Dr. Galántai Zoltán

E-privacy olvasókönyv

Dialógusok a privacyről és az internetről – meg a cyberpornóról, a megfigyelésekről és egyebekről

TARTALOM

„A telekép egyszerre volt vevő- és adókészülék. Akármilyen hangot idézett elő Winston – az egészen halk suttogáson kívül –, a készülék felvette. Sőt: ameddig a fémlap látómezején belül tartózkodott, nemcsak hallhatták, hanem láthatták is. Azt persze nem lehetett tudni, hogy egy adott pillanatban megfigyelik-e az embert. Bizonytalan volt, hogy a Gondolatrendőrség milyen gyakran és milyen rendszer szerint kapcsolódik be egy-egy magán-teleképkészülékbe. Még az is elképzelhető volt, hogy mindenkit állandóan figyelnek. Mindenesetre akkor kapcsolódhattak be akárkinek a készülékébe, amikor csak akartak. Az embernek abban a tudatban kellett élnie – s abban a tudatban is élt, ösztönné vált megszokásból –, hogy minden hangját hallják, s kivéve, ha sötét van, minden mozdulatát figyelik.

Winston továbbra is hátat fordított a teleképnek. Így biztonságosabb volt, bár nagyon jól tudta, hogy még a hát is áruló lehet."

(Orwell: 1984. Szíjgyártó László fordítása)

Bevezetés helyett: adattorony

A floridai Virginia Beach az óceán partján fekszik, és valósággal vonzza a turistákat – a turisták pedig a bűnözőket vonzzák, ezért a város elhatározta, hogy bekamerázza a tengerpartot meg a belvárost. Ehhez olyan arcfelismerő kamerákat akartak használni, amik az arc 80-120 meghatározott pontjának távolságából afféle digitális mintázatot hoznak létre, és ezt hasonlítják össze az adatbázisban tárolt bűnözők arcának digitális mintázatával. Majd pedig szükség esetén riasztják a rendőrséget.

A jogvédők egyáltalán nem értenek egyet az elképzeléssel – a túlnyomó többség azonban igen. „Ez a mi védelmünket szolgálja. Ha nem csinálunk semmi rosszat, akkor nincs miért nyugtalankodnunk”, mondta a 39 éves Bonnie Satterlee pennsylvaniai Johnstownból, amikor az arcfelismerő kamerákról kérdezték, és ez nyugodtan tipikus álláspontnak tekinthető (nem csupán az Amerikai Egyesült Államokban, de például Magyarországon is).

Pedig abból, hogy valakinek nincs titkolnivalója, még nem következik, hogy nem lehet ellene felhasználni a róla gyűjtött adatokat. 1993-ban egy Edwin Black nevű amerikai tudósnak feltűnt, hogy a washingtoni Holokauszt Múzeumban egy IBM Hollerith D-11 típusú lyukkártya-osztályozó berendezés áll közvetlenül a bejárat mellett. A rajta olvasható felirat szerint az IBM szervezte meg azt az 1933-as németországi népszámlálást, „melynek során a nácik a zsidókat azonosították”, írja Black.

A D-11 előtt állandóan annyian csoportosultak, hogy végül ki kellett cserélni egy kisebb gépre, mert valóságos forgalmi dugó alakult ki. De a mintegy 15 millió múzeumlátogatóból egyedül Black-nek jutott eszébe feltenni azt a kérdést, hogy vajon mi köze is van az IBM-nek a második világháborús náci népirtáshoz, és az, amit a következő években sikerült előásnia, több mint megdöbbentő volt. Amennyire tudni lehet, csupán véletlen egybeesés, hogy könyvének, Az IBM és a holokausztnak a megjelenésekor rögtön sor került egy perre is: ezt 2001. február 9-én a washingtoni Cohen, Milstein, Hausfeld & Toll ügyvédi iroda indította a holokauszt öt túlélőjének nevében. Black viszont rögtön arra az álláspontra helyezkedett, hogy jobb lenne, ha a jogászok kimaradnának a dologból (ugyanis, mondta, az IBM-nek a nácikkal való kapcsolata elsősorban nem jogi, hanem morális kérdéseket vet fel). Úgyhogy most számunkra sem annyira az az érdekes, hogy a pert hamarosan meg is szüntették (Michael D. Hausfeld, a felpereseket képviselő ügyvéd szerint azért, mert azok a német cégek, amelyek több milliárd dolláros alapot hoztak létre a túlélők számára, most kijelentették, hogy máskülönben nem fizetnek). Hanem inkább az, hogy ettől kezdve biztosak lehetünk benne, hogy adott esetben egyáltalán nem veszélytelen dolog, ha hagyjuk, hogy bármilyen adatunkhoz hozzáférjenek – még akkor sem, ha ismét csak elvileg rettenetesen törvénytisztelő és becsületes állampolgárok vagyunk.

Black szerint „Tudatosítanunk kell magunkban, hogy miképpen állították össze a maguk feketelistáit a nácik, nehogy egyszer majd mások megint mások ellen állíthassanak össze hasonló listákat”.

Eközben több mint életveszélyes lenne lebecsülni az adatok és az adatgyűjtési technológiák szerepét. Egy Rudolf Cheim nevű holland zsidónak a bergen-belseni koncentrációs táborban az IBM németországi leányvállalata, a Deusche Hollerith Machinen Gesselschaft (röviden: Dehomag) által gyártott Hollerith-kártyákkal dolgozva alkalma nyílt megfigyelni, hogy a hármas és a négyes oszlopban található lyukak azt jelölik, hogy az illetőt miért szállították munkatáborba (a 3-as a homoszexualitást; a 9-es a köztörvényes bűnözőt; a 12-es a zsidót; a 8-as a cigány származást jelölte). A 34-es oszlopban található 3-as lyuk a „természetes”

halált; a 4-es a kivégzést; az 5-ös az öngyilkosságot; a 6-os a „különleges bánásmódot” (gázkamra, tarkólövés), stb. jelentette, és persze minden táborlakóról volt egy lyukkártya az azonosító számával – elvégre így könnyebben lehetett számon tartani őket...

Lyukkártyák segítségével szervezték meg a nácik a vasúti menetrend összehangolását (és minden vasútállomást elláttak lyukkártyarendszerrel), hogy gyorsabban jussanak el a szerelvények a frontra (vagy a koncentrációs táborba). Mindeközben a Dehomag továbbképzéseket tartott a náci tisztek számára, és évi másfél milliárd lyukkártyát állított elő; a lyukkártyát használták fel a zsidók tudományos alaposságú kiéheztetésére; újabb és újabb gépeket adtak bérbe a náci államnak és biztosították hozzá a megfelelő „support”-ot, hogy azok üzemképesek maradjanak.

Persze a Dehomag tette azt is lehetővé, hogy „azonosítsák” a zsidókat, és „magát a ‘faji’ besorolást, tehát a nem vallás, hanem nemzedékekre visszamenő származás szerinti osztályozást is a Dehomag találta ki”. Black meglehetősen keserűen jegyezte meg könyvének németországi bemutatóján, hogy „német hatékonyság és amerikai találékonyság” ötvözete volt mindaz, ami történt, és ez tette lehetővé azt is, hogy az egész társadalomra kiterjesszék a Hollerith-féle módszert: a foglalkozásokat, a betegségeket és a nemzetiségi hovatartozást lyukkártyára vitték fel. Méghozzá nem csak a bűnözők, az ellenállók és az „alacsonyabb rendű fajok”, hanem mindenki esetében... még valamikor az 1930-as években Friedrich Zahn „árja tudós” azon lelkendezett, hogy „a központi statisztikai hivatalok együttműködésével folyamatos megfigyelés alatt tarthatóak a nyilvántartott személyek”, miközben a Dehomag Litcherfelbében 55 (!) vasúti kocsinyi lyukkártyát tárolt 50 százalékos páratartalmon és 21-24 C közötti hőmérsékleten, hogy szükség esetén mindig legyen belőlük utánpótlás.

Heinrich Himmler személyesen kezdeményezte az SS statisztikai évkönyv összeállítását, a Dehomag pedig olyan „klienseket” mondhatott magáénak, mint például a müncheni Katolikus Temetkezési Vállalat meg az eisenachi Egyházi Tanács, és erre kellőképpen büszke is volt. Az egyik plakátjukon egy gyárépület felett óriási lyukkártya volt látható, és a rajta keresztülhaladó fénysugarak bevilágították az épület minden zugát. „A Hollerith átvilágítja az Ön cégét, és ezzel segíti a felügyeletet, valamint a szervezést.” Egy másik plakáton a lyukkártya egy, az égen lebegő, óriási szemből türemkedett ki: „Lássunk mindent a lyukkártya szemével.”

De túlzásról persze szó sincs: a náci Belügyminisztérium még azt is felvetette, hogy nem kellene-e egy 25 emeletes adattornyot építeni, ahol az emeletek 12-12 szobája a hónapoknak; a szobák 28-31 szekrénye pedig, a 70 millió nyilvántartott német születési dátumának felelt volna meg (az újszülöttek adatait a szülők vallásának megjelölésével 1935 óta dolgozták fel lyukkártyán – akárcsak a házasságkötések minden adatát). És így tovább.

Érdemes tehát elgondolkodni rajta, hogy ma milyen megoldások állnak azoknak a rendelkezésére, akik egy totális ellenőrző rendszert akarnak kidolgozni.

Már a náci Németországban kifejlesztettek egy ujjlenyomatszortírozó rendszert (ezt a titkosszolgálat sürgősen ki is sajátította magának), de ez a 21. sz. elejének mércéjével mérve nem lehetett valami hatékony.

A ‘80-as évek közepén az FBI 23 millió bűnöző ujjlenyomatát tartotta nyilván; egyedül Kalifornia állam pedig 7,5 millióét – de egy San Francisco-i nyomozó arra a megállapításra jutott, hogy ha át akarná nézni a náluk tárolt mindössze 330 ezret, és hajlandó lenne heti hét napon keresztül napi nyolc órát ezzel tölteni, akkor 33 év alatt végezne vele. Aztán 1985-ben megjelent az AFIS (Automated Fingerprint Identification System), ami képes volt másodpercenként 5-600 ujjlenyomatot összehasonlítani az adatbázisban találhatóakkal – vagyis egymillióhoz alig fél órára volt szüksége. Az Amerikai Igazságügyi Minisztérium jelentése

szerint amikor először alkalmazták az AFIS-t, akkor a San Francisco-i Rendőrség már nyolc éve és sok ezer munkaórán keresztül kutatott az ujjlenyomat-adatbázisban a második világháborús koncentrációs tábor egy túlélőjének, annak a Miriam Slamovich-nak a meggyilkolása ügyében, akit 1978-ban, a saját otthonában lőttek le. A gyilkos ugyan tökéletesen tiszta ujjlenyomatot hagyott a tett színhelyén, de mivel nem volt gyanúsított vagy egyéb nyom, amin el lehetett volna indulni, nagyon kevés esély volt rá, hogy hagyományos, kézi keresési módszerekkel megtalálják azt az adatbázisban. A rendőrség nyomozói azonban kitartóan foglalkoztak az üggyel, és amikor üzembe helyezték az AFIS-t, az 6 perc alatt kikereste, úgyhogy Slamovich feltételezett gyilkosát még aznap elfogták.

Azóta a számítógépek nagyságrendekkel lettek gyorsabbak, és igazán nem nehéz arra gondolnunk, hogy mivel a technika önmagában semleges (nem pedig jó vagy rossz), ezért szintén fel lehet használni a bűnözők elfogása helyett az állampolgárok megfigyelésére vagy arra is, hogy ugyanolyan embertelenül visszaéljenek az adatokkal, mint ahogyan a nácik tették – csak éppen ma már mérhetetlenül hatékonyabban. A hitleri Németország a bizonyíték rá, hogy a rólunk kezelt adatok roppant veszélyesek lehetnek, és bár jogunkban áll feltételezni, hogy a jövőben nem fordulhat elő semmi ilyesmi (vajon miért is nem?), ez egyáltalán nem látszik biztonságos álláspontnak.

Ugyanúgy nem, mint ahogy az sem lenne jó ötlet, ha egy idegennek a kezébe nyomnánk egy megtöltött pisztolyt, megkérnénk, hogy szorítsa a fejünkhöz, és közben erősen bíznánk benne, hogy a ravaszt viszont nem fogja meghúzni. Ésszerűbb inkább ki sem próbálni a dolgot. Az én álláspontom szerint igenis érdemes mindent megtenni azért, hogy az adatainkhoz ne férhessen hozzá bárki csak úgy.

Ez a könyv arról szól, hogy miért nincs igaza Bonnie Satterleenek a pennsylvaniai Johnstownból, amikor az óceán partján sétálva azt állítja, hogy csak azoknak kell tartaniuk a megfigyelésektől, akik valóban elkövettek valamit.

Szereplők

J. Edgar Hoover:

John Edgar Hoover (1895. január 1. – 1972. május 2.) az FBI igazgatója volt 1924-től egészen halála napjáig.

Az I. Világháború alatt az Igazságügyi Minisztériumnak dolgozott és az Ellenséges Idegenek Regisztrációs Szekciójának (Enemy Aliens Registration Section) vezetője lett, majd 1919-ben a szintén az Igazságügyi Minisztériumon belül újonnan létrehozott Általános Titkosszolgálati Részleg (General Intelligence Division) irányítójává nevezték ki. Itt 1921-re állítólag 450 000 „gyanús" ember adatait tartották nyilván.

Az Espionage Act (1917) és a Sedition Act (1918) alapján akciókat kezdett a baloldali és a radikális mozgalmak ellen. (Az ötlet persze nem tőle származott: az Espionage Act alapján ítélték például 10 év börtönre 1917-ben a baloldali Rose Pastor Stokes-t, mert azt írta egy levélben a Kansas City Starnak, hogy „az a kormány, ami a spekulánsokat szolgálja, nem szolgálja a népet, és én a népért vagyok, míg a kormány a nyerészkedőkért.")

Hoover 1921-től a Bureau of Investigation igazgatóhelyettese, majd 1924-től az igazgatója volt. A szervezetet 1935-ben nevezték át Federal Bureau of Investigation-re, és 1939-től a legnagyobb hatalmú belső elhárítási szervezetté nőtte ki magát.

Hoover a feltételezések szerint valóságos kartotékrendszert vezetett azokról a közéleti szereplőkről és politikusokról, akiket befolyása alá akart vonni, de ezt nem lehet bizonyítani, mert titkárnője, Miss Helen Gandy Hoover halála után főnöke személyes iratainak nagy részét azonnal megsemmisítette.

Az a Hoover, aki ebben a könyvben szerepel, a valóságban természetesen soha nem létezett, és így nem is formálhatott véleményt az alább következő kérdésekről.

Szerző:

Név: Galántai Zoltán

Születési hely és idő: 1964. augusztus 12., Dunaújváros

Állampolgárság: magyar

Lakhely: Gödöllő

Legmagasabb végzettség: Ph.D. (multidiszciplináris műszaki tudományok, informatikai és filozófiai tudományok)

Családi állapot: nős, két gyerek

Szemszín: barna

Hajszín: barna

Vércsoport: Rh+

Testmagasság: 180 cm

Testsúly: 72 kg

Különös ismertetőjegy: nincs

Beosztás: egyetemi docens (BME), a Privacy International nemzetközi vezetőbizottságának a tagja

Éves jövedelem: (törölve)

Érdeklődési kör: elektronikus privacy, szólásszabadság

Egyéb tevékenység: a Privacy Hírlevél főszerkesztője

Káros szenvedélyek: (törölve)

Politikai beállítottság: (törölve)

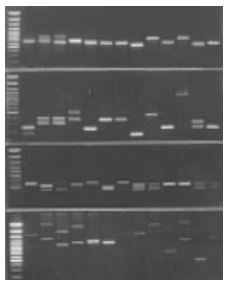
Vallás: (törölve)

Szexuális szokások: (törölve)

Web site: http://www.nagytestverdij.hu

e-mail cím: zoltan.galantai@bigbrotherawards.org

Ujjlenyomat, írisz- és DNS-kód:



Vízi Patkány:

„… igaz, hűséges barát, házias, életvidám, segítőkész, jólelkű, szolid, nagylelkű, önfeláldozó, nagy képzelőerejű költő”.

(*Kenneth Grahame:*

Békavári uraság és barátai)

Amúgy pedig lelkes privacyvédő és a legtöbb (bár korántsem az összes) esetben a Szerző szócsöve.

Ugyan kit érdekel a privacy? (és egyáltalán: mi is az)

A Szerző meséje: A privacy és a csillagok

Mark Twain szerint „Ha nem tetszik New York időjárása, akkor várjál egy órát”, és akkor biztosan tetszeni fog, ugyanis a világ talán egyetlen nagyvárosában sem követi egymást ilyen szeszélyesen és kiszámíthatatlanul az eső, a köd és a napsütés. Vagyis – amennyiben a fényszennyezéstől eltekintünk is – a „Big Apple” nem éppen ideális hely az amatőr csillagászok számára.

Ehhez képest Darin Stephens, a Bushnell optikai cég termékmenedzsere szerint itt több távcsövet adnak el, mint az ország bármelyik más részén – és ezeket persze nem az égitestek megfigyelésére használják. Witold Rybczynski, Az otthon: egy gondolat rövid története című könyv szerzője azt írja, hogy az utóbbi pár ezer évben, a városok kialakulásával együtt létrejött egy olyan hallgatólagos megállapodás is a városlakók között, mely szerint „nem kukkolunk”. De a gyakorlat erre rácáfolni látszik, úgyhogy mára külön „kukkolás elleni” ipar alakult ki, és a New York Window Film például négyzetlábanként 5-6 dollárért kínál olyan fóliákat, amik az egyik irányból átlátszatlanná változtatják az ablakunkat (de a CP Films Vista Soft Horizon fóliája is nagyjából ugyanennyibe kerül).

Vízi Patkány: Kezdjük talán a „privacy” fogalmának meghatározásával. 1890-ben két bostoni jogász, Louis D. Brandeis és Samuel D. Warren vetették fel, hogy mindenkinek joga van a „privacyhoz”, vagyis mindenkit megillet „az „egyedülhagyatás joga” (the right to be let alone). Szerintük azért volt szükséges felhívni a figyelmet a magánélet sérthetetlenségére, mert a legújabb technológiák: a fényképezés, a gyorssajtó, a beszélgetések rögzítésére alkalmas fonográf és a telefon lehetővé tették, hogy bárkinek minden addiginál durvábban és gyorsabban (meg persze hatékonyabban) gázoljanak bele a magánéletébe.

Ami például a fényképezést illeti, az 1850-es évek közepén még tükör sem volt minden amerikai vagy angol háztartásban... és az végképp lehetetlen volt, hogy valakit a tudta és beleegyezése nélkül lefényképezzünk, hiszen valóságos műterem kellett hozzá. Aztán 1888-ban megjelent az Eastman Kodak („Ön megnyomja a gombot, a többi a mi dolgunk”), és egyre többen kezdtek arra panaszkodni, hogy lesből lekapták őket, és ez tökéletesen új problémákat vetett fel, akárcsak 100 évvel később a számítógépek vagy az internet viharos elterjedése, és...

Hoover: Ugyan, kit érdekelnek a legújabb technológiák! Kezdjük talán azzal, hogy nincs is értelme az egésszel foglalkozni. Az amerikai Kongresszus, mint mindig, most is tárgyal mindenféle, az internetes privacy védelmét szolgáló törvényjavaslatokat, a helyzet azonban az, hogy a privacy egy cseppet sem fontos a felhasználóknak... legfeljebb beszélni szeretnek róla.

„A privacy olyan, mint az időjárás: mindenki panaszkodik a privacysértések miatt, de senki nem tesz ellene semmit”, írja a New York Times, és ez tökéletesen igaz. A Jupiter Research egy 2002. júniusi felmérése szerint a felhasználók 70 százaléka állította azt, hogy aggódik internetes privacyjének megsértése miatt, illetve egy másik felmérés szerint az interneten vásárlók fontosnak tartanák, hogy az e-kereskedelmi site-ok – úgynevezett privacy policyn keresztül – közzétegyék, hogy miként kezelik a felhasználók adatait...

Vízi Patkány: Ezek nagyon is figyelemre méltó számok.

Hoover: Azok hát, csak másként, mint ahogyan gondolnád. Ugyanis eközben a Privacy Leadership Initiative egy 2001-es felméréséből viszont az derül ki, hogy az internetezőknek alig 3 százaléka olvassa el figyelmesen a privacy policyt; és 64 százalékuk pedig legfeljebb

egy pillantást vet rájuk – vagy soha meg sem keresi őket. Amikor a Yahoo! nemrégiben megváltoztatta az adatkezelési elveit, ez a site látogatóinak alig 0,3 %-át érdekelte. Pedig eléggé jelentős változásokról volt szó.

Vagy hogy egy másik példát említsek: feltűnően kevesen használnak privacyvédő szoftvereket és így például olyanokat, melyek lehetővé teszik az anonim szörfölést a weben; cookie-menedzsert, aminek a segítségével ellenőrzésük alatt tarthatnák, hogy a különböző site-ok milyen azonosítókat (ezek a cookie-k) tehetnek le a gépükre, és akkor arról még nem is beszéltem, hogy csak nagyon ritkán találkozni valakivel, aki titkosítja a leveleit. Felőlem aztán nyugodtan hajtogathatják azt a felhasználók, hogy milyen fontos nekik a privacy – ezekből a számokból világosan kiderül, hogy korántsem az. Nem véletlenül mondja azt Esther Dyson, a világhírű számítástechnikai szakember, hogy „Nekem úgy tűnik, hogy az emberek demokráciát akarnak, de gyakran nem hajlandóak érte semmire, legyen bár szó szavazásról vagy arról, hogy megtegyék a legelemibb lépéseket privacyjük megvédéséért". Másfelől viszont „amikor a McDonalds 20 cent kedvezményt ajánl a hamburgereire, azonnal hajlandóak megadni minden személyes információt". És a Jupiter felméréséből is az derül ki, hogy 100 internetezőből 82 bármit hajlandó elárulni egy újonnan induló kereskedelmi site-nak csak azért, hogy némi árengedményt kapjon. Egy Eric Goldman nevű jogász (Marquette University Law School) egyenesen azt kérdezi, hogy „Ha ezek az emberek a lehető legkevesebbet sem hajlandóak tenni a saját (privacyjük) védelmében, akkor miért kellene a kormánynak foglalkoznia ezzel?"

Vízi Patkány: Azért én kapásból tudok példát mondani arra, hogy az embereket igenis érdekli a privacyjük: a magánéletük sérthetetlensége. Az amerikai Indiana államban, ahol meglehetősen komolyan veszik a telefonos zaklatásokat, a telefonos direktmarketing-cégeknek rendszeresen közzé kell tenniük a „do-not-call" listákat, amikre azok iratkoznak fel, akik nem akarják, hogy vasárnap délután is mindenféle idétlen üzleti ajánlatokkal bombázzák őket. Steve Carter indianai államügyész szerint ezen a listán 2002. októberében 1,188,948 név volt megtalálható – vagyis a lakosságnak mintegy a fele. Erősen hajlok arra a feltevésre, hogy ez a szám nagyjából megmutatja, hogy az embereknek a különböző túlzó állításokkal ellentétben (amik az „egyáltalán nem fontos"-tól a „mindenkinek ez a legfontosabb"-ig terjednek) mi a valódi álláspontjuk. És bár akadnak, akiket szemmel láthatóan tényleg nem érdekel az egész, a kormánynak akkor is feladata lenne, hogy...

Hoover: Nocsak, nocsak! Legjobb tudomásom szerint te vagy a Szerző szócsöve, nem pedig én, és mégsem tetszik neked az önszabályozás?

Vízi Patkány: De hol van itt az önszabályozás?

Hoover: Hát ott, hogy szerintem nyugodtan bízzuk a piacra, hogy mennyi privacyt biztosít a felhasználóknak, és ha az egyik cég túlságosan pofátlan lesz, akkor legfeljebb nem tőle fognak vásárolni, hanem valaki mástól. Tulajdonképpen az emberek fogják eldönteni, hogy mekkora privacyre van vagy nincs szükségük, az üzlet pedig majd igazodik hozzájuk. „A vásárlói viselkedés majd megmondja a cégeknek, hogy milyen szintű privacyt kell nyújtaniuk", mutat rá Goldman.

Vízi Patkány: Akkor most álljunk meg egy pillanatra, ugyanis nekem is van egy idézetem. Lawrence Lessig jogászprofesszor viszont, aki az internetes szólásszabadság egyik legismertebb szakértője, arra mutat rá, hogy „Hagyomány, hogy félünk a kormányzati szabályozástól, ám szemet hunyunk a magánszféra által érvényesített szabályozás fölött".

Hoover: Vagyis? Szerinted mi a megoldás?

Vízi Patkány: Nem biztos, hogy tudok egyértelmű választ adni. Egy, a számítógépes szakember John Glimore-nak tulajdonított mondás szerint „az internet hibaként értelmezi a korlátozásokat és létrehozza a kerülő utakat”. Ez azonban bármilyen jól hangozzék is, ostobaság, ugyanis az internet most is ugyanúgy szabályozva van, mint bármelyik másik média, és...

Hoover: Ez neked szabályozás? Hiszen teljes az anarchia!

Vízi Patkány: Dehogyis! Ha jobban belegondolsz, éppen az állami szabályozás az, ami biztosítja, hogy egyáltalán működhessen az internet, mert az állam az, ami gondoskodik róla, hogy az én weblapomon csak én jelentethessem meg az írásaimat; hogy más ne használhassa az én e-mail címemet, stb. Amiből viszont az következik, hogy – cserébe ezekért a szolgáltatásokért – az államnak joga van bizonyos követelésekkel fellépni a haszonélvezővel, a tulajdonossal, a szolgáltatóval... nevezd, ahogy tetszik... szemben. Az amerikai Legfelsőbb Bíróság már 1984-ben kimondta, hogy a bevásárló központok kötelesek helyet biztosítani a szólásszabadság gyakorlására. Vagyis az állam igenis beavatkozott abba, hogy mit tesznek a gazdag üzletemberek, de – túl azon, hogy ezt a szólásszabadság érdekében tette – ehhez azért volt joga, mert másfelől ő biztosította, hogy egyáltalán működhessenek a plázák.

Hoover: Tehát akkor szerinted is az lenne a legjobb, ha mindent az állam szabályozna?

Vízi Patkány: Na, ezt azért nem mondanám, ugyanis minden szabályozásnak akadnak hátulütői. Először is ott van ugye az átfogó törvények alkalmazása, ahol...

Szerző: Ilyen például a magyar adatvédelmi törvény is.

Vízi Patkány: Ha te mondod... az effajta szabályozás rendszerint a FIPS-ből (lásd a függelékben), vagyis az adatok kezelésére az Amerikai Egyesült Államokban még az 1970-es évek elején kidolgozott privacy-alapelvekből kiindulva átfogóan és kevés elemre visszavezetve mondja meg, hogy mit szabad (illetve nem szabad) tenni akkor, ha személyes adatokat kezelünk.

Hoover: Tehát úgy gondolod, hogy ezt lenne érdemes választani?

Vízi Patkány: Hát... David Banisar, a Privacy International igazgatóhelyettese szerint itt az szokott gondot okozni, hogy „Egy átfogó rendszer megléte önmagában még nem biztosíték arra, hogy az adott országban valóban megfelelő védelemben részesülnek a privacyvel kapcsolatos jogok... a legerősebb törvény sem ér semmit, ha nem párosul hatékony végrehajtással”. Akár úgy is fogalmazhatnék, hogy egy törvény éppen annyit ér, mint amennyire betartják.

Szerző: Magyarországon is ez a fő probléma. Az, hogy bár „jogaink és intézményeink egy része már megfelel a nyugati kritériumoknak, gyakorlatunk azonban még nem”, ahogyan Székely Iván társadalmi informatikus jegyzi meg egyhelyütt.

Vízi Patkány: Vannak azért itt más problémák is. Peter Swire, az Ohio State University jogászprofesszora éppen nemrégiben írt arról, hogy a jelenlegi amerikai közhangulat túlságosan is emlékeztet a kommunizmus elleni boszorkányüldözések hangulatára, és attól lehet tartani, hogy a terrorizmus elleni harcra hivatkozva vissza fogják szorítani az emberi jogokat.

Hoover: Hé, az Első Alkotmánymódosítást (lásd a függelékben) senki nem támadja, és nem akarja korlátozni! Akkor meg mi a probléma? Bush elnök semmi mást nem csinál, mint ami ebben a helyzetben a kötelessége, és eközben egy ujjal sem nyúl hozzá a híres alapjogaitokhoz!

Vízi Patkány: Köszönöm a végszót, Hoover, ezzel ugyanis már el is jutottunk a lényeghez. „Az 1970-es évek közepén köztudott volt, hogy az FBI, a CIA és más ügynökségek törvénytelenségeket követnek el és engedély nélküli megfigyeléseket meg lehallgatásokat hajtanak végre", mondja Swire. „Nem szabad megengedni, hogy a terrorizmusellenes szabályozások az elmúlt évtizedek kommunistaellenes gyakorlatát kezdjék követni." Még akkor sem, ha ezt éppen az emberek védelmére hivatkozva teszik. Mint mindjárt látni fogjuk, a kormányzat „stratégiája" súlyos tévedésen alapul, és ez az a pont, ahol már vissza is kanyarodhatunk a keretszabályozások problémáihoz. Ugyanis – folytatja Swire – az adminisztráció arra hivatkozik, „hogy megvédik az Alkotmány által biztosított privacyjogokat. Ez kétségtelenül jól hangzik – sajnos azonban a jelenlegi, hatékony privacyszabályozások legtöbbje nem az Alkotmányon alapul, hanem különböző törvényeken". És ezekre igenis szükség van, hiszen egy adott terület (mint amilyen az egészségügy vagy az adatbázisok) esetében nem várható el a bíróktól, hogy minden egyes pernél visszanyúljanak az alapokhoz, és neki kezdjenek néhány nagyon általános szabályt értelmezni. Ebben az esetben fennállna annak a veszélye, hogy a különböző bíróságok – a különböző értelmezéseknek köszönhetően – tökéletesen eltérő következtetésekre jutnak, és az egész áttekinthetetlenné válna.

De mindent egybevetve az átfogó szabályozás még mindig szerencsésebb megoldás a szektoriálisnál, ahol – ismét csak Banisar szerint – „a technológia haladásával egyes konkrét szabályok könnyen rugalmasságukat veszthetik".

Hoover: Vagyis mint nálunk, az Amerikai Egyesült Államokban is? Annak is megvannak a maga előnyei, ha a telefonos lehallgatások például pontosan szabályozottak, de az interneten azt művelnek a fiúk, amit akarnak, mert az internet ugye nem telefon.

Vízi Patkány: Igen, éppen erre gondoltam. Hogy a szektoriális szabályozás mindig csak egy meghatározott területre terjed ki (mondjuk a vezetékes telefonra), de ha megjelenik egy új technológia, akkor a törvényalkotóknak újabb szabályokat kell alkotniuk. Állandóan loholnak a változások után, de vajmi kevés esélyük van rá, hogy utol is érjék. Elvégre e szerint a modell szerint csak azt lehet szabályozni, ami már létezik, és a bíróságok arra kényszerülnek, hogy amikor egy új problémával találkoznak, akkor ismét hozzanak egy precedensértékű döntést.

Hoover: Igen, mint például a Legfelsőbb Bíróság annak a marihuána-termesztőnek, Danny Lee Kyllonak az ügyében. 1992-ben két nyomozó Agema Thermovision 210 hőkamera segítségével megállapította, hogy a ház falának... hogy finoman fogalmazzak... sajátos hőmintázata van, és ebből rájöttek, hogy Kyllo speciális lámpákat használ a kábítószer termesztéséhez. Úgyhogy annak rendje és módja szerint házkutatási parancsot kértek, és persze találtak is több mint 100 palántát. A közismerten liberális San Francisco-i Bíróság 1999-ben nem is látott semmi kivetnivalót a dologban, de 2001. június 11-én a Legfelsőbb Bíróság fogta magát, és úgy döntött, hogy mégsem lesz így jó, mert máskülönben sérül a Negyedik Alkotmánymódosítás... ami ugye védelmet biztosít az indokolatlan házkutatások ellen (lásd a függelékben). Lassanként kezdem érteni, hogy miért nem tetszik neked a szektoriális szabályozás, és hogy őszinte legyek, nekem is egyre kevésbé rokonszenves, hiszen ez nem is volt házkutatás, és egyáltalán nem is mentek be hozzá. Akkor meg mire fel, hogy...

Vízi Patkány: Ennél azért kissé bonyolultabb a helyzet, Hoover! Még a konzervatív beállítottságú Antonin Scalia bíró is úgy fogalmazott, hogy ebben az esetben az volt a leglényegesebb kérdés, hogy a modern technológia mennyire „csökkentheti a garantált privacyk körét... Ahol, miként itt is, a kormány olyan eszközöket alkalmaz, melyeket nem használnak elterjedten a mindennapi életben, és melyek lehetővé teszik, hogy a megfigyelők fizikai behatolás nélkül megtudják, hogy mi történik a ház falai mögött, ott a megfigyelés 'házkutatásnak' minősül, és házkutatási parancs nélkül nem lehet végrehajtani". Sir Edward

Coke már 400 évvel ezelőtt kimondta, hogy „A saját háza mindenki számára kastély és erőd, és védelmet biztosít számára az igazságtalanság és erőszak ellen, illetve lehetővé teszi, hogy megpihenjen”; és most a bíróság ennek szellemében járt el.

Hoover: Azért korántsem mindenkinek tetszett Scalia érvelése! Túl azon, hogy a Legfelsőbb Bíróság mindössze 5-4 arányban állt ki ennek a Kyllonak a védelmében (vagyis erősen ingott a léc), a liberális beállítottságú John Paul Stevens bíró például amellett volt, hogy meg kell különböztetni a „falon keresztüli” megfigyeléseket a „falon kívüli” megfigyelésektől (ez utóbbiak nem a ház belsejében lévő állapotot vizsgálják). Mivel itt mindössze „falon kívüli” megfigyelés történt, a nyomozóknak igenis joguk volt hőkamerát használni. Kár, hogy sokan voltak ugyan, akik józanul gondolkodtak, de nem elegen.

Vízi Patkány: Szerintem viszont nem kár, és a történetnek különben sincs még vége. Elvégre Scalia azt állapította meg, hogy a kormány nem alkalmazhat a mindennapi életben még gyakorlatilag ismeretlennek számító eszközöket. Tehát ha majd a sarki vegyesboltban is hőkamerát árulnak, akkor a nyomozók számára is szabad lesz a vásár, és...

Hoover: Jól van, jól van, pontosan értem, hogy mit akarsz mondani. Úgyhogy most már azt is elárulhatnád, hogy mi a bajod az önszabályozással. Elvégre ez volt a kiindulópont.

Vízi Patkány: Ja igen, az önszabályozás. Egy-egy iparág képviselői időnként össze szoktak állni, és etikai kódexeket, viselkedési normákat meg hasonlókat dolgoznak ki – és rendszerint az egész nem ér semmit. Persze tudom, hogy az internetezők az önszabályozást szokták preferálni, mert nem akarják, hogy az állam beleszóljon a dolgaikba, meg hozzá is vannak szokva a szabadsághoz és az anonimitáshoz...

Hoover: ... talán kissé túlságosan is.

Vízi Patkány: ...de ebből még nem következik, hogy a Nagy Testvér, vagyis az állam helyett jobb, ha a Kis Testvérekre, vagyis a különböző cégekre bízzuk, hogy eldöntsék: mit és hogyan szabad és mit nem.

Mert ha ők hoznak létre egy „önszabályozó szervezetet” (amit természetesen ők is pénzelnek), akkor könnyen előállhat az a helyzet, hogy az önszabályozó szervezetnek az egyik szponzorát kellene megbüntetnie... és mivel ez roppant kínos tud lenni, ezért inkább nem teszik.

A TRUSTe például, ami a saját állítása szerint „független, nonprofit” szervezet, és elvileg az lenne a célja, hogy „megbízhatóvá” tegye az internetet a felhasználók számára, egyszerűen megtagadta, hogy eljárást indítson az őt anyagilag is támogató Microsoft, illetve realNetworks ellen, pedig azok a szoftvereikbe rejtett kémprogramokat (úgynevezett spyware-t) használtak a felhasználóik különböző internetezési szokásainak megfigyelésére... De ebben nincs semmi meglepő. Ha te az előbb a Jupiter Research-re hivatkoztál, akkor én most hadd hivatkozzam a Forrester Research szakértőire, akik már 1999-ben azt írták egy kutatási jelentésükben, hogy „a TRUSTe, a BBBOnline és az egyéb, hasonló, független privacyvédő csoportok megélhetési forrását az elektronikus kereskedelmet folytató társaságok jelentik, így ezek a csoportok egyre inkább az ágazat, nem pedig a fogyasztók érdekeit képviselik”.

Dyson meglehetősen kiábrándultan fogalmaz: „Azok a csoportok, melyek azt mondják, hogy a fogyasztók érdekeit védik, gyakran saját ügyeikre összpontosítanak, – s ezeknek több közük van a washingtoni hatalmi harcokhoz és a pénzszerzéshez, mint a tényleges fogyasztói érdekekhez.”

Hoover: Vagyis?

Vízi Patkány: Vagyis egyelőre senki nem teheti meg, hogy nem védi a privacyjét.

Hoover: Vagy legalábbis nem tehetné meg.

Vízi Patkány: Igen, nem tehetné meg, hogy nem védi a privacyjét az interneten vagy bárhol másutt. Tehát ha nem válaszol a kéretlen reklámlevelekre (azaz spamekre); él a törvény adta jogaival...

Hoover: Egy átlagos internetezőnek sejtelme sincs róla, hogy milyen törvények vannak.

Vízi Patkány: ...titkosítást használ, és...

Hoover: titkosítás? Ugyan már... a Privacy Leadership Initiative 2001-es felmérése szerint az internetezők alig 10 százaléka használ valamilyen privacyszoftvert – ha ugyan egyáltalán igaz ez az adat. Közben meg ugyanezek az internetezők fennen hangoztatják, hogy ők lennének a legilletékesebbek a privacyjük megvédésében: szintén a Privacy Leadership Initiative mutatta ki azt is, hogy az internetezők a saját felelősségüket egy 10 pontos skálán 7,7-re becsülik, míg az üzleti vállalkozásokét 7,2-re és a kormányokét alig 6,9-re. Akkor meg oldják meg maguk!

Vízi Patkány: Ez azért túlzás... Egyes problémák megoldása messze meghaladja az erejüket és a lehetőségeiket. Egyáltalán nem mindegy például, hogy opt-out vagy opt-in modellt követ az ország.

Hoover: Nem hát, és akinek van egy kis esze, az az opt-out-ra szavaz, hiszen ez az, ami lehetővé teszi, hogy az emberek letiltsák bizonyos, rájuk vonatkozó adatok kezelését.

Szerző: Magyarországon is opt-out van.

Hoover: Persze, hogy az van, hiszen az opt-in közönséges ostobaság... és roppant káros is. Nem csak az iparnak okozna komoly nehézségeket, de még a fogyasztók is ráfizetnének – a szó szoros értelmében. Privacy ide vagy oda, ezt bizony mindenki megsínylené.

Vízi Patkány: Az opt-int? Mármint ha a különböző cégeknek előbb engedélyt kell kérniük, ha adni-venni akarják a ránk vonatkozó adatokat? És ugyan miért?

Hoover: A Napnál is világosabb. Az amerikai Online Privacy Alliance 2001. márciusában megvizsgálta a kérdést (persze ez is egy, az állami szabályozás helyett az önszabályozást támogató szervezet), és arra a következtetésre jutott, hogy az adatok szabad áramlása teszi lehetővé, például a reklám célcsoportjának jobb behatárolását – márpedig minden, nem megfelelő embernek szóló üzenet a reklámozás és végső soron a termék költségeit fogja növelni. Csak hogy egy konkrét példát is mondjak: Az adatok „átlátszósága" a jelzálog-üzletben például évi 85-től 100 milliárd dollárig terjedő megtakarítást tesz lehetővé, míg a nem jelzáloggal foglalkozó hitelügyletek esetén további 150 milliárd dollárét. Azaz minél többet tud a pénzintézet a felhasználóról, annál jobban fel tudja becsülni a kockázatokat, és annál „testreszabottabb" feltételek mellett tud üzletet ajánlani a kérelmezőnek.... azt hiszem, ez kellőképpen nyomós érv. Az Information Services Executive Council pedig azt mutatta ki, hogy a kiskereskedelem jelenleg évi 1 milliárd dollárt takarít meg a megfelelő információknak köszönhetően, és e nélkül a katalógusok vagy az online kiskereskedelem költségei 3,5 – 11 százalékkal mennének fel.

Ráadásul a privacy túlzott erőltetése kiiktatná az úgynevezett „adataggregátorokat" (kb. összesítő, ilyen az Acxiom és az Experian) is. Ha egy nagy ruhagyártónak mondjuk 25 millió emberről vannak adatai, az adataggregátorok szolgáltatásait igénybe véve könnyedén meg tudja állapítani, hogy kiket érdemes – a vásárlás reményében – megszólítani, az opt-in viszont azt eredményezné, hogy míg jelenleg az emberek kb. 90 százaléka nem tiltja le az adatai kezelését, addig a jövőben csupán 10 százalék adna engedélyt rá... Sőt, még arról is vannak adataim, hogy az USA-ban azért alacsonyabb a kölcsönök kamata, mert nálunk szabadabban mozognak az információk, és a bankok jobban fel tudják becsülni, hogy mennyire kockázatos, ha hiteleznek valakinek.

Vízi Patkány: Hmm... Nem mondom, elsőre persze egészen meggyőzően hangzik, de egyfelől nem lennék meglepve, ha kiderülne, hogy ezek az adatok jócskán túlzottak. Elvégre egy opt-inellenes, önszabályozáspárti szervezet végezte a felméréseket...

Hoover: Ez nem érv!

Vízi Patkány: ...másfelől pedig miközben senki sem tagadja, hogy az opt-innek lennének költségei, ugyanakkor az is valószínűnek látszik, hogy az internetes kereskedelmet például fellendítené. Jason Catlett, a fogyasztói privacyt védő Junkbusters vezetője szerint „az amerikaiak nagy része nem bonyolít le távolról vásárlásokat, és ennek az az egyik fő oka, hogy a privacy megsértésétől félnek".

Hoover: Ez legalább olyan hitelesen hangzik, mint amikor én hivatkozom egy önszabályozó ipari szervezet felmérésére.

Vízi Patkány: Rendben, akkor mondok mást. Catlett említi azt is, hogy mennyire feltűnően elfogult az Online Privacy Alliance. Azt ugyanis még véletlenül sem tanulmányozták, hogy milyen pozitív hatásai lehetnének az opt-innek. Pedig elég lett volna egy kicsit körülnézniük, és rögtön látnák, hogy máshogy is lehet csinálni. Olaszországban (ahol még az európai uniós előírásnál is szigorúbbak az adatvédelmi törvények) akár két év (!) börtönt is kaphat, aki előzetes hozzájárulás nélkül továbbítja a személyes adatokat – arról viszont valahogy lemaradtam, hogy az olasz ipar emiatt lenne válságban... És ha mindez nem lenne elég, akkor azt is hadd tegyem hozzá, hogy az sem nagyon érdekelne, ha valamivel többe kerülne a sajtos kifli, mert nem kezelheti bárki szabadon az adataimat.

Szerző: A BM Központi Adatfeldolgozó Hivatal 2000-ben százmillió Ft-os bevételre tett szert azzal, hogy különböző cégeknek eladja az állampolgárok adatait, és...

Hoover: Na látod, Vízi Patkány! Ha ezt megszüntetnénk, akkor az állam komoly pénzektől esne el!

Szerző: Szerintem most nem ez az érdekes. Hanem az, hogy bár erre egy 1992-es törvény engedélyt ad (egy magyar állampolgár adatai jelenleg 6-30 Ft-ba kerülnek attól függően, hogy floppyn vagy öntapadós matrican kérik-e őket), az akkori adatvédelmi biztos, Majtényi László már 1999-ben azt írta egy ajánlásában, hogy legalábbis vitatható, hogy mennyire fér össze az állami alapnyilvántartás feladataival (vagy éppen az adatvédelmi törvény szellemével), amikor eladják a gyerekek adatait a Hasbronak.

Értsd: amennyiben alapjognak tekintjük a privacyt, úgy az állam – hacsak nem nagyon indokolt – nem foszthat meg tőle minket. És az, hogy egyesek szert tegyenek az adataink eladásából némi mellékjövedelemre, mindennek tekinthető, csak nyomós indoknak nem.

Vízi Patkány: Aha, szerintem sem. Sőt, akár tovább is mehetünk. Banisar például azt is mondja, hogy „A privacy, azaz a magánélet, magántitok és személyes adatok védelme alapvető emberi jog, amely egyben több más értékünknek – így az emberi méltósághoz fűződő jognak vagy a gyülekezési és szólásszabadságnak – is alapja." Tehát aki lemond a privacyről, az intsen nyugodtan búcsút a többi alapvető jogainak is.

Hoover: Én még mindig nem értem, hogy honnét ez a félelem. Azt talán még csak-csak hajlandó vagyok elfogadni, hogy vissza lehet élni a személyes adatokkal (mint ahogyan bármi mással is), de az interneten például rendszerint statisztikai célokra meg ilyesmire kellenek a felhasználói információk.

Vízi Patkány: Vagy nem. „Az információk egy része csupán statisztikai célra használható – mondja Dyson – ám a többségüket a marketingügynökök azért akarják megszerezni, mert magát az egyént akarják nyomon követni... (őket) természetesen nem az érdekli, hogy kik

vagyunk; csak az, hogy mit akarunk venni (vagy mire lehet bennünket rábeszélni!). A viselkedésünket akarják megjósolni. A baj csak az, hogy az általuk összegyűjtött információ természetéből fakadóan továbbterjed."

Hoover: No nézd csak, már megint a régi nóta. Azóta ezt ismételgeti mindenki, amióta elkészült az első teljesen elektronikus számítógép, az ENIAC (aminek egyébként akkora volt az energiaigénye, hogy a bekapcsolásakor elhalványultak egész Philadelphia fényei), és még olyanok is akadnak, akik összetévesztik a privacyvédelmet a géprombolással. Szerintük az az egyetlen biztos módszer, ha összetörjük a komputereket.

A legjobb példa erre a felfogásra Harvey Matusow: mondhatom, gyanús egy alak volt. Nem csak azért, mert tizenegyszer házasodott; és nem is csak azért, mert a False Witness (Hamis tanú, 1955) című könyve megjelenésekor öt év börtönre ítélték, és...

Vízi Patkány: És a könyv arról szólt, hogy Matusow az FBI és Joseph McCarthy szenátor fizetett „tanújaként" miként vádolt meg embereket az Amerika-ellenes tevékenységet vizsgáló bizottságok előtt, noha korábban ő is a kommunista párt tagja volt. Egy időben sikerült is kiérdemelnie az „Amerika legutáltabb embere" címet... Amúgy pedig a False Witness nagyban hozzájárult ahhoz, hogy lezáruljon a McCarthy-féle boszorkányüldöző korszak.

Hoover: Igen, igen, de mondom, hogy nem ez a fontos. Hanem az, hogy Matusow 1969-ben létrehozta az International Society for the Abolition of Data Processing Machines (ISADPM) nevű szervezetet (kb. számítógép-uralom ellenes nemzetközi szervezet), aminek a fénykorában 1500 tagja volt, és ezek a fanatikusok fennen hangoztatták, hogy „a számítógép a teremtőjét legyőző szörnyeteg", úgyhogy itt az ideje, hogy felvegyék ellene a harcot... „Világ emberei, egyesüljetek!"

Nevetséges. Harc, méghozzá azáltal, hogy nem megsemmisítik a lyukkártyákat, hanem – bizonyos lyukak elhelyezésével – gondosan „átprogramozzák", és így zavarják össze az elektronikus agyakat; a levélbélyeget nem a megfelelő oldalra ragasztják fel, hogy a számítógép ne boldoguljon vele; meg az olyan ostoba és haszontalan információk terjesztésével, hogy miként postáztassunk 10 tonna kétszersültet az ellenségünknek, és így tovább. „Hogyan idegesíts fel egy komputert; hogyan zavarjad össze; hogyan tegyed tönkre"... Azt hiszem, az ilyesmit szokták manapság neoluddizmusnak nevezni, és innét már egyenes út vezet az Unabomber néven hírhedtté vált Ted Kaczynskiig, aki pályafutását zseniként kezdve a Harvardon szerzett fokozatot matematikából 20 éves korában. De ahelyett, hogy szakmai folyóiratokba publikált volna, azt hajtogatta, hogy a technikát mint olyat teljes egészében el kell utasítani, mivel „a technika 'jó' részei nem választhatóak el a 'rossz' részektől", és ennek megfelelően az egyetlen megoldás az lehet, ha 18 éven keresztül bombát küldözgetünk mindenkinek, aki bármivel is hozzájárulhat a technikai fejlődéshez, és közben megölünk három embert, és további 28-at megsebesítünk, és...

Vízi Patkány: Akkor most itt álljunk meg egy pillanatra, ugyanis abból, hogy valaki nem ért egyet a technológia előretörésével, még nem következik feltétlenül, hogy neki fog állni embereket gyilkolni. Ez egyszerűen csúsztatás, Hoover! És különben is inkább arról kellene beszélnünk, hogy miért kezdtek el az emberek félni a számítógépektől.

Hoover: Azért, mert ostobák. Egy technológia önmagában mindig semleges, miként már említettük, vagyis sem nem jó, sem nem rossz, ezért teljesen felesleges félni tőle.

Vízi Patkány: Igen, de azt is hozzátették, hogy egy megfelelően kifinomult technika viszont megfelelően kifinomult lehetőséget teremt a visszaélésekre, és ugye éppen ez a felismerés vezetett magához Brandeis és Warren cikkéhez is. Pedig hol volt akkor még Orwell.

„Az, hogy az adatok a papíralapú rendszerből számítógépes rendszerbe kerülnek – mondja a privacyszakértő Alan F. Westin – veszélyt jelent a szabadságjogokra, a privacyre, sőt, az egész emberi létre is, mivel olyan egyszerűvé válik a hozzáférés."

Hoover: Westin? Az a Westin, aki egy 1978-as kongresszusi meghallgatáson olyan meggyőzően érvelt a „privacy ellen irányuló invázióval" kapcsolatban, hogy ennek köszönhetően született meg az egyik első, a fogyasztók privacyjét védő törvény, a Fair Credit Reporting Act?

Szerző: Várjál még egy kicsit, Hoover, mindjárt erről is szó lesz.

Hoover: Oké, oké, csak arra voltam kíváncsi, hogy tényleg róla van-e szó.

Vízi Patkány: Róla hát.

Hoover: Érdekes. Mármint az az érdekes, hogy amikor találkoztam vele, akkor éppen az Equifax nevű adatgyűjtő óriáscég fizetett tanácsadója volt, és én személy szerint nem igazán értem, hogy miként fér össze ez a kettő, és...

Vízi Patkány: Igen, gyakorlatilag tényleg eladta magát. De azt azért senki sem vitatja, hogy a számítógép igenis jelenthet veszélyt, és ha megnézzük, hogy mi történt az 1950-es években, akkor egyáltalán nem nehéz megérteni Westin aggodalmait. Akkoriban ugyanis, lévén a számítógép roppant drága, a számítástechnika roppant kevesek privilégiuma volt, és még itt, az Újvilágban is sokan támogatták az „egységes huzalozású állam" (vagy ha úgy jobban tetszik, akkor „kibernetikus állam") gondolatát. Elvégre milyen kényelmes is lenne, ha egy gombnyomással bármit meg lehetne tudni... persze közelről sem mindenki nyomogathatná a gombokat, hanem csak a kormányszervek meg az üzleti és a politikai élet vezetői. Azaz a vezetők általában.

A többiek (értsd: az állampolgárok, a beosztottak és mindenki más) pedig, akik eddig is hátrányos helyzetben voltak, most még hátrányosabb helyzetbe kerülnének. És ha ehhez még azt is hozzávesszük, hogy az első nagy adatkezelők a tudományos intézetek mellett a hadiipari központok és a nyilvántartó hivatalok voltak... nos, mára legalább az világossá vált, hogy az emberek két legfőbb ellensége – vagy ha finomabban akarok fogalmazni, akkor az emberek önrendelkezését akadályozó két legfőbb tényező – az állam és a piac. Mert ugye az előbbi igényeinek a minél engedelmesebb és minél átláthatóbb üvegállampolgár, az utóbbinak pedig az egyéni igényekkel egyáltalán nem fellépő tömegvásárló felelne meg a legjobban.

Mivel a számítástechnika lehetővé teszi például úgynevezett profilok elkészítését, a dolog innentől kezd igazán eldurvulni: akkor, amikor valakit egy adathalmaz alapján ítélnek meg, és neki nemhogy arra nincs lehetősége, hogy a hibás adatokat korrigálja, de arra sem, hogy legalább tudomást szerezzen róla, hogy ki és milyen, rá vonatkozó információt kezel. Meg hogy milyen preferenciák alapján ítélik meg a róla készült számítógépes profilt. Vagy hogy esetleg nem az eredetitől eltérő céllal használják-e fel az adatokat.

Nem véletlen, hogy a francia igazságszolgáltatás szerint például tilos bármilyen, emberi viselkedésre vonatkozó igazságszolgáltatási vagy közigazgatási döntést kizárólag automatizált információkezelésből (pl. profilok) származó adatok alapján meghozni.

Hoover: Huh, mindjárt halálra rémülök a rám leselkedő szörnyű veszélyektől! De talán nem ártana, ha valami konkrétumot is mondanál e helyett az általános propagandaszöveg helyett. Lehet, hogy azt valamivel meggyőzőbbnek találnám.

Vízi Patkány: Akkor legyen.... és kezdjük talán azzal, hogy itt minőségi különbségekről van szó. Ahogy mondani szokás, az ember meg tudja magát védeni azoktól a privacysértésektől, amiket a kerítésen átkandikáló szomszédai jelentenek – tehetetlen viszont az állammal vagy a nagy adataggregátorokkal szemben.

A Cator és Guy Woolford testvérpár 1899-ben alapította meg Atlantában a Retail Credit Co-t: abból indultak ki, hogy a biztosító társaságok (illetve később már a munkáltatók is) szeretnének minél többet tudni az ügyfélről (potenciális alkalmazottról), nem szeretnek viszont mások magánügyeiben turkálni, és ezért kellőképpen hálásak, ha elvégzi helyettük valaki a piszkos munkát. És a számításuk be is vált: hamarosan számos irodát nyitottak az ország különböző pontjain, és fiatal, ám nem túlságosan képzett alkalmazottaik még azt is feljegyezték, hogy a megfigyelt személy milyen whiskyt iszik a legszívesebben (az viszont, hogy a dohányzási szokásokról is beszámoljanak az egészségbiztosítónak, soha nem jutott eszükbe). 1972-ben egy „lekáderezett" San-Francisco-i döbbenten tudta meg, hogy a róla készült jelentés szerint „nőiesen használja a kezét és nőies a beszédstílusa is".

Nem kevésbé döbbenetes az az aranyszabály sem, mely szerint „Ha kétségeid vannak, írjad le" (és aztán juttasd el a feljegyzést a megrendelőnek). A hivatalos útmutató szerint „Amennyiben azzal kapcsolatos információ jut a tudomásunkra, hogy (a megfigyelt személyt) letartóztatták, megvádolták vagy elítélték, de – az állítást alátámasztandó – nem lehet hozzájutni a helyi rendőrség adataihoz, **AKKOR IS BE KELL ERRŐL SZÁMOLNUNK**. Ám eközben ügyelnünk kell rá, hogy a megfelelő nyelvezetet használjuk, tehát fogalmazzunk így: »A helybéliek arról beszélnek, hogy az illetőnek gondjai voltak a rendőrséggel, ám az ezt alátámasztó rendőrségi adatokhoz nem sikerült hozzájutnunk.«"

Hoover: De hiszen ez így teljesen korrekt!

Vízi Patkány: Gondolod? Gondolod, hogy azok, akikről ilyen „információk" alapján állítanak össze profilokat, elfogadhatónak tartják ezt? Mert szerintem nem, és a Retail Credit 1975-re már annyira népszerűtlenné vált, hogy inkább új nevet választott magának, és most Equifaxként működik.

Ami persze – az érintettek számára – nem valami nagy különbség: egy 1990 utáni kongresszusi vizsgálat azt állapította meg, hogy egyáltalán nem izgatják magukat a különféle panaszok meg a hibás adatok kijavítására vonatkozó kérelmek miatt, noha az ilyen cégek által szállított információk 21-33 százaléka (!) hibás – a saját bevallásuk szerint.

És nem sokkal jobb a helyzet a Retail nagy riválisa, a TRW esetében sem (amit a fentebbi receptnek megfelelően később Experiannek kereszteltek át). A történet ez esetben akkor kezdődött, amikor egy detroiti biofizikus, egy bizonyos Harry C. Jordan az 1950-es években örökség révén belecsöppent az üzletbe, és ez meghatározta a cég „technikabarát" beállítottságát is. Az 1980-as évek végétől például felfedezték maguknak az adatbázis-marketinget – vagyis azt, hogy a reklámok 70 százaléka nem a megfelelő emberekhez jut el. Ha viszont rendelkezésünkre állnának a vásárlóról a pénzügyi adatok mellett a vásárlási szokásaira, lakásviszonyaira, családjának nagyságára, hobbijára stb. vonatkozó információk, akkor egyből könnyebb lenne a dolgunk... Egy szakértő szerint nem történik más, mint hogy „egyetlen tollból egy egész ülő kacsát csinálunk", amit már csak le kell durrantani.

Hoover: Én azért vigyáznék az ilyen kijelentésekkel, Vízi Patkány! Próbálj meg nem túlzásokba esni. Egyfelől ha a vásárló célzott reklámot kap, akkor ő is jól jár, másfelől pedig talán valami rossz tudományos-fantasztikus regényben elképzelhető, hogy a Kis Testvérek tökéletesen ellenőrzik a vásárlókat, a valóságban azonban semmiképp.

Vízi Patkány: Nos, a tények kissé mást mutatnak. Ami a számokat illeti, amikor az Experian 1996-ban a brit GUS-hoz (Great Universal Stores) került, akkor a külföldi üzleti élet is hozzáférhetett 170 millió amerikai fogyasztó adataihoz (40 más ország összesen 708 millió fogyasztójának adataival együtt).

Vagy hogy egy másik, szintén óriási számot említsek: az ezredforduló előtti Amerikában évente 37 milliárd reklámlevelet postáztak... A Metromailnek, Amerika legnagyobb direkt marketing cégének (aminek ugyanaz a tulajdonosa, mint az Experiannek) gyakorlatilag minden amerikai háztartásról vannak adatai, és évente 4,1 millió újszülött neve kerül be az adatbázisukba.

Vagy nézzük csak azt az esetet, amikor a Lotus és az Equifax 1990-ben összefogott, hogy egy CD-t dobjanak piacra Lotus Marketplace: Households (A Lotus színtere: az otthonok) címmel, és ebben minden – ismétlem, minden – lakás címe és minden elképzelhető demográfiai információ szerepelt volna. Tehát a kisvállalkozások ugyanolyan célzott reklámkampányokat folytathattak volna, mint amilyeneket 30 évvel korábban még csak az óriáscégek – de több mint harmincezer tiltakozó levél szerencsére elég volt ahhoz, hogy a Lotus elálljon az ötlettől.

Közben az adatgyűjtési módszerek egyre kifinomultabbak lesznek: a legtöbb nagy élelmiszerbolt-hálózat például az árukon található vonalkódok segítségével és a hitelkártyával való fizetés elterjedésének köszönhetően már ma is nyomon tudja követni az egyes vásárlók fogyasztói szokásait (és persze a légitársaságoktól átvett és a „törzsutas" kártyát helyettesítő, különféle „pontgyűjtő" kártyák is ezt segítik).

Az pedig – szerintem – már-már rémisztő, hogy a Safeway 2002. nyarán olyan bevásárló kocsikat kezdett Kaliforniában tesztelni, amiken érintőképernyők vannak, és ha megengedjük, hogy a rendszer leolvassa az összes vásárlásunkat (és így a vásárlási szokásainkat is) nyilvántartó Safeway Club Cardunkat, akkor ezért cserébe – fogalmazzunk talán így – jelentős, több centes kedvezményeket kaphatunk, és ráadásul a bevásárló pultok között sétálva „testre szabott reklámok" fognak felvillanni a szemünk előtt. Közben ismét csak az áruház jár jól, a vásárlók ugyanis valósággal megvadulnak az állítólagos kedvezményektől, és „ha valaki eddig átlagosan 80 dollárt költött egy alkalommal, akkor most 100-at fog", jegyzi meg a témával foglalkozó Chris Boone. Ismétlem, mindezt cserébe azért, hogy pontosan tudják rólunk, hogy milyen gyakran vásárolunk sört vagy kotont...

Ha pedig valaki felhív egy ingyenes szolgáltatást, akkor számíthat rá, hogy automatikusan rögzítik a telefonszámát stb.

Utána pedig jönnek a reklámok meg a hirdetések: a fejlett fogyasztói társadalomban egyes becslések szerint naponta mintegy 1,000-1,500 ilyennel találkozunk a televízióban és a rádióban, illetve az internetet meg az újságokat böngészve – és persze a postaládánkban is a nagy halomnyi kéretlen levél formájában.

Szerző: A magyarországi reklámpiac évente kb. 220 milliárd forintot forgalmaz, és ennek kb. 6%-a ilyen, a levelesládánkba betuszkolt „szemétposta", ami fejenként mintegy 11 kg kéretlen reklámküldeményt jelent (vagyis országos szinten évi 110,000 tonna papírt).

Vízi Patkány: Ezért mondja a reklám-visszaélésekkel foglalkozó Jeffrey Robinson, hogy „mindannyian üvegfalú szobákban élünk."

Hoover: Na, azért valamiféle védelem mégiscsak létezik a vásárlók számára. Fogyasztóvédelmi szervezetek, etikai kódexek, törvényi szabályozások...

Vízi Patkány: Hát persze, Hoover, hát persze. És egyedül az a probléma, hogy az ipar (legyen bár szó az áruházakról, az adataggregátorokról vagy Hollywoodról) meglehetősen nagy pénzek felett rendelkezve meglehetősen hatékonyan tud lobbizni a céljai érdekében.

Hoover: Amerikában azért csak elfogadták a Fair Credit Reporting Act-et, nem? És ez kimondottan a felhasználók védelmét szolgálja. Elvégre az a célja, hogy gátat szabjon a személyes adatok gátlás nélküli továbbadásának az iparban.

Vízi Patkány: Persze. De akkor azt is tegyed hozzá, hogy az adatkezelők azért csak kaptak némi ajándékot a Kongresszustól: azt a kitételt, mely szerint nem lehet beperelni őket azért, ha a hibás adatok révén mintegy „rágalmazást" vagy privacysértést követnek el.

Hoover: Azért a fogyasztókat sem féltem. Ők ugyanis ilyenkor azért szoktak pert indítani, mert ugye – éppen ennek a törvénynek az értelmében – ezeknek az adatkezelőknek azonnal korrigálniuk kellene a hibás adatokat.

Vízi Patkány: Vagyis megpróbálják megvédeni magukat. Hogy csak az egyik legismertebb esetet említsem, az 1990-es évek elején Keith és Phyllis Mirocha (Indiana) azt vették észre, hogy a TRW és a Trans Union szerint 60 ezer dollár tartozásuk van, miközben a valóságban egyetlen centnyi sem volt. De ennek ellenére az terjedt el róluk a pénzszektorban, hogy „rosszul fizető adósok". Úgyhogy amikor a TRW egy évvel később még mindig „feketelistásként" kezelte őket, és emiatt nem sikerült ingatlankölcsönt felvenniük, akkor bírósághoz fordultak, és annak rendje és módja szerint nyertek is.

Akár azt is mondhatnám, hogy bár a cégek keresztül látnak rajtunk, vajmi kevéssé érdekli őket, hogy nem optikai csalódásról van-e szó csupán, és nagyjából hasonló a helyzet az állammal is, ami olykor bizony...

Hoover: Gondolom, most jönnek az információs utópiák meg a többi blabla, hogy az embereknek szabadon kellene eldönteniük, hogy milyen információkra van szükségük; illetve, hogy mit hajlandóak közzé tenni magukról.

Vízi Patkány: De...

Hoover: De ez egyszerűen lehetetlen: az állam például, amit te nagy előszeretettel nevezel Nagy Testvérnek, működésképtelenné válna, ha – ad absurdum – a privacyvédők még azt is meggátolnák, hogy népszámlálást végezzünk. Másfelől meg ott vannak a titkosszolgálatok, államtitkok (amik nem véletlenül nem kerülnek nyilvánosságra) stb., úgyhogy az ilyesmiről még álmodozni sem érdemes.

Vízi Patkány: Ha már a népszámlálást említetted, hadd emlékeztesselek arra, hogy ennek is meglehetnek a maga veszélyei. Egy statisztikus még valamikor 1849-ben arra panaszkodott a Kongresszus előtt, hogy ahányszor egy-egy új kérdés jelenik meg a népszámlálások kérdőívén, az emberek bizalmatlanokká válnak – szerintem erre minden okuk meg is volt. Az állam egyre többet akart megtudni róluk, és túl azon, hogy emiatt kellett (mármint azért, hogy jobban nyilván lehessen tartani az embereket) bevezetni a vezeték- *és* keresztnév használatát (illetve 1936-ban a Social Security Numbert, a társadalombiztosító számot is), 1850-ben a hatóságok már kíváncsiak voltak a válaszoló nevére, nemére, életkorára, bőrszínére, születési helyére és idejére, családi állapotára, végzettségére és vagyonára, továbbá arra is, hogy nem vak, süket, őrült vagy idióta, büntetett előéletű vagy szegény-e. A rabszolgáktól persze kevesebb dolgot kérdeztek, mint a szabadoktól, és közben állandóan azt hajtogatták, hogy soha nem fognak visszaélni az adatokkal.

Amikor 1890-ben a Hollerith-féle lyukkártya-gépekkel kezdték a válaszokat feldolgozni (ezekből fejlesztették aztán ki a II. Világháború IBM-adatfeldolgozó gépeit), a Census Bureau azzal biztatott mindenkit, hogy „az Ön adatait 60 millió honfitársáéval együtt dolgozzuk fel", vagyis miért is kellene attól tartania, hogy éppen az önére leszünk kíváncsiak. Nem egy irodalmi remekmű, de sokat elárul a korabeli hozzáállásról:

A népszámlálási biztos éneke

Népszámlálási kérdezőbiztos vagyok,
Bármely ajtón bármikor bekopoghatok.
Kérdőív, toll és hatalom:
Mindezeket a magaménak mondhatom.

Bárkitől bármit kérdezhetek,
Előttem az emberek térdre hullnak.
Hadd lássam a pénzügyeid, ide a kulcsokat!
Valljad be, hogy nem vagy-e elmebeteg.

Nem tetszik a dolog? Ne hibáztass érte:
Az állam rendelte el, én csak végrehajtó vagyok,
Az állam nevében járok el, a törvény hozott létre,
hogy begyűjtsem rólad az összes adatot.

(New York Sun, 1890)

Ugyanekkor a Hollerith-gép az embereket a szó szoros értelmében különböző kategóriákba sorolta (mivel a lyukkártyákat – a rajta található információk alapján – egy mechanizmus különböző dobozokba szortírozta szét). És az sem mellékes, hogy a gépi feldolgozás tette lehetővé a „ha kétséged van, akkor kérdezz!" elv megvalósítását is, vagyis azt, hogy (mivel utána nagyon csekély többletmunkával úgyis fel lehet dolgozni, ezért) érdemesebb minden elképzelhető dologra azonnal rákérdezni. A legjobb példa erre az internet, ahol gyakorlatilag ugyanazzal a ráfordítással gyűjthetünk be valakiről egy vagy ötven adatot, és közben még demokratizálódott is a folyamat. Erre most már nem csak a nagy cégeknek vagy éppen az államnak van módja, hanem gyakorlatilag bárkinek, aki rácsatlakozik a hálózatra, és lassanként a sok millió Nagyon Kis Testvér társadalma leszünk.

Hoover: Még mindig nem értem, hogy mi a bajod a népszámlálásokkal.

Vízi Patkány: Az, hogy csúnyán vissza lehet velük élni. Az általad emlegetett ENIAC-ot a hadsereg fejlesztette ki; az első, kereskedelmi forgalomban kapható elektronikus számítógépet, az UNIVAC-et pedig néhány évvel később a Census Bureau, és ez akár szimbolikusnak is tekinthető... Amikor 1890-ben azt állították, hogy nem fognak visszaélni az adatokkal, akkor nem mondtak igazat: addigra már régen megtették – méghozzá a népszámlálási hivatal és a hadsereg együttesen.

„Akik nem bíztak a Népszámlálási Hivatalban, azok legrosszabb álmaikat látták megvalósulni az észak-déli polgárháború alatt", állapítja meg Robert Ellis Smith privacyszakértő.

William Tecumseh Sherman északi tábornok ugyanis 1864-ben azokat az adatokat használta fel a déliek ipari és kereskedelmi központjainak meghatározására, majd pedig megsemmisítésére, amiket a déli állampolgárok az 1860-as népszámlálás során bocsátottak a Census Bureau rendelkezésére. Sherman olyannyira tisztában volt a népszámlálási információk fontosságával, hogy köszönő levelében azt írta, hogy „A háború utolsó időszaka bebizonyította, hogy milyen értékesek ezek a statisztikai adatok és táblázatok, és nagyon is valószínű, hogy nélkülük nem lettem volna képes végrehajtani azt, amire így képes voltam".

Éppen ez az, amit a FIPS szerint nem lenne szabad tennünk: a meghatározott célra gyűjtött adatokat más célra felhasználni. Ez korántsem az egyetlen ilyen eset: a II. Világháború idején az amerikai katonai vezetés ismét csak a Népszámlálási Hivataltól akarta megszerezni az országban élő japán-amerikaiak nevét és lakcímét, hogy aztán „elkülönítő táborba" zárhassák őket. A Census Bureau erre ugyan nem volt hajlandó – de arra igen, hogy kiadja azokat a „statisztikai" adatokat, melyek alapján aztán meg lehetett állapítani, hogy hol vannak a kolóniáik.

Hoover: Mintha bizony csak az állam csinálna ilyesmit! A Crystal Eastman és Roger Baldwin által 1920-ban alapított, nagy hírű ACLU (American Civil Liberties Union): az Újvilág egyik legtekintélyesebb jogvédő szervezete legalábbis kezdetben egyetértett a japánok internálásával; az 1950-es években pedig a vezetőség éppen nekem adott ki titokban információkat a tagjairól, és egyetértett azzal is, hogy a Kommunista Pártot „a hatalom átvételére törekvő nemzetközi összeesküvés" résztvevőjeként bélyegezzék meg.

Amivel egyszerűen azt akarom mondani, hogy azért arra is oda kell figyelni, hogy a különböző kérdések megítélése történetileg, sőt, a helytől függően is változhat, és amikor a privacy védelméről szónokolsz nekem, akkor közben valahogy mindig elfelejted megmondani, kinek a privacyjéről beszélsz.

Vízi Patkány: Nem gondolod, hogy ez az ACLU kissé egyoldalú, hogy azt ne mondjam, elfogult bemutatása? Háromszázezer tagja van, és ha már mindenképpen felsorolásba akarnék bocsátkozni, akkor a leginkább az EPIC-kel (Electronic Privacy Information Center); a GILC-kel (Global Internet Liberty Campaign) meg a PI-jal (Privacy International) együtt kellene említenem. Ezek között a szervezetek között leginkább az a különbség, hogy míg az EPIC inkább „jogi szinten" tevékenykedik, a Privacy International pedig inkább aktivista és a Nagy Testvér Díjtól kezdve különféle megmozdulásokig rengeteg akciót szervez világszerte, addig a GILC afféle ernyőszervezet, ami összefogja az adott témával foglalkozókat.

Hoover: Úgy látszik, vannak (és én biztosan nem tartozom közéjük), akinek tetszenek az olyan kampányhadjáratok, mint amilyen az ACLU legutóbbi megmozdulása is volt, ahol azt hajtogatták, hogy „őrizzük meg Amerikát biztonságosnak és szabadnak", és eközben a terroristaveszély ellen elfogadott Patriot Act ellen... hmm... nem akarok erős szavakat használni... agitáltak. Ennek része volt egy olyan televíziós hirdetés is, ami egy kezet mutat – és a kéz széttépi, majd újraírja az amerikai Alkotmányt, és egy hang azzal vádolja meg az amerikai igazságügy-minisztert, hogy megsértette az Első és a Negyedik Kiegészítést. Rossz még belegondolni is.

Szerző: Ízlés kérdése. De mivel a dologról a későbbiekben még úgyis lesz szó, egyelőre talán hagyjuk is – bár azt azért megnézném, hogy hogyan reagálnának Magyarországon egy hasonló kampányra az érintettek. Mert Aschroft igazságügy-miniszter nagyon ügyesen azt válaszolta, hogy „Örülök, hogy olyan országban élek, ahol az ACLU kritizálhat engem, és nyilvánosan vitathatja az általam alkalmazott eljárásokat", mivel ez azt jelzi, hogy továbbra is szólásszabadság van.

Hoover: És ennek közelről sem minden igazi amerikai hazafi örül. De hogy mi lenne nálatok? Nehéz kérdés: a jog, illetve konkrétabban fogalmazva a privacy nyilvánvalóan mást jelent a demokratikus hagyományokkal rendelkező országokban (mint amilyen Amerika is), ahol elsősorban az a kérdés, hogy több kényelmet vagy több biztonságot? És teljesen mást jelent az olyan helyeken, mint mondjuk Magyarország, ami meglehetősen késői és fejlett formájában importálta a számítástechnikát – arról azonban a jelek szerint elfeledkezett, hogy az ACLU szerint a komputerhasználathoz megfelelő jogi garanciák is kellenek.

És akkor azt még nem is említettem, hogy akár társadalmi rétegenként is eltérő lehet, hogy kinek mi a fontos. Nálunk teszem azt elsősorban a személyes szabadságot és annak védelmét szokták emlegetni; a skandináv országok lakosai viszont alapvetően megbíznak az államban, mert azt a közösség megvalósult akaratának tekintik.

Vízi Patkány: Ebben ugyan igazad van, de egyes módszerek semelyik privacyfelfogás szerint sem engedhetőek meg – és ilyen többek között az információ-felhalmozás is. Az 1960-as évekre beindult ugyan Amerikában a „nagyüzemi" adatgyűjtés, de minden ügynökség körömszakadtáig védte a saját információit, és ez oda vezetett, hogy az úgynevezett Ruggles-

Bizottság 1965-ben több mint 600, egymástól független állami adatkezelőt számolt össze. Ezért azt javasolták, hogy az állam „hozza létre a Federal Data Centert, aminek joga van hozzáférni a különböző ügynökségek számítógépszalagjaihoz és egyéb, géppel olvasható adatforrásaihoz", mivel ez sokkal olcsóbban és hatékonyabban működő rendszert eredményezne.

Hoover: De hiszen ez tényleg olcsóbb lenne!

Vízi Patkány: Akkor most én hivatkozom arra, hogy a viszonylagosságot is figyelembe kell venni: nem csak az számít, hogy mi az olcsóbb, hanem az is, hogy milyen megoldás fogadható el – és milyen nem. Mindig figyelembe kell venni az összes szempontot – nem pedig csak azt, hogy mennyibe kerül.

Szerző: Pontosan. Magyarországon az Alkotmánybíróság például az 1991/15. számú határozatában mondta ki, hogy az egységes és mindenütt használható személyazonosító szám alkalmazása alkotmányellenes, mivel így az egy meghatározott emberre vonatkozó adatokat túlságosan is egyszerű lenne összegyűjteni, majd pedig személyiségprofilt létrehozni belőle. És bár mindenki tudta, hogy ez nem kis pénzbe fog kerülni, nem ez volt az elsődleges. Választani kellett egy milliárdos beruházás meg aközött, hogy mindenki afféle a hatalom számára tökéletesen átlátható és nyomon követhető üvegállampolgár legyen-e. És az adatvédelmi biztos ajánlása nyomán ugyanezért nem hoznak végül létre a bankok számára nálunk olyan, központi adósnyilvántartást sem, amiben mindenki (tehát nem csak a késedelmes fizetők) szerepelnének.

Vízi Patkány: Igen, lényegében itt is ugyanaz volt a probléma, mint egy mindent átfogó, központi adatbázisnál. „Egy nemzeti és így szükségképpen sokfelhasználós, személyes adatokat tároló rendszer lényegesen nagyobb veszélyt jelent a privacyre, mint több, egymástól független adatbázis", jegyzi meg a számítógéptudós Roger Clarke, hiszen – még ha a hatalom nem is élne vissza a lehetőségekkel (bár ezt egy hatalomról eléggé nehéz elképzelni), akkor is ott van a számtalan, hozzáférési jogokkal rendelkező ügynök, beosztott, adminisztrátor, adatfeldolgozó stb., és máris száz sebből vérzik az egész. Csak éppen míg egy kisméretű adatbázisnál csupán néhány, addig itt minden adathoz hozzáférhetne a korrupt, felelőtlen vagy bosszúszomjas alkalmazott.

Tehát bár a Bureau of Budget 1966-ban közzétette a Federal Data Centerre vonatkozó elképzeléseket, és bár széles körben idézték a közgazdász Edgar Dunnt, aki szerint a várható pénzügyi haszon bőven ellensúlyozza a privacy csorbulásának veszélyeit, a tervből nem lett semmi.

Hoover: Mert rossz volt az időpont. 1962-ben jelent meg Rachel Carsontól a Néma tavasz, ami ráirányította a figyelmet a környezetvédelemre – és 1964-ben az újságíró Vance Packard The Naked Society (A meztelen társadalom) című könyve, ami viszont a legújabb adatgyűjtési módszerekre, illetve arra irányította rá a figyelmet, hogy ezek az adatok éppúgy lehetnek hibásak is, mint jók. A Federal Data Centernek (amit szoktak National Data Centerként is emlegetni) semmi esélye sem volt.

És a FEDNET-nek sem volt semmi esélye: ezt nyolc évvel később John E. Holt nevű bürokrata találta ki a General Services Administrationnél (Holtot Gerard Ford (még alelnökként) sürgősen le is fokozta, hogy később (már elnökként) aztán visszahelyezze a pozíciójába – és rábízza az egész intézmény privacyvédelmét).

Vízi Patkány: És 1974-ben szerencsére a mai szemmel morbidnak tűnő, AIDS (Automated Integrated Digital Services) nevű terv is hasonló sorsra jutott.

Hoover: Látom, hogy nem érted a lényeget. Nem a kormány akart mindenféleképpen túlhatalmat szerezni, de egy központi adatbázisra előbb-utóbb nagy szükség lett volna. Hiszen gondolj csak bele: egy 1976-os amerikai felmérés szerint 85 kormányügynökség 6723 egymástól független adatbázis-rendszerében összesen 3,8 milliárd név szerepelt (vagyis minden név jó néhányszor). 1980-ban a kiskereskedelem pénzforgalmának a felét, az autó- és házkereskedelmet pedig gyakorlatilag a hitelből bonyolították, és a kereskedőknek égető szükségük volt a hitelinformációkra. Ugyanis az amerikaiak több mint egyharmada addigra már nem ott élt, ahol megszületett (és ahol pontosan tudták róla, hogy mennyire megbízható), miközben minden ötödik család évente költözött új vidékre (és közben persze elvárták, hogy bárhol hitelt tudjanak felvenni). Ja igen, és tíz emberből nyolc kötött egészségbiztosítást, hogy fizetni tudja az orvosi ellátás költségeit és a korábbiakkal ellentétben immár nem csak a szegények kényszerültek arra, hogy felvegyék a kapcsolatot a kormánnyal (ami ilyenkor persze nem Nagy Testvér, hanem Jóságos Apuka), mert ott voltak a különböző állami ösztöndíjak az oktatásban; a mozgássérülteket segítő programok és a speciális adókedvezmények... és még hosszan sorolhatnám egészen a jogosítvány megszerzéséig bezárólag (egyes államok pedig csak akkor adtak vezetői engedélyt, ha a vezető megkötötte a baleset-biztosítást).

Summa summarum, az amerikai intézményeknek és cégeknek nem is maradt más választásuk, mint minden lehető adatot begyűjteni az állampolgárokról, akik persze folyamatosan panaszkodnak emiatt.

Vízi Patkány: De még ha igazad lenne is, ettől egy központi adatbázis ugyanolyan veszélyes marad, a felmerülő problémákat pedig biztosan meg lehet oldani elkülönített rendszerekkel is. Mert máskülönben... Hadd mondjak egy példát.

2002. augusztusának elején a tokiói tüntetők azt skandálták az utcán, hogy „a tehenek 10, az emberek 11 jegyű számok", és egyes városokban valóságos beköltözési hullám kezdődött.

A tehenek azért „10 jegyűek", mert 2001. őszén a BSE miatt 10 jegyű azonosítót vezettek be számukra a felkelő nap országában, hogy állandóan nyomon lehessen követni a mozgásukat – az emberek pedig azért 11 jegyűek, mert a kormány 2002 augusztusában beindította azt a programot, ami első lépésben a „koseki" nevű, elavult és nehézkes papír alapú regisztrációs rendszer felváltását célozta meg egy 11 jegyű azonosító szám révén.

A mind a 126 millió japánt tartalmazó adatbázisba a legalapvetőbb személyi adatoknak (név, cím, születési hely és idő, nem, 11 jegyű azonosító) kellett volna bekerülniük, hogy könnyebbé váljon a különböző szolgáltatásokhoz és információkhoz való hozzáférés. Koji Ishimura, az információs törvények szakértője szerint „A kormány azt hangoztatja, hogy ez az azonosító 93 különböző célra használható fel. De van itt egy nagyobb projekt is: az E-kormányzat, és ha ez megvalósul, akkor (az adatokat) 16,000 különböző adminisztratív célra lehet majd felhasználni". Ami kétségkívül szép elképzelés, ám nem sokat ér, ha az emberek olyan fokon nem szimpatizálnak a gondolattal, hogy inkább új életet kezdenek egy olyan városban, ami (noha kötelező lenne) megtagadja a rendszer alapjául szolgáló Jumin Kihon Daicho-hoz (röviden: Juki-Net) való csatlakozást. Többek között így tett Jokohama, Japán egyik legnagyobb városa is (3,4 millió lakossal), más polgármesterek pedig kijelentették, hogy az első probléma felbukkanásakor kiszállnak.

Amire nem is kellett sokáig várni. Toranosuke Katayama, a posta és a telekommunikáció dolgaiban illetékes miniszter azt állította, hogy a rendszer tökéletesen biztonságos, és a benne keringő adatok védelmére azért nem alkottak külön privacytörvényt, mert felesleges lett volna: így is 8,300 dollárnak megfelelő pénzbüntetés és 2 évig terjedő szabadságvesztés vár arra, aki személyes információkat szivárogtat ki a Juki-Netből. Az Asahi Shimbun című lap viszont július második felében 1948 ember megkérdezésével végzett felmérést, és ebből az

derült ki, hogy a lakosságnak nem kevesebb mint 86 százaléka tartott attól, hogy mégis adatok juthatnak ki a rendszerből, illetve akár a hivatalnokok, akár a crackerek visszaélhetnek az univerzális személyazonosító szám nyújtotta lehetőségekkel. Az is sokat nyomott a latban, hogy ez az egész túlságosan is emlékeztette az embereket a II. Világháború idején működő, megfigyelésen és megfélemlítésen alapuló megoldásra.

Augusztus 5-én azért beindult a Juki-Net – két nappal később pedig Osaka egyik, Moriguchi nevű peremvárosában 741 háztartásnak (vagyis összesen 2,584 embernek) kézbesítettek ki más állampolgárokra vonatkozó szenzitív információkat. A nekik címzett levél a valóságnak megfelelően tartalmazta a személyes adataikat – és emellett véletlenszerűen mások személyes adatait is. És azóta szemfüles adattolvajoknak egy kisebb japán város, Iwashiro mind a 9,600 lakosának minden Juki-Netes adatát is sikerült ellopniuk.

Hoover: Ez már megint a régi nóta, hogy az emberek nem szeretik, ha megszámolják és ennek megfelelően számon tartják őket. Az iamnotanumber (nem vagyok szám) című internetes honlap is azt hajtogatja, hogy ők nem számok; Ari Schwartz, a Center for Democracy and Technology társigazgatója meg éppenséggel a Juki-Netre hivatkozott egy kongresszusi meghallgatáson, amikor (akárcsak az iamnotanumber) egy olyan, egységes vezetői jogosítvány ellen akart érvelni, ami egy központi adatbázissal lenne összekapcsolva.

Igazán kíváncsi lennék, hogy mikor hozakodik valaki azzal elő, hogy az állatok sem számok, és őket is megilleti a privacy: a teheneket vagy a kutyákat.

Vízi Patkány: Szerintem a vízi patkányokat feltétlenül... de a tréfát félretéve: a Dog Fancy című amerikai kutyamagazin címlapján 2002. májusában az a kérdés volt olvasható, hogy „Személyes adatnak számítanak-e a kutyád egészségével kapcsolatos információk?”

Hoover: Na ne idétlenkedjél már, hogyan is számíthatnának annak? Vagy esetleg szegény kutyáknak is szembe kell nézniük a személyiséglopásból eredő problémákkal, és előfordul, hogy valaki más jelentkezik be Bodri nevében a kutyakozmetikushoz? Vagy esetleg őket is szemétpostával és spammel bombázzák?

Vízi Patkány: Ha őket nem is, de a tulajdonosukat biztosan. A cikk írója, egy bizonyos George M. Dennis, J.D. egyébként nem ezzel foglalkozik, hanem azzal, hogy az Amerikai Állatorvosok Társulata etikai szabályzatának 1999-es módosítása igenis kimondja, hogy a kutyák egészségügyi adatait is bizalmasan kell kezelni – és egyes amerikai államokban fogadtak is el ezzel kapcsolatos törvényeket. De ezek persze nem mindenek felett álló törvények, és adott esetben – mondjuk bírósági végzés birtokában – figyelmen kívül lehet hagyni őket. Például akkor, ha felmerül a gyanú, hogy állatkínzás történt. A lényeg mindenképpen az, hogy azért kell az ilyesmit (is) bizalmasan kezelni, mert a kutyánk kórtörténetéből velünk kapcsolatos következtetéseket is le lehet vonni. És ez viszont már privacy a javából. Mint ahogy gyakorlatilag minden más is az.

Cyberpornó

Hogyan mentette meg egy orgazmus az életemet

Valamelyik éjszaka egy New York-i hotelben a televízió-csatornákat váltogattam. Egyszerre csak az egyik, mindenki számára hozzáférhető, nem előfizetős adón megjelent egy érzéki, fiatal hölgy, aki nem viselt semmit, de olajtól fénylett az egész teste és miközben a szőnyegen hentergett, a legintimebb módon simogatta magát... Néztem egy ideig – a képernyőhöz szögezett a dolog szociológiai jelentősége", írja Robert Bork amerikai bíró Slouching Towards Gomorrah (kb. csoszogva tartunk Gomorra felé) című könyvében, aki szerint a modern liberalizmus a „romlás ügynöke", és a fő bűnösök az egyetemek, a feministák, a homoszexuálisok, a művészek – meg persze az ateisták és a vallási szakadárok.

Kétség sem fér hozzá, hogy más New York-iakat is a képernyő elé szögezett a fentebb leírt jelenet „szociológiai jelentősége", és az egészben leginkább az az ironikus, hogy noha Bork kikel mindenféle szexuális perverzió ellen (mármint minden olyan ellen, amit ő tart annak), amikor 1987-ben Reagan elnök a Legfelsőbb Bíróság tagjai közé jelölte, akkor a liberális washingtoni City Paper újságírói sürgősen felkeresték a lakhelyéhez legközelebb eső videotékát, és megszerezték az általa végignézett filmek listáját (hátha kiderül róla, hogy nagy pornórajongó). Sokan nem szerették volna ugyanis, ha Bork még több hatalomhoz jut: egyes nőmozgalmak szerint tendenciózusan a gyengébb nem ellen ítélt, és tartani lehetett tőle, hogy akár az abortuszt is megpróbálná betiltani.

Ehhez képest nem találtak valami sokat: a 146 kikölcsönzött videó között leginkább Walt Disney és Hicthcock képviseltette magát, de egy Mély torok típusú erotikus produkció még véletlenül sem. És ismét csak ehhez képest a történet azért megfelelő publicitást kapott ahhoz, hogy az emberek erről kezdjenek pletykálni az estélyeken, és a Szenátus – extrém nézetei miatt – végül nem fogadta el Borkot.

Ami persze több kérdést is felvet. A privacy felől nézve először is azt, hogy a videotékások miért tárolják a világon mindenütt (és így Magyarországon is) a megnézett filmek listáját időtlen időkig, amikor ez legalább olyan „érzékeny" adat lehet, mint a kutyánk egészségi állapota.

Másfelől pedig azt, hogy miközben általános a pornográfiával szembeni „hivatalos" ellenérzés (senki nem szokott nyilvánosan lapozgatni egy Playboyt), aközben, miként a biológus Susan Blackmore rámutat, szinte kizárt, hogy akadna, aki nem olvas végig egy-két oldalt, ha a fejezet a „Hogyan mentette meg egy orgazmus az életemet" címet viseli.

Ezt a kérdést persze egyáltalán nem öncélúan vetem fel, hanem azért, mert az internet elterjedésével a dolog egyre inkább előtérbe kerül. Noha akadnak, akik arra hivatkozva szeretnék teljes mértékben betiltani (vagy legalábbis alapvetően korlátozni) a cyberpornográfiát, hogy máskülönben egy kiskorú is illetlen képekbe ütközhetne, azért vannak olyanok is, akik amellett érvelnek, hogy ha hagyjuk a „szabályozáspártiak" akaratát érvényesülni, akkor ez akár a jelenlegi internet gyökeres átalakításához is elvezethet.

Hoover: Éppen ideje, hogy beszéljünk végre a pornográfiáról is, hiszen roppant veszélyes dolog. És még mindig nem szentelnek neki kellő figyelmet, pedig már az 1940-es évek elején, egészen pontosan az American Magazine 1941. februári számában Camps of Crime (A bűn táborai) címmel megírtam, hogy az amerikai motelek nagy része a bűn melegágyának tekinthető. Márpedig nem kevesebb mint 35 ezer volt belőlük.

Vízi Patkány: Igen, emlékszem rá. „Az FBI aktái tele vannak arról szóló esetekkel, hogy a gengszterek egy nem megfelelően ellenőrzött motelben húzzák meg magukat, miközben a nyomozók tűvé teszik értük az országot... A nagyobb hotelek azonnal jelentik a gyanús figurák feltűnését... ezek a turistaszállások (vagyis motelek) azonban a város külső peremén helyezkednek el, ahol a rendőrség már nem tud hatékonyan fellépni... A bejelentkezők adatait nem ellenőrzik rendszeresen a detektívek... gyakran még vendégkönyv sincs", és így tovább.

Hoover: Pontosan, ahogy mondod, Vízi Patkány! És akkor a marihuána-dealerekről még nem is beszéltünk. Pedig olyan ártatlanul kezdődött az egész... a 20-30-as évekre nagyon megugrott az autók száma, és a gépkocsitulajdonosok gyorsan rájöttek, hogy a hagyományos szállodák nem megfelelőek a számukra.

Vízi Patkány: Ez tökéletesen érthető. Elvégre a szállodák leginkább a városközpontokban voltak, a pályaudvarok közelében – vagyis autóval nehezebb volt őket megközelíteni; viszonylag sokba került az éjszakai szállás (nem pedig csupán egy dollárba, mint a kezdetben a töltőállomások mellett felhúzott épületekben); és sok helyen azt is megkövetelték, hogy a szállóvendég megfelelően legyen öltözve.

Hoover: Persze, de nem ez a lényeg. Hanem az, hogy az autózás elvezetett a motelekhez, a motelek pedig a hagyományos amerikai erkölcs hanyatlásához.

Vízi Patkány: Mármint miért?

Hoover: Mert ezekben a motelekben majdhogynem olyan szabadon és anonim módon mozoghattak az emberek, mint a mostani internetezők a világhálón, és ha nincs megfelelő ellenőrzés, akkor máris kész a baj. Tovább rontotta a helyzetet, hogy ekkoriban még különálló épületek voltak (nem úgy, mint ma), tehát még arra sem kellett tekintettel lenni, hogy mi hallatszik át a válaszfalon... és innentől kezdve elszabadultak az indulatok. Jellemző, hogy a korabeliek csak úgy emlegették ezeket a helyeket, mint „Mr. és Ms. Jonas Motel", „Forró Ágy Motel", „Ne Mondjad El Senkinek Motel" meg hasonlók.

A Southern Methodist University diákjai 1935-ben például Dallas környékén párokra oszolva azt vizsgálták, hogy miként élnek az amerikaiak a rendelkezésükre álló szabadsággal, és azt tapasztalták, hogy egyetlen hét végén kétezer (!) pár fordult meg 38 motelben, és amikor az egyik helyen összehasonlították 109 autósnak a vendégkönyvben feltüntetett adatait a valódi adatokkal (a rendszámok alapján), akkor az derült ki, hogy 102-en hazudtak! Az egyik motel-tulajdonos be is vallotta, hogy „vendégeim kilencven százaléka erkölcstelen célokra használja a helyet", és ez mindent egybevetve nagyobb veszélyt jelentett az amerikai erkölcsiségre, mint az, hogy olykor a motelekben megbújó bűnözőkkel is meggyűlt a bajunk. Mint például Bonnie Parkerrel és Clyde Barrowval, a hírhedt sorozatgyilkosokkal, akiket a Red Crown Cabin Campben zártunk körül.

De hogy visszatérjek a szexuális kicsapongásokhoz, akadtak azért jóravaló helyek is. A virginiai Roanoke például csak olyan „vendégeket" volt hajlandó fogadni, akik – a rendszámtábla tanúsága szerint – 50 mérföldnél messzebbről érkeztek (vagyis turisták voltak); a Colonial Cottages tulajdonosa pedig Louisville-ben azt írta ki a '40-es évek elején, hogy „NEM HELYIEKNEK – kizárólag turisták részére". Szerintem egyáltalán nem véletlen, hogy Nabokov hírhedt Lolitájának főszereplője, a pedofil Humbert Humbert professzor is annyira kedvelte a moteleket . „A paradicsom börtöncellájának" nevezte őket, és nagyon örültem, amikor arról olvastam, hogy a kéziratot egymás után négy nagy amerikai kiadó utasította vissza. Amikor pedig a francia Olympia Press nagy nehezen mégiscsak megjelentette 5000 példányban, angolul, akkor kitört a botrány: még a brit kabinet is foglalkozott vele. Új-Zélandban pedig be is tiltották.

Vízi Patkány: 1955-ben viszont Graham Greene már az év három legfontosabb könyve közé sorolta a New York Times hasábjain, és hamarosan felkerült a sikerlisták élére is... de nem is annyira ez az érdekes, mint inkább az, hogy én a helyedben óvatosan bánnék az efféle ítéletekkel. Túlságosan hosszú ugyanis az idők folyamán itt vagy ott betiltott könyvek listája... és aztán ezekről a könyvekről lassanként csak kiderült, hogy nincs is semmi probléma velük.

Mark Twain Huckleberry Finnjével a massachusettsi Concord könyvtárigazgatójának az volt a baja, hogy „sokkal jobban megfelel a csőcselék ízlésének, mint az intelligens és tekintélyes embereknek" (úgyhogy sürgősen feketelistára is tette); a szintén Mark Twain-féle Éva naplójával kapcsolatban pedig a szintén massachusettsi Charlton könyvtárosai azt kifogásolták 1906-ban, hogy az egyik egész oldalas illusztráció Évát bizony Éva-kosztümben ábrázolja. James Joyce Ulyssesét (arra hivatkozva, hogy túlságosan „obszcén") 15 évre tiltották ki az Egyesült Államokból valamivel később; 1930-ban Voltaire Candide című művét foglalták le (ismét csak az „obszcénségre" való hivatkozással); Arisztophanész Lüszisztratéjét; Chaucer Canterbury meséit; Boccaccio Dekameronját; Defoe Moll Flandersét; illetve az Ezeregy éjszaka meséinek különböző kiadásait pedig az 1873-as Federal Anti-Obscenity Act (más néven Comstock Law, azaz szövetségi obszcénség elleni törvény) alapján nem engedték postai úton terjeszteni. Ez a törvény ugyanis tiltotta az „erkölcstelen", „szeméremsértő", „trágár" és „obszcén" anyagok levélben való továbbítását – mint ahogy tiltotta többek között a születésszabályozással kapcsolatos információk terjesztését is. És bár ma már nincs életben, a számítógépes hálózatokra is kiterjedő Telecommunications Reform Bill (1996) azért jó néhány elemet átvett belőle.

Hoover: Mondd csak, Vízi Patkány, nem csúsztatsz te most véletlenül?

Vízi Patkány: Nem értem, hogy mire gondolsz.

Hoover: Arra, hogy felsorolsz néhány könyvet, amiket annak idején valamiért betiltottak, és ezzel kimondatlanul bár, de azt sugallod, hogy lám-lám, mekkora ostobaság is az, ha megszűrjük, hogy mik jussanak el az olvasóhoz. Pedig abból, hogy született néhány hibás döntés, még nem következik, hogy maga az elv – vagyis a tartalom filterezése – is hibás lenne. Hiszen azt valószínűleg te sem vitatod, hogy a kiskorúakat meg kell óvni a pornográf anyagoktól.

Vízi Patkány: Persze, hogy nem. Bár végső soron elképzelhető lenne más megoldás is: a középkorban, ugye, amikor az egész család egyetlen szobába összezsúfolódva lakott, és a gyerekek akaratlanul is tanúi voltak, amint a szüleik... szóval érted.

Hoover: Hát éppen ez az – ezért tilos a kiskorúak számára a pornográfia. Azt még a pornográfia ellenzői sem vitatják, hogy a szexualitás hozzátartozik az életünkhöz – más kérdés azonban, hogy mennyire kell közkinccsé tenni. Havelock Ellis brit pszichológus még 1928-ban megállapította, hogy „a szexuális aktus ugyanúgy nem tartozik a társadalomra, mint a többi testi funkciók". Vagyis nem kell mutogatni, és éppen elég baj, hogy Alfred Kinsey, az Indiana University kutatója 1948-as, 12,000 ember megkérdezésén alapuló felmérése során arra a megállapításra jutott, hogy az amerikai férfiak jóval több mint fele megszegi a szexualitással kapcsolatos törvényeket – gondolok itt a prostitúcióra, házasságtörésre, fajtalankodásra, szodómiára meg a többi hasonlóra.

Szerző: Tegyük gyorsan hozzá, hogy az Amerikai Egyesült Államokban a szodómia az orális és anális szexet jelenti.

Hoover: Persze, hogy azt.

Vízi Patkány: Meg azt is tegyük hozzá, hogy nagyjából ugyanannyira jogos betiltani a pornográfiát, mint a nőknek szóló rózsaszín szerelmes füzeteket.

Hoover: Ezt most én nem értem.

Vízi Patkány: Pedig nyilvánvaló. Mármint nyilvánvaló, hogy eléggé nagy mértékben meghatároz minket evolúciós múltunk, és az utóbbi pár millió évben kimondottan előnyös volt a promiszkuitás. A férfiak gyakran meghaltak egy-egy vadászat során, a törzsnek viszont az volt az érdeke, hogy a nők újabb és újabb gyerekeket szüljenek. Vagyis viszonylag kevés férfi; viszonylag sok nő – semmi sem szólt a „holtodiglan, holtomiglan" kizárólagossága mellett. A monogámia gondolata alig néhány ezer éves, miközben evolúciósan még mindig ugyanazok a kis csoportban élő vadászó-gyűjtögetők vagyunk. És mint ahogy a férfiak – a fentebb említett evolúciós okokból – a meztelenségre (pornográfia) és a nő elérhetőségére (prostitúció) „indulnak be", a nők ugyanígy vannak az érzelmekkel.

Ők nem a vadászatra, hanem a barlang körüli életre és az egymással folytatott állandó kommunikációra; az érzelmi kötődésre és az érzelmekre specializálódtak, tehát nyilvánvalóan ez érdekli őket ma is. És ezt kapják meg a családi szappanopera-sorozatoktól meg a rózsaszín regényektől. „A nő és a férfi más-más evolúciós fejlődés végtermékei; s ezt a munkamegosztás kényszere hozta magával. A férfi vadászott, a nő gyűjtögetett...

Ahogy testük megváltozott, hogy jobban alkalmazkodjék sajátos funkcióihoz, úgy változott agyuk is...

Azok, akik tagadják a gondolatot, miszerint biológiai természetünk hatással van viselkedésünkre, ezt gyakran a legjobb szándéktól vezérelve teszik: a nemek közötti előítéletek ellen harcolnak. Ugyanekkor viszont összezavarják az *egyenlő* és az *egyforma* fogalmát, holott... a férfiak és a nők... egyszerűen nem *azonosak*", olvasható a Pease-szerzőpáros által, a férfi és női agy különbségeiről írott ismeretterjesztő könyvben.

Hoover: Na, ez már megint másról beszél, mint amiről kellene! Ugyanis nem a pornográfiáról, hanem arról volt szó, hogy miért kell megóvni a gyerekeket a pornográfiától, úgyhogy most én is az evolúciós múltra hivatkozom. Arra, hogy a szex mintegy belénk van programozva, és ha a gyerekek túlságosan korán találkoznak vele, akkor erős kísértést éreznek majd, hogy ők is kipróbálják – még mielőtt alkalmasak lennének arra, hogy megszüljék és felneveljék a gyerekeiket. Az pedig, hogy adott esetben a férfiakat (is) eltiltjuk a pornográfiától (vagy legalábbis alapvetően korlátozzuk a hozzáférésüket), egyáltalán nem nagy ár azért, hogy megvédjük a serdülőket attól, hogy tönkre tegyék a saját életüket még mielőtt felnőttek lennének. És ezért is kell minden áron meggátolni, hogy az interneten pornográf anyagokhoz férjenek hozzá.

Vízi Patkány: Most meg te csúsztatsz, Hoover! Normál esetben a pornográfia mint olyan nem tiltott, csak...

Hoover: Oké, ha a pornográfia mint olyan, nem is, de a gyermekpornográfia igen, és ezt a kérdést egyáltalán nem szabad lebecsülni! A Pew Internet & American Life Project egy 2001. eleji felmérése szerint az amerikaiak 92 százaléka gondolja úgy, hogy az internet legnagyobb problémája a gyermekpornográfia és 50 százalékuk tekinti ezt a „lehető legförtelmesebb bűnnek". A probléma méreteire jellemző, hogy egy bécsi konferencián Dr. Agnes Fournier de Saint Maur az Interpoltól (Head of the Trafficking in Human Beings Branch) arról számolt be, hogy egyetlen nemzetközi akció során több mint egymillió pedofil képet; 67 gigabyte-nyi gyermekpornográfiát; 624 CD-ROM-ot, 38 komputert és 3227 floppyt foglaltak le.

Szerző: Akkor most álljunk meg egy pillanatra, és tisztázzuk, hogy több, különböző kérdésről van szó: először is a pornográfiáról (és persze az internetes pornográfiáról); másfelől pedig a gyerekpornóról. És végül majd a különböző határesetekről is beszélnünk kellene; azt viszont nem szeretném, ha összekevernénk ezeket a kategóriákat.

Vízi Patkány: Persze, persze, én is így gondoltam, és amikor Hoover közbevágott, éppen azt akartam mondani, hogy a demokratikus országokban rendszerint csak a pedofília tiltott, illetve a szex olyan formái, amik az egyik partner akarata ellenére valóak. Viszont bármikor előfizethetsz egy pornócsatornára, vagy bármelyik újságárusnál vehetsz magadnak egy pornólapot. Nem is olyan régen a Southern Voice című amerikai hetilapban az jelent meg, hogy „Államunk képviselője, Doug Teper olyan törvényt terjesztett elő, melynek értelmében Georgiában a paráználkodásra, házasságtörésre és szodómiára vonatkozó tiltást ki kellene írni a szállodai szobák falára. Azok számára pedig, akik nem *comprende* az angol nyelvet, Temper valamiféle 'nemzetközi szimbólumrendszert' akart bevezetni. Ragadjon tehát papírt és ceruzát a kedves olvasó, engedje szabadon szárnyalni a fantáziáját, és a végeredményt küldje el nekünk. A legjobbakat publikálni fogjuk."

Hoover: Nagyon vicces kedvedben vagy, Vízi Patkány, mondhatom! De hiába is hivatkozol a pornóújságokra: normál esetben egy felnőtt nem hagyja elöl az ilyesmit. Az interneten viszont mindenki oda kattint, ahová akar, és egy serdülő még akkor is pillanatokon belül beleütközik egy pornó site-ba, ha véletlenül nem keresi. A következtetés nyilvánvaló.

Vízi Patkány: Vagyis az internet tulajdonképpen a „pornográf mocsok" gyűjtőhelye, nem?

Szerző: 2000-ben az ORTT akkori elnöke, Körmendy-Ékes Judit is azt hajtogatta, hogy a magyar internetezők főleg pornográf oldalak nézegetésére használják a világhálót. Azt persze nem tudta megmondani, hogy honnét veszi ezt, és később bocsánatot is kért.

Hoover: Akármit is mondotok, a gyerekekre nézve igenis veszélyes az internet. Steve Largent kongresszusi képviselő már 2001-ben arra hívta fel a figyelmet, hogy a különböző file-megosztó rendszerek (mint amilyen a Napster vagy a Gnutella) „hozzáférést biztosítanak a gyerekek számára... a képi erőszak és a szex legrosszabb fajtáihoz" – még akkor is, ha esetleg nem is keresnek ilyesmit. Amikor egy vizsgálat során Britney Spears képeket akartak letölteni, akkor ezek 70 százaléka pornóképnek bizonyult, és persze semmik köze nem volt a pop sztárhoz. A BearShare file-sharing rendszerben pedig a tíz leggyakoribb kereső szó az volt, hogy Divx, Porn, Star Trek Voyager, Sex, XXX, Teen, Saving Private Ryan, Preteen, Lolita és Madonna, és ez szerintem tökéletesen igazolja azok félelmeit, akik emiatt tartanak az internettől.

Vízi Patkány: Jó, akkor kezdjük az elején: azzal, hogy miként jutottunk idáig. Ugyanis az a helyzet, hogy amint feltűnik a színen egy új kommunikációs eszköz, az erkölcsvédők rögtön aggódni kezdenek.

Hoover: Például a telefon miatt is? Hát ez igencsak nehezen hihető.

Vízi Patkány: Pedig pontosan így van. Sőt, ugyanez volt a helyzet az írással is. Egy bizonyos Philippe de Novare lovag valamikor a 15. sz.-ban azt hangoztatta, hogy „Nem helyénvaló, hogy a leányok megtanuljanak olvasni és írni, hacsak nem készülnek apácának, mert különben amikor nagykorúak lesznek, szerelmes leveleket írhatnak és kaphatnak" – De la Tour Landry lovag pedig azt válaszolta erre, hogy éppen ellenkezőleg: „a leányok (igenis) tanuljanak meg olvasni, hogy megtanulhassák az igaz hitet és védekezni tudjanak a lelküket fenyegető veszélyek ellen", és a forgatókönyv azóta sem sokat változott.

„Történetileg nézve – olvasható a téma szakértőjének számító Leslie Shade tanulmányában – az elektronikus kommunikáció (új) technológiáinak megjelenése gyakran morális ellenkezésbe ütközött: az otthon szentsége elleni fenyegetésnek tekintették", és a televízió például így lett a „családi élet lerombolója"; a videó esetében pedig egyenlőségjelet tettek az otthoni videózás és a pornográfia között.

Hoover: És nem véletlenül. „Amikor a felnőtteknek szánt videók is eljutottak a kölcsönzőkbe, a videomagnók eladása drámaian megszaporodott”, írja, az internetezés pszichológiájával foglalkozó Patricia Wallace, és azt is megemlíti, hogy a pornográfia az egyik olyan, „ütős alkalmazás”, ami képes eladni egy-egy új technológiát.

Vízi Patkány: Ami viszont nem jelenti azt, hogy szükségképpen beigazolódnának akár a pornóval kapcsolatos félelmek, akár a várakozások. A videotékák forgalmának nagy részét nem a pornófilmek teszik ki... A telefon esetében egyébként amiatt aggodalmaskodtak a szülők, hogy az udvarlók majd ellenőrzés nélkül susoghatnak lánygyermekeik fülébe. Hogy el ne felejtsem, az amerikai Képviselőház 1956-ban foglalkozott azzal a váddal is, mely szerint a Kinsey-jelentés „aláássa az amerikai család” intézményét.

De mindez mintha csak előjáték lett volna ahhoz a hisztériához képest, amit az internet váltott ki.

Hoover: Nagyon is megalapozott félelmek ezek, Vízi Patkány, nagyon is megalapozottak. Nem szabad alábecsülni őket.

Vízi Patkány: Márpedig nekem éppen ezzel az állítólagos megalapozottsággal van némi problémám. Ugyanis azzal kezdődött az egész, hogy egy Phillip Elmer-Dewitt nevű szerző 1995. június 3-án a Time magazin címlap-sztorijában (On a Screen Near You: Cyberporn) arról írt, hogy a hálózaton található felvételek nem kevesebb mint 83,5 százaléka (!) szexkép vagy „cyberpornó”, és ezek roppant „népszerűek, mindenütt jelen vannak és meglepően perverzek”.

Az eredmény: számos amerikai évekig azért nem mert titkosítást alkalmazni, mert attól félt, hogy akkor elterjed róla, hogy biztosan van valami rejtegetnivalója – és nagy valószínűséggel pornó-, sőt, pedofíliakedvelő.

A cikk persze gyorsan híressé – majd pedig hírhedtté vált, amikor kiderült, hogy Dewitt a Carnegie Mellon Egyetem posztgraduális diákjának, Martin Rimm-nek a tanulmányát használta fel anélkül, hogy ellenőrizte volna az adatok valódiságát, és a Time magazin végül lényegében ugyanúgy elnézést kért az olvasóktól, mint Körmendy-Ékes néhány évvel később a magyar internetezőktől.

Csak éppen közben jóval több kárt okozott még akkor is, ha hamarosan nyilvánvalóvá vált, hogy Rimm lényegében Michael Mehtának és Dwaine Plazának, két kanadai egyetemistának a dolgozatát „használta fel” – miután a saját szája íze szerint átalakította kissé. Tehát például a helyett a megállapítás helyett, hogy „az internet potenciális lehetőséget nyújt a pornográfia terjesztésére”, úgy fogalmazott, hogy „az internetet egyre inkább pornográfiára használják”. Vagy miközben az eredeti tanulmányban az szerepel, hogy „a pornográf anyagok számítógépes hálózatokon keresztül történő cseréje újdonságnak számít”, aközben Rimm azt írja, hogy „a számítógépes hálózatok használatának egyik leggyakoribb célja a szexuálisan explicit képek cseréje”.

És ez még akkor sem kis különbség, ha az utóbbi megfogalmazás sokkal inkább alkalmas arra, hogy felkeltse a nagyközönség érdeklődését.

Mint ahogy az sem mindegy, hogy a Mehta – Plaza szerzőpárostól Rimm arra hivatkozva kérte el a kéziratot, hogy a nagy tekintélyű Carnegie Mellon könyvet ad ki a témáról, és abban önálló fejezetként megjelenteti; és persze az sem, hogy miközben Mehta és Plaza a gyerekpornográfia egyetlen példájával sem találkozott, Rimm nagy merészen azt fejtegette, hogy az internet milyen „nagy mértékben könnyíti meg a gyerekpornográfia másolását és terjesztését”.

Hoover: Ami persze tökéletesen igaz.

Vízi Patkány: Egy „tudományos” dolgozat esetében azért nem árt az állításokat tényekkel is alátámasztani... De térjünk vissza egyelőre a „hagyományos” pornográfiához, illetve ahhoz, hogy már csak a két dolgozat eltérő nyelvezete is megér egy misét. A paraphilia kifejezés (abnormális szexuális aktivitás – mintha bizony a pornográfia feltétlenül az volna) Rimm-nél 82-szer szerepel – a kanadaiaknál egyszer sem; a pornografer pedig 70-szer (az eredeti dolgozatban ismét csak egyszer sem); a hard-core 52-szer, míg Mehtáéknál 0, azaz nulla esetben fordul elő. Akárcsak a pedofília, amit Rimm 41-szer ír le; és 21-szer használja a „fuck”-kifejezést is (a kanadaiak viszont anélkül is tudtak tudományos dolgozatot írni, hogy közben „baszást” emlegetnének); stb.

A Kongresszusban mindenesetre már június 26-án Rimm tanulmányára, illetve a Time cikkre, nem pedig a tudományos kritikákra hivatkoztak bizonyos Exon és Grassley szenátorok, amikor a „megfelelő szabályozást” sürgették.

„Ha a félrevezető információkat népszerűsíteni kezdik, akkor azok még félrevezetőbbé válnak... Az internetes szabályozásokkal kapcsolatos vitát meg a többi, a média által fontosnak tartott kérdéseket a tények és a megbízható információkon alapuló vélemények alapján kell megítélni ahelyett, hogy teret engednénk a hisztériának”, mondták utóbb Donna L. Hoffmann és Thomas P. Novak professzorok (Vanderbilt University) a Rimm-tanulmánnyal kapcsolatban.

Hoover: Szerintem éppen hogy ideje volt keményen fellépni. Már az 1990-es évek elején mindenki tisztában volt vele, hogy az internetes pornográfia lesz az első olyan e-commerce szektor, amiből pénzt lehet csinálni. Úgy is mondhatnám, hogy ez volt a húzóágazat (a Forrester Research 2000-ben 1 milliárd dollárra becsülte a pornó site-ok éves bevételét). Legfőbb ideje volt hát korlátozni a káros hatásokat.

Szerző: Az úgynevezett C-törvények (C, mint children, vagyis gyerekek) éppen erre szolgáltak volna.

Vízi Patkány: Pontosan. Közülük az első a CDA volt (Communications Decency Act, azaz kommunikációs illetlenségi törvény): a Telecommunications Act of 1996-os részeként írta alá Clinton elnök, és két év börtönt, illetve 250,000 dollár pénzbüntetést helyezett kilátásba azok számára, akik szándékosan „obszcén vagy illetlen” – például pornográf – anyagokat juttatnak el 18 éven aluliak számára.

Szerző: Tehát, ha jól értem, akkor azok számára is, akik például az interneten tesznek közzé pornográf anyagokat, elvégre az ilyenek tisztában kell legyenek vele, hogy kiskorúak is hozzáférhetnek... ami viszont indokolatlanul korlátozta volna a szólásszabadságot.

Hoover: Szerinted. Meg különben is: hogy jön az ide egyáltalán? Mármint a szólásszabadság.

Vízi Patkány: Jó kérdés – hadd mondjak egy példát. 1995-ben Kalifornia állam „bűncselekménnyé nyilvánította a pornográf kiadványok automatából történő árusítását”, írja Lessig, ugyanis a törvényhozók abból indultak ki, hogy a gépek képtelenek megállapítani, hogy valaki nyolc vagy nyolcvan éves. Hacsak valamiféle felnőttazonosító-számmal nincsenek felszerelve – de azt meg senki nem tudja, hogy miként lehetne ezt megvalósítani.

Hoover: Nagyon helyes!

Vízi Patkány: Közelről sem mindenki szerint: a szólásszabadság aktivistái ugyanis azt állították, hogy a megfogalmazás túlságosan széles (overbreath), hiszen gyakorlatilag azt írja elő, hogy csak emberek árulhatnak pornográf anyagokat, és ez viszont két okból is sérelmes. Egyfelől, mert akadnak, akik szeretnének ugyan pornográf anyagokhoz jutni, de kellőképpen szégyellősek ahhoz, hogy ne merjék egy hús-vér embertől megvenni: elvégre ki mer pornókazettát kölcsönözni egy videotékából, ha minden nap oda jár...

Szerző: Én biztosan nem.

Vízi Patkány: Én sem, és éppen ez a probléma. Másfelől mert az automatából árult anyagok valamivel olcsóbbak, és akadnak, akiknek ez egyáltalán nem mindegy. Márpedig a szólásszabadság kiterjed a pornográf anyagokra is. Vagyis az embereknek joguk van hozzájutni – méghozzá a lehető legkedvezőbb módon.

Hoover: Hát ez igencsak nyakatekert érvelés... ugye, nem azt akarod mondani, hogy a bíróság bedőlt neki?

Vízi Patkány: Nem hát. A Legfelsőbb Bíróság 1997. március 17-én elutasította az ügy felülvizsgálatát, és ezzel végleg le is zárult a kérdés. Lessig szerint azért, mert „Ezen a területen, amióta világ a világ, az a szabály, hogy ha gyerekekről van szó, a kérdés nem igazán az, hogy a szabályozás túlságosan korlátozza-e a szólásszabadságot, hanem az, hogy a szabályozás nagyobb mértékben korlátoz-e, mint az szükséges volna... az egyetlen lényeges kérdés, vajon van-e kevésbé korlátozó módja ugyanazon – cenzúrát jelentő – cél elérésének. Ha nincs, a törvényt helybenhagyják."

A dolognak az a szépsége, hogy ugyanezen a héten tartották a meghallgatásokat a CDA-val kapcsolatban is.

Hoover: Aha, de akkor viszont a CDA-t sem volt okuk megsemmisíteni.

Vízi Patkány: Nem mondanám. A Legfelsőbb Bíróság a törvény egyes részeit 1997. június 26-án 7:2 arányban szólásszabadság-ellenesnek minősítette. A pert egyébként az általad nem különösebben kedvelt ACLU indította (és nyerte meg); a CDA viszont annak az Exon szenátornak a műremeke, aki annak idején olyan lelkesen búj ta (és idézte) Rimm műveit.

Stewart Dalzell bíró azt írta állásfoglalásában, hogy amennyiben meg akarjuk védeni a szólásszabadságot a digitális világban (is), akkor mindenáron kerülni kell a tartalom alapú szabályozást. „Ugyanis bármilyen ilyen kísérlet – függetlenül attól, hogy mennyire nemes céljaink vannak – porig égetheti a globális falut".

Ezen a ponton egyértelműnek tűnt, hogy az ügynek nem lesz folytatása, és David Sobel az EPIC-től meglehetősen optimistán ki is jelentette, hogy „úgy látom, hogy a jövőben vajmi kevés lehetőség fog nyílni az internet (túl)szabályozására".

Hoover: Akkor magyarázd már meg, kérlek, hogy miért döntött így a Legfelsőbb Bíróság! Azok alapján, amit Lessig mondott, nem tűnik éppen logikusnak.

Vízi Patkány: A fentebb említett ACLU vs. Reno perben a szólásszabadság hívei arról győzték meg a bíróságot (megint csak Lessig szerint „megkérdőjelezhető aktivizmussal" és persze átütő sikerrel), hogy egyelőre várni kell „az állam mint csendőr" nevű csodafegyver bevetésével: a piac, a szülők vagy valami más úgyis meggátolja majd, hogy a gyerekek pornográf anyagokhoz jussanak a világhálón, és a végén minden jóra fordul. Pontosan, mint a mesében.

Hoover: Hmmm. Ha jól értem, akkor kétféle megoldás lenne elképzelhető: vagy egy megfelelő törvény (az állam részéről), vagy az úgynevezett egyéni szűrés (a szülők, iskolák, könyvtárak stb. részéről). Tulajdonképpen az utóbbi ellen sem lenne kifogásom.

Vízi Patkány: Neked talán nem, a valóságban azonban a filterezés legalább ugyanolyan súlyos problémákhoz vezet, mint egy rossz törvény, és csúnyán vissza is lehet vele élni. És alkalmasint még arra sincs szükség, hogy az állam vezessen be mindenféle ostoba szűrési előírást – már maga az a tény, hogy filterezni tudunk, majdhogynem végzetes lehet. Cass Sunstein szerint...

Hoover: Fogadjunk, hogy már megint egy amerikai alkotmányjogász!

Vízi Patkány: Az hát. Szerinte a modern demokráciák a közszolgálati funkciót ellátó hírforrások nélkül működésképtelenné válnának, mivel szükség van rá, hogy az emberek időnként olyan információkhoz is hozzájussanak, amikre maguktól nem keresnének rá – és amikről nem is gondolnák, hogy léteznek egyáltalán. Amikor végignyálazzuk kedvenc napilapunkat, éppen ez történik és az valószínűleg nagyjából még az elviselhető mértékű filterezés kategóriájába tartozik, hogy (politikai ízlésünknek megfelelően végezve az „előszűrést") vagy jobb-, vagy baloldali lapokat olvasunk.

Továbbá az sem mellékes, hogy ezek a „közszolgálati hírforrások" biztosítják azokat a „közös tapasztalatokat", amelyek mintegy ragasztóanyagként tartják össze a társadalmat. Mert ugye ha nincsenek közös információink és élményeink, akkor miről is beszélnénk a másikkal – és persze az is problémát jelent, hogy az emberek lehetőleg inkább elkerülik az ellentétes nézetekkel való szembesülést ahelyett, hogy újra átgondolnák sajátjukat. „Amikor oly sokféle vélemény áll a rendelkezésünkre, akkor sokan fogják azt a megoldást választani, hogy csak a nekik tetsző hangokra figyeljenek", mondja Sunstein. A reklámpszichológiában közhelynek számít, hogy miután megvettünk egy meghatározott típusú autót, gyakrabban és szívesebben nézzük meg a vele kapcsolatos hirdetéseket – ugyanis a hirdetés azt sugallja, hogy milyen jól választottunk.

Ez a folyamat természetesen nem az internettel kezdődött. Most, a 21. sz. elején például elviselhetetlenül sok televíziós csatorna van, és ezért a legnépszerűbb amerikai televíziós showt ma kevesebben nézik, mint ahányan az 1970-es évek tizenötödik helyezettjét nézték... Ha valaha attól féltünk, hogy a polgárokat „az információ szűkössége" fenyegeti, akkor mostanra visszájára fordult a tendencia, és Hollywood-ra évente 300 ezer (!) kéretlen forgatókönyv zúdul (és a témák között szinte bármi előfordul a golfozó Jézusig bezárólag); Nagy-Britanniában pedig évente 50 ezer új könyvet adnak ki.

Szerző: Gondolom, ezért is szokás előírni, hogy a kereskedelmi csatornák is ennyi vagy annyi közszolgálatiságot kötelesek felmutatni. Mármint azért, hogy mindenki hozzájusson ezekhez a közösséget összetartó alapinformációkhoz.

Hoover: Jól értem, hogy az internet állítólagos szabadsága éppen a szabadság ellen dolgozik? Másfelől meg ha – pusztán a játék kedvéért – elfogadjuk egy pillanatra, hogy a közszolgálati média és a demokrácia elválaszthatatlanok egymástól; illetve ha azt is hozzátesszük, hogy a közszolgálati média tipikusan 20. sz.-i jelenség volt, akkor legalábbis kíváncsi vagyok, hogy a 21. sz. is a demokrácia kora lesz-e.

Vízi Patkány: Pedig nagy baj lenne, ha nem. Egy Amartya Sen nevű közgazdász körüljárta kissé a kérdést, és arra a következtetésre jutott, hogy a történelem során egyetlen, szabad választásokon és szabad sajtón alapuló rendszerben sem volt éhínség. Ha kissé jobban belegondolsz, te is rá fogsz jönni, hogy miért: „az éhínség szociális produktum, nem pedig élelemhiány", mondja Sunstein, és így a demokratikusan megválasztott (és hasonlóképpen demokratikusan leváltható) kormányra a szólás- és sajtószabadságnak köszönhetően kellőképpen nagy nyomás fog nehezedni, ha baj van. Vagyis „a szólás- és sajtószabadság nem csupán a művelt osztályok luxusa, ugyanis növeli annak az esélyét, hogy a kormányok az emberek érdekében lépjenek fel."

Szerző: Tehát csak csínján a tartalomhoz való hozzáférés szabályozásával, ha jót akarunk.

Vízi Patkány: Igen. A Sunstein-féle önfilterezési problémára pedig az lehet a megoldás, ha nem abból indulunk ki, hogy a technikai lehetőségek miatt felvetődő problémákra feltétlenül és kizárólag technikai választ kell adni. Jelen esetben legalább ugyanolyan fontos lenne már az általános iskolában megtanítani a jövő e-állampolgárainak nem csak azt, hogy hová kattintsanak, ha le akarnak tölteni valamit, hanem azt is, hogy miként éljenek egy, a

korábbitól tökéletesen különböző világban. Akár azt is mondhatnám, hogy olyan ez, mint a szavazás: ha az emberek nem mennének el, akkor nem működne a demokrácia. Amikor az Amerikai Egyesült Államok létrehozásakor Benjamin Franklin kijött a Convention Hallból, akkor az épület előtt várakozó tömeg egy tagja azt kérdezte tőle, hogy „Mit adtok nekünk?"; ő pedig azt válaszolta, hogy „Köztársaságot – ha meg tudjátok őrizni."

Sunstein ehhez azt teszi hozzá, hogy „egy alkotmány szövege valószínűleg jóval kevésbé fontos, ha a köztársaság fennmaradásáról van szó, mint az állampolgárok cselekedetei".

Hoover: Kivételesen majdhogynem egyetértek veled – azzal a megszorítással, hogy szerintem a kizárólag a pornográfia-ellenes (de minden más online tartalmat békén hagyó) filterezés azért nagyon is járható út. Felteszünk egy megfelelő szoftvert egy iskolában vagy egy könyvtárban (meg persze otthon is), és már kész is vagyunk. Mert máskülönben... hadd mondjak néhány adatot.

2000. szeptemberében 3 millió, 17 évesnél fiatalabb amerikai keresett fel pornó site-okat; 21,2 százalékuk 14 éves sem volt, és ugyanebben az évben 200 ezerre becsülték az amerikai internetpornó-függők számát, miközben 1999-ben azt mutatták ki, hogy az internetező tinédzserek több mint fele látogatott már meg pornográf, gyűlöletre uszító stb. weblapot, és...

Vízi Patkány: Ne is folytassad, hiszen már megbeszéltük. Én sem azt mondom, hogy nem kell valamit tenni, hanem azt, hogy a filterezés két okból sem működik. Az egyik az, hogy a technika nem elég fejlett hozzá: a Cybersitter nevű filterszoftver például azt a mondatot, hogy „Clinton elnök ellenzi a homoszexuális házasságot", úgy alakítja át, hogy „Clinton elnök ellenzi a házasságot", és ez ugye azért meglehetősen otromba ferdítés... Egy másik vizsgálat során pedig olyan filtert találtak, ami a „Pen is Mightier" (a toll erősebb) című weblapot azért szűrte ki, mert a „pen is"-t pénisznek olvasta.

De vannak statisztikai adataink is. Az Electronic Frontier Foundation (EFF) és az Online Policy Group (OPG) a két legelterjedtebben használt filterprogramot, a N2H2 Besst meg a SurfControlt használva és közel egymillió weblap átvizsgálása után jutott arra a következtetésre 2002-ben, hogy ha egy iskola ilyet tesz fel a gépeire, akkor még abban az esetben is meggátolja, hogy a diákok több tízezer hasznos oldalhoz hozzáférjenek, ha a lehető legkevésbé szigorú beállításokat választja. Vagy azért, mert az adott hely rosszul van besorolva – vagy pedig azért, mert a besorolás ugyan helyes, de a besoroláshoz indokolatlanul tartozik tiltás.

Hoover: Ez talán nem is olyan nagy ár a gyerekek biztonságáért.

Vízi Patkány: Lehet. De kissé mintha megváltozna a helyzet, ha az internetet oktatási eszköznek akarod tekinteni. A lehető „legmegengedőbb" beállítások esetében az államilag előírt tananyaggal kapcsolatos keresési eredmények 0,5 – 5 százaléka blokkolódik – a lehető legszigorúbb beállításoknál pedig akár a 70 százaléka is. Egy keleti parti iskolában az N2H2 Bess az alábbi, határozottan abszurd blokkolási arányokat mutatta:

- tűzfegyverek: a keresési eredmények 50 százaléka blokkolva
- ittas vezetés, rabszolgaság, genocidium, hamis tanúzás: 33 százalék blokkolva
- rokon- és ellenszenvek: 32 százalék blokkolva
- rövid versek írása vagy diktálása: 32 százalék blokkolva
- fogantyúval és lábtámasszal ellátott, alul rugós bot ugráláshoz (pogo-stick): 46 százalék blokkolva

„A populisták politikai programjának és tevékenységének vizsgálata": 100 százalék blokkolva...

Úgyhogy még olyan szólásszabadság-védők is akadnak, akik szerint az lenne az üdvözítő megoldás, ha kizárólag a kormányzat írhatná elő, hogy mit lehet kifilterezni és mit nem.

Hoover: Azt hiszem, kezdem elveszíteni a fonalat.

Vízi Patkány: Pedig nem is olyan bonyolult. A becslések szerint jelenleg a blokkolt site-ok mintegy fele van rosszul besorolva (és kerül emiatt tiltólistára). Ha a kormány kifilterezne egy site-ot, akkor ezt a döntést bíróság előtt lehetne megtámadni (és meg lehetne győződni róla, hogy nem megy-e túl a tiltás az alkotmányosság határain) – egy magáncég esetében azonban nincs ilyen jogorvoslati lehetőség. Azt vesznek fel a tiltólistájukra, amit nem szégyellnek, a napvilágra kerülő tévedések miatt pedig csak a vállukat vonogatják – amúgy pedig üzleti titokra hivatkozva semmit sem árulnak el. Ez elég meggyőző érv, gondolom.

Hoover: Ha jobban belegondolok, egyáltalán nem az. Az EFF ugyanis nyilvánvalóan filterezésellenes, és közelről sem lehet elfogulatlannak nevezni.

Vízi Patkány: Nehéz lenne ugyanezt ráfogni a Henry J. Kaiser Family Foundationre, ami a felmérése eredményeit a Journal of the American Medical Associationben jelentette meg, és ami arra hívja fel a figyelmet, hogy a legtöbb filterprogram szemrebbenés nélkül blokkolja az olyan kifejezéseket, mint például „biztonságos szex", „koton", „abortusz", „homoszexuális", „leszbikus" – márpedig ezek az esetek túlnyomó részében az egészségügyi site-okon fordulnak elő, nem pedig a pornóoldalakon. Ráadásul az is kiderült, hogy a leglazább beállítások mellett az egészségügyi site-ok 1,4, míg a legszigorúbb beállításoknál közel 25 százalékuk válik hozzáférhetetlenné. A leginkább persze akkor, ha a „biztonságos szex"-szel foglalkoznak (megengedő konfiguráció mellett 9, szigorúnál mintegy 50 százalékuk); és az erkölcsvédelemnek áldozatul estek például az American Medical Association női kérdésekkel, valamint a Food and Drug Administrationnek a hererákkal kapcsolatos beszámolóját tartalmazó weblapjai is. Meg egy, a diabéteszes gyerekekkel foglalkozó website; egy on-line kotonáruház; egy homoszexuálisok és leszbikusok betegségeivel foglalkozó oldal; a Columbia Encyclopedia születésszabályozással foglalkozó szócikke; a tinédzserterhességek elleni kampány weblapja – lényegében minden, amit el tudunk képzelni.

Amennyiben pedig azt is megemlítjük, hogy a pornográfiaszűrés hatékonysága nem sokat változik: a minimálistól a maximális erősség felé haladva 87-ről 91 százalékra nő, akkor azt hiszem, van min elgondolkodnunk.

Hoover: Például azon, hogy ez csupán azt mutatja, hogy a jelenlegi szoftverek nem eléggé hatékonyak, és kezdem belátni, hogy mégiscsak igaza volt a Legfelsőbb Bíróságnak, amikor azt mondta, hogy akkor várjunk egy kicsit a filterezéssel. De közben azért arról se feledkezzünk el, hogy miközben teljesen odáig vagyunk, hogy a szűrőprogramok meggátolják a diákokat bizonyos információkhoz való hozzáférésben, aközben nem is ezek jelentik a legnagyobb akadályt. Ma már a Google nevű kereső például ki szokta javítani a hibásan bepötyögött szavakat – ugyanis az amerikai fiatalok nem tudnak helyesen írni, és máskülönben nem lennének képesek megtalálni az őket érdeklő dolgokat.

Vízi Patkány: Nem mondhatnám, hogy meggyőztél, Hoover. Még ha lenne is tökéletesen működő filterprogramunk, arra a kérdésre, hogy miként állítsuk be, és mit szűrjünk ki vele, mindenképpen nekünk kellene válaszolni. Azaz ismét csak nem – vagy nem csupán – technikai kérdésről van szó. A National Research Council (NRC) Fiatalok, Pornográfia, Internet című tanulmánya szerint „nincs egyetlen vagy egyszerű ellenőrzési módszer arra, hogy elérjük: a kiskorúak kizárólag (a számukra is) megfelelő tartalmakhoz férjenek hozzá a weben... Az egyoldalú megközelítés nem működik: önmagában sem a technikai megoldások, sem a törvényi vagy gazdasági szabályozások, sem az oktatási módszerek megváltoztatása nem lehet hatásos." Ezért is jegyzi meg a kötet egyik szerkesztője, Richard Thornburgh, hogy

a konklúzió „csalódást fog okozni azok számára, akik valamiféle technológiai ‘gyors megoldásra’ számítottak az internetes pornográfia kihívásaival szemben.”

Az egyik, a kötet összeállításában részt vevő jogász, Bob Corn-Revere, pedig azt is hozzáteszi, hogy „Az a probléma ezzel a témával, hogy a tipikus kongresszusi reakció az, hogy előbb lőnek, és csak aztán kérdeznek”, vagyis nekiállnak túlszabályozni, és csak utána gondolkodnak el. Pedig „A tanulmányból... annyi (mindenképpen) kiderül, hogy nem indokoltak a nagyon heves reakciók”.

Talán mondanom sem kell, hogy nem az egyik (a szólásszabadság-védők) vagy másik oldal (a harcos pornográfiaellenzők) híveinek a képviseletéről van itt szó. Herbert Lin, a kötet társszerkesztője felhívja rá a figyelmet, hogy a bizottság sem tudott megállapodásra jutni azzal kapcsolatban, hogy valójában mennyire káros a kiskorúakra nézve a pornográfia. Ami persze nem is csoda, hiszen maga a „pornográfia” sem jól definiált, és egyeseknek mást jelent, mint másoknak. Mint ahogy egyébként ebben az esetben a „védelem” (mármint a kiskorúak védelme) jelentése sincs rendesen meghatározva; és ebből a szempontból meglehetősen homályosnak tűnik a „kiskorú” fogalma is, hiszen más lehet jó (vagy nem jó) egy hat meg egy tizenhat éves számára. Úgyhogy legfeljebb abban lehetünk biztosak, hogy ha ennyire bizonytalanok a fogalmak, akkor meglehetősen nehéz bármiről is érdemben vitázni.

Hoover: Meg egy-két más dologban is. Így például abban, hogy az Első Kiegészítés nem védi az obszcenitást, amit úgy szokás definiálni, hogy „olyan, szexuálisan explicit anyag, ami bizonyos, meghatározott módokon sérti a kortárs társadalmi normákat...” Jut eszembe, Vízi Patkány, ebből már levezethető, hogy nem volt indokolt a régebben pornográfia vádjával betiltott könyvekre hivatkoznod az előbb (hiszen az ízlés és a társadalmi norma nagyon is változó).

Ugyancsak nem védi az Első Kiegészítés a gyermekpornográfiát, vagyis azt sem, amikor gyerekek szerepelnek szexuális aktus közben, vagy szeméremsértő módon teszik közszemlére a genitáliáikat. A harmadik kategória pedig az a nem obszcén és nem gyermekpornográf anyag, ami viszont obszcén lenne a kiskorúak számára – tehát számukra szabályozni kell a hozzáférést, a felnőttek számára viszont nem.

Vízi Patkány: Ugye nem volt a közelben logikatudós, amikor ezt a jogászok kiötlötték? Szerintem ez a „sérti a társadalmi normákat” túlságosan megfoghatatlan. Inkább arra kellene koncentrálni, hogy kizárólag akkor szabad korlátozni, ha nincs más megoldás.

Hoover: Értelek én: most lényegében a „clear and present danger” elvére akarsz hivatkozni, mely szerint a szólásszabadság csak akkor nyirbálható meg, ha máskülönben világos és közvetlen veszélyre kellene számítanunk (a Szerző kedvéért, aki nem amerikai, hanem európai, a szólásszabadság helyett mondjuk inkább úgy, hogy véleménynyilvánítási szabadság, hogy jobban értse). Háborús időkben sem tilthatjuk meg, hogy valaki kritizálja a kormányt – azt viszont igen, hogy a háború ellen uszítson, mint ahogy Charles T. Schenk is tett 1917-ben, amikor pacifista röplapokat osztogatott a katonáknak – aztán a bíróság előtt arra hivatkozott, hogy az Első Kiegészítés védi a szólásszabadsághoz való jogát.

Vízi Patkány: Pontosan. A bíróság pedig úgy döntött, hogy Schenk tevékenysége világos és jelenvaló veszélyt jelentett az államra nézve, és az azért mégiscsak túlzás, hogy a szólásszabadságra hivatkozva megengedjük ezt. Oliver Wendell Holmes úgy fogalmazott a Legfelsőbb Bíróságon, hogy „A szólásszabadság legszigorúbb védelme sem védi meg azt, aki minden ok nélkül tüzet kiált egy színházban, és ezzel pánikot okoz”, aminek a következtében az emberek eltaposják egymást. Vagyis: „Minden esetben az a kérdés, hogy az adott körülmények között használt szavak... olyan világos és közvetlen veszélyhez vezetnek-e, amit a Kongresszusnak joga van meggátolni.”

Hoover: Na, most belesétáltál a csapdámba, Vízi Patkány! Az általad olyannyira kedvelt Legfelsőbb Bíróság ugyanis 1991-ben kimondta, hogy az Első Kiegészítés nem védi az ahhoz való jogot, hogy egy nő meztelenül táncoljon egy Las Vegas-i kaszinó bárjában.

Vízi Patkány: Tényleg? És miért nem?

Hoover: A Stanford Egyetem jogászprofesszora, Gerald Gunther szerint „A bíróság azt mondta ki, hogy a közerkölcs győzedelmeskedik a kifejezéshez (és így a szólásszabadsághoz) való jogon". Az Első Kiegészítést ugyanis nem azért találták ki, hogy lehetővé tegye az unatkozó férfiak felizgatását – jó, hogy már nem amellett próbálunk érvelni, hogy a nyilvános helyen végzett önkielégítést is védi a szólásszabadság, mivel az is a véleménynyilvánítás egy formája... Ez a politikára és a társadalmi életre vonatkozik, nem pedig az erkölcstelenségre – ami adott esetben éppen olyan veszélyes lehet, mint Schenk röplapjai. Nem véletlen, hogy az Alkotmányt elfogadó amerikai tagállamok is büntették az istenkáromlást és/vagy a szentségtörést... és ez a tiltás ésszerű módon más területekre is kiterjedhet. Mármint ha komoly a veszély. És a pornográfia ellen küzdők szerint éppen ez a helyzet.

Amikor Reagan elnök létrehozta a Meese-bizottságot (ezt persze az USA 75. igazságügy-minisztere, Edwin Meese III vezette), annak egyik tagja, James C. Dobson arra hívta fel a figyelmet, hogy „a pornográfia terjesztői... aláássák és ledöntik országunk tartópilléreit. Meg kell állítanunk a rombolást, mielőtt minden a földdel lesz egyenlővé... egyetlen pillanatnyi vesztegetni való időnk sincs." Meese egy sajtótájékoztatón azt is elmondta, hogy 1970 óta „a pornográfia tartalma radikálisan megváltozott, és egyre nagyobb és nagyobb hangsúly van az extrém erőszakon." Vagyis jó okunk van minél... khmmm... keményebben fellépni a pornográfia ellen.

Vízi Patkány: És a cél érdekében a bizottság tagjai hajlandóak is voltak bármit megtenni, mint tudjuk. Meese megpróbálta leállítani a National Coalition Against Domestic Violence (Nemzeti Koalíció a Családon Belüli Erőszak Ellen) támogatását, mondván, hogy az a leszbikusok érdekeit képviseli. Az államügyész Henry Hudson a hozzá tartozó washingtoni megyében rendeletet bocsátott ki, mely szerint minden felnőtteket megcélzó „adult" boltot be kell záratni. Frederick Schauer jogászprofesszor (University of Michigan) amellett érvelt, hogy a pornográfiára azért nem érvényes az Első Kiegészítés, mert az nem beszéd (illetve kommunikáció), hanem kizárólag szexuális tevékenység. A jogász Park Elliott Dietz (University of Virginia) vendégelőadó volt az FBI Akadémián és bizonyosra vette, hogy a „deviáns" képek előtt történő maszturbálás erősíti a devianciára való hajlamot (ha ugyan nem ez a deviancia kiváltó oka). Diane D. Cusack pedig az arizonai Scottsdale polgármester-helyetteseként arra szólította fel az embereket, hogy fényképezzék le a felnőtt mozikból kijövőket, illetve autóik rendszámtábláját, és juttassák el ezeket a „bizonyítékokat" a rendőrségnek.

Meg vagyok róla győződve, hogy Thurgood Marshall alkotmánybírónak volt igaza, amikor 1969-ben kijelentette, hogy „ha az Első Kiegészítés jelent egyáltalán valamit, akkor azt jelenti, hogy az állam nem mondhatja meg senkinek, hogy mit olvasson, miközben egyedül van otthon."

Hoover: Szép gondolat – kár, hogy kétszeresen is nem igaz. Az internet esetében nyilván-valóan nem; de amúgy általában, a pornográfia speciális válfajára, a gyermekpornográfiára nézve sem.

Ami az előbbit illeti, a pornó site-oknál általános gyakorlat, hogy hitelkártya-számot kérnek a bejelentkezőtől. Ám az American Savings Education Council felmérése már 1999-ben azt mutatta ki, hogy a 16-22 év közötti fiatalok 28 százaléka rendelkezik ilyen plasztik-lapocskával – és ez a tendencia azóta csak tovább erősödött, mert a hitelkártya-cégek így

kívánnak részesedni az on-line kereskedelem bevételeiből (ami a Jupiter Research becslése szerint évi 4,8 milliárd dollárt fog kitenni 2006-ban). Akadtak persze más, hasonlóképpen kudarcra ítélt szűrési kísérletek is: a Leisure Suit Larry nevű, „felnőttjátékokat" kínáló site például néhány évvel ezelőtt az első belépéskor a közelmúlt történelmével kapcsolatos kérdéseket tett fel, hogy ellenőrizze a látogató életkorát (például: „Ki az a Spiro Agnew?"), de aztán hamar kiderült, hogy az IQ (és persze a hitelkártya-birtoklás) sem áll közvetlen korrelációban az életkorral.

Szerző: Tényleg, ki az a Spiro Agnew?

Hoover: 1969 és 1973 között Amerika 39. elnökhelyettese, aki többek között arról a kijelentéséről ismert, mely szerint a vietnami háború ellenzői „roskatag sznobok pimasz hordájaként" jellemezhetőek, de most foglalkozzunk inkább azzal, hogy a fentebbiekből még a szólásszabadság legelvakultabb hívei számára is ki kell derülnie, hogy ez az az eset, amikor az államnak igenis be kell avatkoznia az internet működésébe a kiskorúak védelmében, és ebből a szempontból tökéletesen érthető, ha például az iskoláktól és a könyvtáraktól megköveteli, hogy filterszoftvert használjanak. Hiszen egyelőre nincs jobb, és a „majd meglátjuk, talán egyszer" talán megfelel a Legfelsőbb Bíróság szája ízének, de akinek a gyerekeit kell felnevelnie, az nem várhat a végtelenségig. Arról nem is beszélve, hogy ha az állam adja a pénzt az Internethozzáférés biztosításához, akkor joga van megmondani, hogy milyen tartalmak legyenek – és milyenek ne legyenek – hozzáférhetőek.

Vízi Patkány: Ez túlzott egyszerűsítés, Hoover. A kérdés az, hogy a könyvtár nyilvános fórumnak tekintendő-e, ahol csupán a legnagyobb óvatossággal szabad korlátozni a szólásszabadságot (miként a könyvtárosok állítják), vagy „az a döntés, hogy a könyvtárak nem engednek hozzáférést a könyvtári gépeken keresztül a pornóanyagokhoz, nem a szólás-szabadsággal, hanem a könyvtár beszerzési stratégiájával hozható kapcsolatba" (miként az amerikai állam állítja).

Mert ez utóbbi esetben – hacsak meg nem követeljük, hogy pornókazettákat is szerezzenek be férfiolvasóik nagyobb örömére – nehéz lenne a szűrés ellen érvelni. Jan LaRue, a Concerned Women for America igazgatója pedig erre még egy lapáttal rátéve azt is hozzáteszi, hogy „A pornográfia nézegetéséhez nem fűződnek alkotmányos jogok és egy könyvtárnak semmi oka nem lehet rá, hogy hozzáférést biztosítson a 18 éven felülieknek szóló anyagokhoz az adófizetők pénzén."

Ez még nyitott kérdés, de előbb-utóbb majd csak állást foglal a Legfelsőbb Bíróság a könyvtári filterezést megkívánó CIPA-val (Children's Internet Protection Act) kapcsolatban, hiszen már most is foglalkozik vele, és az, hogy miként fog dönteni, már csak azért is roppant izgalmas, mert a jelek szerint az amerikai állam nagyon is tanulékony, ha az internet szabályozásáról van szó.

Szerző: Amennyiben?

Vízi Patkány: Hogy miért tanulékonyak? A megsemmisített CPA helyett már 1998-ban előálltak a COPA-val (ahol a COPA persze azt jelenti, hogy Child Online Protection Act), ami megtiltotta volna a „kiskorúakra káros" anyagok internetes, kereskedelmi célú forgalmazását, amennyiben ezekhez – így vagy úgy – a kiskorúak is hozzáférhetnek.

Hoover: Mondanod sem kell, hogy ezt is megsemmisítette valamelyik amerikai bíróság. És lefogadnám, hogy a szólásszabadság védelmére hivatkozva.

Vízi Patkány: Nyertél. Úgyhogy ezt követően jött a fentiekben már említett CIPA, ami nem próbálja meg frontális támadással „betiltani a pornográfiát", hanem csak megpróbálja nyilvános helyekről hozzáférhetetlenné tenni, és ami azt illeti, meglehetős sikerrel: míg 2001-

ben a Library Journal szerint a könyvtárak 31, addig egy évvel később már 43 százaléka használt filterszoftvert (és az iskolák mintegy háromnegyede). Nem mondanám, hogy egyszerű kérdés. És igazából a gyermekpornográfiáé sem olyan egyértelmű, mint gondolnánk.

Hoover: De hiszen megállapodtunk benne, hogy a gyermekpornográfia tilos!

Vízi Patkány: Meg hát. Csak hát abban nem állapodtunk meg, hogy mit is értünk a gyermekpornográfia alatt, és amikor megszületett a CPPA (Child Pornography Prevention Act), akkor ebben az volt olvasható, hogy a virtuális – vagy ha úgy jobban tetszik: „morphed" – gyermekpornográfia is tilos, vagyis tilos a „kiskorúnak látszó" vagy számítógéppel generált, valójában nem létező gyerekeket például szexuális aktus közben ábrázolni.

Hoover: Tökéletesen helyes álláspont, így ugyanis hatékonyabban lehet felvenni a küzdelmet azok ellen a pedofilok ellen, akik mind valódi, mind virtuális képeket felhasználnak vágyaik kielégítéséhez. Ennek az eljárásnak az a további előnye, hogy a virtuális gyermekpornó nem szolgáltat „üzemanyagot" annak a végtelenül mocskos pornóiparnak, ami aztán élő és valóban létező gyerekeket is beszippant. És végül azt se felejtsük el, amire Robert Flores, a National Law Center for Children and Families igazgatóhelyettese hívja fel a figyelmet, nevezetesen, hogy ma már nincs az a szakértő, aki teljes bizonyossággal el tudná különíteni a számítógéppel generált képeket a valóditól. Vagyis ha nem tiltjuk be a virtuális gyermekpornográfiát is, akkor lehetetlen lesz elítélni a pedofilokat (mint ahogy már volt is rá példa, hogy arra hivatkozva próbáltak kibújni a felelősségre vonás alól, hogy nem is „igazi" a kép).

Vízi Patkány: A pedofília szerintem is büntetendő – sőt, undorító – dolog. De nem az büntetendő, ha valaki élvezi az ilyen képek nézegetését, hanem az, ha gyerekeket kényszerít mindenféle mocskos dolgokra. Vagyis a pedofil képek nyilvánvalóan azért tiltottak, mert ezek előállításához élő gyerekeket kell „igénybe venni".

Szerző: Tehát, ha jól értelek, akkor nem maga a kép a bűncselekmény, hanem az, ahogyan eljutunk hozzá, és így a virtuális gyermekpornográfiát nem is lehet betiltani.

Vízi Patkány: Pontosan. Ráadásul veszélyes precedenst teremtene, ha elleneznék, hogy egyesek valóságban nem létező képeket generáljanak ahelyett, hogy illegális képeket szereznének be. Emellett – teszi hozzá a felnőttipart tömörítő Free Speech Coalition jogásza, John Feldmeier – a törvény betűjének értelmében nem csupán egyes filmekbe lehetne belekötni (mint például a Rómeó és Júliába vagy akár a Trafficbe), ahol felnőtt színészek játsszák el, hogy kiskorúak szerelmeskednek; de például a gyermekszerelmet ábrázoló antik vázákkal is gondok lennének...

Úgyhogy engem egyáltalán nem lepett meg, amikor a Legfelsőbb Bíróság 2002. április 16-án a fentebbiekkel összhangban a CPPA ellen ítélt, mondván, hogy az egyrészt túlságosan széleskörűen van megfogalmazva és a művészi alkotásokat is korlátozná; másfelől pedig – ismét csak a fentebbiek értelmében – semmi sem indokolja a virtuális gyermekpornográfia betiltását.

És az sem lepett meg, hogy a Kongresszus mégsem adta fel, és sürgősen előálltak a Child Obscenity and Pornography Prevention Act-tel (COPPA; ezt egyelőre nem fogadták el). Az új törvénytervezet megpróbálja kicselezni a Legfelsőbb Bíróságot, és miközben kiemelten tiltja a serdületlen gyermekek pornográf ábrázolását, aközben meghagyja a lehetőséget a vádlottnak, hogy bizonyítsa be a bíróság előtt, ha tudja, hogy csupán virtuális pedofíliáról van szó. Ami viszont legalábbis érdekes ötlet: mármint, hogy a vádlottnak kell bizonyítania az ártatlanságát.

Szerző: Várjunk csak egy pillanatra! A COPPA nem azt jelenti, hogy Children's Online Privacy Protection Act?

Vízi Patkány: Igen, valóban van egy másik COPPA is, ami azt tiltja meg, hogy 13 év alatti gyerekektől személyes adatokat gyűjtsünk szülői hozzájárulás nélkül... De vissza a pornográfiához, aminek amúgy majdnem a végére is értünk: már csak a Mark Foley képviselő nevéhez fűződő Child Modeling Exploitation Prevention Actet (CMEPA) kell megemlítenünk, ami nemes egyszerűséggel tiltottá tenné minden 17 éven aluli gyerek fényképének kereskedelmi célú forgalmazását. A hivatkozási alap az, hogy nem egy site kínál – úgy havi 40 dollár ellenében – hozzáférést nagyon is lengén öltözött, macijukkal nagyon is célzatosan játszó kislányok fényképeihez és videofelvételeihez. Az eredmény pedig az lenne (feltéve persze, hogy elfogadnák a CMEPA-t), hogy a fotósok nem adhatnak tovább kiskorúakat ábrázoló felvételeket és a reklámipar sem választhatna katalógusból gyerekképet egy termékéhez.

Jonathan Zittrain alkotmányjogász (Berkman Center, Harvard Law School) rögtön rá is mutatott, hogy az ötlet „alkotmányosan reménytelen", ugyanis 10 évre zárhatnák rács mögé azt, aki csupán egy gyerekfotót kínál megvételre vagy felhasználásra, és semmi mást.

A National Center for Missing and Exploited Childrennek és a hasonló szervezeteknek viszont nagyon is tetszik a dolog, mivel korábban ők hangoztatták, hogy be kellene tiltani ezeket a „gyerek modell" site-okat. És annyiban meg is tudom őket érteni, hogy valóban gyomorforgató 9-10 éves kislányokat olyan pózokban látni, mint a pornó site-ok modelljeit – csak éppen ők fel vannak öltözve, és nem simogatják magukat bizonyos helyeken. Csak majdnem...

Hoover: Még mindig nem győztél meg – szerintem a pornó igenis káros. Sőt rosszabb: akár veszélyes is lehet. Amikor azt vizsgálták, hogy milyen összefüggés van az Amerikai Egyesült Államokban a Playboy, a Hustler meg a hasonló magazinok árusítása és a nemi erőszak között, akkor azt találták, hogy Alaszka és Nevada volt az első mind ezek forgalmazásában, mind pedig az ilyenfajta bűncselekményekben.

Vízi Patkány: Úgy látszik, ez egy olyan terület, ahol mindenre van ellenpélda is. Amikor Dániában megszüntették a pornográf anyagok gyártásának és terjesztésének korlátozását, akkor – az erkölcsvédők várakozásaival ellentétben – éppen hogy csökkent az exhibicionizmus, a leskelődés, a gyerekek zaklatása, és így tovább (ami akár a virtuális pedofília melletti érv is lehetne). Azaz a pornográfia szabályozásának lazítása ebben az esetben inkább jótékony hatásúnak bizonyult.

Hoover: Az 1970-es évek elején a 25,000 dolláros költséggel forgatott Deep Throat százmilliós bevételt hozott készítőinek, miközben a Playboyban és a Penthouseban a szexuális erőszakot bemutató képek száma az ötszörösére nőtt. Arra pedig egészen egyszerűen megcáfolhatatlan kísérleti bizonyítékaink vannak, hogy az erőszakos pornográfia igenis erőszakosabbá teszi a férfiakat a nőkkel szemben.

Vízi Patkány: És ezt nem is vitatja senki, és abban is majdnem mindenki egyetért – gondolom –, hogy az erőszakos pornográfia nem kívánatos. De egy ilyen megállapítással ugyanúgy nem jutunk közelebb a megoldáshoz, mint ahogy annak idején az úgynevezett V-chip sem segített megoldani a „gyerekekre leselkedő erőszakos műsorok" problémáját.

Szerző: Pedig ezt legalább olyan komoly problémának szokás tekinteni, mint az internetes pornográfiát, amit sok fiatal szerint a felnőttek egyszerűen túllihegnek. Elvégre nagyobb valószínűsége van – mondják – annak, hogy csatornakattintgatás közben beleszaladnak egy brutális (és nagyon is naturálisan ábrázolt) gyilkosságba, mint annak, hogy „véletlenül" elkezdenek meztelen nőkről vagy egymással szeretkező férfiakról készült képeket nézegetni.

Vízi Patkány: Igen, a televízió legalább ugyanolyan problematikus, és ezért elsőre mintha még lett is volna valami a V-chip-ben (v mint violence, azaz erőszak): 1996-ban az újraválasztási kampány során Clinton arra szólította fel a Kongresszust, hogy az követelje meg az

új készülékekbe egy olyan elem beépítését, aminek a segítségével a szülők blokkolni tudnák a szerintük nem a gyerekeiknek való adásokat. Clinton úgy fogalmazott, hogy a V-chip lehetőséget biztosítana a szülőknek arra, hogy „több beleszólásuk legyen a gyerekeik (szellemi) fejlődésébe", és a Kongresszus 1996. februárjában el is fogadta az új törvényt.

Aztán szinte menetrendszerűen jött a Henry J. Kaiser Family Foundation, és egy 800 szülőn alapuló felmérés során kimutatta, hogy sokan nem is tudják, hogy V-chip van a televíziójukban (pedig 1999 óta minden 13 inchesnél nagyobb képernyőjű készülékben megtalálható, és a háztartások legalább 40 százaléka rendelkezik egy ilyennel). Ha pedig tudják, rendszerint akkor sem érdekli őket, mivel vagy annyira bíznak a gyerekük ízlésében, hogy soha ki sem próbálták (és az esetek közel kétharmadában ez a helyzet), vagy pedig úgyis jelen vannak, amikor az bekapcsolja a TV-t.

Mindent egybevetve: ez a tartalomfilterező kütyü nem igazán sokaknak kell, és az ACLU (igen, megint csak az ACLU) azt is hozzáteszi, hogy ezáltal az állam mintegy a szülő helyett döntene arról, hogy mit szabad nézni és mit nem. Meg azt is, hogy nem árt kesztyűs kézzel bánni a besorolásokkal: a Legfelsőbb Bíróság az 1968-as Interstate Circuit v. Dallas ügyben azt mondta ki, hogy alkotmányellenes egy filmet a „gyerekek számára nem megfelelőnek" minősíteni az alapján, hogy az „a brutalitást, a bűncselekményhez vezető erőszakot vagy a züllöttséget úgy írja le vagy mutatja be, hogy az bűn elkövetésére vagy a bűnre bátorítja és buzdítja" a gyerekeket. Az ilyen meghatározások ugyanis túlságosan általánosak és gyakorlatilag mindenre rá lehet őket húzni.

Szerző: Érdekes, 2002-ben fogadták el Magyarországon az új médiatörvényt, és ez bizony azt mondja, hogy „Azt a műsorszámot, amely alkalmas a kiskorúak fizikai, szellemi vagy erkölcsi fejődésének súlyosan kedvezőtlen befolyásolására, különösen azáltal, hogy pornográfiát vagy szélsőséges, illetve indokolatlan erőszakot tartalmaz, az V. kategóriába kell sorolni.... Az V. kategóriába sorolt műsorszám nem tehető közzé". Vagyis ez is kellőképpen általánosan fogalmaz ahhoz, hogy bármire rá lehessen húzni (gondolom, kellőképpen tetszene is az amerikai Legfelsőbb Bíróságnak).

De hogy még izgalmasabb legyen, az ORTT az új törvénnyel kapcsolatos határozatában arra hivatkozik, hogy a pornográfia a büntető törvénykönyv értelmében tiltottnak minősül – de a valóságban ez csak a gyermekpornográfiára igaz.

Vízi Patkány: Nem hinném, hogy ez a törvény akár Magyarországon is kiállná az alkotmányossági próbát. Mint ahogy sokak szerint ugyanez a helyzet a különböző pornófilterek alkalmazásával is: az internetjogász Jonathan D. Walllace például azt mondja, hogy a fitlerprogramok sem kevésbé és túlzóan és széleskörűen szűrnek, mint az a bizonyos, az 1968-as döntés által megsemmisített kategorizálás.

Szerző: Jó, jó, ez nem különösebben meglepő következtetés. De lassanként azért arra is kíváncsi lennék, hogy akkor szerinted mi a megoldás.

Vízi Patkány: Hát... én személy szerint hajlok arra, hogy az NRC azon következtetésével értsek egyet, hogy egy úszómedencébe igenis bele lehet fulladni. Tehát körülkeríthetjük; hozhatunk különféle rendelkezéseket, stb.; a legbiztosabb azonban, ha megtanítjuk a gyermekeinket úszni.

Hoover: Ez nagyon szép gondolat... sajnos azonban nem világos, hogy a gyakorlatban mit jelent.

Vízi Patkány: Rendben. Kissé konkrétabban fogalmazva: szerintem az állam, ha nagyon akarja, akkor megteheti ugyan, hogy a nyilvános helyekről (könyvtárak, iskolák) való internetezésnél nem engedi meg, hogy a gyerekek hozzáférjenek az internetes pornográfiához –

eközben azonban az érintett helyekre kell bíznia, hogy azok miként oldják meg a védelmet. Egy könyvtárban mondjuk, ahol egy könyvtáros állandóan ott sétál a számítógépek között, teljesen fölösleges más eszközöket is igénybe venni. De ha úgy gondolják, akkor filterezzenek nyugodtan; vagy tartsanak fenn elkülönített számítógépállomásokat a felnőtteknek és a gyerekeknek olyanokat, amiket az olvasó pulttól is ellenőrizni lehet.

Ez a filterezési szabadság – egyáltalán nem mellékes módon – azt is lehetővé tenné, hogy a különböző normákat elfogadó közösségek különböző szűréseket valósítsanak meg.

Hoover: És otthon?

Vízi Patkány: Ja, otthon? Hát mint eddig: bízzuk a szülőre! Elvégre eddig is az ő dolga volt, hogy ne hagyja elöl a pornóújságot, ha nem akarta, hogy a gyerek végiglapozza.

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 chicagoit 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 rendszámtábla-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 hálószobájába, 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 Citiben (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.

Vízi Patkány: 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 fókuszálnak 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 drogdealernek 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 enélkül 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 veszélymodell, 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 begyűjte-

nek 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 szemmeltartására 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 iratainkat 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 Nobeldíjas 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 beavatkozásellenesség 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 gyeremzéstől, 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 jogász-professzor (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 hasonlókért 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.

A terroristaellenes harc Maginot-vonala

A Szerző meséje: Az apagyilkos kivégzése

1752. március 2-án az apagyilkos Damiens-t kétkerekű kordén szállították az Église de Paris főkapuja elé, miközben két font súlyú, égő viaszfáklyát tartott a kezében. Ezt követően „a fenti kordén, a Gréve téren és az ott felállított vérpadon, mellbimbóit, karját, combját és lábait harapófogóval tépkedték, miközben azt a kést tartotta jobb kezében, mellyel az apagyilkosságot elkövette s azokat a testtájakat, hol a tüzes harapófogó éri majd, kéntűzzel égették, olvasztott ólomba, forró olajba, égő gyanta, viasz és kén közé vetették, majd testét négy ló (segítségével) felnégyelték, végtagjait és testét tűzzel emésztették, hamuját szétszórták a szélben."

Ami a felnégyelést illeti, írja a Gazette d' Amsterdam, „Ez az utolsó művelet igen sokáig tartott, mert a négy ló nem szokott a húzáshoz; négy helyett hatot-hatot kellett befogni, s mivel ez sem bizonyult elegendőnek, kénytelenek voltak feldarabolni szerencsétlen combjait, elvágni idegeit, fejszével széthasítani az izületeket..."

Bouton rendőrtiszt pedig a felnégyeléssel kapcsolatban arról számol be, hogy „Két-három próbálkozás után Samson hóhér és az, amelyik fogóval kínozta, kést húztak elő a zsebükből, s a combokat leválasztották a törzsről; a négy ló, nekifeszülve, magával ragadta a két combot, méghozzá először a jobb oldalit, utána a másikat; majd a hóhérok ugyanígy járta el a két karnál, a vállaknál, a hónaljaknál, a négy végtagnál; egészen a csontig kellett vágni a húst, s a lovak, erejüket megfeszítve, kiszakították először a jobb karját, aztán a másikat.

A négy végtagot összeszedvén, a gyóntatók odamentek, hogy beszéljenek vele, de a hóhéra azt mondta, hogy meghalt, habár az az igazság, hogy a két szememmel láttam, amint mozog, felle jár az állkapcsa, mintha beszélne. Az egyik hóhér elbeszélte, hogy nem sokkal utána, amikor a test törzsét felemelte, hogy a máglyára hajítsa, még életben volt." Egy másik forrás szerint...

Hoover: Na, most már elég! Ezt egyszerűen nem vagyok hajlandó tovább hallgatni!

Vízi Patkány: Én sem – bár vannak más álláspontok is. Miután 2001. szeptember 11-én terrortámadás érte az Amerikai Egyesült Államokat, akadtak, akik megpróbáltak a kínzások visszaállítása mellett érvelni – vagy legalább célozni rá, hogy tulajdonképpen megfontolandó a dolog. A Newsweek amúgy elfogulatlannak tartott kolumnistája, Jonathan Alter például úgy fogalmazott, hogy mostanában „még a liberálisokban is felmerül a kínzás (visszaállításának) gondolata", még ha nem is a gumicsővel való verésről van szó. Csak arról, hogy a terroristatámadással kapcsolatban holtpontra jutott nyomozásnak valamiképpen „kezdőlökést" kellene adni (és jónéhány baloldali értelmiség is egyetértett vele).

És hasonlóképpen: a Fox News Channelen Shepard Smith műsorvezető azt kérdezte, hogy joga van-e a végrehajtó szerveknek bármit, akár szörnyű dolgokat is megtenni, hogy kiderüljön, hogy ki a bűnös, majd azzal folytatta, hogy „Jon DuPure riportja következik. Önök döntenek." Mintha bizony ez olyan kérdés lenne, amiben dönteni kell.

Egy héttel korábban pedig a CNN Crossfire című műsorában a konzervatív kommentátor, Tucker Carlson egyenesen azt hangoztatta, hogy „a kínzás rossz dolog. De ne feledjük, hogy vannak ennél szörnyűbb dolgok is, és bizonyos körülmények között ez a lehetséges kisebbik rossz. Ugyanis más dolgok még inkább azok."

A történész Jay Winik eközben arról értekezett a Wall Street Journal október 23-i számában, hogy a Fülöp-szigeteki hatóságok hogyan kínozták meg a terrorista Abdul Hakim Muradot: eltörték a bordáit, lánccal verték, cigarettával égették stb., – és nem jutottak semmire. De ekkor néhány biztonsági szolgálatos eljátszotta, hogy a Moszadtól jött, és magukkal viszik, Murad mégiscsak megtört. Ezáltal sikerült meggátolni, hogy közel egy tucat kereskedelmi gépet megsemmisítsenek a terroristák, és eggyel a CIA virginiai központjára zuhanjanak. „Némelyekben felmerülhet a kérdés, hogy mi történt volna, ha Murad amerikai őrizetben van?", mondja Winik.

A Slate online magazinban Dahlia Lithwick még eggyel továbblépve pedig már egyenesen azt fejtegette, hogy „kétségtelenül hatékony módszer a terroristák és kapcsolataik megkínzása".

Hoover: Na, akkor pontosítsunk egy kicsit: Alter a későbbiekben például arra hívta fel a figyelmet, hogy attól, hogy valaki foglalkozik a kínzás visszaállításának gondolatával, nem feltétlenül támogatja azt („én a bírósági jóváhagyással beadott sodium pentothalt támogatom, nem pedig a bírósági engedéllyel végzett kínzást", jegyezte meg).

Vízi Patkány: A Fox News producere, Bill Shine viszont azt mondta, hogy az elfogott terroristák „csak ülnek és hallgatnak, pedig lehet, hogy olyan információk birtokában vannak, amelyek amerikai életeket menthetnének meg itthon és külföldön", úgyhogy nem csoda, ha az emberek azt kezdik latolgatni, hogy miként lehetne kiszedni belőlük mindent – „természetesen az alkotmányos jogok tiszteletben tartásával".

Hoover: Állj, állj! Ekkoriban az emberek a bároktól a családi vacsorákig mindenütt erről vitatkoztak, tehát legalábbis furcsa lett volna, ha nem vitatkoznak róla az újságírók is... az pedig az általad oly nagy tiszteletben tartott szólásszabadság indokolatlan korlátozása, ha nem hagyod, hogy ezt a témát boncolgassák. Különösen, hogy Michael Lewin amerikai filozófus-professzor már 1992-ben arról írt a Newsweekben, hogy „vannak olyan élethelyzetek, amikor a kínvallatás nemhogy megengedhető, hanem egyenesen erkölcsi szükségszerűség. Képzeljük el például, hogy egy terrorista Manhattan szigetén bombát rejtett el, amely július 4-én délben fog felrobbanni, hacsak... Tegyük fel, hogy a végzetes nap délelőttjén sikerül a terroristát elfogni, de ő – a merénylet érdekében a haláltól sem visszariadva – nem hajlandó felfedni a robbanószerkezet hollétét... Ha nincs más mód az ártatlan életek megmentésére, mint az, hogy az elkövetőt a létező legkínzóbb fájdalomnak vessük alá, vajon milyen érv szólhat a vallomás kikényszerítése ellen? Úgy gondolom, semmilyen... (de mindig vigyázni kell arra, hogy) csak nyilvánvalóan bűnösöket kínvallassunk és csak az ártatlanok védelmében, és a két kategória között húzódó határvonal maradjon mindig világos. A nyugati demokrácia útvesztésének veszélye persze akkor is fennáll, ha csak a közrend fenntartása érdekében okozunk testi fájdalmat."

A Harvard egyetem sztárjogásza, Alan M. Dershowitz a terroristatámadást követően elevenítette fel ezt az érvelést, és hogyha korábban úgy vélte, hogy még mindig jobb, ha inkább bűnösöket is futni hagyunk, mint az, ha ártatlanokat is lecsukunk...

Vízi Patkány: Egyesek szerint vitatható felfogás.

Hoover: Vitathatónak éppen vitatható. De most már Dershowitz kezdte másképp látni, és nem csupán amellett érvelt, hogy – tekintettel a bioterrorizmus veszélyeire – újra kellene gondolni a karanténtörvényeket; de amellett is, hogy a bíróságok adhassanak ki – eseti jelleggel – kínzási engedélyt. Elvégre olykor csak így tudhatjuk megvédeni az ártatlanok életét.

Na, erre mit lépsz, cimbora? Ez azért elég meggyőzőnek tűnik.

Vízi Patkány: Akkor kezdjük az elején: a szólásszabadsággal. Persze, hogy nem korlátozhatom a kínzásról folytatott vitákat – de ha ők megengedhetik maguknak, hogy ilyen ostoba és veszélyes dolgokat fejtegessenek, akkor nekem is jogom van rámutatni, hogy – miként Kenneth Roth (Human Rights Watch) is hangsúlyozza – a kínzással kicsikart vallomások gyakran hamisak, mivel a szerencsétlen áldozat végül már bármit megtenne csak azért, hogy megszabaduljon a gyötrelemtől.

Ami egyébként oda vezet, hogy értelmetlenné válik az egész, ugyanis nem az a cél, hogy az illető azt mondja, hogy „igen, bombát rejtettem el itt vagy ott", hanem az, hogy abban az esetben bírjuk rá a vallomásra, ha ez tényleg igaz. Hiszen ezáltal emberéleteket menthetünk meg.

Ráadásul a kínzástól egyenes út vezet a terrorhoz és a diktatúrához. Az Amnesty International példája szerint: „Valaki beismeri, hogy bombát rejtett el: a kínvallatás életeket menthet. Az illető gyanúsítható azzal, hogy bombát helyezett el: a kínvallatás igazolhatja a gyanút. Valakinek a barátja bomba elrejtésével gyanúsítható: a kínvallatás elvezethet bennünket a gyanúsítotthoz. Az illető veszélyes nézeteket vall, és nem kizárt, hogy megfordult a fejében egy robbantásos merénylet gondolata: a kínvallatás felfedi gonosz terveit. Valaki ismer valakit, aki veszélyes nézeteket vall, és akár még a fenti gondolat sem áll tőle távol: a kínvallatás egy egész lehetséges elkövetői kört fedhet fel. Az illető megtagadja, hogy a gyanúsított hollétéről vallomást tegyen: a kínvallatás az ilyen elzárkózó magatartástól másokat már visszatartana", és így tovább, és így tovább, amíg csak azon nem kapjuk magunkat, hogy mindent ezt az egyetlen „eszközt" használva akarunk megoldani.

Hoover: akkor most hadd hívjam fel rá ismételten a figyelmedet, hogy kizárólag elméleti problémáról van szó. Az USA-ban nem állították vissza a kínvallatást – és nem is tervezik.

Vízi Patkány: És te olyan biztos vagy ebben, hogy ez tényleg kizárólag elméleti vita? Mert én nem: a Washington Post 2002. decemberében bizony arról számolt be, hogy az afganisztáni Bagram légi bázison olykor 24 órán keresztül folyamatosan vallatják a foglyokat, miközben vakítóan erős fényű lámpát irányítanak az arcukba (hátha majd megtörnek ettől); és az is elő szokott fordulni, hogy átadják őket a „megválaszolandó kérdések" listájával együtt egy olyan titkosszolgálatnak (mondjuk a jordániainak, az egyiptominak vagy a marokkóinak), ami brutális módszereiről közismert. És ebből nagyon is jól látszik, hogy mennyire megváltozott szeptember 11. után a hozzáállás... és ez milyen durva, sőt, embertelen túlkapásokhoz vezethet. „Nem verjük ki belőlük a ****t . Ehelyett olyan országokba küldjük őket, ahol az ottaniak kiverik belőlük", nyilatkozta az egyik névtelenséget kérő illetékes.

Hoover: Akkor én is egy neve elhallgatását kérő illetékesre hivatkozom, aki úgy fogalmazott, hogy „ha időnként nem sértjük meg valakinek az emberi jogait, akkor nem tudjuk végrehajtani a feladatunkat" – ugyanis máskülönben képtelenség kiszedni az igazságot a foglyokból.

Emellett azt is tudomásul kell vennünk, hogy a válsághelyzet nem különösebben alkalmas az emberi jogok tiszteletben tartására.

Vízi Patkány: Hogyhogy?

Hoover: Ha ebből a szempontból nézed végig az amerikai történelmet, rögtön be fogod látni, hogy igazam van. Amennyiben választani kellett a biztonság és a szabadság között, akkor az amerikai elnökök – legyen szó bár John Adamsról, Abraham Lincolnról, Woodrow Wilsonról vagy Franklin Rooseveltről – mindig is az előbbit választották. Az 1790-es évek végén, amikor mindenki egy lehetséges francia támadástól rettegett, elfogadták az Alien and Sedition Acts-et: ez lehetővé tette, hogy gyakorlatilag bárkit lecsukjanak, aki nem ért egyet a kormány álláspontjával; Lincoln válogatás nélkül zárt börtönbe köztiszteletben álló polgárokat,

jogászokat, gondolkodókat, csak mert ellenezték a háborút. Állítólag összesen 13,535 embert, és a legtöbbjüknek maximum az volt a bűne, hogy a déliekkel szimpatizált.

És ez még közelről sem minden.

1918-ban a háborúra hivatkozva elfogadták a Sabotage and Sedition Acts-et, és ennek már végképp nem sok köze volt a szólásszabadsághoz: bárki rács mögött találhatta magát, ha profán vagy „hűtlen" módon nyilvánult meg. Végül pedig ott van Roosevelt, aki a II. Világháború kezdetén habozás nélkül aláírta a japán származásúak deportálásáról rendelkező Executive Order 9066-ot... és ez 110,000 ember kitelepítését jelentette.

Én ezt tulajdonképpen megnyugtatónak találom.

Vízi Patkány: A tömeges deportálásokat?

Hoover: Nem. Nem a deportálásokat, hanem azt, hogy akár azt is mondhatnám, hogy a demokrácia olyan, mint egy gumiszalag: időnként jól megfeszítik, de aztán úgyis visszaugrik az alaphelyzetbe, és minden megy tovább a maga útján. Winik említi, hogy az elnökök – talán Lincoln kivételével – olyankor hozták ezeket a döntéseket, amikor nem is fenyegetett közvetlen veszély, de végül mindig jóra fordult a dolog.

Most viszont még a közvetlen veszély is jelen van, úgyhogy minden korábbinál inkább szükség van a megszorító intézkedésekre – de azért nem kétlem, hogy idővel majd helyre áll a rend.

Vízi Patkány: Hacsak el nem szakad a demokrácia gumiszalagja, miként a nácik uralomra-jutásakor is történt. Mert azért az sem bír ki mindent.

Hoover: Én nem hasonlítanám a mostani helyzetet a náci hatalomátvételhez, Vízi Patkány!

Vízi Patkány: Én sem... csak arra akartam rámutatni, hogy az ilyesminek mindig fennáll a veszélye... és szerintem most jobban, mint az utóbbi évtizedekben bármikor.

És nem csak az Amerikai Egyesült Államokban, de Németországban vagy mondjuk Nagy-Britanniában, ahol egy, közvetlenül a WTC lerombolása után végzett felmérésből az derült ki, hogy miközben az IRA 30 évig tartó terrortámadásai hatására sem érezték a britek szükségét a pontosabb azonosítást lehetővé tevő személyi igazolvány bevezetésének, most a legtöbben támogatták volna – a privacyvel kapcsolatos kérdésekkel pedig egyszerűen nem foglalkoztak.

85 százalék nem csupán a fényképet, a szemszín feltüntetését és hasonlókat találta volna felettébb kívánatosnak, de az ujjlenyomat rögzítését is, és háromnegyedük szívesen ott látta volna a DNS-ujjlenyomatát is a személyiben, míg hozzávetőleg ugyanennyien a büntetett előéletet; kétharmaduk pedig a vallási hovatartozást is.

Szerző: Sokan gondolkoztak hasonlóképpen Magyarországon is. Az egyik legnagyobb tekintélyű liberális lap, a Magyar Hírlap a szeptember 12-i nyitólapon azt fejtegette, hogy „A szabad világ tegnap óta minden korábbinál élesebben gondol arra: meg kell védenie magát, és minden eszközzel harcolnia kell a terrorizmus ellen. Kényelmetlenebb élet lesz az, amely ma kezdődik, több ellenőrzéssel, kevesebb egyéni szabadságjoggal, kevesebb mozgástérrel. Mert a szabad világ rákényszerül, hogy minden eszközzel megvédje az emberek életét, mert ennél nagyobb érték nem létezhet."

Vízi Patkány: Az újságírókat olykor orvosilag tiltják el a gondolkodástól?

Hoover: Szerintem nagyon is logikus ez az érvelés. Hiszen nézzük csak, mi történt például a titkosítás esetében is: az amerikai kormány nagylelkűen megengedte, hogy mindenki a lehető legnagyobb biztonságban kommunikáljon – a terroristák pedig ezt kihasználva tudnak állandóan újabb és újabb akciókat szervezni... a Priceton Survey Research Associates 2001.

szeptember 13-14-i felmérése szerint az amerikai állampolgárok 72 százaléka értett egyet azzal a kijelentéssel, hogy egy titkosítást korlátozó törvény „valamiképpen" vagy „nagyon" hasznos lenne a terrorizmus elleni harcban (és csupán 9 százalék kételkedett abban, hogy a titkosítás szigorúbb kontrollja képes lenne meggátolni egy újabb szeptember 11-ét). Egy ilyen törvény azt mondaná ki, hogy a titkosító eszközöket olyan hátsó ajtóval (back door) kell ellátni, ami a végrehajtó szervek számára lehetővé teszi a hozzáférést bármilyen kódolt információhoz.

Vagyis az amerikaiak levonták a megfelelő következtetést. Meg a kormányok is: amikor Judd Gregg amerikai szenátor a titkosító szoftverek nemzetközi korlátozására szólított fel, akkor például Ausztrália is egyetértett ezzel.

Vízi Patkány: Valóban ez volt az egyik oldal álláspontja. A másik oldal – és így például Simon Davies – viszont arra hívta fel a figyelmet, hogy legalábbis vitatható eljárás sokkos állapotban lévő emberek vélekedése alapján ítéletet alkotni. És ugyanezt mondta Phil Zimmermann, a legelterjedtebb titkosító szoftver, a PGP (Pretty Good Privacy) megalkotója is; illetve azt, hogy „nem biztos, hogy a hátsó ajtók alkalmazása meggátolná az ilyen szörnyű terrorcselekményeket". Ráadásul, a titkosításnak elsősorban nem a terrorcselekmények lehetővé tételében, hanem a felhasználói privacy védelmében van szerepe (és arról sem szabad elfeledkezni, hogy segítséget nyújthat a politikai aktivistáknak és ellenállóknak az elnyomó rendszerek elleni küzdelemben).

Hoover: Vagyis ez nagyobb súllyal esik latba, mint az, ha ismét több ezer áldozata lesz egy terrortámadásnak?

Vízi Patkány: Már megint félreérted, Hoover. Amikor valaki amellett érvel – minként a szerző által felhozott példában szereplő magyar újságíró is –, hogy mivel a demokráciát ilyen méretű terrortámadás érte, ezért a demokratikus alapjogokat kell korlátozni, akkor az egyik legtipikusabb logikai hibát követi el.

Hoover: Éppen ellenkezőleg: a demokrácia túlságosan nagy mozgásteret engedett a demokráciaellenes erőknek, és ezen most változtatni kell. A World Trade Center megsemmisítése valószínűleg kellőképpen alátámasztja az érvelésemet.

Vízi Patkány: Ugyan már! Abból, hogy Amerika ellen ilyen méretű terrortámadást lehetett intézni, még nem következik (vagy hogy egészen pontos legyek: nem szükségszerűen következik), hogy ezt a demokratikus, az emberi jogokat messzemenően tiszteletben tartó társadalmi rend tette lehetővé.

Hoover: De hiszen demokrácia volt, amikor sor került az Al-Kaida akciójára. Nem nehéz párhuzamot vonni a két dolog között.

Vízi Patkány: Ezzel az erővel azt is kijelenthetném, hogy minden arra vezethető vissza, hogy... hogy mondjuk az USA-ban szélviharok szoktak pusztítani. Elvégre tény, hogy szélviharok szoktak pusztítani; és az is tény, hogy sor került a terrortámadásra. Vagyis: akár összefüggés is lehet a két dolog között.

Hoover: Ezt te sem gondolod komolyan.

Vízi Patkány: Nem hát. Mint ahogy te sem gondolhatod komolyan, hogy nem hasonlóan értelmetlen párhuzamba állításról van szó akkor is, amikor a demokratikus rendet teszed felelőssé a tragédiáért. Amennyire én tudom, még Hitler ellen is kíséreltek meg merényletet.

Hoover: Hát... ebből még mindig nem következik, hogy ne kellene a titkosítást szigorúbban ellenőrizni. Az ugyanis vitathatatlan, hogy nagyon is vissza tudnak vele élni a terroristák.

Vízi Patkány: Ez leginkább közönséges kriptoparanoia. Az USA illetékesei mindig is rettegtek attól, hogy az ellenség akár titkosítást is bevethet, és a II. Világháború alatt a United States Office of Censorship például megtiltotta az olyan virágküldemények továbbítását, amihez dátumot, keresztrejtvényt vagy akár csak egy rövid üdvözlőkártyát mellékeltek. Ami viszont közönséges rövidlátásra vall, mert...

Hoover: Gondolom, azt akarták meggátolni, hogy az ellenséges ügynökök így kommunikáljanak egymással.

Vízi Patkány: Azt hát. De közben mintha elfeledkeztek volna arról, hogy az ellenséges titkos ügynök a virágok számával, színével... vagy bármi mással is kódolhatja a titkos üzenetet. Tehát egyáltalán nem volt célravezető az amerikai kormányok magatartása, amikor a begubózást választották, és az 1970-es évek közepéig egyetlen titkosítási módszert tartottak elfogadhatónak: az olyat, amihez kizárólag ők férhetnek hozzá.

Amikor az újságíró David Kahn elhatározta, hogy könyvet jelentet meg a titkosítás történetéről, akkor az NSA-nak (National Securtiy Agency), a világ legnagyobb hatalmú titkos szervezetének a legmagasabb rangú vezetői napokon keresztül tipródtak rajta, hogy mit tegyenek. Próbálják valahogy megszerezni a copyright-jogokat, aztán süllyesszék el a kéziratot? Törjenek be Kahn lakására? Stb., stb. A szerencsétlen újságíró még az NSA által megfigyeltek listájára is rákerült, és attól kezdve az ügynökök lehallgathatták a telefonjait és elolvashatták a leveit.

Aztán persze úgyis megjelent a Codebreakers – és persze nem dőlt össze a világ. Viszont jellemző módon a következő nagy előrelépés sem a titkosszolgálati berkekből származott: két outsider, Whitfield Diffei és Martin Hellmann jött rá arra a ma kettős kulcsúnak nevezett módszerre, ami lehetővé teszi, hogy teljesen biztonságosan kommunikáljunk – méghozzá anélkül, hogy előtte találkoznunk kellene, és ki kellene cserélnünk a titkosító kódot. És végül ismét csak egy kívülálló, az előbb már emlegetett Phil Zimmermann volt az, aki megalkotta az első, széles körben elterjedt kettős kulcsú titkosító szoftvert, a Pretty Good Privacyt. Ezt 1991 júniusában egy segítőtársa laptopról, pénzbedobálós utcai telefonkészülékeken keresztül töltötte fel az elektronikus világ hirdetőtáblára, a BBS-ekre, hogy mindenki számára hozzáférhető legyen. Zimmermann jelmondata szerint „Ha törvényen kívül helyezzük a titkosítást, akkor csak a törvényen kívülieknek lesz titkosításuk."

Hoover: Ha jól emlékszem, bíróság elé is akarták állítani, mert megsértette az USA exporttörvényeit – amelyek egyébként lényegében ugyanúgy kezelték a titkosító programokat is, mint a különösen veszélyes fegyvereket.

Vízi Patkány: Igen, de végül nem csukták le. Sőt, megkapta a pozitív amerikai Nagy Testvér Díjat is a privacy védelmében kifejtett tevékenységéért. Ma azt mondanánk, hogy a jog is az ő oldalán volt: a titkosító eszközökkel kapcsolatos kiviteli korlátozásokról már 1978-ban megállapította az Igazságügyi Minisztérium felkérésére vizsgálódó jogász, John Harmon, hogy ezek „alkotmányellenesnek minősülnek... mivel korlátozzák a titkosítással kapcsolatos tudományos és matematikai eredmények terjesztését", és így nyilvánvalóan megsértik az Első Kiegészítést is.

Hoover: Túl azon, hogy azóta sokkal kevésbé szigorúak a törvények, akik nagyon akarták, azok mindig ki tudták játszani. 1995-ben az MIT, a világ egyik legrangosabb műszaki egyeteme például olyan könyvet adott ki, ami több száz oldalon keresztül semmi mást nem tartalmazott, mint C nyelven írt programkódot. Még a betűtípust is úgy választották meg hozzá, hogy a szkennerek és a karakterfelismerő programok a lehető legkönnyebben boldoguljanak vele. A hagyományos, nyomtatott könyvekre ugyanis nem terjedt ki a titkosító

szoftverekre érvényes tiltás és így a PGP-t – ebben a formában – törvényesen is lehetett exportálni.

Aminek persze az lett a következménye, hogy a világ legnagyobb PGP-használóivá pillanatokon belül a terroristák meg a maffiózók nőtték ki magukat.

Vízi Patkány: Ez nem egy olyan szellem, amit csak úgy vissza lehet gyömöszölni a palackba. John Young, a Cryptome.org fenntartója a titkosítás betiltásával kapcsolatban azt mondta annak idején, hogy a megfelelően biztonságos szoftvereket tükröző site-ok úgyis „multiplikálódni fognak, és elképzelhető, hogy az emberek elkezdik majd a titkosított szövegeket tartalmazó floppykat postán küldözgetni egymásnak, ha az interneten túlságosan erős lesz a megfigyelés." Röviden és tömören: nincs visszaút.

Hoover: Pedig én nagyon is jól el tudnám képzelni, hogy az erős titkosításba beépítünk egy „hátsó ajtót", amin keresztül a kormányügynökség szükség esetén mégis hozzáférhet az összes információhoz – miközben az a kívülállók számára továbbra is elérhetetlen marad. Több mint kínos volt, amikor csak úgy sikerült megszerezni a maffiózó Nicodemo S. Scarfo Jr. által tárolt adatokat, hogy „billentyűleütés-lehallgatót" telepítettek a számítógépére. Ugyanis Scarfo is PGP-t használt.

Vízi Patkány: És az is kínos volt, amikor kiderült, hogy kár volt annyira erőlködni. Ugyanis eléggé egyszerűen kitalálható titkosítási kulcsmondatot választott magának: azt, hogy NDS09813-050. Azaz jogerős büntetését töltő apja börtön-nyilvántartási számát...

Hoover: Rendben, elismerem, hogy ebben az esetben valóban lehettek volna egy kicsivel találékonyabbak a fiúk – de akkor mit lépsz az Afganisztánban talált számítógépekre?

Vízi Patkány: Mármint azokra, amiken a Wall Street Journal riporterei megtalálták az al-Kaida titkosított anyagait Kabul elfoglalása után?

Hoover: Pontosan. Ha ilyen jól emlékszel az esetre, akkor biztosan arra is emlékszel, hogy a titkosítást azért volt viszonylag könnyű feltörni, mert a Windows 2000-et futtató komputeren csupán 40 bites DES-t (Data Encryption Standard) használtak – méghozzá azért, mert a 2001. márciusáig érvényben lévő amerikai exportkorlátozások értelmében nem engedtek ennél jobbat külföldre vinni. Az összes lehetséges kombináció végigpróbálásához így alig öt nap is elég volt – de mint Brian Gladman brit titkosítási szakértő mondja, ha 56 bitesnél erősebb lett volna, akkor „gyakorlatilag lehetetlenné válik a dolog".

Vízi Patkány: Azt elfelejtetted megemlíteni, Hoover, hogy Gladman szerint ennek ellenére sem érdemes visszaállítani az exportkorlátozást. Elvégre a terroristáknak sokkal egyszerűbb megoldások is a rendelkezésére állnak: például megváltoztatott jelentésű szavakat használnak vagy egyszerűen elmennek egy internet-kávézóba, és onnan veszik fel egymással a kapcsolatot.

Úgyhogy a titkosítási korlátozásokat a beépített hátsó ajtókkal együtt a legjobb lesz gyorsan elfelejteni. Különösen, mivel az úgynevezett stratégiai célpontok megvédéséhez (mint amilyen például egy atomerőmű) szükség van a cybertér biztonságának növelésére is – és ez erős titkosítás nélkül bizony nem megy. Nem kisebb és a kormánynak nem kevésbé elkötelezett ember, mint Bill Crowell, az NSA volt igazgatóhelyettese mutatott rá, hogy „a titkosítás meggyengítése oda vezetne, hogy a nemzeti infrastruktúra kevésbé lesz biztonságos", és ezért döntött úgy végül az amerikai vezetés is, hogy nem építenek be semmiféle hátsó ajtót. Ahogy Bob Goodlatte kongresszusi képviselő mondta: „itt most nem a privacy versus biztonság, hanem a biztonság versus biztonság a kérdés."

James Lewis, (Center for Strategic and International Studies, Washington, D.C.) szerint miközben a back door hatására az amerikai gazdaság meggyengülne, aközben az összes terrorista meg a világ minden más országa átállna a nem az Újvilágból származó programok használatára. Az Al-Kaida pedig némi emberáldozatot sem sajnálna azért, hogy megszerezze a minden titkos zárat nyitó csodakulcsot... És akkor arról még nem is beszéltünk, hogy hány évig tartana, amíg minden törvénytisztelő állampolgár (és minden ilyen cég) áttérne az új szoftverekre.

Szóval teljes képtelenség az egész, és nem véletlen, hogy végül nem lett belőle semmi.

Hoover: Tulajdonképpen akár igazad is lehet... másfelől azonban ha az előbb azzal érveltél, hogy nem biztos, hogy a túlságosan nagy szabadság tette lehetővé a terrortámadást, akkor én most azzal érvelek, hogy az viszont biztos, hogy ha mindenkit megfelelően az ellenőrzésünk alatt tudunk tartani és állandóan nyomon tudunk követni... nos, akkor egészen biztosan könnyebb lesz a gazfickókat is elkapni. És éppen erre irányult Larry Ellison javaslata is.

Szerző: az Oracle-os Ellisonra gondolsz a digitális személyi igazolvány tervével, ugye?

Vízi Patkány: Akinek a CIA volt az első megrendelője; aki a cége nevét is egy CIA-s projekt nyomán választotta, és aki a világ legnagyobb adatbázis-gyártója?

Hoover: Persze, hogy rá. Ő mondta azt, hogy „nekünk, amerikaiaknak, olyan személyi igazolványra van szükségünk, mely a bedigitalizált fénykép mellett az ujjlenyomatunkat is tartalmazza. Emögött persze ott kell lennie az adatbázisnak, tehát amikor keresztülsétálok a repülőtér bejáratán, és azt mondom, hogy Larry Ellison vagyok, akkor a kártyát be kellene helyezni egy leolvasóba, és a rendszer ellenőrizné, hogy igazat beszéltem-e."

De az is elképzelhető lenne, hogy más biometrikus azonosítók (tenyérlenyomat, íriszmintázat, stb.) kerüljenek bele az adatbázisba. Maga a rendszer pedig „önkéntes" lenne ugyan, de ez csupán annyit jelent, hogy aki nem rendelkezik digitális személyi igazolvánnyal, az beszálláskor nagyon alapos és mindenre kiterjedő vizsgálatra számíthat majd.

Ja igen, és még valami: a nemzeti adatbázis össze lenne kapcsolva a már létező bűnügyi és bevándorlási adatbázisokkal is. „Úgy gondolom, hogy az amerikaiak 99,99 százaléka akarni fogja ezt az igazolványt", nyilatkozta egy interjúban Ellison, ez ugyanis minden korábbinál jobban segítene kiszűrni a terroristákat. Különösen, hogy azoknak a külföldieknek, akik jelenleg „zöld kártyával" tanulnak, vagy dolgoznak az USA-ban, kötelező lesz.

Vízi Patkány: De ez az egész privacy-szempontból... hogy is mondjam csak...

Hoover: Megint csak Ellisonra hivatkozom, aki szerint egy digitális világban egyszerűen illúzió privacyről beszélni, és „ezt az illúziót kell feladni, nem a privacyt. Ma már semmi akadálya nincs, hogy felmenjünk az internetre, megszerezzük a szomszédunk bankszámla-kimutatását; kiderítsük, hogy hol dolgozik és mennyit keres; hogy késett-e a jelzálog-kölcsön visszafizetésével, és még millió más dolgot". Ami azért nem is olyan nagyon nagy baj, mert rendszerint egy karóra megvásárlásakor is többet árulunk el magunkról, mint a repülőtéren.

Vízi Patkány: Nekem ez akkor sem szimpatikus.

Hoover: És ha most úgy fogalmaznánk át a kérdést, mint Ellison teszi? Ha biztonságban akarunk utazni és „van két repülőtársaságunk, A és B, és míg A-nál igazolnunk kell, hogy azok vagyunk, akiknek állítjuk magunkat, a B járatra viszont mindenki felszállhat, aki megvette a jegyet, akkor vajon melyiket választanánk?"

És különben is: megmondanád, hogy mi rossz van a személyi igazolványban, amit a világ rendkívül sok országában használnak már most is? Azt még Simon Davies is elismeri, hogy „nehéz olyan országot találni, ahol ne lenne ilyen".

Vízi Patkány: Már megint hibásan érvelsz, kedves Hoover.

Szerző: Bizony. Halmai Gábor magyar alkotmányjogász is megjegyzi, hogy „Az a tény, hogy egy jogintézményt a nemzetek többsége és a nemzetközi jog is elvet, önmagában még nem teszi elfogadhatatlanná egy adott ország alkotmányos rendszere szempontjából". Ez visszafelé is igaz: attól, hogy valamit sok helyen csinálnak, az még nem válik automatikusan legitimmé.

Vízi Patkány: Az USA-ban 1930 óta vitatkoznak egy, a Social Security Cardon alapuló nemzeti személyi igazolvány rendszer létrehozásáról, amihez a jelenlegi elképzelésekben egy minden amerikai állampolgár adatait tartalmazó központi komputer-nyilvántartás is tartozik (és ez meglehetősen rosszul hangzik). A kormányzati tisztviselők azt remélik, hogy ezzel vissza lehetne szorítani az illegális bevándorlások számát – szerintem pedig rettenetesen vissza lehetne vele élni. Vagyis nem önmagában az az érdekes, hogy személyi igazolvány-e, hanem az, hogy milyen; milyen célokra és hogyan akarják felhasználni; közben hogyan kezelik az adatokat, és a többi.

Ami pedig Davies vélekedését illeti, éppen az általa vezetett Privacy International foglalkozott behatóan azzal, hogy hányféleképpen lehet az állampolgárok ellen fordítani: a dél-afrikai apartheid például arra használta, hogy ne hagyja a feketéket szavazni.

Hoover: Most én érvelek ugyanazon logika alapján, mint az előbb te: abból, hogy egyes helyeken visszaélnek vele, nem feltétlenül következik, hogy a személyi igazolvány, mint olyan feltétlenül elvetendő megoldás lenne.

Vízi Patkány: Malajziában a terrorizmus elleni harc, illetve a 21. sz. felé való nyitás jegyében nemrégiben vezették be a minden 12 évesnél idősebb állampolgár számára kötelező „Mykad"-ot. Ez egyfelől biometrikus azonosítóval (ujjlenyomattal) ellátott személyi igazolvány; másfelől jogosítvány, útlevél és nagyjából minden egyéb, ami még elképzelhető.

Wan Mohamad Ariffin, a smart card projekt igazgatója le is vonta a megfelelő következtetést: „A terroristatámadásokat követően számos kormány – és többek között az USA kormánya is – az eddiginél hatékonyabb eszközöket fog keresni az emberek nyomonkövetésére... – mondta -. Hajlandóak vagyunk megosztani velük a rendelkezésünkre álló technológiát, mivel ez hozzájárulhat a biztonsági problémák megoldásához."

Hoover: Szerintem ideje, hogy emlékeztessed magadat, Vízi Patkány, a szélsőségek kapcsolatos aranyszabályodra!

Vízi Patkány: Amennyiben?

Hoover: Deborah Hurley harvardi számítógépes terrorizmus-szakértő szerint miközben szeptember 11. után újra kell gondolnunk, hogy milyen szintű megfigyelés az, ami már nem engedhető meg az állam részéről, és miközben a hi-tech jogosítványok például nehezebben hamisíthatóak és jobban védenek a személyiséglopással szemben, aközben azért arról se feledkezzünk el, hogy a szélsőséges szabadság meg a szélsőséges ellenőrzés között számos átmenet létezik.

Ez esetben még a te kedvenc szerződ, Garfinkel is mintha az én oldalamon állna, hiszen a terrorizmus elleni harccal kapcsolatban azt nyilatkozta, hogy inkább a nagy cégek, mint az állam privacysértésétől kell tartanunk. „Az, amivel a kormány megsérti privacynket, csupán a töredéke annak, amit az üzleti élet követ el ellenünk... (Végső soron) bízom az államban. Ugyanez viszont nem igaz a legtöbb céggel kapcsolatban."

Vízi Patkány: Az ACLU-nak viszont egy cseppet sem tetszik az új személyi igazolvány, mert az lehetővé tenné „a kormányzat számára az ellenzékiek megfigyelését, miként ez az Amerikai Egyesült Államok történetében újra és újra megtörtént".

Ráadásul ha egyszer egy rendszer elkezd kiépülni, akkor – emlékszel még, Hoover? – nincs megállás: a következő lépésben már a távolsági buszon vagy a pályaudvarokon is digitális személyit kérnének tőlünk... és végül már a vegyes boltban sem szolgálnának ki minket enélkül.

Hoover: Na ne mondjad, Vízi Patkány! Ez még egy olyan társadalomban sem feltétlenül igaz, ahol állandóan magunkkal kell hordanunk a személyit. Vagy Magyarországon talán így van?

Szerző: Nem.

Vízi Patkány: Nagy különbség viszont, hogy Magyarországon nem digitális személyit használnak, hanem közönséges papíralapút – a két megoldás között nagyjából akkora a távolság, mint a hagyományos és az arcfelismerő kamera között.

Hoover: Nézzük akkor a másik oldalról a dolgot: a személyi igazolvány biztonságot nyújtana többek között azoknak az arabos kinézetű férfiaknak, akik Koránt olvasnak a repülőtéren.

Ellison pedig azt mondja, hogy „a kérdés nem az, hogy a kormány fenntarthat-e adatbázist az állampolgárokról és kezelheti-e az ID-card információit, hiszen már most is ezt teszi. A kérdés az, hogy miként tehetjük ezeket hatékonyabbá – például a bűnözés elleni harcban... Több adatbázisra lenne szükségünk? Éppen ellenkezőleg. Ma éppen az a baj, hogy túlságosan sok van belőlük. Az egyetlen dolog, amit megtehetünk, hogy nehezebbé tegyük a terroristák életét, az, hogy a miriádnyi, kormányzati adatbázisban tárolt információt egyetlen helyre gyűjtjük össze”, ez ugyanis azt eredményezné, hogy a bűnüldöző szervek hatékonyabb adatbányászatot képesek folytatni.

Egy másik alkalommal pedig azt jegyzi meg, hogy „az Amerikai Egyesült Államokban hosszú időre visszanyúló hagyományai vannak a kormányzattal szembeni gyanakvásnak. De eddig annyira el voltunk foglalva azzal, hogy megvédjük magunkat a saját kormányunkkal szemben, hogy nem tettük lehetővé a kormány számára, hogy megvédjen minket.”

Vízi Patkány: Kezdem egyre kevésbé érteni az érvelésedet! Miért is lenne bármiféle „védelemre” szüksége azoknak az „arabos kinézetű” férfiaknak, akik nyilvános helyen olvassák a szent könyveket? Egy szabad országban az ilyesmi nem tilos – tehát erre nem lehet érvként hivatkozni.

Azt pedig a legszívesebben meg sem említeném, hogy ha jobban odafigyeltél volna az elején, akkor most pontosan emlékeznél rá, hogy milyen végtelenül veszélyes dolog egyetlen központi adatbázisra alapozni. Szerinted egy terrorista mit nem lenne hajlandó feláldozni azért, hogy ezt megsemmisítse, vagy hogy a céljainak megfelelően átírja a benne található információkat?

Hoover: Jól van, na, nem kell túldimenzionálni a dolgot! Te is pontosan tudod, hogy a digitális személyi igazolvány kérdése lényegében lekerült a napirendről, és határozottan valószínűtlen, hogy az Ellison által javasolt formában bármikor is bevezetnék.

Vízi Patkány: Tudom, de azért van min eltűnődnünk, amikor azt próbáljuk meg felmérni, hogy milyen hatással lehetnek a privacyre a „terrorizmus fenyegetésére adott válaszok”. Amivel persze nem azt akarom mondani, hogy mindegyik ötlet ugyanarra a kaptafára készült: a TIPS például...

Hoover: Mostanra tökéletesen kiismertem a taktikádat, cimbora. Nekiállsz az olvasókat mindenféle digitális személyivel riogatni, noha magad is tudod, hogy soha nem fog megvalósulni. Utána nekiállsz a TIPS-ről mesélni, noha maga is tudod, hogy a programot már régen eltörölték, és...

Vízi Patkány: Na igen – csak ha ezzel akarsz érvelni, akkor talán azt sem ártana megmagyaráznod, hogy akkor miért akarták korábban mégis bevezetni. Azaz szerintem a TIPS igenis kimondottan jellemző az amerikai kormány jelenlegi hozzáállására, és ha a személyes véleményemre vagy kíváncsi, akkor még azoknál a viselkedés-előrejelző rendszereknél is riasztóbb ötleten alapul, mint amiket legalább az 1990-es évek közepe óta fejlesztenek a világ legkülönbözőbb részein.

Szerző: Részleteznéd egy kicsit, Vízi Patkány?

Vízi Patkány: Persze. A Steve Maybank (University of Reading) és David Hogg (University of Leeds) által még jócskán a terroristatámadás előtt megalkotott prototípus például zártláncú kamerarendszeren keresztül figyelve – állítólag – képes a viselkedésük alapján kiszűrni a bolti tolvajokat; a repülőtéri merénylőket és...

Szerző: Azt még csak-csak értem, hogy azt, aki éppen sajtos stanglit akar lopni a közértből, a kutatók szerint sajátos mozgássorok és viselkedési minták jellemzik – azt viszont a legkevésbé sem, hogy miként lehet fellépni az ellen, aki mindössze „gyanúsan" viselkedik.

Hoover: Egy biztonsági őr eddig is megkérhetett, hogy azonosítsad magad. Mostantól annyi lesz a különbség, hogy a gép riasztja a biztonsági őrt, aki így feltehetően jóval hatékonyabban fog dolgozni, és csak azokat zaklatja majd, akiket tényleg érdemes.

Vízi Patkány: Aha, és ha valami katasztrofális melléfogás történik, akkor ki tartja a hátát? Vagy fogalmazhatnék úgy is, hogy nem minősül-e indokolatlan zaklatásnak – és így nem ellentétes-e a Negyedik Kiegészítéssel –, ha pusztán azért, mert egy program „gyanúsnak" találja, feltartóztatunk valakit és átkutatjuk?

Hoover: Mondtam már, hogy a biztonsági őr is ugyanezt csinálja.

Vízi Patkány: Van azért egy kis különbség. Nevezetesen, hogy a biztonsági őr érti, hogy mit csinál, és felel is a tetteiért – ami viszont nem mondható el egy algoritmussal kapcsolatban.

Hoover: Az arcfelismerő kameránál is a program választja ki, hogy ki minősül gyanúsnak.

Vízi Patkány: Azért az nem teljesen ugyanaz, hogy arról beszélünk-e, hogy két digitális mintázat (az adatbázisban tárolt és a megfigyelt arcáról frissen felvett) hasonlít-e egymásra; vagy pedig arról, hogy megpróbáljuk megjósolni, hogy az illető miként fog viselkedni a közeljövőben... még Maybank is elismeri, hogy bár „ritka, hogy valaki egy parkolóban a kocsik között lődörögne (és ne lenne potenciális autótolvaj)... azért van ilyen."

Simon Davies szigorúbban fogalmaz: „ez egy rettenetesen veszélyes, a totálisan ellenőrzött állam felé tett lépés", ahol valaki (méghozzá feltehetően az aktuális hatalom képviselője) eldönti, hogy mi tekinthető „normális viselkedésnek", és attól kezdve a rendszer csakis ezt hajlandó elfogadni. Mindenki más számíthat rá, hogy pillanatokon belül felbukkan egy biztonsági őr. Vagyis: olyan társadalmi környezet jön létre, ahol minden korábbinál jobban kontrollálnák a viselkedést – és azonnal fellépnének minden eltérés ellen.

Hoover: Vagy pedig nem. Megszólal a jelzés; az operátor vet egy pillantást a képernyőre és látja, hogy nem történt semmi, csak két szerelmes vitatkozik.

Vízi Patkány: Igen, ha jól van kiépítve a rendszer. De lehet, hogy nem fog megbízhatóan működni, miközben ezek a technológiák már itt vannak a nyakunkon. Sergio Velastin (King's College, London) Cromatica nevű rendszere a londoni földalattiban többek között arra is figyelmeztetni fogja az operátorokat, ha valaki a szerelvény elé akarja vetni magát, és Frank Norris, a London Underground illetékese szerint ez ellen (ami kb. hetente egyszer fordul elő) nem csupán azért kell fellépni, hogy megakadályozzunk egy személyes tragédiát, de azért is, mert egy öngyilkos hosszú időre megbéníthatja a forgalmat... Akárhogyan nézem is, nekem ez

a hozzáállás legalább olyan furcsa, mintha valaki azt mondaná, hogy a terrortámadásokat azért kell meggátolni, mert sok törmelék marad utánuk, és drága a romeltakarítás.

De hogy visszatérjünk a különböző „megelőző" technológiákhoz, a legmesszebbre Steve Kirsch, az InfoSeek alapítója merészkedik, akinek agyszkennelő rendszere a „multifaceted electroencephalographic response analysis"-en (röviden: MERA) alapul. A delikvenst beültetik egy megfelelően felszerelt székbe, és miközben egy képernyőn szavak villannak fel meg mindenféle hangok hallatszanak, aközben mérik az agyi aktivitását – és ez alapján megállapítják, hogy tervez-e mindenféle gonosz dolgokat. Illetve, hogy részt vett-e egy adott bűntény elkövetésében, ugyanis ha olyan részleteket is megjelenítünk a számítógép-monitoron, amit csak az elkövető ismerhet, akkor a válaszreakciói alapján le lehet leplezni.

A repülést pedig úgy lehetne a Kirsch-féle módszer segítségével biztonságossá tenni, hogy ha valaki nem akar a kontinens egyik feléből a másikba vonattal utazni, akkor néhány évente aláveti magát egy agyszkennelésnek, ahol azt vizsgálják, hogy miként reagál ismert terrorista cselekményekkel kapcsolatos információkra. Alig tíz perc az egész...

Hoover: És tegyük hozzá, hogy az agyszkennelést az FBI is tesztelte, és az eredmények szerint 100 százalékosan megbízhatónak bizonyult.

Vízi Patkány: Meg azt is tegyük hozzá, hogy ez a tesztelés egyelőre mindössze 21 ember bevonásával történt... vagyis közelről sem eléggé meggyőző ahhoz, hogy ne csupán a nemzet biztonságát építsük rá, de az egyes emberek megítélése is ezen alapuljon.

Mint ahogy éppen a megbízhatatlanság az egyik fő gond azzal a TIPS-szel (Terrorism Information and Prevention System) kapcsolatban is, amit az előbb már említettünk, és ami lényegében arra az ötletre épül, hogy kérjük meg a villany- és gázóra-leolvasókat, postásokat, buszvezetőket és kamionsofőröket (vagyis mindenkit, aki munkája során gyakran kapcsolatba kerül másokkal), hogy azonnal jelentsék, ha valami gyanúsat tapasztalnak.

Pillanatokon belül azon kaphatjuk magunkat, hogy a televízió-szerelőnkkel beszélgetünk a közel-keleti helyzetről vagy a pizzafutárral arról, hogy milyen újságokra érdemes előfizetni – az pedig feljelent minket a TIPS-en keresztül. „A Bush-adminisztráció szeptember 11-ét követő terroristaellenes taktikái... abban hasonlítanak egymásra, hogy egyik sem bízik a demokratikus intézményekben és a szabad társadalomban", jegyzi meg a New York Times.

A TIPS-nek az a meglehetősen ambiciózus célja volt, hogy minden 24. amerikait beszervezzen, és ezzel nem csupán az abszolút számokat tekintve, de arányaiban is nagyobb bázist építsen ki, mint annak idején az NDK-ban a Stasi. Az persze szintén nagymértékben támaszkodott a lakossági „együttműködésre", de az amerikai kormány által tervezett 4 helyett „alig" 1 százalékot vont be.

A különböző besúgói (vagy ha nem akarok senkinek a lelkébe gázolni, akkor: informátori) hálózatok eddig nem tartoztak tipikusan a demokratikus rendszerek eszköztárába, és ennek megvan a jó oka. Többek között az is, ami a Project on Justice 1992-es megállapításai között (Harvard University) olvasható: hogy az ilyen jelentések megbízhatósága mindig kérdéses, egyesek ugyanis szeretik kiszínezni az igazságot, mások pedig minden valóságalap nélkül hazudnak és rágalmaznak.

A TIPS esetében az „informátorok" beszámolói az Igazságügyi Minisztérium adatbázisába kerültek volna be, hogy később felhasználják őket – persze nem csupán a minisztérium munkatársai, de a különböző kormányügynökségek és a helyi rendőrségek is hozzáfértek volna. Mondhatni, majdnem mindenki – kivéve persze azt, akiről a „feljegyzés" készült, és aki azzal sem lett volna tisztában, hogy megfigyelik, és lényegében feljelentgetik… Akár személyes bosszúból is.

Hoover: Méghogy személyes bosszú! Inkább a nemzet megvédéséről van szó: Bush már Knoxville-ben, 2002. április 8-án rámutatott, hogy „ez egy olyan program, amelynek keretében a kamionosok bármit jelenthetnek, ami gyanús... ha valaki valami gyanúsat lát... akkor jelentenie kell. Így meg lehet szervezni azt, ami ma is a napi gyakorlat része társadalmunkban, és akkor a haza biztonságosabb és jobban felkészült lesz."

Vízi Patkány: Éppen ellenkezőleg. Ha terrorista lennék, akkor már a TIPS említésére is összefutna a nyál a számban, hiszen ez roppant hatékony módja lehetett volna az egész amerikai demokrácia lerombolásának. Például azért, mert az emberek állandóan attól rettegnének, hogy valaki feljelenti őket – és ez nem igazán lenne összhangban a hagyományos szabadságjogokon alapuló társadalommal.

Az ACLU szerint „az adminisztráció azt akarja elérni, hogy a telefon- és gázszerelők a kormány által kézben tartott kukkolókká váljanak", és az ACLU-s Laura W. Murphy ezt azzal egészíti ki, hogy „a nemzetiségi érzéseket és a vallásosság megnyilvánulásait képzetlen emberek fogják (fel)jelenteni anélkül, hogy ezeknek bármi köze lenne a bűnözéshez" vagy terrorizmushoz.

Feltehetően nem véletlen, hogy a nyomozók, ügyészek és hasonlók alapos képzést kapnak, mielőtt bedobnák őket a mélyvízbe – és utána aztán felelnek is a döntéseikért. Több millió amerikain viszont nem igazán lehet semmit számon kérni – vagyis hiányzik a megfelelő visszacsatolás is.

Ezért is mondta azt a konzervatív Dick Armey, hogy a kormánynak nem kellene „arra biztatni az állampolgárokat, hogy kémkedjenek a többiek után". A liberális Patrick J. Leahy úgy fogalmazott, hogy „figyelnünk kell. De nincs szükségünk olyanokra, akik (minket) figyelnek", és azt is megemlítette, hogy „A Justice Department 1917-ben létrehozta az American Protective League-t (APL), melynek tagjai jelentették, ha valaki kritizálta a kormányt... néha újságárusító helyekre csaptak le és egyeseket kátrányba meg tollba forgattak."

Az APL-nek 600 városban mintegy 250,000 tagja volt: jobbára olyan, tehetős férfiak, akik a katonai szolgálathoz öregek, ahhoz viszont túlságosan fiatalok voltak, hogy ne akarjanak semmit „tenni a hazáért". Az a benyomásom, hogy a TIPS valójában ennek a felmelegített és modernizált változata: „A gáz- és villanyóra-leolvasáson keresztül minden háztartáshoz hozzáférhetünk", mondta az I. Világháború végén egy, a kansasi Wichitában élő APL-es.

Orrin G. Hatch republikánus szenátor pedig azt mondta (immár 2002-ben), hogy „nem akarunk egy orwelli, 1984 típusú társadalmat, ahol az emberek jelentéseket írnak a szomszédaikról."

Hoover: A TIA éppen ezt a problémát küszöbölte ki.

Vízi Patkány: Igen, hogy egy kissé még nyomasztóbb megoldással álljon elő. A Privacy Council 2002. közepi felmérése azt mutatta, hogy a nagy cégek rendszerint nagyon is készségesen vesznek részt egy olyan programban, amit leginkább korporációs TIPS-nek nevezhetnénk, és többek között a hotelek, az autókölcsönzők, az utazási irodák több mint fele adott át információkat a különböző szövetségi ügynökségeknek szeptember 11. után. Természetesen önként és bármiféle bírósági végzés nélkül.

Vagy hogy még egy példát mondjak az efféle együttműködésre: a Professional Association of Diving Instructors 2002. tavaszán több mint 2 millió búvárengedéllyel rendelkező ember adatait szolgáltatta ki a Federal Bureau of Investigation-nek (FBI) anélkül, hogy közülük bárki ellen bírósági eljárás folyt volna... az FBI egyszerűen arra volt kíváncsi, hogy ki lehet képes egy víz alatti terrorakció végrehajtására.

Larry Ponemon, a Privacy Council igazgatója egyenesen azt állítja, hogy „nem nevezhetem meg a forrásaimat, de egy, a kémkedésben részt vevő szövetségi ügynök szerint (mára) gyakorlatilag minden amerikai állampolgárt besoroltak” és nyilvántartanak a nyilvános, illetve magánkézben lévő adatbázisokat felhasználva. És ha ez igaz, akkor már csak az a kérdés, hogy van-e még egyáltalán értelme a Negyedik Kiegészítésről beszélni.

Hoover: De nem lehet tudni, hogy igaz-e.

Vízi Patkány: A TIA (Total Information Awareness) viszont – sajnos – nagyon is igaz. Nem kisebb célt tűz maga elé, mint összegyűjteni minden amerikai és nem amerikai „információs mintázatát”, hogy az összes potenciális terroristát, illetve bűnözőt nyomon lehessen követni még azok alapján az „alacsony intenzitású/alacsony sűrűségű” információnyomok alapján is, amiket azok a mindennapi életben hagynak maguk után. Ehhez persze első lépésben a lehető legtöbb adatot kell begyűjteni kezdve azon, hogy valaki mikor hajtott le az autópályáról és mikor telefonált egyet és utoljára melyik web site-ot kereste fel egészen az egészségügyi adatokig és a bankszámlainformációkig bezárólag.

Ezért is hívják Totális Információs Éberségnek. Mit ne mondjak, találó név.

Szerző: Ha ezt megcsinálják, akkor tényleg igaza lesz annak a New York Times olvasónak, aki szerint Orwell nem is tévedett olyan sokat: mindössze tizennyolc évet.

Vízi Patkány: Ehhez persze nem csupán az kell, hogy tényleg begyűjtsék az összes elképzelhető adatot, hanem az is, hogy ezeket az adatokat aztán megfelelően fel is tudják dolgozni, és bár ehhez „forradalmian új adatbányászati megoldásokat” akarnak kifejleszteni, legalábbis kétséges, hogy ez mennyire sikerülhet majd.

Hoover: Nincs ebben semmi képtelenség. Ramano Rao, a szövegkereső rendszerek fejlesztésével foglalkozó Inxight (Sunnyvale, Kalifornia) vezetője szerint például technikai szempontból „jól megalapozott elképzelés... a legújabb eredményeket használja fel”, és az adatbányászatot már eddig is kiterjedten alkalmazták a hitelkártya-csalások kiszűrésére. A HNC Software (San Diego) programját például a hitelkártya-cégek szokták bevetni: ha egy olyan kártyával, amivel eddig leginkább ruhavásárláskor fizettek, hirtelen nagy mennyiségű és drága elektronikus berendezést rendelnek az interneten keresztül, akkor a rendszer riaszt – ennek köszönhetően sikerült a felére visszaszorítani az ilyesfajta bűnözést.

Azaz a TIA esetében nem történik más, mint a kormány – amit ti olyan szívesen neveztek Nagy Testvérnek – elkezdi ugyanazokat a módszereket alkalmazni, mint amit a Kis Testvérek, vagyis a cégek eddig is alkalmaztak. A jövőben össze lehet majd kapcsolni a repülőtéri megfigyelő-kamerákból származó képeket és a repülőtérről tárcsázott telefon-számokat, hogy aztán „gyanús mintázatokat” keressenek az információkban, és ha valamire tényleg rábukkannak, akkor jöhet a humán analízis.

Vízi Patkány: A különböző adatgyűjtési módszerekből leszűrt eredmények korántsem mindig megbízhatóak – ugyanis nem biztos, hogy sikerül kimutatni az ok-okozati összefüggéseket. A matematikus Karen Kafadar (University of Colorado, Denver) azt hozza fel példaként, hogy a rendszeresen sörözők nagyobb valószínűséggel kapnak tüdőrákot, mint mások – de nem azért, mert a sörnek van ilyen hatása, hanem azért, mert aki sok sört iszik, az valószínűleg dohányzik is. És ez viszont nem derül ki a statisztikából.

Mindent egybevetve tehát azon múlik az egész, hogy mennyire hatékony az adatbányászat. És „ez sok nagyságrenddel nehezebb feladat”, mint megtalálni a hitelkártya-csalókat, mondja Robert Grossman, a National Center for Data Mining (University of Illionis, Chicago) igazgatója. Elvégre ha a rendszer 99 százalékos hatásfokkal működne is, akkor is millió és millió tévedést követne el egyetlen nap alatt (lévén szó óriási mennyiségű adatról).

Ráadásul annak nem csupán előnyei vannak, ha nagyon sok információ áll a rendelkezésünkre: a National Security Agency (NSA) ugyan már 2001. szeptember 10-én lehallgatott olyan, arab nyelvű üzeneteket, melyekből következtetni lehetett (volna) arra, hogy terrorista-támadás készül – de a fordítók csak szeptember 12-én jutottak odáig, hogy foglalkozni kezdjenek vele.

Eamonn Keogh számítástechnikai szakértő (University of California-Riverside) pedig arra is felhívja a figyelmet, hogy a szokásosnál nagyobb adatbázisokból könnyen lehet olyan, használhatatlan vagy triviális eredményeket kibányászni, mint amilyen például az is, amikor az egészségügyi információkat tanulmányozva megállapítjuk, hogy a nők gyakrabban szülnek, mint a férfiak.

Márpedig ahhoz, hogy itt valóban iszonyatos mennyiségű információt fognak kezelni, kétség sem fér: a szakértők azt mondják, hogy csupán azért használjuk a TIA-val kapcsolatban is az „adatbázis" kifejezést, mert jobbat még nem sikerült kitalálni.

Hovver: Ez a vita még korántsem zárult le: legalább ugyanilyen neves adatbázis-szakértők állítják azt is, hogy minél nagyobb és komplexebb az adatbázis, az eredmények annál pontosabbak lesznek.

Vízi Patkány: És azok az adatbázis-szakértők arra is megesküsznek, hogy a TIA képes lesz még be sem következett eseményeket is előre jelezni és az ilyen előrejelzések alapján a hatóságok felléphetnek majd?

Mert ha jól tudom, ez is a tervek között szerepel. Mint ahogy a biometrikus azonosításra is nagy hangsúlyt kívánnak helyezni, hogy aztán szép kényelmesen lehessen nyomon követni az állampolgárokat, például az arcfelismerő rendszerek és a mozgásazonosító szoftverek összekapcsolásával (ilyesmit fog tudni többek között a Human ID at a Distance, az Emberazonosítás Távolról nevű program is).

Hoover: Ezeket a lépéseket a terrorizmus elleni harc teszi szükségessé, és amint vége lesz a harcnak, minden visszazökken a megszokott kerékvágásba.

Vízi Patkány: Ez alapvető tévedés, Hoover! A kolumnista David Cole azt fejtegette 2002. közepén, hogy „A nemzetbiztonsági szervek gyakran hivatkoznak arra, hogy az állampolgári jogok csupán a háború miatt és csupán időlegesen szorulnak vissza. A mostani háború azonban valószínűleg állandósulni fog: Donald Rumsfeld védelmi miniszter azt mondta, hogy addig nem fog véget érni... amíg egyetlen, globális fellépésre képes terrorista szervezet is létezik. Mivel pedig erre a modern technológiának köszönhetően gyakorlatilag mindenkinek módja van, soha többé nem lesz béke... és egyedül abban lehetünk biztosak, hogy még jobban meg fogják csonkítani a privacynket, a szabadság- és az alapjogainkat."

Hoover: Látom, hogy most is az történik, mint eddig minden fejezet végére: lassanként teljes defenzívába kényszerülők. De annyit azért szeretnék megjegyezni, hogy nem nagyon veszem észre sehol az alapjogaink sérülését. Legfeljebb néhány szigorítás történt, de semmi több.

Vízi Patkány: Ehhez képest én úgy veszem észre, hogy a Bush-adminisztráció egyszerűen kettéválasztja a jogot, hogy úgymond hatékonyabban tudjon fellépni a terroristagyanús elemek ellen, és míg a „becsületes" állampolgárokat továbbra is békén hagyják, addig a többiek (legyenek bár amerikaiak vagy külföldiek) ellen anélkül lehet majd vizsgálatot indítani; anélkül lehet ítélkezni felettük; és anélkül lehet bebörtönözni őket, hogy részesülnének a szokásos védelemben (és például ügyvédjük lehetne). Ott van például a „piszkos bombás" Jose Padilla, aki jelenleg a Haditengerészet egy hajóján üldögél, és addig egészen biztosan nem fog ügyvéddel beszélni, „amíg a terrorizmus elleni háború véget nem ér".

Hoover: Ahelyett, hogy nekiállnál vagdalkozni, próbáld inkább megérteni az egész logikáját, ami „egyszerűen más, mint az általunk megszokott és elfogadott, a bűncselekmények esetén alkalmazott büntetőjogi procedúra”, mondja egy magát megnevezni nem kívánó amerikai tisztviselő. „Ez ugyanis külön arra szolgál, hogy megfelelően tudjuk kezelni a háború során elfogott embereket.” Elvégre a terrorizmus nem csupán a bűnözés, de a háború egyik formája is. Azt talán nem kell hosszan magyarázni, hogy háború idején nem a szokványos, hanem a háborús jog érvényes.

Még akkor is, ha adott esetben amerikai állampolgárról van szó.

Vízi Patkány: Ami viszont azt jelenti, hogy – hacsak közbe nem lép a Legfelsőbb Bíróság – a jövőben elég lesz terroristaellenes tevékenységgel meggyanúsítani valakit, és az már el is felejtheti mindazokat a jogokat, amik hagyományosan megilletnék. Ez viszont tökéletesen lehetetlenné fogja tenni az elfogulatlan ítélkezést, hiszen a bírósági tárgyalás és az ügyvédi védelem nem öncélúak, hanem arra valóak, hogy az igazság derüljön ki, és ha ezeket – azzal érvelve, hogy a terrorizmus elleni háború törvényei másmilyenek – eltöröljük, akkor vége a dalnak.

Pontosan ugyanúgy, mint ahogy a kínzás visszaállítása esetén is vége lenne.

A Bush-adminisztráció „a nemzet biztonságára hivatkozva a végrehajtó hatalom olyan kiterjesztésére törekszik, ami felett nincs bírósági kontroll”, mondja Kate Martin, a nonprofit Center for National Security Studies (CNSS, Washington) igazgatója. „Az ilyesfajta lépések inkább kötődnek ugyan az állami jogi hatalomgyakorláshoz, mint a J. Edgar Hoover-féle politikai kémkedéshez, de sokkal veszélyesebbek. A jog ugyanis bármely visszaélés kiszolgálója lehet.”

Hoover: Hmm, hát ez nem volt különösebben sportszerű... Mindenesetre hadd válaszoljam azt, hogy az általad olyannyira tisztelt amerikai Alkotmány szerint „az Elnök a főparancsnoka az Egyesült Államok szárazföldi haderejének és hajóhadának, valamint az egyes államok miliciájának, amikor az utóbbiakat az Egyesült Államok tényleges szolgálatában alkalmazzák”. Azaz úgy is felfogható ez az egész, hogy mivel háborút folytatunk a terrorizmus ellen, ezért Bush a nemzet katonai főparancsnokaként hoz döntéseket.

Vízi Patkány: Ez viszont lényegében azt jelenti, hogy az elnöknek egymagában is joga van bárkit (és így amerikai állampolgárokat is) ellenséges harcosnak tekinteni (és az ilyen – a fentebbiek értelmében – nem fog semmilyen jogi védelemben részesülni). Bár azt én sem vitatom, hogy a végrehajtó szerveknek háború idején joguk van elfogni az ellenség harcosait, az teljesen más kérdés, hogy nem alkotmányellenes-e, ha ez a besorolás egyedül Bush döntésén alapul. Különösen, hogy per pillanat a hagyományos háború kereteit szétfeszítő terrorizmusellenes küzdelemről van szó, ahol amúgy is nehezebb viszonyítási pontokat találni... ha ugyan nem teljesen lehetetlen.

Hoover: Pedig volt már precedens az ilyesmire. A II. Világháború idején a Legfelsőbb Bíróságnak például semmi kifogása nem volt az ellen, amikor a katonai bíróság egy, a náciknak dolgozó amerikai szabotőrt ítélt el.

Vízi Patkány: Végeredményben tehát nagyon is elképzelhető, hogy az állam szép fokozatosan ki fog csusszanni a hagyományos jogi ellenőrzés alól, miközben mindent megtesz, hogy minél jobban ellenőrizze az állampolgárait.

Szóval ennyit arról az információs utópiáról, ahol az állampolgár mindent tud az államról, miközben róla semmit sem tudnak a hivatalos Nagy Testvérek... Az EPIC és a Privacy International által 2002. szeptemberében közösen kiadott kötet szerint a kormányok (a terrorizmus elleni harc ürügyén) jelenleg mindent megtesznek azért, hogy megkönnyítsék titkosszolgálataik számára a megfigyeléseket és lehallgatásokat. „Világszerte témává vált a

totális azonosítás", írja Sarah Andrews, a tanulmány összeállítója. „Akár nyilvános helyen tartózkodunk, akár internetezünk, bármikor és bárhol azonosíthatnak minket."

Amihez – miként ebből a fejezetből is kiderülhetett – „hogy megerősítsék a nemzet biztonságát és csökkentsék egy lehetséges terroristatámadás veszélyét, a kormányok... a jogi szabályozást és az új technológiákat egyaránt igénybe veszik".

Hoover: Stewart Baker, a National Security Agency volt szakértője (Steptoe & Johnson, Washington) viszont azt kérdezi, hogy tényleg jobban örülnének neki a jogvédők, ha a világ megváltozása miatt kellene panaszkodniuk, nem pedig a törvények módosítása miatt?"

Vízi Patkány: Inkább ne menjünk bele: szerintem túl sokszor megbeszéltük már, hogy az alapjogok feladásából semmi jó nem származik. Russell Nelson számítógépes szakértő annak idején azt mondta a titkosítással kapcsolatban, hogy „az USA Maginot-vonala a titkosító szoftverek exportjának korlátozása. Nagy, drága, minden ésszerűség ellenére is fenntartják, és ha egyszer vége a háborúnak, akkor nehéz megszabadulni tőle", és szerintem most éppen a terrorizmus elleni harc Maginot-vonalát építjük ki.

Az Amerikai Egyesült Államok mellett szigorításokat és új szabályozásokat vezettek be többek között Ausztráliában, Franciaországban, Indiában, Kanadában, Nagy-Britanniában, Németországban, Szingapúrban és Svédországban, és persze az EU is a kiterjedt és előzetes elektronikus adatgyűjtés bevezetésén dolgozik... „Az internet megfigyelőeszközzé változott, és a jövőben a számítógépek elsődleges funkciójává fog válni a megfigyelés lehetővé tétele", mondja Simon Davies, akit már meglehetősen sokszor idéztem.

Nagy általánosságban pedig azt lehetne hozzátenni, hogy a különböző kormányok egyre inkább kiterjesztik és összekapcsolják a már létező adatbázisokat is, és például a szociális programokból meg a közlekedési adatbázisokból származó információkat összevetve próbálnak számítógépes profilokat létrehozni, hogy ki tudják szűrni az „ellenséget" (aztán persze így vagy úgy, de össze fogják kapcsolni az egyes országok adatbázisait is). Az egész szigorításban az a legkülönösebb, hogy majdhogynem az összes törvénymódosítási javaslatot már évekkel korábban is előterjesztették, de akkor nem mentek át.

Szeptember 11. után viszont érdemi viták nélkül fogadták el őket, „mivel az emberek immár nem tették fel azokat a (nagyon is indokolt) kérdéseket, mint korábban", olvasható a tanulmányban, és legalább részben ennek tulajdonítható, hogy noha egy szabályozás keresztülvitele rendszerint meglehetősen sokáig tart, majdhogynem sokkoló, hogy hány új törvényt fogadtak el a világ különböző pontjain még 2001. vége előtt.

Az utóbbi időszakra mindent egybevetve tehát a privacy-törvények gyors meggyengülése volt a jellemző; meg az, hogy minden korábbinál nagyobb mértékűvé vált az adatmegosztás a cégek, a rendőrség és a nemzetbiztonsági szolgálatok között. Emellett világszerte növekedett persze a lehallgatások száma is, és bozóttűzként terjednek az olyan, állítólag az egyes emberek azonosítására és követésére alkalmas technológiák, mint amilyen az arcfelismerő kamera vagy a digitális személyi igazolvány. És bár nem akarok messzemenő következtetéseket levonni, a helyzet – legalábbis számomra – nem tűnik különösebben bíztatónak.

„Azok, akik a pillanatnyi biztonság érdekében alapvető szabadságjogokat adnak fel, sem a szabadságot, sem a biztonságot nem védik meg", mondta annak idején Benjamin Franklin.

Szerző: Hát így állunk.

Zárszó helyett

A Némi digitális önvédelem

Talán semmi sem változik olyan gyorsan, mint éppen ez a terület, ezért nem érdemes belemenni a jelenleg alkalmazható, konkrét megoldások egyes részleteibe. Ugyanekkor viszont létezik néhány olyan, általános alapelv, aminek a betartása sokat segíthet, ha tényleg úgy gondoljuk, hogy tenni akarunk valamit a privacynk védelmében.

Elöljáróban meg kell említeni, hogy a dolog korántsem biztos, hogy egyszerű lesz – ugyanis valamit valamiért.

- Egyfelől a privacybarát megoldások sok esetben valamivel drágábbak, mint a hagyományosak;
- másfelől külön odafigyelést és bizonyos mértékig a témával való foglalkozást is igényel, ha privacy-tudatosan akarunk élni.

Most pedig lássuk a részleteket:

Mindig figyeljünk rá oda, hogy mit töltünk ki akár on-line, akár a mindennapi életben – és mérlegeljük, hogy megéri-e.

Lehetőleg adjunk inkább általánosabb választ („18 évesnél idősebb” ahelyett, hogy „32 éves”), ha erre mód van; illetve mindig mérlegeljük, hogy az információk kiadásáért cserébe kínált előnyök valóban megérik-e. Érdemes például utána számolni, hogy egy „törzsvásárlói kedvezmény” tényleg jó befektetés-e, amennyiben 1 százalék megtakarítást kínál a személyes adatainkért cserébe (ez az 1 százalék egy 10000 Ft-os vásárlásnál 100 Ft-ot jelent). Emellett soha ne sajnáljuk az időt az apróbetűs rész elolvasására sem; illetve tájékozódjunk (és szükség esetén kérdezzünk rá), hogy miként fogják kezelni az adatainkat; milyen felhatalmazás és milyen szabályozás alapján teszik ezt; kitől származnak a birtokukban lévő és ránk vonatkozó információk, meddig fogják kezelni azokat, stb. Az adatvédelmi törvény értelmében jogunk van ezeket megtudni. Ahogy az Adatőrségen című könyv fogalmaz: „Alkotmányos jogunk van személyes adataink védelméhez”. Azaz: mindig ismerjük pontosan a jogainkat (még akkor is, ha ez némi időbe kerül).

Soha ne adjunk ki szenzitív adatokat telefonon vagy interneten keresztül, ha nem ismerjük azt, aki kéri őket.

Ide kapcsolódik személyes adataink megóvása általában véve is: tehát például e-mail-ezés közben, ha csak lehetséges, titkosítsunk. Nem azért, mert titkolnivalónk van, hanem azért, mert senkire nem tartozik, hogy mit írunk.

Ugyanez a logika szól amellett is, hogy lehetőleg ne használjunk nem nyílt forráskódú programokat, mert azokról soha nem lehet tudni, hogy milyen hátsó kapuk, adatcsapdák és egyebek vannak beléjük építve (a nyílt forráskódú esetében viszont – legalább elvileg – lehet). A Linux vagy például a FreeBSD mára könnyen kezelhető és megbízható operációs rendszerré nőtték ki magukat, amikkel ugyanúgy bármit meg lehet csinálni, mint a „fizetős” operációs rendszerek esetében.

Különösen figyeljünk oda a gyermekeink privacy-jére. Ne csak az adataikat ne adjuk ki – különböző kedvezmények reményében –, hanem arra is tanítsuk meg őket, hogy legyenek kellőképpen óvatosak a külvilággal szemben.

A társadalom privacyje a mi ügyünk is: figyeljünk oda például a közterületek bekamerázására, és követeljük meg a hatóságoktól, hogy ha a mi érdekünkben járnak el, akkor bizonyítsák is be az eljárás hatékonyságát.

A Magyar Köztársaság alkotmánya szerint:

„59.§ (1) A Magyar Köztársaságban mindenkit megillet a jóhírnévhez, a magánlakás sérthetetlenségéhez, valamint a magántitok és a személyes adatok védelméhez való jog."

Hogyan tiltsuk le személyes adataink kezelését?

dr. Kalas György Szemétposta c. kiadványa alapján

Az állami adatkezelés letiltása Magyarországon:

Cím*:_____
_____

Nyilatkozat az adatszolgáltatási korlátozásról

A polgárok személyi adatainak és lakcímének nyilvántartásáról szóló 1992. évi LXVI. torvény 2. §-ának (1) bekezdésében biztosított jogommal élve nem járulok hozzá a nyilvántartásban tárolt személyi és lakcímadataimnak a törvényben megjelölt célokon túl való felhasználásához.

Tudomásul veszem, hogy a jegyző, a fővárosi, megyei közigazgatási hivatal vagy a Belügyminisztérium Központi Adatfeldolgozó, Nyilvántartó és Választási Hivatal megkeresésére – eseti engedélyem alapján – az adatszolgáltatási tilalmat feloldhatom.

Kelt:_____200_____

_____
személyi igazolvány száma és olvasható aláírás

Lakhely: _____
Tartózkodási hely:_____

* *Megjegyzés*: A "Nyilatkozatot ajánlott levélben kell a lakó (tartózkodási) hely szerint illetékes jegyzőnek vagy megyei (fővárosi) közigazgatási hivatalvezetőnek, esetleg közvetlenül a hivatalos adatkezelőnek megküldeni (KÖANYV, 1094 Budapest, Balázs B. u. 35.)

A céges adatkezelés letiltása Magyarországon:

Nyilatkozat név és lakcímadatok felhasználásának megtiltásáról

Címzett cég neve:_____
Címe:_____
Tisztelt Cím!

Alulírott az 1995. évi CXIX. tv. 20-21. §-okban foglaltakra hivatkozással felszólítom Önöket, hogy az alábbi személyes adataimat a birtokukban lévő valamennyi üzletszerzési listájukról töröljék, továbbá megtiltom, hogy azt a jövőben ilyen célból felhasználják vagy harmadik személynek átadják:

Név / cím: _____

Kérem tájékoztatásukat, hogy személyes adataimat kitől szerezték és kérem azon harmadik személyek címlistájának megküldését, akiknek személyes adataimat eddig továbbadták.

Kérem intézkedésüket, hogy a fenti nyilatkozatomban foglaltakat az adatkezeléssel érintett harmadik személyek is teljesítsék.

A fentiek alapján kérem írásos tájékoztatásukat bejelentésem teljesítéséről.

Tisztelettel:

Kelt:_____200_____

_____
olvasható névaláírás

Függelék

Az Első Alkotmánymódosítás (1791)

„A Kongresszus nem alkothat olyan törvényt, amely vallást alapít, vagy vallás gyakorlását tiltja, amely korlátozza a szólás- és sajtószabadságot, a nép jogát a békés gyülekezéshez, amely akadályozza, hogy a nép panaszainak orvoslása érdekében kérvényeket juttasson el a Kormányhoz."

A Negyedik Alkotmánymódosítás (1791)

„A népnek azt a jogát, hogy személyük, lakhelyük, irataik és ingóságaik az indokolatlan házkutatások és foglalások ellen védve legyenek, nem lehet megsérteni. Ilyen parancsokat csak esküvel vagy esküpótló nyilatkozattal alátámasztott alapos gyanú esetén lehet kiadni, pontosan megjelölve a kutatás helyét, a lefoglalandó dolgokat vagy a letartóztatandó személyeket."

FIPS (1973)

A Code of Fair Information Practices öt alapelvet mond ki:

Személyes adatokat kezelő rendszerek nem működtethetőek titokban.

Az érintettnek joga van megtudni, hogy milyen adatokat tárolnak róla, és azokat mire használják fel.

Az érintettnek módja kell legyen megakadályozni, hogy egy meghatározott céllal begyűjtött, vele kapcsolatos adatokat a beleegyezése nélkül más célra használjanak.

Az érintettnek joga kell legyen a vele kapcsolatos adatok helyesbítésére vagy kiegészítésére.

A személyes adatokat létrehozó, tároló, használó vagy továbbadó szervezetnek meg kell győződnie róla, hogy a személyes adatokat kizárólag az eredetileg meghatározott célra használják, és meg kell gátolnia a velük való visszaélést.

(U.S. Department of Health, Education and Welfare, Secretary's Advisory Committee on Automated Personal Data Systems, Records, Computers, and the Rights of Citizens viii (1973))

A magyarországi Nagy Testvér Díjak

„*Az Orwell által elképzelt totális diktatúra nem az egyik napról a másikra jön létre... az apró szabadságjogok és a privacy állandó megnyirbálása fog elvezetni hozzá."*

(New Scientist Editorial, 2001. május 5.)

A Privacy International (PI) 1998-ban hozta létre a Big Brother Awardot; ezt különböző országokban minden évben azoknak a kormányzati szerveknek, cégeknek, és magán-személyeknek stb. osztják ki, akik a legtöbbet tették azért, hogy megvalósuljon Orwell disztópiája, ahol a Nagy Testvér mindenkit figyel. Pozitív e-privacy díjat pedig azok kapnak, akik a legtöbbet tették ez ellen.

A Privacy International 2001-ben adott engedélyt a Technika az Emberért Alapítványnak (TEA) a díj magyarországi mutációjának létrehozására és évenkénti kiadására.

Az első Magyarországi Nagy Testvér Díj, 2001. november 28.

Állami szervek Nagy Testvér Díja:

Igazságügyi Minisztérium a munkahelyek és iskolák bekamerázására vonatkozó törvénytervezet miatt.

Az IM javaslata lehetővé kívánta tenni, hogy nyilvános helyeken, sőt, nevesítve oktatási intézményben és munkahelyen azt ott jelenlévő személyek megfigyelése céljából kép- és hangfelvételt rögzítő berendezést helyezzenek el, ehhez mindössze annyi szükséges, hogy a megfigyelés tényéről és az eszköz helyéről tájékoztatást adjon az elhelyező. Ezen kívül a javaslat előírta, hogy ha a felvételen bűncselekmény, szabálysértés vagy fegyelmi vétség gyanúja észlelhető, akkor a felvétel erre vonatkozó részét haladéktalanul át kell adni az eljárás lefolytatására illetékes hatóságnak. A javaslat leplezetlenül a személyek megfigyeléséről és lehallgatásáról szólt, mely a magánszférába történő egyik legdurvább beavatkozás. A „jelen lévő személyek" megfigyelése, mint adatkezelési cél nem felel meg az alapjogok korlátozására fennálló alkotmányossági kritériumoknak.

A törvénytervezeteket tudomásunk szerint olyan kritikák érték, mely miatt az IM átdolgozza javaslatát, azonban ez nem változtat azon, hogy eredeti szándékuk az információs önrendelkezési jog széles körű, elfogadhatatlan korlátozása volt.

Cégek Nagy Testvér Díja:

Tesco-Global Rt Budaörs: az alkalmazottak kamerás megfigyelése miatt.

Az alkalmazottak tájékoztatása és beleegyezése nélkül kamerával figyeli a dolgozóit, a felvételeket tárolja és például munkaügyi viták esetében bizonyítékként visszajátssza nekik.

Magánszemélyek Nagy Testvér Díja:

Répássy Róbert képviselő: a lex Répássy-ért

A Répássy által kidolgozott törvénymódosítás a kötelező sajtó-helyreigazítás mellett bevezette a válaszadás jogának elnevezett intézményt is. Az általánosan elterjedt vélekedés szerint a lex Répássy mögött az újságírók megfélemlítésének szándéka áll.

Ráadásul a MÚOSZ-választmány szerint mind a Polgári-, mind pedig a Büntető Törvénykönyv eddig is lehetővé tette a médiában megjelent és sérelmesnek tartott tényállítás, illetve vélemény miatt személyiségi jogi per indítását.

Közönségszavazatok Nagy Testvér Díja:

Az Országimázs Központ: ebben a kategóriában 39,4 százalékot kapott az internetes szavazóktól, tehát egyértelműen első lett.

Az adatvédelmi biztos ajánlása szerint (amit az OK továbbra is figyelmen kívül hagy):

- vizsgálatot kell folytatni az Országjáró postázásával összefüggő jogellenes adatkezelésekkel kapcsolatban
- gondoskodni kell a lemondó nyilatkozatok, illetve az azokról készült adatállományok megsemmisítéséről
- a jövőben a közérdekű információk terjesztésére olyan megoldást kell választani, amely garantálja a személyes adatok védelméhez fűződő alkotmányos alapjog maradéktalan érvényesülését. A jelenlegi jogi szabályozás szerint állami szervek tájékoztató anyagokat névre szólóan azoknak küldhetnek, akik azt (nevük és lakcímük megadásával) kérik

Pozitív e-privacy díj:

Dr. Majtényi László mint adatvédelmi biztos.

Az utóbbi években vitathatatlanul ő tette a legtöbbet az állampolgárok információs magánszférájának megvédéséért.

A 2001-es zsűri tagjai voltak:

Bojár Gábor (Graphisoft)
Enyedi Ildikó filmrendező
Mérő László matematikus
Orosz Csilla rádiós újságíró
Pelle Andrea jogász (TASZ)

A második Magyarországi Nagy Testvér Díj nyertesei, 2002. november 7.:

Magyarországon 2002-ben másodszor került kiosztásra a Nagy Testvér Díj.

Az, hogy egy szervezet vagy egy magánszemély díjat nyert, nem jelenti azt, hogy a zsűri szerint törvénysértés történt volna – azt viszont igenis jelenti, hogy a zsűri megítélése szerint az adott tevékenység súlyos veszélyt jelent(het) a magánszférára nézve. A díjnak az a célja, hogy erre hívja fel a figyelmet.

A döntést hozó zsűri 2002-ben az alábbiakat találta „méltónak" a Nagy Testvér Díjra:

Cégek Nagy Testvér Díja:

Microsoft: a Passporton keresztül adatokat gyűjtött a felhasználók internetezési szokásairól anélkül, hogy erről tájékoztatta volna őket; a Windows 2000 SP3 telepítéséhez olyan licencet kell elfogadni, melynek értelmében a Microsoftnak joga van a számítógépen található szoftverekről adatokat gyűjteni; a Microsoft Media Player folyamatosan loggolja, hogy a felhasználó milyen zeneszámokat hallgat, stb. A Microsoft Nagy Testvér Díjat kapott az Amerikai Egyesült Államokban és Spanyolországban is.

Állami Szervek Nagy Testvér Díja:

Magyar Rádió: a Magyar Rádió munkatársait írásban kötelezték, hogy az átvilágítás eredményét mutassák be – noha erre a Rádiónak nem lett volna joga.

Magánszemélyek Nagy Testvér Díja:

Lakat T. Károly: közszolgálati televízió munkatársaként a Való Világ házba tett látogatásáért és különösen a gyilkosság elkövetésével gyanúsított kiskorú S. K.-val folytatott televíziós interjúért, illetve eddigi, a médiában való tevékenységéért.

Közönségszavazatok Díja:

BSA: hatóságnak tünteti fel magát és fenyegetően lép fel a felhasználók ellen, noha csupán egyes szoftvergyártók érdekképviseletére létrehozott nonprofit szervezet.

Megjegyzés: Az Országgyűlési Biztosok Hivatala (Péterfalvi Attila, a jelenlegi adatvédelmi biztos nevében, aki ennek a kategóriának a nyerésre esélyes jelöltje volt), 2002. november 4-én juttatott el nekünk a jelöléssel kapcsolatban további, máshogyan nem hozzáférhető információkat, és a Zsűri ezeket is figyelembe véve jutott 5:1 arányban arra az álláspontra, hogy a kérdésben nem tud dönteni, mivel nem állnak megbízható adatok a rendelkezésére.

Az üggyel kapcsolatban több nyílt levelet intéztünk Péterfalvi Attila adatvédelmi biztoshoz. Ugyanis úgy gondoltuk, hogy az ügy egyenlőre nem zárult le. Mivel eddig (*a kézirat nyomdába adásáig*) nem sikerült érdemi választ kapni, jelenleg is ez a helyzet.

Pozitív E-privacy Díj:

Linux-felhasználók Magyarországi Egyesülete (LME) a nyílt forráskódú Linux terjesztéséért és a honosításban vállalt szerepért. A nyílt forráskód a leghatékonyabb eszköz a beépített hátsó ajtók és az egyéb, a felhasználók megfigyelését lehetővé tevő megoldások ellen.

Az LME – Majtényi László volt adatvédelmi biztos után másodikként – nyerte el a pozitív díjat.

Ezúton javasoljuk mindenkinek, hogy személyiségi jogainak védelmében használjon kizárólag nyílt forráskódú szoftvereket (elvégre máskülönben soha nem lehet biztos benne, hogy milyen hátsó ajtók, kémprogramok stb. vannak az általa futtatott programokban).

Megjegyzés: a zsűri tagjai éles vitát folytattak a Big Brother Show, illetve a Való Világ jelöléséről, de végül arra a következtetésre jutottak, hogy ebben az esetben nem kívánnak állást foglalni, mivel alapvetően ízlésvitáról van szó, és ezért egyik kategóriában sem jelölték.

A 2002-es zsűri tagjai voltak:

Enyedi Ildikó filmrendező
Mérő László matematikus
Mihancsik Zsófia újságíró
Orosz Csilla rádiós újságíró
Pelle Andrea jogász (TASZ)
Tordai Csaba jogász (INDOK)

Felhasznált irodalom

Abolins, J. D.: FC: Are your pet's medical records private? DogFancy mag reports... (Politechbot.com, 2002. május 21.)

Ackerman, Elise – Rogers, Paul: Support grows for Ellison's national ID card proposal (Silicon Valley, 2001. október 16.)

Asaravala, Amit: Why Online Age Checks Don't Work (WiredNews, 2002. október 10.)

Baard, Erik: Buying Trouble. Your Grocery List Could Spark a Terror Probe (VillageVoice, 2002. július 24-30.)

Banisar, David: A privacy védelmének modelljei (in.: az Odaátra nyíló ajtó. Az Adatvédelmi Biztos Irodája, Budapest, 2001.)

Bardsley, Marilin: J. Edgar Hoover (The Crime Library, Story Archive)

Black, Edwin: Az IBM és a Holokauszt (Árokszállásy Zoltán fordítása, Atheneum 2000 Kiadó, 2001)

Brekke, Dan – Vesely, Rebecca: CDA Struck Down (WiredNews, 1997. június 26.)

Bright, Martin: Surgical tags plan for sex offenders (Guardian, 2002. november 17.)

Brown, Doug: Is Privacy Too Expensive? (ZDnet Interactive Week, 2001. április 30.)

Burdeau, Cain: Appeals court upholds Louisiana sodomy law (New OrleansNet LLC, 2002. november 22.)

Califa, Pat: Public Sex: The Obscene, Disgusting, and Vile Meese Commission Report (Cultronix, 1986/2)

Canedy, Dana: Tampa Scans the Faces in Its Crowds for Criminals (New York Times, 2001. július 4.)

Carroll, Jim: Surviving the Information Age (Prentice Hall, 1997)

Clarke, Roger: THE RESISTIBLE RISE of THE NATIONAL PERSONAL DATA SYSTEM (Australian National University, 1991)

Delio, Michelle: Rent-a-Car Motto: Speed Bills (WiredNews, 2001. július 12.)

Dyson, Esther: 2.0 verzió. Életünk a digitális korban (HVG, 1998. Kozma Zsolt fordítása)

Eng, Paul: I, Chip? Technology to Meld Chips into Humans Draws Closer (ABCNews, 2002. február 25.)

Foucault, Michel: Felügyelet és büntetés. A börtön története (Gondolat Kiadó, 1990. Fázsy Anikó és Csűrös Klára fordítása)

Garfinkel, Simson: Database Nation. The Death of Privacy in the 21st Century (O'Reilly, 2000)

Gates, Bill: The Road Ahead (With Myhrvold, Nathan és Rinearson, Peter, Viking, 1995)

Gilbert, Aloire: „Smart" carts on a roll at Safeway. Think flashy banner and pop-up ads are limited to the Web? Think again (CNet, 2002. október 28.)

Gleiser, Robert L.: Alan Dershowitz: Civil Libertarian for Torture (Upstream, 2001. november 9.)

Goldman, Eric: On My Mind: The Privacy Hoax (Forbes.com, 2002. szeptember 26.)

Goldman, Jim: FDA Launches Investigation Into VeriChip (ABCNews, 2002. május 17.)

Goldstein, Ritt: US planning to recruit one in 24 Americans as citizen spies (Sydney Morning Herald, 2002. július 15.)

Graham-Rowe, Duncan: Warning! Strange behaviour (New Scientist, 1999.december 11.)

Greene, Thomas C.: Brain-scans can defeat terrorism, InfoSeek founder claims (The Register, 2001. október 3.)

Greenhouse, Linda: Justices to Review Internet Pornography Filters (New York Times, 2002. november 13.)

Greenhouse, Linda: Supreme Court Bars High-Tech Snooping (New York Times, 2001. június 12.)

Halbfinger, David M.: Police Dragnets for DNA Tests Draw Criticism (New York Times, 2003. január 4.)

Halmai Gábor: Kommunikációs Jogok (Új Mandátum Könyvkiadó, 2002)

Hamilton, Alexander – Madison, James – Jay, John: A föderalista. Értekezések az amerikai alkotmányról (Balabán Péter fordítása, Európa Könyvkiadó, 1998.)

Harmon, Amy: Survey About Accountability Online (New York Times, 2001. július 10.)

Herman, Burt: IBM, Holocaust Author Denies Claims (NewsDesk, 2001. február 23.)

Hinsliff, Gaby: Bid to outlaw DNA trophy hunters (Guardian Unlimited, 2002. március 3.)

Hoffman, Donna L. – Novak, Thomas P.: A Detailed Analysis of the Conceptual, Logical, and Methodological Flaws in the Article: „Marketing Pornography on the Information Superhighway" (1995. július 2., Vanderbilt University eLab)

Horne, Terry: No-call phone privacy list rings up dollars for state (Indiana Star, 2002. október 17.)

Innes, Brian: A kínzás és kínvallatás története (Canissa Kiadó, é. n., Dr. Képes György fordítása)

Javorniczky, István – Majtényi, László (szerkesztők): Adatőrségen. Történetek a Tüköry utcából (Emberi Jogi Információs és Dokumentációs Központ, 1999.)

Johnson, Steve: Software sought to expose terrorist cells (Mercury News, 2001. október 9.)

Johnston, Jennifer: Big Borders bookshop is watching you (Sunday Herald, dátum nélkül)

Jones, Nicola: Here comes Big Brother (New Scientist, 2001. szeptember 22.)

Kaczynski, Ted: Unabomber's Manifesto

Kalas, György: Szemétposta, avagy mit tehetünk a postaládánk és személyes adataink védelmében (REFLEX Környezetvédelmi Egyesület, é. n.)

Keane, John: Média és demokrácia (Helikon Kiadó, 1999. Kulcsár Vera fordítása)

Kettmann, Steve: Privacy Czar: Past Haunts Present (WiredNews, 2002. október 19.)

Knight, Will: Controlling encryption will not stop terrorists (New Scientist, 2001. szeptember 18.)

Knight, Will: Malaysia pioneers smart cards with fingerprint data (New Scientist, 2001. szeptember 21.)

Knight, Will: Weakened encryption lays bare al-Qaeda files (New Scientist, 2002. január 17.)

Lake, David: An Eye for Eye. More companies are looking to retinal and finger scans for better security. (The Industry Standard, 2001. július 16.)

Lane, Charles: In Terror War, 2nd Track for Suspects. Those Designated 'Combatants' Lose Legal Protections (Washington Post, 2002. dec. 1.)

Lebihan, Rachel: Aust: Encryption crackdown gets thumbs down (ZDNet Uastralia, 2001. szeptember 17.)

Lemos, Robert – Losen, Stephanie: Proposed crypto limits draw broad criticism (CNet, 2001. szeptember 26.)

Lessig, Lawrence: Hogyan szabályozzuk a szólást az interneten? (Fundamentum, 1999/1. Jóri András fordítása)

Levy, Stephen: Crypto (Penguin Books, 2002).

Loper, George Edward: Blast from the Past: Early TIPS Corps Did More Harm Than Good In Hunt for Subversives (loper.org, 2002. október)

Manguel, Alberto: Az olvasás története (Park Kiadó, 2001. Széky János fordítása)

Marcoff, John – Schwartz, John: Many Tools of Big Brother Are Up and Running (New York Times, 2002. december 23.)

McAuliffe, Wendy: Americans back encryption controls (MSNBC, 2001. szeptember 18.)

McCarthy, Kieren: Brits want ID cards, not worried about privacy (The Register, 2001. október 24.)

McCullagh, Declan: Call It Super Bowl Face Scan I (WiredNews, 2001. február 2.)

McCullagh, Declan: Can't Scan Without a Warrant (WiredNews, 2001. június 12.)

McCullagh, Declan: Porn Panel Plays It Safe (WiredNews, 2002. május 2.)

McCullagh, Declan: Reporters Scowl at Face Scanners (WiredNews, 2001. augusztus 9.)

McCullagh, Declan: Smut Filter Snags Non-Smut, Too (WiredNews, 2002. március 27.)

McCullagh, Declan: The Case of the Two Cybersex Studies (1995. július 24.)

McCullagh, Declan: Too Broad a Ban on Child Models? WiredNews, 2002. május 9.)

McWilliams, Peter: Ain't Nobody's Business If You Do (Prelude Press, 1996)

Norris, Clive: End of Award Report to the Economic and Social Research Council (1997, L210252023)

Olsen, Stephanie: ACLU decries face-recognition tools (CNet, 2002. január 3.)

Overby, Stephanie: Iceland's Dilemma: Privacy vs. Progress (CIO Magazine, 2001. július 15.)

Pasanella, Marco: Room to Improve: Tactics for Privacy in a City of Snoops (New York Times, 2001. június 14.)

Pease, Allan – Pease, Barbara: Miért nem képesek többfelé figyelni a férfiak és miért nem tudnak eligazdni a térképen a nők? (Fiesta, 2000. Szűr-Szabó Katalin fordítása)

Pew Internet & American Life: Americans say new email laws needed (NUA, 2001. április 3.)

Polen, Ben: ACLU Exec Voices Concerns (WiredNews, 2001. december 31.)

Pool, Itiel de Sola (editor): The Social Impact of the Telephone (The MIT Press, Cambridge, Massachusetts, 1993)

Priest, Dana – Gellmann, Barton: U.S. Decries Abuse but Defends Interrogations. 'Stress and Duress' Tactics Used on Terrorism Suspects Held in Secret Overseas Facilities (Washington Post, 2002. december 26.)

Puzzanghera, Jim: ANTI-TERROR PLAN RISKS MANY FALSE FINDINGS. Database monitor far from a reality (Mercury News, 2002. december 26.)

Restnick, Paul – Richardson: See No Evil: How Internet Filters Affect the Search for Online Health Information (Henry J. Kayser Family Foundation, 2002)

Robinson: Jeffrey: Manipulátorok. Vásárló leszel ha tetszik, ha nem (Athenaeum 2000Kiadó, 2001. Gere István fordítása)

Rutenberg, Jim: Torture Seeps Into Discussion by News Media (New York Times, 2001. november 5.)

Scheeres, Julia: Airport Face Scanner Failed (WiredNews, 2002. május 16.)

Scheeres, Julia: Face Scanners Turn Lens on Selves (WiredNews, 2001. július 31.)

Scheeres, Julia: Live From N.Y.: Security Cam Hams (WiredNews, 2001. május 3.)

Scheeres, Julia: London's Privacy Falling Down (Wired News, 2002. november 2.)

Scheeres, Julia: They Want Thei ID Chips Now (WiredNews, 20002. február 6.)

Schlesinger, Arthur M. (ed.): Writings and Speeches of Eugene V. Debs (New York: Hermitage Press, 1948)

Schwartz, John: Password Protection With Prison Stripes (New York Times, 2001. augusztus 6.)

Sebok, J. Anthony: IBM AND THE HOLOCAUST: The Book, The Suit, And Where We Go From Here (FindLaw, 2001. március 12.)

Shade, Leslie Regan: Is there Free Speech on the Net? Censorship in the Global Information Infrasturcture (in: Cultures of Internet. Virtual Spaces, Reral Histories, Living Bodies, Sage Publications, 1996. Edited by Rob Shields)

Shallit, Jeffrey: Book Review: „Slouching Towards Gomorrah" (University of Waterloo, Ontario, Canada)

Simons, John: Greed Meets Terror. Can biometric systems foil terrorists? Probably not--but try telling that to Wall Street (Fortune, 2001. október 29.)

Smith, Robert Ellis: Ben Franklin's Web Site. Privacy and Curiosity from Plymouth Rock to the Internet (Sheridan Books, 2000)

Sunstein, Cass: republic.com (Princeton University Press, 2001)

Sz. n.: A history of surveillance cameras in England 1961 to 1998 (notbored.org)

Sz. n.: Ashcroft v. ACLU (formerly ACLU v. Reno II). The Legal Challenge to the Child Online Protection Act (EPIC)

SZ. n.: Banned Books Online (University of Pennssylvania Libray)

Sz. n.: Biometrics, Surveillance, National ID Threats to Privacy (Electronic Frontier Foundation, Press Release, 2002. június 13.)

Sz. n.: Children 'find porn through file-sharing' (BBC News, 2001. július 27.)

Sz. n.: Demszky sértőnek tartja Körmendy-Ékes álláspontját (Index, 2000. október 31.)

Sz. n.: Empowering Identification. 50 Years of Collective Corporate Existence (identix)

Sz. n.: Epic Total Information Awareness Page (Electronic Privacy Information Center)

Sz. n.: Esther Dyson on Internet privacy (CNet, 2002. április 27.)

Sz. n.: Europe Drives For Online Privacy (Reuters, 2001. május 15.)

Sz. n.: Glitches in Japanese ID System (AP, 2002. augusztus 5.)

Sz. n.: Gyermekek adatait árusítja a Belügyminisztérium (Korridor, 2001. április 24.)

Sz. n.: Informat Fever (Editorial, New York Times, 2002. július 22.)

Sz. n.: Internet Filtering Software Wrongly Blocks Many Sites (EFFector, Vol. 15, No. 30, 2002. szeptember 27.)

Sz. n.: Japanese ID system reports data leak (CNN, 2002. augusztus 7.)

Sz. n.: Juki Net goes online (Editorial, Asahi Shimbun, Aug. 6)

Sz. n.: Lawyer to drop IBM Holocaust case (ZDNet UK, 2001. március 30.)

Sz. n.: Leaving your mark, morning to night (Milford Daily News, 2003. január 5.)

Sz. n.: Online Pornography Statistics (dilternet.org)

Sz. n.: Parents and the V-chip (Kaiser Family Foundation, 2001. július, Chart Pack)

Sz. n.: Personal data on residents of entire town stolen (japan Today, 2003. január 4.)

Sz. n.: Privacy fears over DNA database (BBC News, 2002. szeptember 16.)

Sz. n.: Remembering Harvey Job Matusow, 1926-2002 (magicmouse)

Sz. n.: Report: Easier than ever to be spied upon. New laws pitch national security vs. personal privacy (CNN, 2002. szeptember 4.)

Sz. n.: Surveillance Cameras Incite Protest (New York Times, 2001. július 16.)

Sz. n.: The Unabomber Case (CNN interactive Time, 1997)

Sz. n.: The Unknown Crisis: Child Pornography on the Internet (Anti Child-Porn Organisation White Paper)

Sz. n.: Violence Chip (ACLU online archives)

Sz. n.: What's Wrong With Public Video Surveillance? (ACLU, 2002)

Sz. n.: WSD (World {Sousveillance, Subjectrights} Day) (Press Release, 2002)

Székely Iván: A magánélet védelme és az információs jogok (in.: Eszmélet, 1995, 27. szám)

Székely Iván: Az adatvédelem és az információszabadság néhány elméleti és gyakorlati aspektusa (egyetemi doktori értekezés, Budapesti Műszaki Egyetem, 1994. A szerző szívességéből)

Thorsberg, Frank: PC World poll highlights privacy concerns (CNN, 2001. október 8.)

Thorwald, Jürgen: Detektívek évszázada (Minerva, 1969, Dr. Auer Kálmán fordítása)

Urban, Andrew L.: Lolita. Without a Gender Agenda? (Cinefile Features, 1998)

Venetianer, Pál: A DNS szép új világa. Kulturtrade, 1998.)

Wacquant, Loic: A nyomor börtönei. A zéró tolerancia világméretű terjedése (Helikon Kiadó, 2001. Köböl Anna fordítása)

Wallace, Jonathan D.: PURCHASE OF BLOCKING SOFTWARE BY PUBLIC LIBRARIES IS UNCONSTITUTIONAL (A Briefing Paper)

Wallace, Patricia: Az internet pszichológiája (Osiris, 2002. Krajcsi Attila fordítása)

Walsh, Edward: High-Tech Devices Require a Warrant (Washington Post, 2001. június 12.)

Weil, Nancy: COMDEX: Invasive technologies don't fight terrorism (NetworkWorldFusion, 2002. november 20.)

Winik, Jay: Security Before Liberty (Wall Street Journal, 2001. október 23.)

Zwick, Jim: Mark Twain on Book Banning: Huckleberry Finn to Eve's Diary (boondocksnet.com)

Köszönetnyilvánítás

Miként annyi más könyvnek, ennek is mindössze egyetlen név van feltüntetve a címlapján – ugyanekkor viszont nagyon is hosszú azoknak a listája, akiknek a segítsége/közreműködése nélkül nem jöhetett volna létre. Megpróbálok közülük néhányat – a teljesség igénye nélkül – felsorolni.

Első helyen a feleségemet kell megemlítenem, aki képes (és ami ennél is több: hajlandó) volt elviselni, hogy az utóbbi hónapokban éjjel-nappal ezen a könyvön dolgozom – régebben soha nem értettem, hogy a szerzők miért érzik kötelezőnek az effajta tiszteletkört. Ma már pontosan értem.

Dr. Székely Iván társadalmi informatikus (CEU) meghatározó szerepet játszott abban, hogy elkezdtem az elektronikus privacyvel foglalkozni és a továbbiakban is minden lehetséges segítséget megkaptam tőle – ezért őszintén hálás vagyok neki. Mint ahogy a Privacy International alapítója és a Nagy Testvér Díj létrehozója, Simon Davies mellett őszintén hálás vagyok Peter Kuhmnak és a Big Brother Awards Austria-nak is: ha segítségre volt szükségem, elég volt írnom egy e-mailt (akár site hostolásról, akár bármilyen más problémáról volt szó).

Folyamatos és nagyon is emberi támogatást kaptam a Technika az Emberért Alapítvány kuratóriumától, név szerint: Keményffy Tamástól, Mink Andrástól, Németh Vilmostól és Orsós Jakab Lászlótól – nem hinném, hogy az ő nevük elválasztható lenne ettől a könyvtől (vagy éppen a magyarországi Nagy Testvér Díjtól).

Mint ahogy elválaszthatatlan az E-privacy olvasókönyv a Soros Alapítványtól is, ami – per pillanat Magyarországon gyakorlatilag az egyedüliként – folyamatosan felvállalja az elektronikus privacy támogatását. Nekik is szeretném megköszönni.

És hasonlóképpen a Nagy Testvér Díj zsűrije tagjainak is, akik – miközben ismert közéleti személyiségek és szakemberek – eléggé fontosnak érezték a kérdést ahhoz, hogy ne csupán a nevüket adják hozzá, de némi időt is szenteljenek rá.

Dr. Galántai Zoltán