinálnak." Már csak azért is, mert a legújabb becslések szerint jóval többen vannak, mint korábban gondoltuk: akár a szexuális bűnelkövetők 10 százalékát is kitehetik.

Vízi Patkány: Témánál vagyunk: feláll a hátamon a szőr, ha arra gondolok, hogy milyen megfigyeléseket tesz lehetővé a technológia a mindennapi életben - és milyen rendszerességgel. A New York Times szerint egy New York-it mintegy 75-ször vesznek filmre egyetlen nap alatt a megfigyelő kamerák; a Chicago Sun - Times pedig úgy becsüli, hogy egy chicagóit naponta 50-szer. A provokatív gondolatairól ismert írónő, Ayn Rand 1943-ban meglehetősen optimistán úgy vélekedett, hogy „A civilizáció a társadalom privacy felé történő fejlődése. Egy vadember teljes élete a nyilvánosság előtt zajlik... és a civilizáció az, ami megszabadítja az embert a többi emberek által történő ellenőrzéstől". Ehhez képest... nos, ehhez képest azóta, hogy ezt Ayn Rand leírta, éppen 50 év telt el.

Szerző: Nem hinném, hogy Budapest egyes részein sokkal jobb lenne a helyzet. Ezért is indítottuk be - természetesen külföldi minta alapján - a Megfigyelők megfigyelése nevű programot, melynek során szépen lefényképezzük a megfigyelő kamerákat, és a felvételt - egy megfelelő térképrészlettel együtt - feltesszük a weblapunkra.

Ami még csak a kezdet, és bőven van hová fejlődnünk: az Institute of Applied Autonomy nevű szervezet (ami többek között távirányítású grafitti-készítő robotot is szerkesztett) kidolgozott egy olyan szoftvert, ami ha rákattintunk az adott város térképén az indulási és a célállomásra, akkor kijelöli nekünk a kameramentes utat.

Hoover: Szépen vagyunk! Ezzel igencsak megkönnyítenék a bűnözők dolgát.

Vízi Patkány: De hiszen annyit beszéltünk már arról, hogy a megfigyelést nem csak a bűnözők akarják (vagy akarhatnák) elkerülni! Az angol Midford Daily Newsban éppen a minap egy meglehetősen kiábrándító összeállítás jelent meg egy tipikus angol állampolgár tipikus napjáról. A magát felfedni nem kívánó újságíró szerint valahogy így néz ki a dolog:

7 óra 00 perc: Az elektronikus nyomkövetés akkor kezdődik, amikor letöltjük az e-mail-jeinket és megnézzük az interneten a reggeli híreket.

7 óra 45 perc: Beugrunk egy kávéra meg egy fánkra munkába menet a friss péksüteményt áruló boltba. A pénztár felett elhelyezett megfigyelő kamera rögzíti a képünket.

8 óra 00 perc: Irány az autópálya, ahol speciális készülék olvassa le a rendszámot. Közben egy gyors mobiltelefon a munkahelyünkre: a mobilszolgáltató gondosan feljegyzi a hívás helyét, idejét, időtartamát stb.

8 óra 27 perc: Lekanyarodunk az autópályáról, és a rendszám- tábla-felismerő kamera ismét működésbe lép.

8 óra 45 perc: Keresztül a belvároson. A Memorial Buildingen elhelyezett rendőrségi kamera – miért is ne - csinál néhány felvételt a kocsinkról.

8 óra 55 perc: Megérkezés a parkolóba - végre ismét egy megfigyelő kamera, ami rögzíti, amint kiszállunk az autóból.

8 óra 57 perc: Elő a mágneskártyával, ami a hivatal ajtaját nyitja: a rendszer feljegyzi, hogy mikor érkeztünk meg.

9 óra 00 perc: Ma sikerült pontosnak lenni - pontosan 9-kor bekapcsoljuk az asztalunkon álló számítógépet, és innentől fogva egy log file-ba kerül, hogy milyen leveleket kaptunk és küldtünk, milyen web site-okat kerestünk fel, stb. Meg persze az is, hogy kinek, mikor, mennyi ideig telefonáltunk.

12 óra 00 perc: Kapkodva bekapott ebéd a közeli gyorsétterem videó-felvevőinek kereszttüzében.

12 óra 08 perc: Pénzfelvétel egy bankautomatából. A kamera az arcunkat, a gép a tranzakció részleteit tárolja el.

12 óra 12 perc: Tankolás. A CCTV a vonásainkat, a számítógép a fizetett összeget rögzíti.

12 óra 35 perc: Két könyv a közkönyvtárból - szerencsére ez is komputerizálva van, és így később bármikor visszakereshető lesz, hogy mikor és mit kölcsönöztünk ki.

12 óra 55 perc: A munka folytatódik: a rendszer rögzíti, hogy a mágneskártyánkkal jöttünk be; a kamera felvételeket készít. A komputer tovább loggolja az adatokat.

18 óra 05 perc: Log off. A CCTV természetesen megörökíti a távozásunkat.

18 óra 32 perc: Ismét fel az autópályára; még egy fénykép.

19 óra 01 perc: Elhagyjuk az autópályát (a rendszámtábla-azonosító rendszer most is működik).

19 óra 14 perc: Még szerencse, hogy a sarki vegyesbolt még nyitva van. Veszünk néhány apróságot; a parkoló kamerája csinál néhány felvételt, és mivel a fizetés bankkártyával történik, ennek is nyoma marad.

19 óra 40 perc: Végre újra otthon. Cseng a telefon (a hívó telefonszáma és a beszélgetés időtartama rögzítésre kerül).

21 óra 45 perc: Vessünk még egy pillantást az elektronikus postánkra (ami persze ismét loggolva lesz).

22 óra 50 perc: Hulla fáradtan az ágyba zuhanunk, és ezzel mára véget is ért a megfigyelés. Elvégre egy demokráciában nem lehet csak úgy poloskát telepíteni az állampolgár háló- szobájába, hogy még azt is kihallgassuk, beszél-e álmában...

Hoover: Bevallom, ez így elsőre valóban riasztóan hangzik - az igazság azonban az, hogy bármit is állítsanak a széplelkű amerikai írónők, a 20. sz. igenis a megfigyelések százada volt, és bőven volt ideje hozzászoknunk.

Vízi Patkány: Na ne mondd!

Hoover: Talán azzal a Kansas Cityben (Missouri) élő temetkezési vállalkozóval, Almon P. Strowgerrel kezdeném, aki 1889-ben arra a felismerésre jutott, hogy a riválisa lefizette a telefonos kisasszonyokat, és azok minden zokogó ügyfelet hozzá kapcsolnak. Úgyhogy gyorsan kitalálta az automata telefonközpontot, ami - elvileg - kizárta az efféle visszaéléseket. De csak elvileg: New York rendőrfőnöke 1916-ban (miután az embereit két lehallgatáson is rajtakapták) már azt hangsúlyozta, hogy „a telefonbeszélgetések - természetüknél fogva - soha nem lehetnek annyira személyesek és privátak, mint a postai levél”, mivel egészen egyszerűen könnyebb - akár véletlenül is - lehallgatni őket.

Vízi Patkány: Vagyis innentől kezdve az volt a vita tárgya, hogy a telefonálás inkább a távirat küldéséhez hasonlít (ahol a szöveg szükségképpen többek kezén is átmegy) vagy inkább a postai levélhez, amit az 1800-as évek közepe óta a ragasztós boríték is védett (a New York Times 1873-ban az új találmányt méltatva külön kiemelte, hogy ez mennyivel biztonságosabb a hagyományos, vörös szalaggal átkötött megoldásnál, és így mennyire elősegíti a bizalmas információcserét).

Végül szerencsére a telefonálás egyenlő levél felfogás győzött, amikor a Kongresszus 1934-ben elfogadta a Federal Communications Actet (Szövetségi Kommunikációs Törvény). Ez kimondta, hogy „egyetlen személy sem jogosult lehallgatni az érintett engedélye nélkül a kommunikációt", és ettől kezdve a telefontársaságok minden adandó alkalommal arra hivatkoztak, hogy az általuk fenntartott rendszernek nem az a célja, hogy lehetővé tegye a gazemberek fülöncsípését, hanem az, hogy lehetővé tegye a kommunikációt - függetlenül attól, hogy ki és milyen céllal kommunikál. Valahogy úgy, mint ma az interneten (de azért lehallgatókészüléket találtak többek között a Legfelsőbb Bíróság készülékeire csatlakoztatva is 1935-ben).

Hoover: Régi szép idők: egyes bíróságok előtt kiválóan lehetett azzal érvelni, hogy mivel a szövegben „személyről" van szó, a megkötés nem vonatkozik a kormányügynökségekre (amik nyilvánvalóan nem tekintendőnek személynek); ráadásul a törvény a lehallgatókészülékeket (poloskákat) sem tiltotta be... és ez a végrehajtó szervek szempontjából nem is volt olyan nagy baj. Elvégre a lehallgatásokra mindig megvolt a jó okunk: az Első Világháború idején a háborúellenes tüntetők; aztán az alkoholtilalom idején az alkoholcsempészek; aztán a II. Világháború; aztán a kommunistaveszély, aztán...

Vízi Patkány: És így tovább, és így tovább. Ha indokot nem is, ürügyet mindig lehet találni (és a hatóságok mindig találtak is), de akkor már érdekesebb az 1939-es Nardone-ügy. Az állami megfigyelésekre, a lehallgatásokra meg egyebekre a terrorizmussal kapcsolatban még úgyis visszatérünk.

Az az év bizonyos értelemben az amerikai jog aranykora volt: a Legfelsőbb Bíróságon Brandeis képviselte a többségi álláspontot, és így az alkoholcsempész Frank Carmine Nardone esetében végül ki is mondták, hogy a „mérgező fa gyümölcse" elvnek megfelelően nem csupán az illegális lehallgatások felvételei, de semmilyen, az illegális lehallgatásból származó információ sem használható fel a bizonyítási eljárás során.

Hoover: De az FBI például azért széles körben lehallgatott mindent és mindenkit az én irányításom alatt, és ezeknek az akcióknak ugyanaz volt a célja, mint például azoknak a térfigyelő kamerák felszerelésének, amikkel ebben a fejezetben foglalkozunk majd. Vagyis a bűnözés visszaszorítása, és nincs az az elvakult privacyvédő, aki vitathatná, hogy a kamera igenis roppant hatékony eszköz az utcai bűnözés elleni harcban. Csak hogy egyetlen példát mondjak: az angliai Cardiff City Centerben 13,4 százalékkal csökkent a bűncselekmények száma a zárt láncú kamerarendszer felszerelése után. Vagy említhetném azt az 1993-as esetet, amikor a brit CCTV-k rögzítették, amint egy 10 és egy 11 éves fiú elrabolta és meggyilkolta a 4 éves Jamie Bulgert, és...

Vízi Patkány: Hadd pontosítsak. Ezzel a történettel mindenki találkozott, aki akár csak egyszer is hallott a térfigyelő kamerákról. A zárt láncú televízió azonban nem rögzítette a gyilkosságot: a két srác elvonszolta magával az áldozatot, megkínozták és csak később végeztek vele. Utána elhencegtek a haverjaiknak - és azok azonnal feljelentették őket.

Szerző: Akárhogy is legyen, Nagy-Britannia ma vitathatatlanul kamera-nagyhatalom.

Vízi Patkány: Ahogy mondod. A járókelőket állítólag átlagosan háromszázszor (!) fényképezik le naponta, miközben minden jel arra mutat, hogy a londoni közlekedési vállalat nem ismeri a Dehomagnak a könyvünk elején említett plakátját, a „lássa a világot egy lyukkártya szemével"-t.

Nemrégiben ugyanis egy olyan hirdetéssel ragasztották tele a várost, amin egy hídon áthaladó emeletes busz látható, felette pedig négy szem - a Transport For London szimbóluma - lebeg. A

szöveg szerint „A figyelő szemeknek köszönhetően biztonságban vagyunk. A CCTV és a Metropolitan Police biztonságosabbá teszi a buszon való utazást.” A cég web site-ján az olvasható, hogy a megfigyelő kamerák „nem csak a vezetőket és a kalauzokat védik, de abban is alapvető szerepük van, hogy az utazás az utasok számára is biztonságosabb legyen”, mivel ha történik valami, akkor meg lehet állapítani, hogy ki volt a bűnös.

Hoover: Nem értem, hogy mi ezzel a baj. Engem például határozottan megnyugtatna, hogy a buszon is biztonságban vagyok.

Vízi Patkány: Tényleg nem érted? Pedig nekem két gondom is van. Az egyik kimondottan technikai jellegű: vajon feltételezhetjük-e, hogy pusztán azért, mert megfigyelő kamerákat szerelünk fel, valóban csökkenni fog a bűncselekmények száma?

Hoover: Márpedig a statisztikák pontosan ezt mutatják.

Vízi Patkány: Mármint azt, hogy a megfigyelt területeken - egyes esetekben - csökkent a bűncselekmények száma, de én azért nem hinném, hogy ha megjelennek a CCTV-k, akkor az utcai bűnözők fogják magukat, és jó útra térnek. Szerintem valószínűbb, hogy keresnek maguknak egy bekamerázatlan területet.

Hoover: Akkor majd azt is bekamerázzuk.

Vízi Patkány: És így tovább, egészen a végtelenségig. És ha végeztünk az összes utcával - ami persze nem lesz olcsó mulatság -, akkor majd jöhet az összes lépcsőház és kapualj és közpark és minden egyéb.

Azt kellene végre észrevenned, hogy ez azért egy soha le nem záruló és ennek megfelelően meglehetősen kilátástalan folyamat, mert tüneti kezelést próbál nyújtani az utcai bűnözés problémáira - ahelyett, hogy a bűnözés okait próbálná felszámolni.

De ha már a konkrét megoldásoknál tartunk: a statisztikák szerint néhány 60 wattos égő az utcai lámpákban jóval hatékonyabb (valamint olcsóbb és kevésbé privacysértő).

Az első brit térfigyelőrendszert egyébként 1985-ben, a bournemouthi tengerparton szerelték fel a huliganizmus elleni védelemül, és a 90-es évek közepén John Major miniszterelnök már azt nyilatkozta, hogy „nincsenek kétségeim afelől, hogy egyesek - a polgári szabadságjogokra hivatkozva - tiltakozni fognak. Nos, a szabadságjogoknak ez a fajtája egyáltalán nem élvezi a rokonszenvemet.”

Bill Gates roppant elégedetten említi, hogy amikor egész Monacót (mind a 150 hektárt) bekamerázták, akkor gyakorlatilag tökéletessé vált a közrend. Túl azonban azon, hogy Monaco meglehetősen extrém példa, Gates a lehető legkomolyabban javasolja azt is, hogy vezessük be az általa „walletPC”-nek, vagyis zsebtárca-számítógépnek nevezett berendezést, ami alkalmas lenne arra, hogy folyamatosan rögzítse és - megfelelő átviteli sebességgel meg háttértárolóval rendelkezvén - mentse le életünk minden eseményét, hogy ha esetleg meggyanúsítanak minket, akkor azonnal rávághassuk, hogy „hé, cimbora, az én életem tökéletesen dokumentálva van... Bármit vissza tudok játszani, ami velem történt, úgyhogy ne szórakozz velem.”

Hoover: Nekem ez is tetszene.

VíziPatkány: Nekem viszont nem. És nem csak azért nem, mert eddig legjobb tudomásom szerint általában azért érvényben volt az ártatlanság vélelme, tehát leginkább nem a vádlottnak kellett bebizonyítania, hogy nem követett el semmit, hanem a vádlónak, hogy az illető igenis bűnös. Hanem azért sem, mert ennél jobb példát nem igazán lehetne találni a zéró tolerancia elvére, és ez már önmagában is ellenszenvessé teszi.

Szerző: Aha, akkor már értem, hogy Farkas György terézvárosi polgármester miért említi a totális bekamerázás előnyei között, hogy el lehet majd kapni mindazokat, akiknek a kutyája odapiszkít a

járdára.

Vízi Patkány: Igen, a zéró tolerancia éppen erről szól. Ahogy Simon Davies, a Privacy International alapítója fogalmazott, a kormány zéró tolerancián alapuló „hozzáállása szerint mindenki potenciális bűnöző", és ehhez a felfogáshoz egy Charles Murray nevű amerikai politológus munkássága szolgáltatta az alapot.

Az illető abból indult ki, hogy mindennek az IQ a kulcsa: kizárólag ettől függ például, hogy ki fogja elvégezni az egyetemet (és ki nem); hogy ki válik milliomossá (és ki hajléktalanná); hogy mennyire „jól" neveljük fel a gyerekeinket - sőt, még az is, hogy ki fog a házasság „szent kötelékében" élni. „A törvénytelen viszonyok - melyek léte korunk egyik legnagyobb szociális problémája (sic!) - erősen függenek az intelligenciaszinttől", olvasható egy tanulmányában, és...

Szerző: Gondolom, ugyancsak kikelne az internetes pornográfia ellen.

Vízi Patkány: Szerintem is. Tehát a lényeg az, hogy Murray biztosra veszi, hogy az összes társadalmi probléma kizárólag biológiai okokra vezethető vissza - ugyanekkor persze egyetlen felmérés sem mutatta ki, hogy a házasságtörőknek akár csak valamivel is alacsonyabb lenne az intelligenciahányadosa, mint a monogámiában élőknek. Ezzel az érveléssel szerintem az a fő baj, hogy amennyiben minden biológiailag determinált, akkor az állam ha akarna, sem tehetne semmit a leszakadók felzárkóztatásáért (elvégre az intelligenciaszintet nem lehet mesterségesen növelni).

„Sokan hajlanak rá, hogy azt higgyék, a bűnözők a város 'rossz negyedeiből' kerülnek ki. Annyiban igazuk van, hogy ezekben a kerületekben aránytalanul sok a csekély kognitív képességgel rendelkező egyén", állítja Murray. Azaz a társadalmi egyenlőtlenségek felszámolása helyett ki kell vonulni erről a területről és inkább a jobb helyzetben lévőket kell megvédeni a többiektől: úgy is mondhatnánk, hogy az állam nem jóléti, hanem büntető állam kell, hogy legyen. Tehát a különböző szociális intézkedések különféle költségekkel és terhekkel járó felvállalása helyett mindenkit magára hagy, akinek segítségre lenne szüksége. És eközben kíméletlenül lecsap mindenkire, aki az utcán szemetel.

Hoover: Igen, ez számomra teljesen logikus: le is kell csapnia. Mivel a bűnözés az „értelmi adottságokból" következik, ezért a cigarettacsikk eldobása; a parkban való vizelés, sőt, tulajdonképpen az is, ha megengedjük, hogy a kutyánk odarondítson a járdára... nos, mindezek arra utalnak, hogy az illető - hogy Murray tapintatos megfogalmazását használjam - „csekélyebb kognitív képességekkel" rendelkezik. George Kelling, a konzervatív kriminológia pápája szerint „ha ma hazudsz, akkor holnap lopni fogsz". Azaz a kisstílű bűnözőket az előtt kell elkapni, hogy valami nagyobb galádságot követnének el. És erre a célra például tökéletesen megfelelnek a térfigyelő kamerák.

Vízi Patkány: Ez is éppen elég nagy baj. De olykor ráadásul még csak nem is ez a cél - hanem az, hogy a jobb helyzetben lévők biztonságban érezzék magukat. Amikor például 1996-ban Baltimore-ban nekiálltak megfigyelő rendszert telepíteni, akkor nem a legszegényebb és legtöbb utcai bűncselekményt produkáló negyedeket kamerázták be, hanem azokat a részeket, ahol a gazdagok szoktak sétálni, és Brian Lewbart, a projekt egyik vezetője be is vallotta, hogy azt akarták, „hogy az emberek kellemesebben érezzék magukat, mivel szemmel láthatóan jelen vannak /ezek/ a biztonsági intézkedések."

Jeffrey Rosen jogászprofesszor (George Washington University Law School) kissé tovább megy, és a jelenséget általánosítva arra is rámutat, hogy (különösen a szeptember 11-i terrortámadás után) világszerte mennyire megnőtt a hajlandóság arra, hogy elfogadjunk olyan technológiákat, melyek súlyosan sértik a privacyt - cserébe viszont nem biztonságot nyújtanak, hanem csupán a biztonság illúzióját. Miként a térfigyelő kamerák is ezt teszik.

Szerző: Világos. Hiszen - miután nem ismerjük arcról a potenciális repülőgép-eltérítőket - nem igazán fogjuk elkapni a térfigyelő kamerák segítségével őket, amint az utcán sétálnak.

Vízi Patkány: A hátrányokat viszont hosszan sorolhatnám. Az ACLU szerint „Az, hogy a rendőrség és az egyéb, a közbiztonságra felügyelő szervek /kamera/rendszereket használnak, különösen problémás egy demokratikus társadalomban", ami persze önmagában még nem jelenti azt, hogy minden esetben el kell utasítani.

Különösen, mivel bekamerázás és bekamerázás között komoly különbségek lehetnek: ha valaki valós időben figyeli, hogy mi történik a szomszéd sarkon, akkor az lényegében olyan (vagy majdnem olyan), mintha ott is állna egy rendőr. Ha viszont rögzítik is a felvételt, akkor kezdődnek a gondok, hiszen innentől kezdve az is kérdéses, hogy miként kezelik az adatokat. Vagyis innentől kezdve jönnek az adatvédelmi problémák.

Hoover: Ugye ezzel nem azt akarjátok mondani, hogy akkor felejtsük el a megfigyelő kamerákat?

Vízi Patkány: Nem, ezt semmiképpen. A szélsőséges álláspontok – talán emlékszel még erre az elvre – mint mindig, úgy most sem különösebben célravezetők, és bizonyos esetekben azért indokolt lehet a bekamerázás. Csak éppen nagyon át kell gondolni, hogy tényleg az-e. Az ACLU is úgy fogalmaz, hogy „Noha nem ellenezzük a CCTV használatát azoknak a terroristatámadásoknak különösen kitett helyeknek az esetében, mint amilyen például a Capitolium is... a nyilvános helyek / általában véve történő/ megfigyelését rossznak tartjuk."

A terroristavadászatban - miként már ezt is megtárgyaltuk - gyakorlatilag teljesen hatástalan, és lényegében hasonló a helyzet a kisebb bűncselekmények esetében is. Egy, a teljesen bekamerázott Nagy-Britanniában végzett, összesen 600 órán keresztül folytatott felmérésből azt lehetett megállapítani, hogy valóban nem csökkentek az adott városközpontban elkövetett bűncselekmények, miközben kiderült, hogy a kamera-operátorok tízből négy esetben minden ok nélkül, „csak úgy", szórakozásból figyeltek meg különböző embereket. Ugyanekkor viszont tízből mindössze három ember tevékenységét monitorozták „bűncselekménnyel kapcsolatos okokból", illetve gyanúból kifolyólag.

Egy másik tanulmány szerint bár a megfigyelő kamera nagyon hatékony lehet a parkolók megóvásában, gyakorlatilag (és ezen még mindenféle Dehomag-stílusú plakátokkal sem lehet segíteni) semmit sem ér a tömegközlekedésben meg a városközpontokban (hiszen mire odaérne a biztonsági őr, a zsebes már régen elfutott. És az sem biztos persze, hogy az operátor észreveszi a lopást).

Amerikai biztonsági szakértők pedig arra hívják fel a figyelmet, hogy „a videoképernyő folyamatos bámulása egyszerre unalmas és hipnotikus hatású... alig 20 perc után a legtöbb ember figyelme mélyen a megengedhető szint alá zuhan" és a megfigyelő egy meztelen nőnél kisebb dologra egészen biztosan nem fog felfigyelni.

Ugyanekkor viszont a megfigyelő kamera egyszerűen tökéletes eszköz, ha visszaéléseket akarunk elkövetni. Egy magas beosztású washingtoni rendőrtiszt nemrégiben úgy próbálta kamatoztatni az adatbázishoz való hozzáférését, hogy információkat gyűjtött egy homoszexuális klub látogatóiról az autók rendszámtáblái alapján, és zsaroló levelet küldött nekik (amennyiben házas emberekről volt szó). Érdemes elgondolkozni rajta, hogy mennyivel jobban vissza lehetne élni egy, az egész várost behálózó kamerarendszer által nyújtott lehetőségekkel.

De ott vannak a személyes célú visszaélések is. A Detroit Free Press beszámolója szerint a michigani végrehajtó szervek birtokában lévő adatbázist egyes hivatalnokok arra használták, hogy nőket kövessenek nyomon (vagy a barátaik számára tegyék ezt lehetővé); megfenyegessenek olyanokat, akikkel vezetés közben zördültek össze, vagy külön élő házastársuk minden lépését kísérjék figyelemmel stb. Gondoljunk csak a fejezet elején olvasható kis összeállításra, ami arról szólt, hogy miként is néz ki az elektronikus megfigyelés a mindennapokban.

És akkor a diszkriminatív hozzáállásból fakadó problémákat még csak nem is említettük, vagyis azt, hogy például Nagy-Britanniában a kamera-operátorok aránytalanul sokszor fokuszálnak más bőrszínű emberekre. „A feketéket 1,5-2,5-ször nagyobb valószínűséggel figyelik meg, mint a fehéreket", illetve mint azt a teljes populációhoz viszonyított előfordulási arányuk indokolttá tenné.

Azt is érdemes kiemelni, hogy a megfigyelők rendszerint saját előítéleteik és preferenciáik alapján döntenek arról, hogy kit érdemes szemmel tartani. Ezért „a fiatalok, különösen ha marginális szociális vagy gazdasági helyzetben vannak, sokkal jobban ki lehetnek téve a

megfigyelésnek, és a hivatalos megbélyegzésnek", mint mások, és így „a CCTV egyszerűen a jogtalanság eszközévé válik" (ami ráadásul a különben sem túlságosan nagy hatékonyság rovására mehet), mutat rá a téma szakértője, Clive Norris. És végül ott van a voyeurizmus: szintén Nagy-Britanniában a rendszerint hímnemű (és rendszerint unatkozó) operátorokat nők megfigyelésekor az esetek tíz (!) százalékában kizárólag kukkolási szándék vezérli.

Hoover: A látszat az lehet, hogy lassanként kezdek teljesen defenzívába szorulni... csak ülök, és hallgatom, amint újabb és újabb érveket zúdítasz rám közös szerzőnk teljes jóváhagyásával. De azt azért nem hagyom szó nélkül, hogy csupa olyan problémákat sorolsz fel, amiket megfelelő szabályozással ki lehetne védeni.

Vízi Patkány: Igen, én is ide akartam kilyukadni. Mármint oda, hogy jelenleg - gyakorlatilag a világon mindenütt - hiányzik a kamerázás megfelelő kontrollja. Különböző kiegyensúlyozó és ellenőrző mechanizmusokra lenne szükség, de a CCTV olyan észveszejtő sebességgel terjedt el, hogy ezekre nem jutott idő.

Ami viszont azért komoly probléma, mert az eddigi tapasztalatok alapján bízvást állíthatom, hogy ha egyszer egy meghatározott célra létrehoznak egy megfigyelő rendszert, akkor azt - abban a pillanatban, amint mód nyílik rá - egészen biztosan fel fogják minden más lehetséges célra is használni.

Vegyük például a washingtoni megfigyelő központot, ahol jelenleg kis felbontású kamerákat alkalmaznak. Ezek a forgalom meg a középületek megfigyelésére igen, az emberek azonosítására viszont nem képesek. Mivel azonban a szükséges infrastruktúrát már kiépítették, a következő lépésben olyan, a személyek azonosítására is használható, nagy felbontású kamerákat fognak felszerelni (elvégre miért is ne), amik akár egy mérföldről is el tudják olvasni az ember kezében tartott újságot; infravörös tartományban működve éjszaka is tökéletes képeket készítenek és megfelelő technikákat alkalmazva „a falon is átlátnak", miközben ugyanolyan arcfelismerő szoftverrel lesznek felszerelve, mint a floridai Tampa utcai kamerái (amiket majd mindjárt részletesebben is megtárgyalunk).

„Amíg nincs világos és egyértelmű megállapodás arról, hogy hol húzzuk meg - az amerikai értékeket megvédendő - a megfigyelés határait, addig fennáll a veszélye, hogy a CCTV afféle megfigyelési szörnyeteggé növi ki magát", írja az ACLU. És persze rendszerint hiányzik a megfelelő törvényi kontroll is.

Szerző: Például nem csak Amerikában, de Magyarországon is.

Vízi Patkány: Az azzal kapcsolatos társadalmi megegyezés, hogy mit tehet (és mit nem) egy kamerarendszer üzemeltetője vagy egy operátor, vitathatatlanul szép dolog - és ugyanilyen vitathatatlanul nem elég. Például az érintetteket a FIPS értelmében nem csak illene, de egyenesen kötelező lenne tájékoztatni arról, hogy a képeket rögzítik-e; és ha igen, akkor milyen feltételek mellett; illetve, hogy mennyi ideig tárolják őket; a kormányszervek (vagy a nyilvánosság és azok, akik a felvételeken szerepelnek) milyen feltételek mellett férhetnek hozzá; hogyan ellenőrzik és tartatják be a törvényi szabályozást; illetve milyen büntetésre számíthat az, aki megszegi azt... inkább nem is sorolom tovább.

Különösen, hogy kissé olyan ez, mint a kvantumfizika, ahol pusztán a megfigyelés ténye megváltoztatja a részecskék viselkedését. Amikor állandóan az jár a fejünkben, hogy a végrehajtó szervek figyelemmel kísérik minden mozdulatunkat (vagy legalábbis fennáll ennek a lehetősége), akkor ugye kevésbé leszünk oldottak és kevésbé érezzük jól magunkat. Jacob Sullum újságíró ezt úgy fogalmazza meg, hogy „Lehangoló dolog tudni, hogy a kormány felfegyverzett ügynökei figyelik az embert. Nem akarunk megütközést kelteni bennük vagy bármilyen más módon magunkra irányítani a figyelmüket... megtanuljuk, hogy óvatosak legyünk, amikor az a kérdés, hogy milyen könyveket vagy újságokat olvasunk nyilvánosan, és nem vesszük kézbe az olyanokat, melyek felkelthetik a láthatatlan megfigyelők érdeklődését. Több gondot fordíthatunk az öltözködésünkre is, hogy nehogy terroristának, bandatagnak, kábítószeresnek vagy drog dealernek nézzenek minket."

Szerző: Hát igen. Valahogy úgy, mint amikor Magyarországon a 2002-es választások két fordulója között az emberek kezdtek nem olvasni politikai lapokat nyilvános helyeken, mivel attól tartottak, hogy a „másik oldal" szavazói majd beléjük kötnek emiatt. Alkalmasint legalább ugyanilyen rossz és feszélyező, ha az állam tartja rajtunk állandóan a szemét, és részben ezért is vált ki a bekamerázás olykor meglehetősen komoly indulatokat. Részben pedig azért, mert a CCTV mintha csak a szemmel látható megfigyelés és ellenőrzés megtestesülése lenne.

Vízi Patkány: Aha, ez mozgatja például a Surveillance Camera Players csoportot New Yorkban. Ezt az anarchista - szabadságpárti - avantgárd társulatot még 1998-ban alapította egy bizonyos Bill Brown, aki úgy gondolja, hogy az utcai kamerák alkotmányellenesek, mivel a Negyedik Kiegészítés - elvileg - védelmet kellene, hogy biztosítson az indokolatlan megfigyelésekkel szemben. Úgyhogy most egyrészt olyan táblákkal a kezükben járkálnak a CCTV-k előtt, mint például „Munkába megyek"; Csak leugrottam vásárolni"; „Harapok valamit"; „Éppen hazafelé tartok"; „Tudjuk, hogy figyeltek"; „Törődjön mindenki a saját dolgával" stb. A biztonsági szolgálatok emberei persze nem kimondottan boldogok... és az operátorok hívására a helyszínre érkező rendőrök sem, akiknek Brown szép komótosan felolvassa a Negyedik Kiegészítést - majd pedig amikor a tüntetésre való engedélyét kérik, akkor ugyanígy felolvassa az Első Kiegészítést is. Amúgy viszont nem kötözködik velük, mert szerinte nem ellenük, hanem azok ellen kell küzdeni, akik a megfelelő profit reményében bekamerázzák az egész világot.

Amúgy Brown nevéhez fűződik a kameraszínházak ötlete is. Átírta például Orwell 1984-ét és Beckett Godotra várva című darabját kamerára: az egész alig két percig tart, és a szereplők beszéd helyett táblákkal kommunikálnak.

Aminek kétségkívül van némi kameraoperátor-pukkasztó mellékíze - miként ez jellemzi az 1998 óta minden december 24-én megrendezésre kerülő és sajnálatosan kis sajtóvisszhangot kiváltó World Sousveillance Dayt is.

Hoover: Ha a „Surveillance" azt jelenti, hogy „felülről nézni", akkor a Sousveillance azt, hogy ugyanezt csinálni - csak éppen alulról, gondolom én.

Vízi Patkány: Pontosan. A résztvevőknek az a feladatuk, hogy pontosan délben felbukkanjanak egy bevásárló központban, és egyikük nekiálljon vadul videózni a megfigyelő kamerákat (vagy legalább úgy tenni, mintha ezt csinálná, és közben az sem baj, ha nincs is film a gépben), miközben a másik magát az eseményt rögzíti (vagy legalábbis úgy tesz, mintha rögzítené). Az MIT-s (Massachussets Institute of Technology) Steve Mann, aki arról vált közismertté, hogy állandóan kábel nélküli számítógépet és webcamet hord magán, azt javasolja, hogy a kamera-megfigyelő nap résztvevőinek pólóját díszítse az a felirat, hogy „az Ön biztonsága érdekében minden Önnel, illetve az Ön környezetével kapcsolatos képet videokamerával rögzítünk és továbbítunk. BÁRMILYEN BŰNCSELEKMÉNY HATÓSÁGI ELJÁRÁST VON MAGA UTÁN."

Az eredmény persze az szokott lenni, hogy a biztonsági őrök roppant idegesek lesznek - de közben legalább sikerül néhány ember figyelmét ráirányítani a problémára.

Hoover: Méghozzá az olyanok figyelmét, akik pontosan ezt csinálják otthon.

Szerző: Én például nem csinálom ezt.

Hoover: Rendben, akkor fogalmazzunk úgy, hogy legalábbis lehetőségük van rá. A webkamerák (röviden: webcam) története 1991-ben kezdődött, amikor a Cambridge University Számítógép Laboratóriumában csak a második szinten, az úgynevezett „Trójai Szobában" volt kávéfőző, és a többi emeleten dolgozó posztgraduális diákok soha nem tudhatták, hogy van-e éppen friss kávé. Úgyhogy végül felinstalláltak egy videokamerát, és egy Paul Jardetzky nevű hallgató írt egy programot a kép „levételére" - Quentin Staffoed-Fraser pedig megírta az XCoffee-t, ami ugyanezt a képet jelenítette meg a számítógép monitorán.

Percenként háromszor frissítve, szürkében és kis felbontásban, de ez akkoriban így is jó volt... 1994. végéig több mint 150 ezren voltak rá kíváncsiak a weben, és innét már töretlen út vezetett

ahhoz, hogy megjelenjenek a kukkolásra épülő internetes szolgáltatások. Mint amilyen az egyik leghíresebb példa, a JenniCam, ahol majdnem élőben nézhetjük végig, amint egy hölgy a mindennapi életét éli (fürdéssel, szépítkezéssel és persze szex-szel együtt). Másfelől pedig elterjedtek az olyan, bárki számára megfizethető mini kamerák, amiket a számítógépünkhöz csatlakoztatva kifigyelhetjük, hogy miként viselkedik a babysitter a gyerekünkkel, amikor nem vagyunk ott.

Vízi Patkány: A webcammel kapcsolatban elfelejtetted megemlíteni az egyik legfontosabb dolgot. Méghozzá azt, hogy amikor 1994-ben a BBC interjút készített a bekamerázott kávéfőzőről egy Daniel Gordon nevű diákkal, akkor az leült a számítógép elé. „Nem kell mást tennünk - mondta -, mint ráklikkelni erre gombra... hogy megjelenjen a kávéfőző képe a monitoron. És... úgy látszik... valaki megitta előlünk az összeset. Azt hiszem, csinálnom kell magamnak, ha én is inni akarok."

Hoover: És ebben mi az érdekes?

Vízi Patkány: Várjad ki a végét. A riporter megkérdezte Gordont, hogy miért nem állítják be úgy a kamerát, hogy ne csak a készülék, de az is látsszon rajta, hogy éppen ki dézsmálja meg a kávét?

Mire Gordon azt válaszolta, hogy jó ötletnek jó ötlet ugyan, de „azt hiszem, mi védeni szeretnénk a bűnösöket is". Vagyis: ha a rendszernek kizárólag az a célja, hogy távolról is meg lehessen állapítani, hogy elfogyott-e az innivaló, akkor azt nem szabad holmi megfigyelőeszközzé alakítani, mert azonnal megszűnne a doktoranduszok „mikrotársadalmát" egyensúlyban tartó rend.

Rosen professzor a biztonságérzetet nyújtó technológiákkal kapcsolatban valami nagyon hasonlóról beszél, amikor azt mondja, hogy az utóbbi években egyre inkább egy „privacy-Csernobilra" emlékeztet a helyzet - pedig ha már mindenképpen abszurd biztonsági berendezésekkel akarjuk telezsúfolni a környezetünket, akkor ezt meg lehet úgy is csinálni, hogy közben ne sértsük meg az egyedülhagyatáshoz való jogot. Például az Orlando International Airporton (Florida) használt „meztelengépet" megalkotó cég most olyan verzión dolgozik, ami a ruha alá rejtett fegyvereket tisztán és élesen láthatóvá teszi ugyan, de - a jelenleg használt verzióval ellentétben - eközben a képernyőn nem jelenik meg a meztelen emberi test. Hasonló megoldás lenne az is, amikor a biometrikus berendezés ellenőrzi ugyan az ujjlenyomatot vagy az íriszmintázatot, de miután ez megtörtént, a vizsgált személy adatait nem tárolja el.

Hoover: Nos, ha már a biometrikus azonosítási módszereknél tartunk... szerintem roppant ígéretes technológia. Sőt, nem is technológia, hanem technológiák, hiszen többféle azonosítási eljárás is van, és mindegyik azon alapul, hogy vagy valamilyen biológiai paraméterünket (mint amilyen mondjuk az ujjlenyomat); vagy pedig egy biológiai változót mérjük meg (mint amilyen az, hogy gépelés közben mikor mekkora erővel ütünk le egy billentyűt).

Vízi Patkány: Gondolom, most nekiállsz az összeset felsorolni.

Hoover: Hát, legalább az alaptípusokat mindenképpen. Először is ott van az íriszazonosítás: ellentétben a retinával, az írisz mintázata már a méhen belüli élet során kialakul és mindvégig változatlan marad. Ha ehhez azt is hozzávesszük, hogy még a két szemünknek is különböző (nagyjából 200 pont alapján meghatározható) mintázata van; illetve azt, hogy az íriszazonosítók kevesebbet hibáznak (átlagosan 1,2 millióból egyet), mint az ujjlenyomat-azonosítók, akkor érthető, hogy miért válnak egyre népszerűbbé. Például a bankautomatáknál, hogy az ügyfélnek ne kelljen megjegyeznie az PIN-kódot.

Vízi Patkány: Vagy említhetnénk azt a rendszert, amit a British Telecom dolgozott ki (feltehetően szintén azért, hogy könnyebbé tegye a felhasználók életét), és ami képes arra, hogy közel 80 km/órás sebességnél is azonosítsa az autóvezető íriszmintázatát.

Hoover: Igen, autópályákon kiválóan lehet majd alkalmazni (és a szemüveg vagy kontaktlencse használata sem rontja a hatásfokot). De hogy tovább folytassam a felsorolást, ott van aztán az

aláírás- és írásanalízis: amennyiben nem csak azt vesszük figyelembe, hogy milyen az aláírás képe, hanem azt is, hogy mikor milyen sebességgel mozgatjuk a tollat és éppen mennyire nyomjuk, akkor gyakorlatilag lehetetlen az eredetit meghamisítani.

Vízi Patkány: Még szerencse, ugyanis a biometriai módszerek terjedésével párhuzamosan egyre inkább elterjedőben van a biometrikus piracy (kb. biometrikus kalózkodás) is. Aminek persze - ha úgy vesszük - komoly történeti gyökerei vannak, mert ide sorolható az is, amikor a 20. sz. elején rátették az ember fényképét egy szappan csomagolására - különösen, ha csinos fiatal nő volt az illető (miközben elfelejtették megkérdezni tőle, hogy ez rendben van-e így). A fotó a későbbiekben is népszerű árucikk maradt: hogy csupán egyetlen kirívó esetet említsek, 1999-ben a South California Public Safety Department nekiállt a birtokában lévő 3,5 millió (!) digitális jogosítványfényképet eladni a New Hamsphire-i Nashauban található Image Data LCC-nek. Méghozzá nem is drágán: egy pennyt kértek hét darabért. És még mielőtt valaki rákérdezne, hogy mire is volt jó ennyi felvétel ennek a bizonyos Image Data LCC-nek, hadd tegyem hozzá, hogy érdekes módon éppen ez a cég kapott egy évvel korábban közel másfél millió dolláros támogatást a US Secret Service-től (gondolom azért, hogy valamiféle képalapú nemzeti nyilvántartást építsenek ki). Amikor a Washington Post megszellőztette a dolgot, Dél-Kalifornia azzal próbált visszatáncolni, hogy ez az eljárás sérti az állampolgárok privacyjét - az állami bíróság viszont úgy döntött, hogy nincs olyan törvény, amiből ez következne, és a fényképek...

Hoover: Ha nagyon ragaszkodsz hozzá, akkor majd még visszatérhetsz az imádott fényképekhez, de egyelőre hadd haladjak a saját ízlésemnek megfelelő sorrendben, és következzen a kéz- és a tenyérgeometria, ami az ujjak hosszúságát és hasonló adatokat figyelembe véve azonosítja az embert. A módszer komoly hátulütője, hogy ezek a paraméterek az élet során változhatnak, de azért az 1996-os atlantai Nyári Olimpián jól bevált a sportolóknál.

Vízi Patkány: Mintha csak a híres Bertillion-rendszer felmelegített változata lenne...

Szerző: Bertillion?

Vízi Patkány: Ő hát. Alphonse Bertillion 1879-ben dolgozta ki azt a biometriai identifikációs rendszert, ami még az ujjlenyomat-azonosítás elterjedése előtt szédületes karriert futott be. Szemből és oldalról készítettek felvételt a delikvensről, és közben megmérték a magasságát; a kar fesztávolságát; a mell kerületét; a fejhosszt; a fejszélességet; a bal középső ujj hosszát és a bal fület, stb.; majd pedig bíztak benne, hogy minden rendben lesz. Hamarosan félmillió ember adatait tartották nyilván 729 különböző kategóriába sorolva, és Bertillion megalkotta a „beszélő arcképet" is, ami a lehető legpontosabban, ismét csak a megfelelő kategóriákba való besorolást használva szóban is leírta a delikvenst.

Hoover: Vagyis mód nyílott arra, hogy azonosítsanak egy visszaeső bűnözőt, aki korábban simán megúszta volna a dolgot, ha nem ugyanahhoz a rendőrtiszthez kerül, mint aki már foglalkozott vele. Nem lehet eléggé hangsúlyozni, hogy a történelem folyamán most először nyílt arra lehetőség, hogy tudományos módszerekkel identifikáljanak valakit.

Vízi Patkány: És ez nem kis szó még akkor sem, ha Bertilliont az a - határozottan rasszista - meggyőződés hajtotta, hogy a módszere segítségével egy szép napon majd el lehet egymástól különíteni a cigányokat és nem cigányokat.

De ez a kortársait feltehetően nem különösebben zavarta, és amikor egy rettegett anarchistát is sikerült lelepleznie, akkor megkezdődött a diadalmenet, és Olaszország, Portugália, Dánia, Hollandia, Ausztria, stb. is átvette a módszert, Spanyolország pedig egyenesen „antropometriai kabinenet" rendezett be a börtönökben.

Aztán... aztán 1903 tavaszán az amerikai Leawenworth fegyházába beszállítottak egy négert, akit a Bertillion-szisztéma segítségével a 2626-os számú fogolyként, egy bizonyos Will Westként azonosítottak - miközben az igazi Will West éppen a fegyház műhelyében dolgozott.

Hoover: És ezzel mit akarsz mondani? Mindenütt előfordulhatnak hibák.

Vízi Patkány: Igen, de éppen azokban az esetekben, amikor egy embert próbálunk meg biometriai módszerekkel azonosítani, nem elég, ha a módszer viszonylag megbízható, megbízható vagy éppenséggel nagyon megbízható: ha mondjuk 99,97 százalékos hatásfokkal dolgozik, de tévedés esetén egy ártatlan ember kerül börtönbe, akkor még ez sem fogadható el. Értsd: amikor egyes emberek sorsáról van szó, akkor nem kezelhető ugyanúgy a statisztikai hiba, mint amikor azt kérdezzük, hogy várhatóan mekkora lesz egy sörétszem átmérője.

Hoover: Nos, akkor neked minden bizonnyal az ujjlenyomat-azonosítás lenne a kedvenced, a daktiloszkópia. Ez olyan bombabiztos, hogy Juan Vucetih, aki a világon elsőként azonosított ujjlenyomat alapján bűnözőt (1892-ben Argentínában), elő is állt azzal az ötlettel, hogy Buenos Aires tartomány minden lakójáról vegyenek ujjlenyomatot, és erre csak azért nem került sor, mert 1917-ben az argentin központi kormány máshogy döntött.

Vízi Patkány: Még szerencse: hadd említsek néhány érvet az állítólag tökéletesen megbízható ujjlenyomat-azonosítás ellen.
Először is azt, hogy ilyenkor akár az ember, akár a rendszer tévedhet; aztán azt, hogy a bűnügy helyszínén szerencsétlen esetben a nélkül is fellelhető lehet valakinek az ujjlenyomata, hogy az bármit elkövetett volna; és rosszakaróink az adatbázisban tárolt ujjlenyomatot is módosíthatják.

Amire már csak azért is érdemes nagyon odafigyelni, mert - mutat rá Simson Garfinkel biztonságtechnikai szakértő - „Minél inkább bízunk egy azonosítási technikában, annál inkább vissza lehet élni vele, és a szándékos csalás lehetősége is mindig fennáll. Ezért aztán az ujjlenyomat valójában nem azonosít senkit: egyszerűen hozzá van kapcsolva egy file adataihoz. Változtassuk meg a file-t, és ezzel megváltoztattuk az azonosított személyt is.”. A modern társadalomban nem a test, hanem a személy létezik, mint - büntetőjogilag is felelős - entitás, viszont a különböző biometrikus „technológiák nem az embert azonosítják, hanem /jobb esetben/ a testet”.

Méghozzá a Cahners In-Stat Group hi-tech piackutató cég szerint már 2001-ben is leginkább a Nagy Testvérek, vagyis a világ kormányai megbízásából: „az ujjlenyomat-azonosító technológiákra költött összeg 75 százalékát a kormányok fizették ki 2000-ben”, mondja a Cahners szakértője, Marlene Bourne, és a különböző bűnüldöző szervek kiadásai tették ki az egy év alatt biometrikus azonosításra költött 228 millió dollár felét. Ehhez képest a különböző cégek „mindössze” 90 millió dollárt szántak a biometrikus azonosító rendszerekre (és az International Biometric Group szerint 16 százalékot fordítottak az alkalmazottaik utáni kémkedésre, vagyis annak megállapítására, hogy valaki mennyi időt tölt kávézással munkaidőben).

Hoover: Hát ez van, pajtás. És a hangazonosítás még ennyire sem fog tetszeni neked - pedig az újabb rendszereket már csak azért sem lehet magnóra felvett szöveggel kicselezni, mert meg tudják állapítani, hogy „élő” beszédről van-e szó. És különben is: az azonosításhoz szükséges szöveg minden esetben változik, tehát nem lehet rá felkészülni (például egy táblán felvillanó számokat kell felolvasni).

Garfinkel számol be róla, hogy a hangazonosításon alapuló „biometria nem demokratikus”: akadnak, akiket egy rendszer soha nem tanul meg azonosítani (persze senki sem tudja, hogy miért).

Vízi Patkány: És persze – jut eszembe – olyanok is akadnak, akiknek viszont valamiért nehezen „olvasható” az ujjlenyomatuk (bármennyire is dicsérted az előbb a módszer megbízhatóságát). Ez nagyjából egy százalékot szokott kitenni, ami ahhoz képest, hogy New York 1998 óta daktiloszkópiát használ a munkanélküli segélyt felvevők azonosítására, nem is olyan kevés. És ennek ugye meglehetősen kellemetlen következményei lehetnek egy olyan 21. sz.-i társadalomban, ahol minden a biometrikus azonosításon alapul.

Hoover: Ahogy mondod, Vízi Patkány, ahogy mondod, de attól tartok, hogy együtt kell élnünk ezzel a gondolattal. Ezen még a Thomas Speeter által kifejlesztett járásjellegzetesség-felismerő

padló sem fog segíteni (ami egy 188 lépésen alapuló minta alapján állítólag 100 százalékos biztonsággal azonosítja az embert), mint ahogy az arcfelismerő kamera sem - ez utóbbi, be kell vallanom, egyelőre nem váltotta be a hozzá fűzött reményeket.

Szerző: Hát ez elég nagy kudarc lehetett, ha még te is beismered....

Hoover: Nem azt mondtam, hogy nem vált be, hanem azt, hogy egyelőre nem, és ez óriási különbség. Az eredeti elképzelés egyszerűen zseniális volt: nevezetesen, hogy - miként ti is említettétek - az ember egy idő múlva képtelen odafigyelni a monitoron történő eseményekre. Tehát miért is ne bíznánk ezt a feladatot a számítógépre, ami levesz az ember arcáról úgy 80 képpontot, hogy...

Vízi Patkány: Nem kevés egy kicsit ez a 80 képpont?

Hoover: A FaceIt, a talán legismertebb ilyen program leírása szerint akár 40 is elég lenne a „nagy biztonsággal történő" azonosításhoz. Tehát meghatározza ezeket a pontokat (mint amilyen mondjuk a szem sarkának távolsága az orrtőtől), és az így kapott adatokból létrehoz egy digitális kódot. Majd pedig ezt összehasonlítja az adatbázisban tárolt kóddal; a hasonlóságokat 1-től 10-ig osztályozza, és 8,5 vagy magasabb szintű egybeesés esetén elkezd visítani - a humán végrehajtó szervek pedig azonnal akcióba léphetnek.

Az első FaceIt rendszert természetesen Nagy-Britanniában, a világ legjobban bekamerázott országában szerelték fel: Newham Borough (London) városközpontját 1998-ban kezdték ilyennel figyelni, és ennek hatására 40 százalékkal csökkent a bűnözés.

Vízi Patkány: Állítólag.

Hoover: Állítólag vagy sem, most foglalkozzunk inkább azzal, hogy két évvel később a Civil Aviation Organization (CIAO), ami már régóta kacérkodott a „géppel olvasható" útlevél gondolatával, kijelentette, hogy az arcfelismerő kamerák felelnének meg legjobban a célnak, és még ugyanebben az évben a tampai Super Bowl kupa döntőjében FaceIttel felszerelt kamerák pásztázták a nézőket.

Vízi Patkány: Nem túlságosan nagy hatásfokkal. Amennyire én tudom, 19 jelentéktelen bűnözőt sikerült ugyan azonosítani, de a tömeg túlságosan nagy volt ahhoz, hogy elkaphassák őket. Ekkor aztán ki is tört a botrány, és az ACLU nyílt levelet írt Tampa illetékeseinek, mivel a hatóságok komolyan megsértették a Negyedik Kiegészítést (a kameraszínházas Brown is erre hivatkozott, ha emlékeztek még).

Szerző: Bizony, hogy megsértették!

Hoover: Érdekes, hogy Eugene Volkoh jogászprofesszor (University of California, Los Angeles) nem pontosan így gondolta. „Szó sincs semmiféle Negyedik Kiegészítéssel kapcsolatos problémáról, amíg a kormány egyszerűen megfigyeli - és esetleg még rögzíti is -, hogy mit csinálnak az emberek a nyilvános helyeken", mondta, hiszen eddig is bevett gyakorlatnak számított például az, hogy a rendőrök erős távcsövekkel kémlelték a lelátókon nyüzsgő tömeget.

Vízi Patkány: Erre viszont én mondom azt, hogy érdekes, mert Marc Rotenberg, az EPIC vezetője viszont arra hívja fel a figyelmet, hogy az automatikus arcazonosítás azért nem pontosan ugyanaz, mint amit eddig a rendőrök csináltak.

Az amerikai jogászszövetség, az ABA (American Bar Association) befolyásos bűnügyi szekciója pedig rendkívül kívánatosnak tartotta, hogy az ilyen megfigyelésekre ne titokban, hanem az érdekeltek tájékoztatásával kerüljön sor. És azt már hozzá sem kell tennem, hogy legfeljebb azoknak a digitális arclenyomatát lenne szabad rögzíteni, akikkel kapcsolatban kiderült valami - de semmiképpen sem mindenkiét.

Szerző: Tampa ezzel a húzásával aztán ki is érdemelte az amerikai Nagy Testvér Díjat, amit köztudottan nem a népszerűségi lista elején állóknak szoktak adni. A kupát pedig a nagyközönség átnevezte Snooper Bowl-nak (kb. szimatoló kupa).

Hoover: Ami persze nem különösebben érdekli a döntéshozókat. Amikor komoly formában kezdtek Tampa Ybor City nevű szórakozó negyedének arcfelismerő kamerákkal való felszerelésének gondolatával foglalkozni, akkor a privacyvédők persze kézzel-lábbal tiltakoztak, és Randall Marshall, az ACLU (Florida) jogi igazgatója azt hajtogatta, hogy „ez újabb példa arra, hogy a technológia lehagyja a személyiségi jogok védelmét", és az egésznek nagyon is „igazi Nagy Testvér hangulata van", bár eddig egyetlen gyanúsítottat sem találtak meg a segítségével. Beth Givens, a Privacy Rights Clearinghouse igazgatója pedig azt tette hozzá, hogy „Számos privacysértő technológia létezik ugyan, de az arcfelismerés vitathatatlanul az első helyen áll".

Még egy alig 100 fős tüntetésre is sor került (ami egyébként már önmagában is jelzi a dolog komolytalanságát). Az egyik tiltakozó pólójának felirata szerint „Házi őrizetben vagyunk a szabadság földjén". Egy másik obszcén mozdulatokat téve azt kiabálta, hogy „Ezt digitalizáld be!" És olyanok is akadtak, akik gázmaszkot, Groucho Marx szemüveget és hasonlókat viseltek.

Ami pedig a helyieket illeti, ki így gondolta, ki úgy: a biztonsági őrként dolgozó Jason Skinner azt mondta, hogy „az emberek privacyje elleni inváziónak" tekinthető az új kamerarendszer - jó néhány üzletember viszont azon reményeinek adott hangot, hogy a közeli jövőben már ugyanúgy hozzá fognak tartozni az arcfelismerő kamerával megfigyelt utcák is a békés civil élethez, mint a közvilágítás...

Vízi Patkány: Annyi eredménye mégiscsak volt a tiltakozásnak, hogy a FaceIt gyártója gyorsan kidolgozta a Privacy Védelmi Alapelveket. Ennek értelmében az embereket tájékoztatni kell a kamerák alkalmazásáról; a képadatbázisok használatát szigorúan szabályozni kell és a visszaéléseket meg kell büntetni. Stb., stb., stb.

Semmi új, de azért jó lenne, ha betartanák.

Közben még az International Biometric Industry Association is rájött, hogy baj lesz, ha nem reagál, és Richard Norton igazgatóhelyettes sürgősen azt nyilatkozta, hogy „Az iparág nyitott és befogadóképes a szabályozással kapcsolatban". Azért nyitott, mivel „nem akarjuk, hogy a / technológia iránti/ bizalmat megrendítse a biometria körüli zavar", ami határozottan ügyes fordulat, mert mintegy azt sugallja, hogy egyelőre van ilyen bizalom.

Debra Bowen szenátor egyébként, aki Kaliforniában törvénytervezetet dolgozott ki az arcfelismerő kamerák szabályozására (ez aztán a biometriai ipar és a rendőrség ellenállása miatt annak rendje és módja szerint meg is bukott), azzal érvelt, hogy „Ha felállítunk egy biometrikus kamerát és mindenkit rögzítünk vele, aki csak az utcán jár, az kissé olyan, mintha mindenkinek a telefonjára lehallgató készüléket szerelnénk, mondván, hogy biztosan akad majd, aki bűnt fog elkövetni."

Hoover: Ne kezdjük elölről, Vízi Patkány.

Vízi Patkány: Nincs szándékomban - csak hirtelen az jutott az eszembe, hogy nem sokkal később rendeztek egy sajtókonferenciát Washingtonban, és ott az egyik újságíró azt a kérdést szegezte neki Joseph Aticknak, a FaceItet forgalmazó Visionics igazgatójának, hogy használják-e már az általa árult technikát olyan országokban is, ahol büntetendő cselekmény ellenzékinek lenni.

Hoover: És használják?

Vízi Patkány: Nem tudok róla. Viszont innentől kezdve nyilvánvaló, hogy az arcfelismerő kamera kb. ugyanolyan minőségi ugrást jelent a közterületek megfigyelésében, mint amilyen annak idején a számítógépesített adatkezelés volt.

Régebben ugyanis ha végigsétáltál egy bekamerázott utcán, akkor legfeljebb annyi történt, hogy egymás után huszonötször mágneses adathordozóra rögzítették a képedet, és szükség esetén

egyenként kellett visszapörgetni valamennyit - valahogy úgy, mint az ujjlenyomatokat az AFIS megjelenése előtti időkben. Mostantól azonban ugyanúgy össze lehet kapcsolni az adott emberről készült felvételeket, mint egy bármilyen más adatbázis adatait - és persze ugyanúgy vissza is lehet élni vele. Akár az FBI, akár az utolsó direktmarketing-hiéna képes lehet rá, hogy tökéletesen nyomon kövesse a mozgásunkat - feltéve, hogy a hely kellőképpen be van kamerázva és az arcfelismerő szoftver megfelelő hatásfokkal működik.

Hoover: És szerinted úgy működik?

Vízi Patkány: Hazudnék, ha azt állítanám, hogy igen, noha a 2001-es év vitathatatlanul az arcfelismerő technológiák éve volt. A Visionics technológiáját választotta a US Immigration and Naturalisation Service a mexikói határon keresztül érkező illegális bevándorlók kiszűrésére; az izraeli hadsereg a Gazai Övezetben; Izland Keflavik nevű repülőtere ezt alkalmazta az ismert terroristák ellen; a South Wales Police pedig a futballhuligánokat azonosította vele (elvégre ez is egy olyan probléma, ami ellen a létező legmodernebb technológiát kell bevetni. Igaz, a mexikói kormány már 2000-ben arcfelismerő kamerákkal próbálta ellenőrizni, hogy egyesek nem akarják-e kétszer leadni a szavazatukat a választások során). A US Army Research Laboratory ekkoriban a FaceItet tartotta a legjobb arcfelismerő rendszernek; a Visionics pedig büszkén hangoztatta, hogy a szoftver több mint 99 százalékos hatásfokkal dolgozik.

A konkurens Viisage ugyanekkor Tom Colatosti (CEO) szerint 99,7 százalékos pontosságra volt képes, és állítólag sikerült már olyan embert is elkapniuk, aki az eredeti felvételekhez képest „tíz évvel volt öregebb, 15 kg-ot hízott és bajuszt növesztett".

A Trump Marina kaszinó (Atlantic City) olyan Viisage-kamerákat vetett be, melyek 9,200 bűnözőt voltak képesek „röptében" azonosítani, mivel állandóan pásztázták a játékosokat, és a felinstallálást követő napokban már sikerült is fülön csípniük hat, korábban Kaliforniában csalásért már letartóztatott szerencsejátékost (és azóta persze több száz további csalót).

Hirtelen mintha mindenre az arcfelismerő kamerák jelentették volna a megoldást: A Borders Group Inc. könyvhálózat például két londoni könyvesboltját (a Charing Crosson és az Oxford Streeten) akarta a tolvajok elleni védekezés nevében arcfelismerő-rendszerekkel bekamerázni, de akkora volt a felháborodás, hogy végül elállt tőle.

Szerző: És mindez szeptember 11. előtt.

Vízi Patkány: Igen, és szeptember 11. még rá is tett egy lapáttal erre a hisztériára. A Harris Poll ekkoriban végzett felmérése szerint az amerikaiak 86 százaléka támogatta volna az arcfelismerő kamerák felszerelését. És még véletlenül sem tűnődtek el rajta, hogy vajon honnét is lenne jó minőségű fényképünk a terroristákról? Márpedig e nélkül nem működik a dolog... (a 19 szeptember 11-i terroristából mindössze kettőnek volt meg a fotója).

De a biometrikus rendszerek gyártóinak árfolyama azért vad szárnyalásba kezdett a tőzsdén, és az ACLU is azt hangsúlyozta (igen, még az ACLU is), hogy nem általában véve az arcfelismerő kamerák alkalmazását ellenzi, és az ellen például semmi kifogásuk nincs, ha csak a fokozott biztonsági ellenőrzést igénylő helyekre belépőket monitorozzák ilyennel.

De az már ekkor is kérdéses volt, hogy például a repülőterek esetében tényleg érdemes-e a biometrikus kamerákat választani, és Bruce Scheiner biztonságtechnikai szakértő némi számolás után egyértelműen „nem"-mel válaszolt. „Ha a rendszer olyan valakit /például egy terroristát/ keres, aki egy a tízmillióhoz arányban fordul elő a népességben, és tízezer esetből egyszer fordul elő hiba, akkor egy helyes azonosításra 1,000 téves riasztás jut", mondta. Az pedig igencsak valószínű, hogy valamikor a sok századik téves riasztás után a kezelőszemélyzet már ügyet sem fog vetni a jelzésekre, mert „mintha csak állandóan farkast kiáltanánk". Akkor meg minek az egész.

Phil Agre informatika-professzor (University of California, Los Angeles) pedig azt írta, hogy elvileg „egyetértek az erősebb repülőtéri biztonsággal. Csak éppen most semmi mást nem csinálunk, mint hogy több berendezést használva rosszabbá tesszük a dolgokat. Minden háború olyan, új intézményeket hagy hátra, melyek többé nem tűnnek el. Ha nem vigyázunk, akkor a mostani hozadéka egy, a mindennapi életbe beleépülő megfigyelőrendszer lesz."

Hoover: Nem térhetnénk rá a lényegre? Unom már az állandó és megalapozatlan siránkozást.

Vízi Patkány: Ám legyen. Az ACLU a FOIA (Freedom of Information Act) által kínált lehetőségekkel élve kikérte az arcfelismerő kamerás megfigyelésekre vonatkozó júliusi és augusztusi adatokat a floridai rendőrségtől, és némi böngészést követően kimutatta, hogy két hónap alatt egyetlen, az adatbázisban fényképpel szereplő bűnözőt sem sikerült elkapni (viszont számos téves riasztás történt). Ráadásul olykor nem csupán eltérő testtömegű embereket, de férfiakat és nőket is sikerült összekeverni.

Hoover: Ennek sokféle magyarázata lehet.

Vízi Patkány: Minden bizonnyal. Például az, hogy a CCTV-operátornak manuálisan kellett ráközelítenie az emberek arcára, és ez bizony nem valami kényelmes megoldás: mintegy 125 ezerből 457-et sikerült így „szemrevételezni" egy éjszaka alatt. A Visionics szóvivője, Frances Zelazny pedig abban vélte megtalálni a magyarázatot, hogy „talán egyetlen bűnöző sem jelent meg ez alatt az idő alatt Ybor Cityben". És különben is, tette hozzá: ez egy ugyanolyan eszköz, mint a fémdetektor a repülőtereken, ahol emberi közreműködésre is szükség van, hogy megállapítható legyen, hogy valóban indokolt volt-e a riasztás.

Az efféle mentegetőzés azonban mit sem változtat a lényegen, vagyis azon, hogy az arcfelismerő kamera még akkor is kezdett leszerepelni, ha szeptember 11. után többek között a bostoni Logan International Airport, a T. F. Green Airport (Providence), a San Francisco International Airport és a kaliforniai Oakland International Airport is használni kezdte - és további száz repülőtérre akarták telepíteni.

Pedig Barry Steinhardt, az ACLU vezetője ekkora már többször is felhívta rá a figyelmet, hogy „az arcfelismerő kamera afféle mánia, nem pedig igazi megoldás... A tampai rendőrség tapasztalatai azt támasztják alá, hogy ez a technológia még nem piacképes."

Hoover: Lehet, hogy számodra kötözködésnek tűnik, de hát logika is van a világon... és abból, hogy a FaceIt kudarcot vallott Tampában, legfeljebb az következik, hogy Tampában nem vált be - de az nem feltétlenül, hogy a repülőtereken is használhatatlan.

Vízi Patkány: Tökéletesen igazad van, kedves Hoover, és erre az ACLU is rájött. Úgyhogy következzen az arcfelismerő kamera drámájának csúcspontja, amikor is a lélegzetét visszatartva figyelő néző végre megtudja az igazságot. Vagyis azt, hogy a Palm Beach International Airporton a kamerák az esetek 53 százalékában voltak képtelenek helyesen azonosítani a repülőtéri alkalmazottakat. „Az előzetes vizsgálatok eredményei... igazolják /azt a feltételezést/, hogy az arcfelismerő technológia egyszerűen nem hatékony és nem használható", fogalmazott meglehetősen sarkosan Randall Marshall (ACLU, Florida).

Hoover: Gondolom, azért a Visionicsnak is megvolt a saját verziója az esettel kapcsolatban.

Vízi Patkány: Meg hát. Arra hivatkoztak, hogy a rendszert nem megfelelően használták, miközben a fényviszonyok sem voltak megfelelőek. Meg arra, hogy Dallas-Fort Worth és a Boston Logan repülőtéren az esetek több mint 90 százalékában sikeresen azonosították a kamerák a „keresett" személyeket (kár, hogy ezek az adatok a vita idején nem voltak hozzáférhetőek, és bemondásra kellett volna elhinni őket). Konkrétan egyébként arról volt szó, hogy a Palm Beach International Airport-on egy hónapon keresztül figyelték, hogy a FaceIt a 250 alkalmazott közül hányszor képes, illetve nem képes kiszűrni a 15 kiválasztottat.

Hoover: És?

Vízi Patkány: 958 esetből a rendszer csupán 455-ször... nem éppen száz százalékos hatékonyság.

Az ACLU szerint egyébként gyakorlatilag életszerű körülmények között végezték a tesztelést, tehát életszerűnek tekinthetőek a felmerülő gondok is: az, hogy az adatbázisban tárolt fényképek nem voltak eléggé jó minőségűek; hogy a fej mozgatása; a nem közvetlen megvilágítás; a napszemüveg mellett a hagyományos okuláré; sőt, egy 10 dolláros baseball sapka is elég volt a biztonsági rendszer kijátszásához.

De az egészben az a legérdekesebb, hogy bár a tények makacs dolgok, az emberek még makacsabbak: Katie Hughes, a tampai rendőrség szóvivője - immár ezen adatok ismeretében - azt nyilatkozta, hogy „a rendszer elrettentő hatással lesz a bűnözőkre... még mindig meg vagyunk győződve arról, hogy a bűnüldözés szempontjából nagyon fontos" az arcfelismerő kamerák alkalmazása.

Persze akadtak azért olyan repülőterek is, melyek egy idő múlva szép csendben megváltak tőlük.

Hoover: És olyanok is akadtak, amelyek nem. Egy ausztrál újság éppen 2003. januárjának elején számolt be arról, hogy a jövőben a Sydney-i repülőtéren számítógéppel összekapcsolt kamerák fognak minden érkezőt lefilmezni, hogy kiszűrjék a potenciális terroristákat meg az egyéb nem kívánatos elemeket.

Vízi Patkány: Elég baj az, ugyanis a dolognak hosszú távon nagyon is súlyos következményei lehetnek - méghozzá olyanok, amiket senki nem akart.

Először is: ha egyszer anélkül terjednek el a biometrikus azonosító rendszerek, hogy megfelelő privacyvédelem lenne beléjük építve, akkor utólag nehéz, ha ugyan nem gyakorlatilag lehetetlen lesz azzal is ellátni őket.

Másodszor: semmit sem ér az egész, ha nincs mögötte egy részletesen kidolgozott veszély-modell, vagyis ha nem tudjuk pontosan, hogy milyen feladatokra és milyen emberek kiszűrésére szánjuk. Meg ha nem tudjuk azt is, hogy azoknak a kiszűrendő embereknek mik a motivációi.

És persze azt is vegyük figyelembe, hogy miközben a rendszeren kívülről származik az információ, hogy kit kell elkapni (és ha rosszul adjuk meg a célpontot, akkor semmire sem jutunk), aközben az azonosítás legfeljebb annyira lesz megbízható, mint a kiindulási információ. Értsd: egy terrorista egy hamis útlevél birtokában pillanatok alatt képes lesz egy immár biometrikus azonosítóval is ellátott, hamis hitelkártyára szert tenni.

És akkor arról még nem is beszéltem, hogy a biometrikus azonosító szisztémák hajlamosak stréber módon túlteljesíteni a feladatukat: ahhoz, hogy megállapítsuk, hogy valaki elmúlt-e 18 éves, és jogosult-e megvenni egy pornóterméket, nem feltétlenül kell a nevét rögzíteni - és még ennyire sem kell létrehozni róla egy számítógépes profilt.

Ugyanekkor lehetetlen előre megmondani, hogy valójában mennyire megbízható egy biometrikus rendszer, mivel a gyártóktól származó információk rendszerint nem tekinthetőek... khmmm... teljesen megbízhatónak. Aki ugyanis egy minden eddiginél szenzációsabb arcfelismerő kamerával akar előrukkolni, az biztosan nem fogja azzal untatni a potenciális vásárlókat, hogy részletesen elmagyarázza, hogy két irányba lehet tévedni. Megtörténhet, hogy valakit hibásan azonosítunk valaki mással (és ha az a valaki más egy terrorista, akkor az érintettnek felettébb kínos a dolog); és az is elképzelhető, hogy nem sikerül kiszűrnünk a keresett személyt (ami szintén hiba persze, de nem azonos az előzővel). A gyártók általában ahelyett, hogy megmondanák, hogy melyik hibatípusról beszélnek, egyszerűen azt választják, ahol jobbak az eredményeik.

És még egy megjegyzés. Azt se feledjük, hogy a hiba itt sokkal nagyobb kockázatot jelent, mint a hagyományos megoldásoknál. Ha valaki elveszíti a hitelkártyáját, hát istenem, kellemetlennek éppen kellemetlen, de azért tud újat szerezni - ha viszont a biometrikus rendszer téved, akkor a személyazonossága kérdőjeleződik meg.

Hoover: Csak semmi pánik, Vízi Patkány! Vannak más, hasonlóképpen ígéretes megoldások is. A New Hawen-i (Connecticut) Acme Rent-A-Car 2001-ben akkor került az érdeklődés középpontjába, amikor kiderült, hogy az AirIQ OnBoard nevű technológiával, GPS-t használva nyomon követi a felhasználóit, és alkalmanként 150 dollárra megbírságolja őket, ha a megengedettnél gyorsabban hajtanak. A privacyvédők persze egyből tiltakozni kezdtek, és...

Vízi Patkány: És tökéletesen igazuk volt. Egy autókölcsönzőnek nem az a dolga, hogy a kormány helyett büntetést sózzon a vezetőkre még akkor is, ha azok nem tesznek kárt az autóban.

Hoover: Ennyire ezért nem egyszerű a dolog. Egyfelől a cég a kölcsönzési szerződés tetejére vastag betűvel nyomtatta rá, hogy igenis ellenőrzik a száguldozókat (és akinek nem tetszik, az minek írta alá), másrészt a legtöbben még a kilátásba helyezett retorziók ellenére is örültek az olyan plusz szolgáltatásoknak, mint amilyen például az volt, hogy figyelmeztették őket, ha túlságosan sokáig parkoltak egy helyen.

Vízi Patkány: Várj csak egy pillanatot, Hoover! A lap tetején olvasható, vastag betűs részt sokan úgy értelmezték, hogy egyfelől a kocsi GPS-sel van ellátva, vagyis ha eltévednek, akkor valamiféle számítógépes térkép lesz a segítségükre; másfelől pedig, hogy ha begyűjtenek egy gyorshajtási cédulát, akkor fizetniük kell az autókölcsönzőnek (elvégre az meg az állam felé lesz kénytelen fizetni miattuk).

És ez korántsem olyan lényegtelen probléma, mint amilyennek elsőre esetleg látszik, ugyanis az AirIQ OnBoard az Intelligent Transportation Society of America tagja. Ennek a létrehozását azért támogatta a Kongresszus még 1991-ben, hogy mielőbb egy intelligens közlekedési hálózatot lehessen kiépíteni. Azaz innentől az a kérdés, hogy vajon meg fog-e jelenni egy újabb, privacysértő technológia az új, intelligens megoldással együtt. Mert a lehetőség ugye megvan rá.

Hoover: Meg hát. A Szerző ennek a fejezetnek az elején említette, hogy a pedofilokat akár percről percre is nyomos lehetne követni, ha nagyon akarnánk. Az ötlet még csak nem is új: Kevin Warwick professzor (Reading University, London) már 1998-ban chipet ültetett magába. Egyébként évek óta alkalmaznak hasonló megoldásokat a háziállatok folyamatos szemmel tartására is.

Vagy ott van például a VeriChip: ezt a Palm Beach-i (Florida) Applied Digital Solutions (ADS) fejlesztette ki; jelenleg hat sornyi szöveget tud tárolni és ezt megfelelő szkennerrel mintegy 1 m távolságból lehet elolvasni. Tökéletesen alkalmas lenne akár arra, hogy a betegek egy rizsszem méretű kapszulában, a bőrük alá ültetve hordják magukkal a kórtörténetüket; akár pedig arra, hogy miután a VeriChipet a megfelelő GPS-technikával kombináltuk, a bűnözőknek szépen beinjekciózzuk a bőre alá, és utána bármikor rájuk bukkanhassunk. Vagy például beültethetnénk a gyerekeknek (hogy ha gyerekrablásra kerül sor, akkor könnyebben megtaláljuk őket); vagy beültethetnénk az Amerikai Egyesült Államokba érkező külföldi diákokba is, hogy mindig tudni lehessen, éppen merre járnak; vagy az Alzheimer-kórosoknak vagy az idős kori szenilitásban szenvedőknek; vagy akár mindenkinek, hogy például a repülőszerencsétlenségben összeroncsolódott holttesteket is egyszerűbb legyen azonosítani... stb. A lehetőségek szinte korlátlanok.

Vízi Patkány: Hát... nem is tudom, hogy valami ostoba technohorrorra vagy inkább egy rémálomra emlékeztet-e ez az egész, de mindenképpen eléggé katasztrofálisnak tűnik.

Hoover: Egyáltalán nem vagy egyedül az ilyen világvége-hangulatú megjegyzéseiddel, Vízi Patkány. Gary Wohlscheid, a The Last Day Ministries nevű vallási csoportosulás vezetője például arról van meggyőződve, hogy a kb. 200 dolláros VeriChip nem más, mint a Fenevad Jele, mert bár egyelőre nem elég kicsi hozzá, hogy a jobb kar mellett a homlokbőrbe is beinjekciózzák, legfeljebb 3-4 éven belül ennek sem lesz akadálya. És akkor „az emberek használni akarják majd. És azoknak, akik visszautasítják, meg kell halniuk", úgyhogy Wohlscheid még egy weblapot is létrehozott, hogy felhívja a figyelmet a veszélyre. Elvégre a Jelenések Könyve 13:16-ban az olvasható, hogy „elrendelte, hogy mindenkinek, kicsinek és nagynak, gazdagnak és szegénynek, szabadnak és rabszolgának jelöljék meg a jobb karját vagy a homlokát, és hogy senki ne adhasson-vehessen, ha nem viseli a vadállat jelét: nevét és nevének számát."

De az ADS azért pillanatokon belül kétezer e-mailt kapott amerikai gyerekektől, amikor bejelentette, hogy önkéntest keres. Pedig ők még csak igazán elsők sem lehettek: a cég orvosi fejlesztésekért felelős vezetője, Richard Seelig sürgősen beültetett magának két VeriChipet, amikor arról értesült a televízióból, hogy a World Trade Center mentési munkálataiban részt vevők a

bőrükre írják fel - biztos ami biztos alapon - a nevüket és a társadalombiztosítási számukat.

Chris Hables Gray pedig, a társadalomtudományok és a technológia professzora (University of Great Falls, Montana) nagyjából ugyanekkor arról beszélt, hogy ez mekkora előrelépést jelent az emberiség számára, hiszen a jövőben nem kell majd mindenhová magunkkal cipelnünk a személyi irataink is.

Vízi Patkány: Gondolom, most jön a Boca Raton-i Jacobs-családról szóló diadaljelentés: Jeffrey Jacobs, Leslie Jacobs és gyerekük, Derek Jacobs. A leírások szerint „tipikusan amerikaiak" és kellőképpen vonzónak találták ezt a lehetőséget, hogy némi hírnévért bevállalják az alig egy percig tartó, helyi érzéstelenítéssel végrehajtott műtétet, amit az ABC Good Morning America című televíziós showja élőben közvetített. Lesile Jacobs még az ilyenkor szokásos ideológiával is előállt: „Nincs mit titkolnom, miért is zavarna tehát, ha egy azonosításra alkalmas chip van a testemben? Most is van ID cardom, tehát miért lenne kifogásom egy chip ellen?"

Illetve azt is hozzátette, hogy „senki nem kényszerít minket a chip használatára. Az adatbázis kizárólag azokat az információkat tartalmazza, amiket mi akarunk, és bármikor hozzáférhetünk a tárolt információkhoz."

Marc Rotenberg (EPIC) viszont azt kérdezte, hogy „Ki fogja eldönteni, hogy kibe legyen beültetve egy ilyen chip? A szülők úgy döntenek majd, hogy a gyereknek szüksége van erre - vagy éppen úgy döntenek, hogy az idős nagyszülőknek ültessenek be...."

Szerintem nem különösebben nehéz kitalálni, hogy mi lesz a fejlődés iránya: Richard Sullivan, az ADS vezetője egy korábbi interjúban már felvetette, hogy alkalmasint minden, az Amerikai Egyesült Államokba látogató idegent ilyen nyomkövető chippel kellene ellátni (a cég később persze igyekezett elbagatellizálni a kijelentést, mert ez már egy átlagos amerikainak is durván hangzott).

Hoover: Mondtam már, hogy nem kell ilyen súlyosan felfogni a dolgot, Vízi Patkány. A VeriChip most beültetett verziója csupán Jacobs-ék telefonszámát, valamint néhány, korábbi orvosi kezeléseikre vonatkozó információkat tartalmazott, és külön kézi számítógép kellett a kiolvasásukhoz. Richard Smith privacyszakértő persze rögtön azt kezdte hangoztatni, hogy ez az egész csupán „szenzációhajhászás és semmi több. Ma még semmi értelme, hogy valaki be legyen chipezve, hiszen a kórházak és a rendőrségek nem rendelkeznek megfelelő leolvasóval."

Meg aztán a történet itt nem is ért véget, ugyanis egyszerre csak közbelépett a Food and Drug Administration (FDA) - ugyanis Keith Bolton (ADS) egy bemutató során elhúzta a speciálisan erre a célra kialakított szkennert Leslie Jacobs implantátuma felett, és a kijelzőn a beteg neve és telefonszáma mellett bizonyos, szívelégtelenségekre vonatkozó információk is megjelentek. Ez olyan információ - mondta Bolton roppant elégedetten -, ami hasznos lehet az orvosok számára „ha az asszony nem tud beszélni, és így megmentheti az életét". A 14 éves Derek Jacobs esetében pedig gyógyszerérzékenységre vonatkozó adatokat olvasott le a szkenner - vagyis az illetékeseknek erősen úgy tűnhetett, hogy a VeriChip egészségügyi életmentő berendezésnek tekintendő, és így az FDA engedélye kell a forgalmazásához. És bár az ADS azt hajtogatja, hogy egyelőre nem tervezi, hogy piacra dobná, az FDA hasonlóképpen konokul kitart amellett, hogy ezt az ő jóváhagyása nélkül úgysem lehetne megtenni. Ki tudja, hogy meddig fog elhúzódni a vita.

Még szerencse, hogy ennek ellenére vannak jól bevált módszereink a rossz fiúk elkapására. A DNS-azonosítás például...

Vízi Patkány: Várjál csak, Hoover! Te a DNS-azonosításról, mint jól bevált módszerről beszélsz?

Hoover: Feltétlenül. Mivel a DNS meglehetősen stabil és az ember halála után még évekig, sőt, esetleg évszázadokig nem esik szét, az amerikai hadsereg már létre is hozott egy DNS-adatbázist, amiben minden egyes amerikai katona DNS-mintája megtalálható. A jövőben egyszerűen el fog tűnni a köznyelvből az „ismeretlen amerikai katona" fogalma. Ha csak egy körömfeketényi darab megmarad belőle, akkor is azonosítani lehet.

Vízi Patkány: Vagy csak azt hiszik. A statisztikák szerint az Amerikai Egyesült Államokban

minden 83,4. szülés ikerszülés és az ikrek 28,2 százaléka egypetéjű iker. Vagyis 1,000 gyerekből mintegy 3 esetében (a populáció 0,338 százalékában) ez a helyzet, és ha nekilátnánk egy nemzeti DNS-adatbázis kiépítésének, akkor pillanatokon belül milliónyi genetikai doppelgänger bukkanna fel.

Magáról a módszerről egyébként annyit érdemes tudni, hogy mivel az emberek génkészlete kb. 99 százalékban azonos, ezért az azonosításhoz csak az eltérést tartalmazó részeket, az úgynevezett „szemét-DNS-t" lehet felhasználni (azért „szemét", mert nem vesz részt a szervezet kialakításában és működtetésében, tehát bizonyos értelemben felesleges - és nyugodtan mutálhat erre-arra, semmilyen következménnyel nem jár).

És most következik a logikai bukfenc: ha a két minta nem egyezik, akkor nyilvánvalóan két különböző személyről van szó - és ekkor megnyugodhatunk. Ha viszont egyezik...

Hoover: Akkor mind a két minta ugyanattól a személytől származik. Vagy esetleg egypetéjű ikrek.

Vízi Patkány: Vagy pedig véletlen egybeesésről van szó - és ezt a lehetőséget valójában soha nem lehet kizárni.

Bár a laboratóriumok általában négy-öt teszt eredményeit kombinálják, hogy minél inkább biztosra mehessenek, dr. David Bing, a Human Identification Trade Association volt igazgatója egy alkalommal azért csak megjegyezte, hogy „A DNS-teszt nem ujjlenyomat-vizsgálat", és soha nem lesz olyan megbízható. Nagy-Britanniában például 1995 óta több mint 100,000 esetben sikerült kapcsolatot kimutatni a rendőrségi DNS-adatbázisban szereplők és bűnelkövetők között (más kérdés, hogy a lefülelt tettesek az esetek közel 90 százalékában koldusok, autótolvajok és kisstílű bűnözők voltak), és hetente átlagosan 800 további esetet derítenek fel a DNS-ujjlenyomat alapján.

Ám olykor azért porszem kerül a gépezetbe: 2001. áprilisában az építész Raymond Easton azért perelte be a manchesteri rendőrséget, mert az betöréssel vádolta, miközben ő - lévén Parkinson-kóros - a lakását is alig tudta a saját erejéből elhagyni. De azért órákon keresztül faggatták (noha még alibije is volt), és amikor DNS-mintát vettek tőle, akkor az bizony egyezett a helyszínen találttal.

Hoover: Vagyis mégiscsak ő volt a betörő.

Vízi Patkány: Dehogy. Egy ilyen eset 1 a 37 millióhoz valószínűséggel fordul elő, és Eastonnak nem volt szerencséje. Azóta tökéletesítették is az ellenőrzést, és jelenleg a becslések szerint 1 az egymilliárdhoz a valószínűsége a véletlen egybeesésnek (feltéve, hogy az egypetéjű ikreket leszámítjuk).

Hoover: Nos, akkor mégis minden rendben van. Amúgy pedig meglehetősen félrevezető Eastont emlegetni, hiszen ez az eset éppen azért lett olyan híres, mert az ilyesmi ritka, mint a fehér holló.

Vízi Patkány: Ennyire azért - sajnos - nem jó a helyzet. Ian Shaw, a kriminológia professzora (University of Lancashire) egyenesen azt állítja, hogy „soha nem fogjuk megtudni, hogy hányan kerültek ártatlanul börtönbe a DNS-teszt miatt".

Hoover: Kissé már megint egyoldalú vagy, Vízi Patkány. A DNS-tesztet 1986-ban alkalmazták először az Amerikai Egyesült Államokban, és 10 év múlva a National Institute of Justice arról számolt be, hogy 28 esetben engedtek szabadon embereket, amikor a DNS-teszt bebizonyította, hogy ártatlanul kerültek rács mögé (és töltöttek ott átlagosan 7 évet).

Vízi Patkány: Igen, ez is igaz... De kanyarodjunk csak vissza egy pillanatra a Védelmi Minisztérium DNS-adatbázisához. Itt a vérből, illetve a száj sejtjeiből származó mintát persze nagyon gondosan tárolják, és így tulajdonképpen a világ legnagyobb genetikai adatbázisát hozzák létre, ahol minden egyes elemhez részletes leírást is csatolnak.

Úgyhogy ez az óriási mennyiségű genetikai információ várhatóan túlságosan is csábító célpont

lesz a tudományos kutatók számára; sőt, akár a genetikai nyomozásokhoz is, és ez nagyon érdekes problémához vezet.

Mármint ahhoz, hogy pusztán a felhalmozásnak köszönhetően a jövőben olyan célokra is fel lehet majd használni ezeket ez adatokat, amire a rendszer létrehozói nem is gondoltak.

Szerző: Mint például Izland esetében is történt?

Vízi Patkány: Igen, ez kiváló példa erre. Izland ideális hely a genetikai vizsgálatokra, mivel mindössze 1,100 évvel ezelőtt települt be, és a mai 280,000 lakos túlnyomó része ugyanannak a kis, 20,000 fős csoportnak a leszármazottja. Tehát ha ismerjük a rokonsági kapcsolatokat (mint ahogy a valaha is élt izlandiak háromnegyedénél ismerjük); és ha rendelkezésünkre állnak a megfelelő orvosi adatok (mint ahogy lényegében ez a helyzet), akkor álmodni sem lehet jobb helyet a genetikai eredetű betegségek vizsgálatához.

Úgyhogy ezen a ponton fel is tűnik a Dr. Kari Stefansson által vezetett DeCode, ami - miután a világ legrégebben működő parlamentje, az izlandi 1998-ban elfogadta az Egészségügyi Szektor Adatbázis Törvényt - 2000. januárjában nemes egyszerűséggel megvásárolta az állampolgárok összes egészségügyi és genetikai adatának 12 éven keresztül való felhasználásának jogát.

Hoover: Ezzel meg mi a bajod? Csak a betegségek okaira akarnak rábukkanni. És különben is: akinek nem tetszik, az élhet az opt-out jogával.

Vízi Patkány: Hogy mi bajom van vele? A genetikai információ a genealógiaival kombinálva... nos, ez már eléggé húzósan hangzik. Ugyanis valahogy senki nem akarja, hogy tudni lehessen róla, hogy például milyen betegségre hajlamos.

Dr. George Annas, az orvosi etika professzora (Boston University, Schools of Law, Medicine and Public Health) a kezdetektől úgy gondolta, hogy a DeCode-nak minden izlandi állampolgártól beleegyezést kellene kérnie, mielőtt az információikat bekebelezi (vagyis opt-out helyett opt-in-re lenne szükség), és az embereknek joguk kellene, hogy legyen ahhoz is, hogy bármikor bármelyik adatukat töröltethessék a nyilvántartásból. Ezzel az állásponttal egyébként mind az EU adatvédelmi biztosa, mind a World Medical Association egyetértett.

Dr. Russ B. Altman, az International Society of Computational Biology elnöke szintén a DeCode-dal kapcsolatban azt mondta, hogy kisebb léptékben ugyan, de ugyanez az eset máshol is megismétlődhet: egyes, többé-kevésbé gátlástalan cégek bármikor szerződésre léphetnek egyes nagy, többé-kevésbé gátlástalan egészségügyi adatkezelőkkel. Márpedig „a kutatások ezen fajtájánál az etikai kérdések a legalapvetőbbek”, ugyebár.

És persze bármikor vissza is lehet élni a genetikai adatokkal: az USA-ban annyira félnek ettől, hogy amikor Clinton megivott egy sört valamelyik angol kocsmában, akkor már jött is a biztonsági szolgálat embere, és szépen celofánba csomagolta a korsót - nehogy valaki hozzáférhessen az elnök génmintájához, és ez alapján megállapítsa mondjuk azt, hogy hajlamos valamilyen betegségre (vagy hogy esetleg nem az apja fia). Ami kissé általánosabban fogalmazva ahhoz a problémához vezet el, hogy ha például a biztosítók (munkaadók) el tudnák érni, hogy az ember legyen köteles megfelelő vizsgálatokat elvégeztetni magán, mielőtt biztosítást köt (illetve mielőtt munkába áll), akkor az alapján, hogy a génjei mire hajlamosítják, igencsak durva diszkriminációra kerülhetne sor.

Hoover: De hiszen ezzel az erővel akár amiatt is tiltakozhatnánk, hogy most is genetikai alapú diszkrimináció folyik, amikor a színvakokat nem engedik hivatásos sofőrnek vagy a vérzékenyeket hentesnek menni!

Vízi Patkány: Ez azért túlzott egyszerűsítés, és ezzel szerintem te is tisztában vagy. Míg a fentebbi természetes, addig nem hinném, hogy ne tekintené mindenki súlyos genetikai diszkriminációnak, ha egy munkaadó nem állna szóba azokkal, akiket a génjeik magas vérnyomásra hajlamosítanak, és ezért számítani lehet rá, hogy az átlagosnál többet fognak betegeskedni.

Az emberi génkészlet feltérképezésére vállalkozó Humán Genom Program munkacsoportja már 1996-ban amellett érvelt, hogy a cég kizárólag akkor vehesse figyelembe a genetikai információkat,

ha azok közvetlenül kapcsolódnak a munka természetéhez.

Szerző: Tehát?

Vízi Patkány: Tehát a magas vérnyomás mindenütt hátrányt jelent – az viszont, hogy valakinek tériszonya van-e, csak akkor számít, ha mondjuk toronydaru-kezelőnek akar menni.

Hoover: Badarság: semmi okunk a „genetikai diszkriminációtól" félni. Ilyesmi legfeljebb a túlzásokra hajló újságírók képzeletében fordulhat elő. Legalábbis egyelőre csak ott.

Szerző: Gondolod? Venetianer Pál molekuláris biológus jegyzi meg, hogy valószínűleg egyikünk „sem tekintené kívánatos jövőképnek", ha elballagnánk leánykérőbe, és ott a családfő azzal fogadna minket, hogy „sajnálom fiatalember, a maga... genetikai teszteredményén az áll, hogy az apoliproteinE4 allélre nézve homozigóta. Ez azt jelenti, hogy az átlagnál sokkal nagyobb valószínűséggel lesz Altzheimer-kóros idősebb korára. Én nem ilyen férjet kívánok a lányomnak."

Venetianer azt is hozzáteszi: „egyáltalán nem a távoli jövő képe. Az apoliproteinE4 gént kimutató egyszerű és olcsó teszt ma is rendelkezésre áll." Azaz a technológia máris megvan, és ha nem társul hozzá megfelelő szabályozás, akkor magunkra vethetünk.

A Gattaca című tudományos-fantasztikus film (ami egy genetikai kasztokon alapuló, tökéletesen orwelliánus társadalmat ábrázol) záró képsoraiban eredetileg Albert Einstein Nobel-díjas fizikust, John F. Kennedy amerikai elnököt, Ray Charles popsztárt és Jackey Joner-Kersee olimpiai bajnok futónőt mutatták volna, miközben a kellemes narrátorhang arra hívja fel a figyelmünket, hogy ha annak idején már létezett volna a genetikai betegségekre való születés előtti szűrés és emiatt lehetőség lett volna abortuszra, akkor ezek az emberek soha nem látják meg a napvilágot... Meg persze könnyen lehet, hogy Te sem, kedves néző (meg Te sem, kedves olvasó).

Szerintem kár volt ezeket a záró képsorokat végül kihagyni a Gattacá-ból.

Vízi Patkány: Szerintem is. De azért azt se tévesszük szem elől, hogy a túlzott beavatkozás-ellenesség is káros lehet. Szerencsére vannak pozitív példáink is: Cipruson Makariosz érsek uralma alatt házasság előtti kötelező genetikai tanácsadást vezettek be, és itt azt ajánlották a pároknak, hogy vizsgáltassák meg, hogy nem hajlamosak-e örökletesen a vérszegénység egy súlyos formájára, a thalasszémiára - mert ha igen, akkor a gyerekük 25 százalékos valószínűséggel ezzel fog születni. Az eredmény: a thalasszémia nagymértékben visszaszorult (ami nyilvánvalóan a köz javára vált), és eközben az egyén jogai sem igazán csorbultak. Elvégre csak a tanácsadás volt kötelező, de a genetikai teszt már nem - és nem tiltották be a betegséghordozók házasságát sem (egy részük azonban önként tartózkodott a gyereknemzéstől, illetve inkább az abortuszt választotta).

De persze egyből megváltozott volna a helyzet, ha elkezdik rögzíteni, hogy ki hordozza magában a betegség génjeit és ki nem; majd pedig mindenkiről összeállítanak egy DNS-profilt.

Hoover: Érdekes. Pedig ha jól emlékszem, akkor Sir Alec Jeffreys professzor, a DNS-ujjlenyomat felfedezője mintha éppen egy totális brit adatbázis létrehozását javasolta volna.

Vízi Patkány: Valószínűleg dühében és elkeseredésében - és mivel arra a következtetésre jutott, hogy a jelenlegi helyzethez képest még az is igazságosabb lenne, ha mindenkit egyformán nyilvántartanának.

Szerző: De miért?

Vízi Patkány: Nagyon egyszerű: a rendőrségi adatbázisba való bekerülés jelenleg tökéletesen egyirányú folyamat. Viszont „Ha mindannyian benne vagyunk, akkor mindannyian közös csónakban evezünk - és megszűnik a jelenlegi diszkrimináció", mondja Jeffreys.

A szigetországban 2002. második felében több mint 1,5 millió DNS-profilt tároltak, és egyes privacyvédő csoportok szerint az unatkozó rendőrségi szakértők betegségekre utaló jelek után kutatgattak azoknál is, akik nem egyértelműen gyanúsítottak. Eközben heti 1,600 DNS-alapú

azonosítás történt és a jelenlegi tervek szerint 2004. áprilisáig 3 millióra akarják növelni az adatbázis elemeinek számát. Az egészet felügyelő Dr. Bob Bramley pedig elégedetten állapítja meg, hogy „egyre több és több személy adatai kerülnek be a Nemzeti DNS Adatbázisba, és ennek megfelelően az információk értéke is egyre nagyobb lesz... A rendőrség úgy véli, hogy ez a bűnözés elleni leghatékonyabb eszköz."

Hasonló ötletekkel egyébként egyes amerikaiak is előálltak. Michael E. Smith jogászprofesszor (University of Wisconsin), aki korábban az ország „DNS jövőjével" foglalkozó bizottság vezetője volt, például úgy gondolja, hogy egy mindenkire nézve kötelező nemzeti DNS-adatbázissal lehetne elejét lehetne venni a rasszista és diszkriminatív DNS-mintavételi eljárásoknak (amikor például sokkal nagyobb arányban vagy éppen kizárólag afro-amerikaiakat vizsgálnak); illetve annak, amikor a nyomozó hatóságok - az orvosi privacyre vonatkozó szabályokat megsértve - a kórházaktól és az orvosi laboratóriumoktól próbálnak mintát szerezni.

Hoover: Ráadásul így gyorsabban és biztosabban lehetne lecsapni a bűnözőkre is, mint most, amikor csak a gyilkosságért, nemi erőszakért és erőszakos bűncselekményekért meg hason- lókért elítéltek DNS-mintája áll a hatóságok rendelkezésére.

Vízi Patkány: Szóval a kisebb léptékű privacysértéseket orvosoljuk nagyobbak elkövetésével? Ráadásul a DNS-mintáknak a begyűjtése időnként már így is több mint vitatható alapokon történik: egy-egy nagy port felverő gyilkosságnál a rendőrség szinte mindig hajlandó egy időre sutba dobni a FIPS-et, és korlátlan DNS-gyűjtésbe kezdeni. Hátha egyszer majd rábukkannak ez elkövetőére is... Tiszta Gattaca.

Hoover: Én inkább úgy fogalmaznék, hogy mindent megtesznek azért, hogy a bűnös mielőbb rács mögé kerüljön. Először 1987-ben, az angliai Leicestershire-ben fordult elő, hogy egy bűncselekményt követően nem csupán a gyanúsítottaktól, de a környéken élő 4000 ember mindegyikétől DNS-mintát vettek; Németországban 1998-ban pedig már 16400 ember DNS-ét vizsgálták meg, mielőtt rábukkantak volna a gyilkosra.

Ami az Amerikai Egyesült Államokat illeti, itt eddig lényegesen kisebb léptékben alkalmaztak korlátozások nélküli DNS-gyűjtést.

Vízi Patkány: Kisebb léptékben, kevesebb sikerrel és jóval több vitával. Az 1990-es évek közepén a Metro-Dade Police Miami külvárosaiban több mint 2000 mintát szedett össze - de a hat prostituált gyilkosát végül a szomszédja feljelentése alapján tartóztatták le. 1998-ban Prince George County rendőrsége (Madison) 400 férfitól vett DNS-mintát, ám a gyilkos soha nem került elő... meglehetősen nagy is volt a felháborodás.

Hoover: Pedig senkinek nem volt rá oka. A megye rendőrfőnöke, John Farrell a USA Today lapjain az eljárást ahhoz hasonlította, mint amikor egy betörés helyszínén mindenki ujjlenyomatait begyűjtik, és ez ellen érdekes módon nem szokás tiltakozni.

Vízi Patkány: Azért közelről sem ugyanarról van szó, Hoover! James Alan Fox, a Northeastern University bűnügyi professzora szerint egy ujjlenyomat bárkihez tartozhat, de egy megerőszakolt és megölt nő hüvelyében talált sperma majdnem biztosan a gyilkostól származik - vagyis ebben az esetben a DNS jóval szenzitívebb adat.

És van még valami, ami a kiterjedt DNS-gyűjtés ellen szól: az, hogy a módszer rendszerint jobban beválik, ha az azonosítást csak a lehetséges elkövetők körének leszűkítése után alkalmazzák. Így találtak meg például Lawrence-ben (Massachusetts) 1999-ben egy gyilkost, miután „alig" 32 férfitól vettek vért.

Hoover: Rendben, akkor szűkítsük le a gyanúsítottak körét, mielőtt mintavételbe kezdünk. Akkor elégedett leszel végre?

Vízi Patkány: A dolog szerintem még így is ellentmondásos lesz. Túl azon, hogy a DNS-azonosítás

eddigi limitált sikere technikai szinten is megkérdőjelezheti a dolgot; illetve túl azon, hogy ezáltal a kormány birtokába kerül olyan emberek DNS-mintázata, akik még csak nem is gyanúsították, az sem közömbös, hogy sérül az állampolgároknak a Negyedik Kiegészítés által az „indokolatlan házkutatások és foglalások" elleni védelmet biztosító kitétele is.

Hoover: Vízi Patkány, kezdesz komolyan felidegesíteni! Mondd csak, tulajdonképpen kinek az oldalán állsz? A kormányén vagy a potenciális bűnözőkén?

Vízi Patkány: Gondoljál csak bele, hogy a nagyarányú DNS-gyűjtések során nem igazán sok minden szól amellett, hogy gyanúsítottként kellene kezelnünk azokat, akiktől a minta származik - ekkor viszont nincs is jogunk mintát venni tőlük... Másfelől pedig egy anonim mondás szerint „az Alkotmány közelről sem tökéletes ugyan, de még mindig mérhetetlenül jobb, mint az, ami alapján ma cselekszik az állam." Vagyis rossz ugyan a kérdésed, de én azért egész jó választ tudtam rá adni.

Első Magyar Jogi Portál
és online Ügyvédi Szaknévsor

JOGI FÓRUM

jogi hírek

interjúk

publikációk

vitafórum

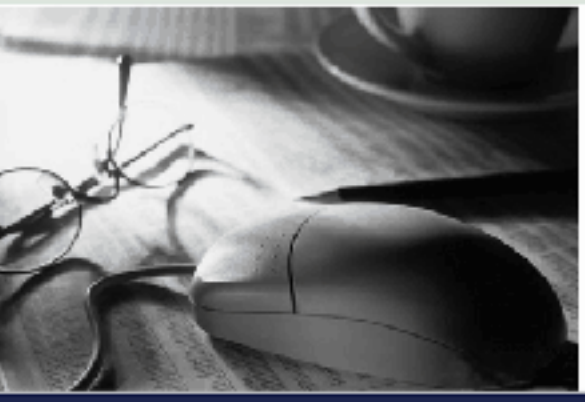
szaknévsor

jogi szakkönyv-katalógus

jogi állásbörze

szakmai rendezvények

heti hírlevél



országos ügyvédi szaknévsor

magyar, angol és német nyelven

ügyfél keres ügyvédet szolgáltatás

www.jogiforum.hu