Matej Kovačič

NADZOR IN ZASEBNOST V INFORMACIJSKI DRUŽBI

55

Matej Kovačič

NADZOR IN ZASEBNOST V INFORMACIJSKI DRUŽBI

Filozofski, sociološki, pravni in tehnični vidiki nadzora in zasebnosti na internetu

Znanstvena knjižnica
Fakulteta za družbene vede
Ljubljana, 2006

Matej Kovačič

NADZOR IN ZASEBNOST V INFORMACIJSKI DRUŽBI
Filozofski, sociološki, pravni in tehnični vidiki nadzora in zasebnosti na internetu

Izdajatelj:
Univerza v Ljubljani, Fakulteta za družbene vede
Kardeljeva ploščad 5, Ljubljana

Zbirka:
Znanstvena knjižnica 55

Urednik:
dr. Niko Toš

Uredniški odbor:
dr. Vlado Benko, dr. Zdenko Roter,
dr. Tomo Korošec, dr. Vlado Miheljak, dr. Niko Toš

Recenzenta:
dr. Slavko Splichal
dr. Alenka Šelih

Likovna oprema:
Polona Mesec-Kurdija

Lektura: Dora Mali

CIP - Kataložni zapis o publikaciji
Narodna in univerzitetna knjižnica, Ljubljana

342.721:004.738.5
004.738.5

KOVAČIČ, Matej, 1974-
Nadzor in zasebnost v informacijski družbi [Elektronski vir] : filozofski, sociološki, pravni in tehnični vidiki nadzora in zasebnosti na internetu / Matej Kovačič. - Ljubljana : Fakulteta za družbene vede, 2006. - (Znanstvena knjižnica / Fakulteta za družbene vede ; 55)

Način dostopa (URL): http://dk.fdv.uni-lj.si/eknjige/EK_Kovacic_2006_Nadzor.pdf . - Opis temelji na verziji z dne 19.12.2006

ISBN-10 961-235-261-5
ISBN-13 978-961-235-261-5

230725632

Knjigo je sofinancirala Agencija za raziskovalno dejavnost Republike Slovenije.

KAZALO

PREDGOVOR

Vprašanji zasebnosti in nadzora, ki ju obravnavam v pričujočem delu, raziskujejo številni raziskovalci in strokovnjaki, s temi problemi pa se ukvarjajo tudi številni aktivisti za varstvo človekovih pravic. Zaradi soodvisnosti je nujno interdiciplinarno in hkratno obravnavanje obeh vprašanj. Gre namreč za problematiko, ki ima družboslovne, pravne, filozofske in tehnološke razsežnosti in se globoko dotika pravic posameznikov oziroma uporabnikov interneta. Ob tem imamo opravka s tehnologijo, ki se silno hitro razvija. Vsi ti razlogi narekujejo, da je poglobljeno raziskovanje tega področja še kako relevantno in aktualno.

Problemi, s katerimi se ubadajo praktično vsi raziskovalci tega področja, zadevajo predvsem odsotnost nedvoumne in jasne definicije, kaj sploh je zasebnost. Vzrok za to nedorečenost pa je delno tudi v tem, da je pojem in obseg pravice do zasebnosti podvržen nenehnim vplivom družbenih in tehnoloških sprememb. Poleg tega je pri preučevanju zasebnosti moč opaziti prevladujoč pristop, značilen predvsem za ameriške avtorje in zasebnostne aktiviste, ki kot grožnjo zasebnosti vidijo predvsem državo; vplivi družbene sfere so pri tem pogosto zanemarjeni. Poleg tega sta vprašanji zasebnosti in nadzorovanja na internetu mnogokrat razumljeni in obravnavani predvsem kot tehnična problema oziroma problema, ki ju je mogoče rešiti zgolj z uporabo tehnologije, njuni družbeni vidiki pa so ob tem zapostavljeni. Ni naključje, da pri varstvu elektronske zasebnosti pogosto naletimo na poudarjanje zgolj tehničnega varovanja in informacijske varnosti, pomen zaščitne zakonodaje in varnostne kulture pa je mnogokrat spregledan.

Prav tako zahteva posebno pozornost vprašanje razumevanja sodobnega nadzorovanja. Nadzorovanje je še vedno pogosto dojeto predvsem v smislu Benthamovega Panoptikona v povezavi z disciplinarno oblastjo. Številni zasebnostni aktivisti nadzor pogosto dojemajo zgolj kot sredstvo izvajanja moči in discipline nad posameznikom. Vendar pa se je sodobno nadzorovanje skozi zgodovino preoblikovalo. Poleg disciplinarne oblasti se je namreč začela oblikovati tudi regulacijska. Če je disciplinarna oblast osredotočena na posameznika, na njegovo "dresuro", podrejanje in discipliniranje, se regulacijska oblast osredotoča na populacijo. Njen namen ni vplivati na konkretnega posameznika, temveč uvajati regulacijske mehanizme, ki naj ohranijo ravnotežje na globalni ravni, in identifikacija tveganja in priložnosti. Zato nadzorovanje danes ni samo neposredno in "prisilno", marveč postaja konsenzualno in vsenavzoče. Slednje je tudi razlog, zakaj so zasebnostni aktivisti, ki opozarjajo na negativne vidike sodobnih tehnologij, pogosto označeni dobesedno kot nazadnjaki, ki želijo zaustaviti napredek, in kot domnevni paranoiki, ki se bojijo povsem neškodljivih in sprejemljivih, pravzaprav celo koristnih tehnologij.

Dodatne težave povzroča tistim, ki preučujejo ta področja, težavnost pri dostopu do relevantnih podatkov, ki bi omogočali preučevanje uveljavljenih nadzorovalnih praks. Preučevanje nadzorovalnih praks in kršitev zasebnosti posameznikov sta s strani akterjev, ki izvajajo nadzor, razumljivo slabo sprejeta in ju skušajo omejevati. Kljub zamislim o transparentnosti delovanja države na področju nadzorovanja posameznikov še vedno vladajo številne arkanske prakse.

Varnost (in še posebej nacionalna varnost) je vse prepogosto izgovor za skrivanje celo najbolj trivialnih podatkov o nadzorovalnih praksah. Ni nenavadno, da je eno poglavitnih "orožij" raziskovalcev vprašanj zasebnosti in zasebnostnih aktivistov povsod po svetu ravno zakonodaja, ki omogoča dostop do informacij javnega značaja.

Do relevantnih podatkov, predvsem podatkov tajnih služb, v nekaterih primerih pa tudi zasebnih podjetij, je težko priti. To se je izkazalo tudi pri zbiranju gradiva za to delo, ko sem za potrebe raziskovanja želel pridobiti statistične podatke o številu prikritih preiskovalnih ukrepov, ki jih izvaja *Slovenska obveščevalno-varnostna agencija*. SOVA je dostop do letnega pregleda števila preiskovalnih ukrepov zavrnila, enako tudi uradni pooblaščenec za dostop do informacij javnega značaja na Vrhovnem sodišču RS, pooblaščenka za dostop do informacij javnega značaja pa pritožbi ni ugodila.

Relevantne podatke je zato pogosto treba dobiti iz sekundarnih virov ali s pomočjo ocen, v nekaterih primerih pa so organizacije za varstvo elektronske zasebnosti (npr. *Statewatch* ter *quintessenz*) pridobile in nato javno objavile tudi zaupne dokumente. Kljub spornosti takega početja so ti dokumenti za raziskovanje izrednega pomena.

Podobno je pri preučevanju zlorab zasebnosti s strani kiberkriminala. Po eni strani so kršitve zasebnosti (v obliki vdorov v informacijske sisteme, kraje podatkov, elektronskega prisluškovanja itd.) za navadne uporabnike interneta pogosto nezaznavne, po drugi strani pa žrtve teh kršitev o tem velikokrat sploh nočejo govoriti, mnogokrat kršitev niti ne prijavijo policiji. Razumljivo je, da tudi akterji, ki izvajajo nezakonit nadzor, t. i. hekerji, o svojih dejavnostih pogosto niso pripravljeni spregovoriti. Zbiranje teh podatkov, predvsem pogovori s hekerji, katerih del je objavljen tudi v tem delu, je zahtevalo precej truda. Zaradi teh težav je tako raziskovanje po svoje podobno obveščevalnemu delu, raziskovalec, ki se želi tudi bolj konkretno spoznati z delovanjem nadzorovalnih tehnologij in z nadzorovalnimi praksami, pa se včasih še sam giblje na meji zakonitega.

Vsekakor se problematika zasebnosti in nadzora na internetu pod vplivom hitrih tehnoloških sprememb in potreb zasebnega sektorja zelo hitro razvija. Problem interneta je predvsem v tem, da tehnologija že sama po sebi, zaradi svojih lastnosti, omogoča nekatere zlorabe zasebnosti v večji meri, kot bi bile mogoče v fizičnem prostoru. Povečana možnost vsenavzočnosti in prepustnost teritorialnih meja je privedla do tega, da izgubljamo zaščitno vlogo prostora. Računalniška omrežja omogočajo decentraliziran nadzor, saj lahko omogočijo povezovanje formalno ločenih nadzornih sistemov prek telekomunikacijskih sredstev. Pomembna lastnost računalnikov pa je tudi njihova zmožnost shranjevanja oziroma arhiviranja podatkov, kar omogoča gradnjo arhivov oziroma dosjejev. Oblike zlorab zasebnosti na internetu so sicer podobne kot v fizičnem svetu, le s to razliko, da se te zlorabe v internetu kažejo drugače in da zaradi tehnologije prihaja do njih v večjem obsegu, saj je (informacijska) tehnologija nadzorovanje poglobila in okrepila. Zato je teoretično in praktično poznavanje informacijsko komunikacijskih tehnologij nujnost, nekakšen predpogoj, s katerim se srečujejo vsi, ki se ukvarjajo z raziskovanjem nadzora na internetu. Prav tako je pri preučevanju kriptografije poleg poznavanja njene zgodovine in vloge v družbi nujno vsaj osnovno poznavanje matematičnih načel njenega delovanja.

Ker gre pri pravici do zasebnosti za vprašanje ene izmed človekovih pravic, ukvarjanje s to problematiko na neki točki zahteva tudi osebno opredelitev. To velja zlasti takrat, kadar pri raziskovanju naletimo na konkretne primere zlorab ali spornost nadzorovalnih praks. Javno opozarjanje na probleme ter ponujanje možnih rešitev pa že pomeni družbeno angažiranje. Zato ni presenetljivo, da so organizacije za varstvo zasebnosti, kot na primer *Electronic Privacy Information Center* ali *Privacy International*, in posamezniki, ki sodelujejo z njimi, hkrati raziskovalne in aktivistične organizacije.

Eno izmed osrednjih vprašanj, ki si jih zastavljam v delu, je vprašanje, ali je internet "tehnologija svobode", kot so nekateri verjeli v začetku 90. let prejšnjega stoletja, ali pa je panoptičnost že vgrajena vanj. Nadzorovalne prakse in uvajanje nekaterih novih tehnologij za zaščito intelektualne lastnine, nastanek monopolov in posledično monokulture na področju operacijskih sistemov za zasebnost na internetu ne prinašajo nič dobrega. Enako velja za družbeni razvoj, predvsem razvoj neposrednega trženja in sodobnih modelov trženja in pooseblјenja storitev, ki zahtevajo zbiranje velikega števila osebnih podatkov. Prav tako ne smemo zanemariti vpliva terorističnih napadov 11. septembra 2001 v ZDA na povečanje državnega nadzorovanja. Splošna ugotovitev je, da vse to ožji pravico posameznikov do zasebnosti. Vprašanje, ki ostane na koncu, pa ni zgolj to, ali je vprašanja zasebnosti smiselno preučevati, temveč predvsem, ali se je za zasebnost treba tudi dejavno bojevati?

ZASEBNOST

Različne študije kažejo, da je zasebnost nekaj, kar je medkulturno in medvrstno univerzalno in ni značilno samo za človeka.[1] Tako nekatere navedbe v bibliji (npr. zavedanje Adama in Eve, da sta gola, zavedanje o goloti Noeta in povezovanje golote s sramoto itd. (Wagner DeCew, 1997: 11)), pa tudi v koranu, judovski tradiciji, antični Grčiji in starodavni Kitajski (Laurant, 2003: 5) kažejo na to, da zasebno sfero poznajo različne kulture in družbe.[2] Vendar pa je tisto, kar danes poznamo pod imenom zasebnost oziroma pravica do zasebnosti, pravzaprav iznajdba razsvetljenstva, torej nekaj, kar nastane na zahodu šele v času nastanka kapitalizma, nekoliko jasneje pa se začne izražati šele ob "nastanku" oziroma kodificiranju univerzalnih človekovih pravic.

Ni naključje, da se pravica do zasebnosti pravzaprav izrazito veže na zahodni kapitalizem in na nastanek individualizma ter človekovih pravic. *Afriška deklaracija o človekovih in ljudskih pravicah* iz leta 1981 (ang. *African Charter on Human and Peoples' Rights*) npr. pravice do zasebnosti sploh ne omenja, na Japonskem se je pravica do zasebnosti pojavila šele po drugi svetovni vojni s prihodom Američanov (Gutwirth, 2002: 26), *Univerzalna islamska deklaracija človekovih pravic* iz leta 1981 (ang. *Universal Islamic Declaration of Human Rights*) pa zasebnost v 21. členu sicer omenja, vendar so nekateri avtorji mnenja, da je obseg razumevanja zasebnosti v islamu bistveno bolj omejen kot v Evropi in ZDA (Gutwirth,2002: 28).

Kljub temu da se zasebnost kot vrednota in posledično kot pravica začne uveljavljati šele v 18. stoletju, pri njenem priznanju ne gre za proces, katerega obseg bi se skozi čas širil, temveč prav nasprotno. Zasebna sfera se skozi zgodovino oži, pravica do zasebnosti pa v zadnjih letih postaja čedalje bolj omejena. Pravo pravico do zasebnosti sicer ščiti in na nekaterih področjih navidezno celo širi (čeprav gre pri teh "širitvah" večinoma zgolj za sledenje tehnološkemu in družbenemu razvoju, pogosto pa celo zgolj za legitimizacijo uveljavljenih praks vdiranja v zasebnost), vendar zasebnost kot vrednota v družbi izgublja pomen.

Zasebnost ščiti svobodo posameznika, zato za tradicionalnega nasprotnika zasebnosti večinoma velja država, vendar se svoboda ne nanaša zgolj na odnos posameznika do politične oblasti, temveč tudi do družbe. Zato je danes pravzaprav poglavitni akter, ki ogroža zasebnost posameznikov, družba, država pa ima ambivalentno vlogo – po eni strani posega v zasebnost posameznikov, po drugi strani pa posameznika varuje pred vplivi družbe. Vloga družbe pri omejevanju posameznikove zasebnosti postane očitna predvsem po zgodovinskem pregledu odnosa med zasebno in javno sfero ter pri analizi sodobnega nadzorovanja, ki kaže, kako se je izoblikovalo tisto, čemur danes pravimo družba nadzora. Da so vplivi na zasebno sfero s strani družbe pravzaprav bistveno bolj problematični kot posegi s strani države, pa kaže primerjava med pravnim varstvom zasebnosti v Evropi in ZDA, predvsem na področju informacijske zasebnosti.

---

[1] Alan Westin je npr. ugotovil, da se tudi živali v določenih obdobjih zatečejo v samoto ali v intimen objem manjših skupin, poleg tega na obstoj zasebnosti kaže tudi branjenje lastnega teritorija (Wagner DeCew, 1997: 12).

[2] Raziskave Elshtainove so pokazale, da je razlikovanje med javnim in zasebnim temeljno za vse znane družbe (Wagner DeCew, 1997: 12).

V sodobni družbi namreč postaja zasebnost tržno blago, s katerim je mogoče trgovati, in ne več pravica, ki jo je treba varovati. Poleg tega je v sodobni družbi zasebnost pogosto dojemana kot ovira, bodisi drugih posameznikov (npr. prostemu razpolaganju z zasebno lastnino v primeru zasebnosti na delovnem mestu, svobodi govora itd.) bodisi javnega interesa (v zvezi z vprašanji javne varnosti in javnega zdravja) ter drugih skupnih pravic in interesov (predvsem ekonomskih in množičnih medijev) (Gutwirth, 2002: 46).

Univerzalne definicije zasebnosti in pravice do zasebnosti ni. Vzrok za to je, da je zasebnost relativna, kontekstualna in subjektivna. Vsakdo ima drugačna pričakovanja glede zasebnosti in ta se spreminjajo tudi glede na družbeni kontekst. Problem definicije zasebnosti je tudi v tem, da zasebnost ščiti svobodo posameznika, "*individualna svoboda pa ne more biti ne napovedana, ne pogojena*" (Gutwirth, 2002: 31), saj ima za vsakogar drugačen pomen. To je tudi razlog, zakaj se tudi pravna teorija izogiba natančnemu definiranju pravice do zasebnosti in zakaj preveč natančno definiranje zasebnosti niti ni zaželeno. Če bi bila namreč preveč natančno definirana, bi se lahko nekoč v prihodnosti izkazalo, da je definirana preozko. Tako se zasebnost v sodni praksi ne nanaša le na pravico biti sam ter zaščito posameznika pred nepooblaščenim in neupravičenim nadzorovanjem, temveč tudi na pravico do svobodnega odločanja o rojstvu otrok, svobodnega odločanja za različne spolne prakse, na podlagi pravice do zasebnosti pa so sodišča posameznike zaščitila tudi pred izpostavljenostjo škodljivim vplivom iz okolja (smrad, hrup, toksične emisije) itd. Namesto doslednega in togega definiranja obsega pravice do zasebnosti se obseg le-te v sodni praksi določa ob tehtanju konkretnih primerov. Žal pa to tudi pomeni, da je širjenje varstva zasebnosti praviloma le reakcija na veljavno stanje, predvsem na tehnični in družbeni napredek.

Zasebnost je torej pomembna zato, ker ščiti svobodo posameznika: posamezniku omogoča svobodno odločanje, odločanje brez vmešavanja in prisile drugih, pri čemer je treba poudariti, da prisila ni nujno samo neposredna, fizična ali vidna, temveč gre lahko tudi za manipulacijo in pritiske normalizacije. V tem oziru se zasebnost nanaša na vzpostavitev meje med posameznikom in drugimi, ki po eni strani preprečuje odtekanje informacij o posamezniku k drugim, po drugi strani pa posameznika ščiti pred zunanjimi vplivi. Zato zasebnost posameznikom omogoča osebno in, kot je pokazala Arendtova, tudi politično in družbeno emancipacijo. Svoboda, avtonomija in samoodločanje so zato bistvene prvine zasebnosti (Gutwirth, 2002: 60). Podobno stališče je glede pravice do zasebnosti zavzela tudi pravna stroka.

Internet je probleme zasebnosti prenesel tudi v virtualni prostor, v katerem informacijsko komunikacijska tehnologija omogoča številne nove tehnične načine zlorab zasebnosti.[3] Poleg tega pri razvoju interneta še vedno pogosto prevladuje ameriški pravni sistem in ameriške korporacije, zato na internetu prevladuje ameriški način obravnavanja zasebnosti, predvsem njegove pomanjkljivosti. Čeprav zakonodaja ščiti zasebnost posameznikov, pa hiter tehnološki

[3] Pred nastankom interneta sta bili sferi javnosti in zasebnosti veliko bolj ločeni. Od nastanka interneta pa te ločitve ni več, sferi sta konvergirali. Uporabnik, ki vstopi v internet, je v obeh sferah hkrati, regulacija ene sfere pa vpliva tudi na drugo. V pričujočem delu se ukvarjam z vprašanjem varovanja zasebnosti na internetu, ne pa tudi z vprašanjem (varovanja) javnosti na internetu.

razvoj nadzorovalnih tehnologij in pritiski družbe zasebnost pravzaprav čedalje bolj ožijo. Zasebnost tako ostaja zgolj možnost za tiste, ki si jo lahko privoščijo, cena zanjo pa je vse višja.

Nastanek sodobne zasebnosti: od polja prisile do polja svobode

Kot rečeno, se je zasebnost v obliki, kot jo poznamo zdaj, se pravi v obliki pravice in pozitivne vrednote, začela oblikovati šele v obdobju razsvetljenstva. Arendtova ugotavlja, da se je zasebna sfera razvila šele z uveljavitvijo novoveškega individualizma (Arendt, 1958/1995: 40), čeprav je delitev na javno in zasebno sfero veljala že prej. Pri tem je bil obseg zasebne sfere včasih sicer večji, a je bil njen pomen bistveno drugačen, kot ji ga vsaj deklarativno pripisujemo danes. Za antiko je bilo značilno, "*da je vse zasebno samo zasebno, da je človek v zasebnem ... živel v nekem stanju oropanosti, in sicer je bil oropan najvišjih zmožnosti in človeških sposobnosti. ...pravzaprav ni bil človek*" (Arendt, 1958/1995: 40). Človek je bil v zasebni sferi bolj primerek rodu, in ne toliko človek (Arendt, 1958/1995: 48). Še več, če zasebnost danes pravzaprav predstavlja polje svobode, je bilo v antični Grčiji ravno nasprotno, saj je bil sedež svobode v javni sferi (na političnem področju), za zasebno sfero pa je bila značilna nujnost (Arendt, 1958/1995: 33): "*Sfera gospodinjstva/gospodarstva je bila zaznamovana s tem, da so življenje v njem narekovale predvsem človeške potrebe in življenjske nujnosti*" (Arendt, 1958/1995: 32). Ta "življenjska nujnost" je bila tudi vzrok, da je bilo le v zasebni sferi upravičeno uporabiti silo in nasilje, kajti sila in nasilje "*sta edini način, kako premagati nujnost... in postati svoboden... Nujnost, ki so ji podvrženi vsi smrtniki, opravičuje nasilje; ljudje se nujnosti, ki jim jo nalaga življenje, osvobajajo nasilno za svobodo sveta.*" (Arendt, 1958/1995: 33) Zaradi tega je tudi "ekonomija" sodila v zasebno in ne v javno sfero, saj je "ekonomsko" veljalo za nekaj, kar je nujno za preživetje posameznika in vrste (Arendt, 1958/1995: 31).[4] Prisiliti in ukazovati je bilo v antiki razumljeno kot predpolitično razmerje, značilno za dom in družino (v kateri je družinski poglavar izvajal despotsko oblast) ter za barbarska cesarstva (Arendt, 1958/1995: 29).

Zaradi obvladovanja življenjske nujnosti znotraj zasebne sfere torej po antičnem pojmovanju ne gospodar ne podložniki niso mogli biti svobodni. Biti svoboden je torej pomenilo svobodo od prisile nujnosti, in to tako nujnosti prisile kot tudi nujnosti ukazovanja (Arendt, 1958/1995: 35). Kraljestvo svobode je bilo v polisu, torej v javnem (kjer med posamezniki niso prevladovala razmerja prisile, temveč prepričevanja in dogovarjanja), in ne v zasebnem, res pa je, da je bilo obvladovanje življenjskih nujnosti pogoj za svobodo v polisu.

Zato sta bili v antiki sferi političnega in zasebnega v izrazitem nasprotju (Arendt, 1958/1995: 27). Sfera zasebnega pa je bila v nasprotju z današnjim časom razumljena predvsem kot polje nesvobode.

---

[4] Tako razumevanje sicer po mnenju Arendtove ni v neposrednem nasprotju s sodobnim razumevanjem zasebnega. Pravi namreč: "*Kljub temu se velja spomniti, da se naše pojmovanje zasebnega v svojem zelo prvinskem in temeljnem oziru v ničemer ne razlikuje od tistega, kar je veljalo od samega začetka zgodovinskega spomina, in sicer, da so vse telesne funkcije 'zasebne' in morajo biti skrite, vse tisto torej, k čemur neposredno sili življenjski proces; samo da so pred stoletji novega veka pod to nujno razumeli vse dejavnosti, ki rabijo ohranitvi posameznika in obstoju vrste*" (Arendt, 1958/1995: 74).

Nastanek krščanstva, ki je od vernikov zahtevalo pogled v lastno notranjost (s kriterijem vesti), je omogočil nastajanje individualnosti in s tem nastanek zasebne sfere kot polja svobode.[5] Dokončni preobrat v razumevanju zasebne sfere se je zgodil v razsvetljenstvu oziroma z nastankom kapitalizma. Takrat je namreč nastala družba, ko so gospodinjske/gospodarske in ekonomske dejavnosti vstopile v prostor javnega političnega področja ter postale kolektivne zadeve (Arendt, 1958/1995: 35, 40) – vzpostavilo se je območje, na katerem so zasebni interesi postali javni interesi, pripadel jim je javni pomen (Arendt, 1958/1995: 37 ter Habermas, 1962/1989: 32).

S tem se je ločnica med javnim in zasebnim zabrisala, pojma pa sta se tudi spremenila: pojem zasebnosti se zdaj postavi ne samo v nasprotje do javnega kot v antiki ali v srednjem veku,[6] temveč tudi (predvsem) do družbenega (Arendt, 1958/1995: 41), hkrati pa je javnost – javnost zasebnikov – zajeta na zasebnem območju (Habermas, 1962/1989: 43). Življenjska nujnost, življenjski proces je tako začel stopati iz zasebne v novo nastalo družbeno sfero. Arendtova pravi, da je družba "*forma, v kateri se je javno etabliral in organiziral življenjski proces sam ... [v njej] dobi odvisnost ljudi od drugih javni pomen zaradi življenja samega* " (Arendt, 1958/1995: 48).

Do prvega opaznejšega preloma v odnosu med zasebno in javno sfero je tako prišlo ob nastanku zgodnjega kapitalizma, ko so ukrepi javne oblasti, ki so prizadeli široke sloje mestnega prebivalstva v njihovi vsakdanji eksistenci, naleteli na prve kritike porajajoče se kritične publike – prej zgolj zasebni interesi zdaj postanejo javni[7] (Habermas, 1962/1989: 37–38). Meščanska javnost, ki je bila sprva zgolj sfera zasebnikov, zbranih v publiko (Habermas, 1962/1989: 40), se je proti javni oblasti postavila z načelom nadzora – publicitete in z odzivanjem javnosti (Habermas, 1962/1989: 41). Predpostavka načela publicitete je seveda bila, da naj bi zakoni ne bili več odvisni od samovolje vladarja, temveč bi postali racionalni in s tem predvidljivi. Arkansko prakso (skrivnega, netransparentnega) vladanja, ki je temeljila zgolj na vladarjevi volji, naj bi nadomestila publiciteta, ki bi temeljila na racionalnosti (Habermas, 1962/1989: 69, 96). S tem nastopi očitna sprememba glede na antični model javne in zasebne sfere: meščanska javnost se je postavila nasproti lastni oblasti (za razliko od grške javnosti, ki ni oporekala lastni vladi), od katere je želela urejanje svojih zasebnih interesov; ti so s tem vstopili v javno sfero (Habermas, 1962/1989: 67 ter Arendt, 1958/1995: 70).

Zato si publika zasebnikov izbori zakonodajno kompetenco, s katero si želijo zagotoviti podreditev javne oblasti zasebnim interesom (Arendt, 1958/1995: 70 ter Habermas, 1962/1989: 101). Vendar je bil ta proces za zasebno sfero dvorezen. Če je postala "*dolžnost kralja ... vladati tako, da so bili priznani in zaščiteni posestniški interesi podložnikov*" (Arendt, 1958/1995: 69), je politika s tem postala nekaj, kar je potrebno za družbeno blaginjo. Vmešavanje oblasti v zasebne zadeve z namenom zagotavljanja javnega dobrega tako postane potrebno in celo zaželeno. S tem pa pride tudi do premika polja svobode in prisile. Če je v antiki polje svobode ležalo v polisu,

---

[5] Seveda so na spremenjeno razumevanje zasebne sfere vplivali še drugi dejavniki, Gutwirth omenja predvsem spremenjeno nadzorstveno vlogo države, vlogo družine pri socializaciji posameznikov ter povečano stopnjo pismenosti, ki je razširila zmožnost intelektualne neodvisnosti (Gutwirth, 2002: 21).

[6] V 16. stoletju pomeni zasebno izključitev z območja državnega aparata (Habermas, 1962/1989: 23).

[7] Habermas ugotavlja, da je bila "*politična naloga meščanske javnosti ... urejanje civilne societete [civilne družbe, m. op.] (v nasprotju z res publica) ... v tem smislu je bila že od vsega začetka hkrati zasebne in polemične narave*" (Habermas, 1962/1989: 67).

prisila pa je bila značilna za zasebno sfero, zdaj svoboda leži v družbenem, "*sila in nasilje [pa] sta lokalizirana v političnem in postaneta monopol države*" (Arendt, 1958/1995: 33).

S tem proces še ni končan. Polje svobode se pomika proti zasebni sferi, ta pa ne ostane statična, temveč se začne členiti še znotraj same sebe, saj se je njen "ekonomski del" začel pomikati v družbeno sfero. Oblikuje se jedro zasebne sfere – intimno (Habermas, 1962/1989: 70), najpomembnejša naloga zasebnosti pa postane zagotavljati intimno (Arendt, 1958/1995: 41).[8] Ta razvoj se v pravu pokaže kot oblikovanje treh skupin temeljnih človekovih pravic,[9] ki se nanašajo na *sfero rezonirajoče publike* (svoboda mnenja in govora, enaka volilna pravica itd.), *svobodni status posameznika, zasnovan v intimni sferi ožje družine* (osebna svoboda, nedotakljivost stanovanja in druge pravice, ki se nanašajo na avtonomijo posameznika) ter *občevanje zasebnih lastnikov v sferi meščanske družbe* (enakost pred zakonom, zaščita zasebne lastnine itd.) (Habermas, 1962/1989: 99).

Posledica te členitve je tudi ambivalentnost zasebne sfere, saj ima v njej posameznik hkrati lastniško in človeško vlogo.[10] Habermas pravi, da je bil posameznik v njej hkrati "*lastnik dobrin in ljudi, pa tudi človek med drugimi ljudmi*" (Habermas, 1962/1989: 70). Zato se je v nadaljevanju ta lastniški del, ki je pomenil svobodno razpolaganje z zasebno lastnino, začel dokončno ločevati od zasebnega področja, zasebna sfera je čedalje bolj postajala prosta ekonomskih funkcij, zasebno področje pa se je začelo ožiti na intimno.

Oženje zasebne sfere: nastanek socialnega

Kriterija pripustitve k meščanski javnosti sta bila dva: izobrazba in posest; javnost pa je bila zagotovljena, če je imel vsak enake možnosti za izpolnitev kriterijev pripustitve: pridobivanje bogastva mora biti odvisno le od posameznika, njegovega talenta, premoženja in sreče, ne pa od prisile drugih (Habermas, 1962/1989: 102–103). Zato so nelastniki izločeni iz meščanske javnosti, publike politično rezonirajočih zasebnikov. Niso državljani, bodo pa to morda nekoč lahko postali, saj imajo za to domnevno enake pogoje kakor drugi; so državni varovanci, deležni zaščite zakonov, a jih ne morejo ustvarjati (Habermas, 1962/1989: 129). Na to sporno predpostavko enake dostopnosti je prvi opozoril Marx s svojo kritiko, da je javnost zgolj maska meščanskega razrednega interesa: človekove pravice jamčijo egoizem, posameznik ne preseže nesvobode lastnika, razpolaganje z zasebno lastnino ne vodi v svobodo avtonomnih ljudi, meščanska pravna država je zgolj ideologija (Habermas, 1962/1989: 141–143). Dotlej v javnost nepripuščene množice začnejo 'vdirati' vanjo – svoje interesne konflikte, ki jih niso mogle rešiti v

---

[8] Po Arendtovi začetki intimnega segajo v pozni rimski čas, v antiki pa ga niso poznali (Arendt, 1958/1995: 40), prvi pa intimno pravzaprav prepozna Rousseau, kar nastanek intimnega uvršča v obdobje razsvetljenstva.

[9] Pravni razvoj teh pravic prežema ideja emancipacije posameznikov od oblasti (Habermas, 1962/1989: 245), ne pa tudi od tedaj šele porajajoče se družbe, iz česar sledi tudi njihovo negativno koncipiranje.

[10] To se kaže tudi v javnosti: posamezniki so se v okviru literarne javnosti sporazumevali kot ljudje (nastanek romana v pismih), v političnem rezoniranju pa kot posestniki o ureditvi svoje zasebne sfere, ki jo določajo v skupnem interesu (Habermas, 1962/1989: 71).

zasebni sferi, prenesejo v javnost in jih s tem spremenijo v politične konflikte (Habermas, 1962/1989: 164). Zato postane v 19. stoletju posebej pomembna reforma volilne pravice z razširitvijo publike volivcev (Habermas, 1962/1989: 149–150).

Pride torej do 'vdora' dotlej nepripuščenih množic in njihovih interesov v javno sfero, ekonomija (razpolaganje z zasebno lastnino) pa dokončno izstopi iz zasebne sfere. Spajanje zasebne in javne sfere je državi prineslo nove, socialne funkcije,[11] ki so bile prej prepuščene zasebni pobudi. Država pa lahko s podelitvijo koncesij zaupa javne naloge zasebnikom (Habermas, 1962/1989: 164–165). Habermas ugotavlja, da se v končni fazi oblikuje "*repolitizirana socialna sfera, v kateri so se javne in družbene institucije združile v eno samo funkcijsko skupnost, ki je ni bilo mogoče več diferencirati po kriterijih javnega in zasebnega*" (Habermas, 1962/1989: 167). Ena izmed posledic nastanka socialne države pa je tudi povečan regulacijski nadzor.

Kaj je to pomenilo za intimno sfero? Habermas ugotavlja, da "*družina postaja vedno bolj zasebna, delovno in organizacijsko okolje pa vedno bolj 'javno'*" (Habermas, 1962/1989: 170). Delo se umika iz zasebnega v novo nastalo socialno sfero, družina pa se pomika proti intimi. Če je dotlej družina skrbela za temeljne potrebe posameznika in če so bile te temeljne potrebe njeno lastno tveganje, je danes posamezni družinski član javno zavarovan. Družina začne izgubljati tudi funkcije vzgoje, varstva, oskrbe, pojavi se osebni in ne več družinski dohodek, oblikuje se razmejitev med prostim in delovnim časom, pri čemer družina zdaj postaja "*porabnik prihodka in prostega časa*". Intimna sfera "*se je zožila na območje ožjedružinske porabniške skupnosti*", ugotavlja Habermas, s tem pa je "*nastal videz intenzivirane zasebnosti v intimni sferi*" (Habermas, 1962/1989: 173–175). Del zasebne sfere se torej odcepi v socialno, preostanek pa se zoži na intimno.

Zasebnost v množični družbi

Vendar pa se oženje zasebne sfere ne ustavi pri zoženju na intimno. Država (če je demokratična) sicer na intimna področja posameznikov ne prodira, zato pa tja prodira družba. To postane očitno predvsem ob nastanku množičnih medijev in sodobnega potrošništva. Po eni strani zasebne zgodbe posameznikov postanejo tržno blago, javnost pa postane sfera objavljanja zasebnih življenjskih zgodb (Habermas, 1962/1989: 190),[12] po drugi strani pa zasebnost postane ovira pri uresničevanju ekonomskih in političnih interesov, saj nadzor čedalje bolj postaja orodje množičnega marketinga in upravljanja družbe.

---

[11] V pravu je to odsevalo v omejevanju lastninske pravice, omejitvah pri popolni neodvisnosti pri določitvi pogodbenih pogojev itd., skratka v posegih države na tista področja, ki so bila prej stvar zgolj zasebne sfere in niso bila deležna državne regulacije.

[12] Značilno je, da s tem v zvezi Habermas pravi: "*Nasploh se množični mediji priporočajo kot naslovniki za osebne stike in težave, kot avtoritete življenjske pomoči...*", ter "*problematiko zasebne eksistence javnost delno vsrka: če je že ne razrešujejo pod vrhovnim nadzorom publicistične javnosti, jo pred njo vsaj prikazujejo*" (Habermas, 1962/1989: 191). Zanimivo je, da se je leta 2004 na internetu zelo razmahnilo pisanje t. i. spletnih dnevnikov – blogov (izraz *blog* izhaja iz angleških besed *web* in *log*), v katerih posamezniki javno pišejo (oziroma objavljajo na spletni strani) svoj dnevnik. Posamezniki torej "na očeh javnosti" javno razgrinjajo svoja najbolj skrita razmišljanja, osebne probleme itd.

Z vdorom dotlej nepripuščenih množic v meščansko javno sfero – z razširitvijo volilne pravice – se javno mnenje vzpostavi kot "najmočnejša sila", hkrati pa nastanek množičnih medijev odpre nove možnosti za širjenje idej in oglaševanja. Kot odziv na to se kmalu pokažejo težnje po obvladovanju javnega mnenja (Habermas, 1962/1989: 152). Do tega obvladovanja je prišlo postopoma, prvi korak pa je bil vdor tržnih zakonov na območje publike (Habermas, 1962/1989: 179), zaradi česar se rezoniranje spremeni v konzumiranje, javnost pa v množico. Arendtova ugotavlja, da je "*na mesto delovanja stopilo obnašanje, ki ga družba pričakuje od vseh svojih članov*" (Arendt, 1958/1995: 43).

S tem je intimna sfera postala bojišče, prostor, po katerem skušajo na potrošnike in volivce vplivati ekonomske in politične instance. Habermas pravi: "*intimna sfera [je] danes postala vpadnica za socialne sile, s katerimi potrošniškokulturna javnost množičnih medijev bombardira ožjedružinsko notranjost*" (Habermas, 1962/1989: 180). Namesto kritične se izoblikuje manipulativna publiciteta (Habermas, 1962/1989: 196), saj publiciteta zdaj rabi manipulaciji publike in legitimaciji pred njo (Habermas, 1962/1989: 197), množični mediji pa začnejo oblikovati 'javno mnenje' (Habermas, 1962/1989: 209). Tisk tako postane "*vhodna vrata privilegiranih zasebnih interesov v javnost*" (Habermas, 1962/1989: 205), saj po njem (oziroma s propagando in oglaševanjem) "*zasebniki kot zasebni lastniki [delujejo] na zasebnike kot publiko*" (Habermas, 1962/1989: 209).[13] Pride do oženja javnega prostora, hkrati pa družba (mediji, oglaševalci) čedalje bolj prodira v intimno sfero.

Bistvo množičnih medijev tako postaja potrošniška vzgoja ter nadzor (Habermas, 1962/1989: 212 in Splichal, 2002: 181),[14] javno mnenje postane sredstvo gospodovanja družbe nad posameznikom (Splichal, 2002: 74), kritične državljane nadomestijo potrošniki, delovanje pa je nadomeščeno z obnašanjem. S tem se pokaže tudi, da "*odmiranje javnega ... spremlja radikalno ogrožanje zasebnega*" (Arendt, 1958/1995: 62).

Brisanje javnega prostora se z razvojem marketinških tehnik, predvsem odnosov z javnostmi (ang. *public relations*), le še nadaljuje, saj te z načrtnim poseganjem v proces javnega mnenja zasebne interese omejene skupine posameznikov – ali podjetij – z manipulacijo spreminjajo v 'javni interes'. Če se je v 18. stoletju javnost razvijala iz jedra same zasebne sfere, danes oglaševalci javnost vzpostavljajo z 'napadom' na zasebni, intimni prostor posameznika. Morda se ta proces najbolj jasno kaže pri poročanju iz sodnih dvoran in parlamenta: če je bila temeljna ideja javnosti sojenj in parlamentarnih debat publiciteta v smislu kritičnega nadzora javnosti nad oblastjo, pa se je sodobno medijsko poročanje o tem sprevrglo v "*predstavo za razvedrilo neprizadetih potrošnikov*" (Habermas, 1962/1989: 229), kot je kritično zapisal Habermas (pravzaprav s tem v zvezi govori kar o "*kulturniškopotrošniškem potvarjanju juridične javnosti*" (Habermas, 1962/1989: 228)).

---

[13] S tem pa je prišlo še do enega obrata: če je bila namreč neodvisnost medijev v liberalnem modelu zavarovana s tem, da so bili v rokah zasebnikov, danes zasebno lastništvo medijev ogroža njihovo kritičnost. Zato regulacijski ukrepi sodobnih držav za t. i. nacionalne medije predvidevajo vsaj delno javno, torej državno lastništvo.

[14] To razliko glede vloge množičnih medijev in vloge tiska v 18. stoletju morda najbolj drastično kaže dejstvo, da so bili v 18. stoletju za pisanje v časopise med drugim zadolženi tudi profesorji, ki naj bi javnosti posredovali "*resnice za vsakdanjo rabo*" (Habermas, 1962/1989: 38), skratka javnost naj bi izobraževali, ne pa z njo manipulirali.

Oglaševanje (ki postaja čedalje bolj usmerjeno) in ustvarjanje javnosti ter medijsko poseganje v zasebno sfero pod krinko t. i. "interesa javnosti"[15] pa kaže, da se zasebna sfera še naprej oži; v končni fazi celo intimno postaja čedalje bolj javno. Zasebnost postaja moteča ovira, ki onemogoča učinkovitost. Agre in Rotenberg pravita, da postaja "*izdelek, ki ogroža učinkovitost in skriva kriminalce ... naravni sovražnik svobode informacij ... koncept brez definicije ali oblike ... [katerega] uveljavljanje je nadležno in drago*" (Davies, 2001: 153).

Oženje zasebne sfere kot način politizacije konfliktov

Na oženje zasebne sfere ne vplivajo samo zunanji (družbeni) vplivi; včasih postane oženje zasebne sfere oziroma njeno izpostavljanje javnosti zavestna taktika podrejenih skupin. Kot je pokazal Habermas, je mogoče s prevajanjem konfliktov iz zasebne sfere na javno, politično področje (Habermas, 1962/1989: 160) zasebne konflikte spremeniti v politične konflikte in s tem laže doseči njihovo rešitev. Benhabibova ugotavlja, da se "*vsi boji proti zatiranju v sodobnem svetu začnejo z redefiniranjem tistega, kar je prej veljalo za zasebno, nejavno, nepolitično zadevo, v vprašanje javne zadeve, stvar pravičnosti*" (Benhabib, 1997: 84). To velja zlasti v primeru različnih oblik diskriminacij ali izvajanja nasilja v zasebni sferi, saj se, kot ugotavlja Benhabibova, zasebno sfero smatra za "*področje zunaj kraljestva pravičnosti*" (Benhabib, 1997: 92).

Fraserjeva opozarja, da gre izključitev določene teme iz javne razprave lahko v prid gospodujočim skupinam in posameznikom na rovaš podrejenih. Gre za vidik, ki ga je skušala izpostaviti feministična kritika zasebne sfere: "*če je pretepanje žene označeno kot 'osebna' ali 'domača' zadeva..., potem to služi reprodukciji spolne dominacije in podrejanju. Podobno velja za vprašanje demokracije na delovnem mestu – če je označeno kot 'ekonomski' ali 'managerski' problem ..., potem to služi ovekovečenju razredne (in pogosto tudi spolne in rasne) dominacije in podrejanju*" (Fraser, 1997: 132).

Zato ne preseneča, da so marginalna družbena gibanja, tipično feministke ali gejevski aktivisti, konflikte iz zasebne sfere skušali spraviti v javnost (npr. feministično geslo "*osebno je politično*"), in sicer na način, da so javno razgalili svojo zasebno in celo intimno sfero. Po mnenju Eleya tako "*feminizem sistematično politizira osebno dimenzijo družbenih odnosov*" (Eley, 1997: 318) ter s tem premika mejo med zasebnim in javnim tudi na področju intimnega (družine, spolnosti itd.). Ta taktika je seveda razumljiva takrat, kadar zasebna sfera postane področje izkoriščanja moči in podrejanja, v skrajno skomercializirani družbi pa je lahko celo kontraproduktivna, saj razgaljenje in videnost s tem postajata tržno blago in celo norma.

Prav tako je napačno razumevanje, da je vse, kar se dogaja v zasebni sferi, že samo zato, ker je zakrito pred javnostjo, nujno podvrženo "korupciji" in "nemoralnosti" (v Benthamovem smislu), kar bi bil lahko celo argument za popolno dekonstrukcijo zasebne sfere. Zasebna sfera namreč lahko predstavlja tudi zaščito in zavetje za posameznika. Zaščito pred družbo in zavetje,

[15] Le-ta je skoraj vedno le interes lastnikov medijev po povečanju prodaje, svoboda tiska pa iz pravice komuniciranja postaja čedalje bolj pravica opravljanja zasebne založniške dejavnosti, kot je pokazal Splichal (Splichal, 2002: 176).

v katerem se lahko razvije v svobodno in avtonomno človeško bitje. Ker vdor v zasebnost lahko spodkoplje osebno avtonomijo, individualnost, dostojanstvo in neodvisnost posameznika (Wagner DeCew, 1997: 20), je zasebnost pomemben dejavnik, ki omogoča svobodo posameznika. Ali kot pravi Sykes: "*Nekateri pravijo, da je zasebnost bistvena za biti človek, vendar je v resnici povsem mogoče biti človek brez zasebnosti. Bolj točno je reči, da je zasebnost nujna za biti svoboden človek*." (Sykes, 1999: 7).

Pomen zasebne sfere

Zasebna sfera se je torej v zgodovini iz sfere življenjske nujnosti premaknila na polje svobode. S tem zasebnost ni več nujno zlo, temveč je postala vrednota, predpogoj posameznikove svobode in emancipacije.

Arendtova v zasebni sferi vidi območje, na katerem je posameznik varen in skrit pred svetom, in sicer na dva načina: pred vplivi iz sveta in pred tem, da posameznik postane viden v svetu. Arendtova namreč pravi, da so "*...lastne štiri stene edini kraj, v katerega se lahko umaknemo pred svetom, ne samo pred tistim, kar se v njem stalno dogaja, temveč pred njegovo javnostjo, pred tem, da smo videni in slišani*" (Arendt, 1958/1995: 73). Zasebnost je torej meja med posameznikom in drugimi, meja, katere naloga je filtriranje pretoka informacij z obeh strani.

V čem je torej pomen te meje? Hannah Arendt v družini, torej v zasebni sferi, vidi prostor, ki omogoča nastanek in razvoj političnih oseb, od družbenih pritiskov neodvisnih posameznikov (Jalušič, 1995: X). Tako Arendtova kot Habermas izpostavita dva vidika zasebnega: osebni prostor, torej prostor intime, in prostor, ki omogoča interesno združevanje, torej delovanje. Za delovanje, neodvisno od družbenih prisil, sta pomembna oba. Ta delitev pa je opazna tudi v pravni kodifikaciji pravice do zasebnosti, na primer v 8. členu *Evropske konvencije o človekovih pravicah*,[16] kjer je pravica do zasebnosti klasificirana na podlagi štirih vidikov pravice do zasebnosti: zasebnega življenja, družinskega življenja, doma in dopisovanja.

Zasebna sfera je torej pomembna zato, ker pravzaprav omogoča delovanje in kritično mišljenje: "*Da bi ljudje sploh lahko bili politična bitja in da bi se lahko zavedli pomena politike in obstoja javnega prostora, vsak posameznik ... potrebuje ... prostor, kamor se lahko umakne. ... V tem prostoru, ki je svojevrstno varstvo pred družbenimi prisilami, se lahko razvije identiteta političnega pariaha*[17] *(v tem je element 'varstva' pred totalitarizmom'). To je prostor, ki lahko ... pomeni pogoj političnega... vsak lahko postane političen ravno zato, ker ni družben in ker ni izpostavljen nobeni družbeni prisili...*" (Jalušič, 1995: IL-L).

---

[16] Svet Evrope. 1950. Evropska konvencija o varstvu človekovih pravic in mednarodnih svoboščin, spremenjena s protokoli št. 3, 5 in 8 ter dopolnjena s protokolom št. 2, ter njeni protokoli št. 1, 4, 6, 7, 9, 10 in 11 (Convention on Human Rights and Fundamental Freedoms as amended by Protocols Nos. 3, 5 and 8 and amended by Protocol No. 2 and its Protocols Nos. 1, 4, 6, 7, 9, 10 and 11), sprejel jo je Svet Evrope leta 1950. Uradni list RS, št. 33/1994, "Mednarodne pogodbe", št. 7/1994, 13. 6. 1994. Konvencijo je državni zbor Republike Slovenije ratificiral 13. 6. 1994. Veljati je začela dne 28. 6. 1994.

[17] Zavestno pariahovstvo je po Arendtovi eden izmed treh možnih odzivov na družbeno izključevanje (npr. antisemitizem) – posameznik ne skuša zatajiti svoje identitete oziroma se asimilirati (parvenujevstvo), temveč jo zavestno sprejme in želi, da ji drugi priznajo obstoj.

V tem kontekstu je stalna rast družbenega, ki izpodriva tako zasebno (in v času množične družbe tudi intimno) kot tudi javno (Arendt, 1958/1995: 48), lahko zaskrbljujoča. Proces "množičnega podružbljanja", ki je delovanje nadomestil z obnašanjem, individualnost s povprečenjem in kritičnost s porabništvom, je po Arendtovi simptomatično viden v nastanku 'behavioristićnih znanosti' (oziroma tistem, kar Foucault imenuje biopolitika). Njihov nastanek "*je končni stadij tega razvoja, v katerem se je množična družba polastila vseh skupin prebivalstva nacije in je družbeno obnašanje postalo merilo za celotno življenje posameznika*" (Arendt, 1958/1995: 47), te 'behavioristične znanosti' (predvsem statistično merjenje) pa so postale ključna vez med nadzorom in 'manipulacijo javnosti'.

Arendtova ugotavlja, da "*ogrožanje svobode v moderni družbi ne prihaja od države, kot domneva liberalizem, temveč od družbe*" (Arendt, 1958/1995: 69), iz tega pa tudi sledi, da državljanske svoboščine lahko zagotavlja edinole država nasproti družbi. Kot bo prikazano v nadaljevanju, ugotovitev Arendtove nazorno kaže, zakaj je stopnja varstva zasebnosti posameznikov v ZDA nižja kot v Evropi. Ameriška zakonodaja je namreč koncipirana kot sistem negativnih svoboščin (to je razvidno predvsem iz njihove ustave), zato je pravica do zasebnosti posameznikov nasproti državi bistveno bolj zavarovana kot nasproti delodajalcem, korporacijam in medijem (to pa za Evropo ne velja v enaki meri, saj je pravica do zasebnosti v Evropi načeloma bolj univerzalna). To se kaže predvsem v praktično popolni odsotnosti varstva informacijske zasebnosti v zasebnem sektorju v ZDA ter zasebnosti na delovnem mestu, ki v ZDA ni dojemana kot pravica, temveč kvečjemu kot boniteta, če je sploh priznana. Hkrati je med ameriškimi borci za zasebnost na internetu mogoče opaziti močan odpor proti kakršnikoli (oziroma t. i. "pretirani") regulaciji varstva zasebnosti s strani države. To kaže na to, da ti kot ogrožujočega akterja še vedno dojemajo predvsem državo.

Arendtova pravi, da je v množičnih družbah in razmerah množičnih histerij vsak "*zaprt v svojo subjektivnost kot v izolirano celico*" (Arendt, 1958/1995: 60). V tem smislu "*živeti samo zasebno življenje pomeni predvsem živeti v stanju, ko smo oropani bistvenih človeških stvari ... oropani možnosti, da storimo nekaj, kar je trajnejše od našega življenja samega*" (Arendt, 1958/1995: 60); Arendtova govori o oropanosti in izgubi realnosti, ki sta "*v modernem svetu privedli do zapuščenosti*", do odsotnosti odnosov (Arendt, 1958/1995: 60), javnega prostora in političnega delovanja. Iz tega sledi, da je pomen zasebnosti predvsem v zagotavljanju možnosti delovanja in v konstituiranju javnega prostora za delovanje: "*samo če se ohranjajo različni prostori svobode, je možno ohraniti tudi politični prostor*" (Jalušič, 1995: IL).

Če se je torej zasebna sfera zožila na intimno in če je tudi intimno, ki ga Arendtova dojema kot "*nekakšen beg pred družbo, ki se je polastila celotnega zunanjega sveta*" (Arendt, 1958/1995: 70), čedalje bolj na udaru sodobne družbe, potem se lahko zgodi, da je edini zasebni prostor, ki ostane posamezniku, njegova subjektivnost. To pa, po Arendtovi, vodi v nekakšno razčlovečenje, deindividualizacijo posameznikov: "*Čisto mogoče je, da se novi vek, ki se je začel z neverjetno obetavnim aktiviranjem človeških sposobnosti, konča z najbolj usodno, sterilno pasivnostjo, kar jih je kdaj poznala zgodovina*" (Arendt, 1958/1995: 336). Procesi čedalje obsežnejšega nadzorovanja in posledično povprečenja (konstrukcije povprečnega in ne več

individualnega posameznika), ki bodo obravnavani v naslednjem poglavju, pa zasebni prostor le še bolj ožijo. "*Osiromašenje javnega prostora spremlja rast družbe nadzora in voajerizma*", pravi Seyla Benhabib (Benhabib, 1997: 93–94).

NADZOROVANJE

Beniger nadzor definira kot "*usmerjen vpliv na zastavljeni cilj*" (Beniger, 1986: 7), obdelovanje informacij pa je temelj vseh k cilju usmerjenih dejavnosti (Beniger, 1986: 8). Nadzorovanje v splošnem pomenu besede zato posameznikom omogoča delovanje, sodobna družba pa brez nadzorovanja ne more obstajati. Vendar pa je treba ločevati med nadzorom nad stvarmi (npr. interakcija z okoljem, upravljanje stvari itd.) in nadzorom nad ljudmi, pri čemer gre za vprašanje prisile in drugih oblik usmerjanja delovanja posameznikov. V nadaljevanju se bomo ukvarjali zgolj z nadzorom nad ljudmi. V tem smislu je nadzorovanje orodje, ki omogoča predrtje meje, ki posameznika ločuje od preostalega sveta. Nadzor je namenjen spoznavanju delovanja posameznikov in s tem gospodovanju nad njimi. Nadzor se lahko pojavlja v obliki zbiranja informacij (na podlagi teh informacij je nato mogoče usmerjati delovanje, pravzaprav obnašanje posameznikov) in neposrednega usmerjanja delovanja ljudi.

Vloga nadzora je v sodobni družbi ambivalentna. Po eni strani je namenjen 'upravljanju' ljudi, po drugi strani pa ljudem sploh omogoča življenje v družbi. Oblast ali družba lahko nadzor uporabljata proti posameznikom, hkrati pa lahko posameznik nadzor uporabi proti državi (ni naključje, da je za aktiviste, ki se ukvarjajo z zaščito zasebnosti, zakonodaja za dostop do informacij javnega značaja pomembno orodje v boju proti prikritemu državnemu nadzoru). Kljub temu da je nadzor mogoče uporabiti dvosmerno, pa sodobna tehnologija omogoča nadzorovanje predvsem v eno smer, torej bolj nadzorovanje posameznikov kot nadzorovanje oblasti. Tehnologija (npr. kriptografija) sicer omogoča izogibanje nadzoru, hkrati pa je ta tehnologija pod nenehnim udarom onemogočanja.

Pravzaprav gre celo pri pravici do zasebnosti za neko obliko "samonadzora" – nadzora nad informacijami o sebi, nad svojimi avtonomnimi odločitvami in nad svojo osebnostjo. Čeprav je nadzor še vedno pogosto razumljen kot nekaj negativnega, nekaj, kar prisiljuje, pa je nadzorovanje danes dobilo bolj prijazen, lahko bi rekli celo hinavski obraz. Postalo je neopazno, a povsod navzoče, postalo je prijazno in prostovoljno (npr. potrošniški nadzor po različnih karticah ugodnosti), predvsem pa je postalo tako rekoč nujno za življenje v sodobni družbi. Slogan iz Orwellovega romana "*Veliki brat te opazuje! / Big Brother is watching you!*" se spreminja v "*Veliki brat skrbi zate / Big Brother is waching out for you*" (Whitaker, 1999: 142).

Življenje v sodobni družbi tako nujno zahteva pristanek na določeno stopnjo nadzora – vidnost je postala norma. In če posameznik pristane na še več nadzora, je deležen še dodatnih ugodnosti. Kako je prišlo do te spreobrnjene vloge nadzora? In kako je nadzor sploh postal sredstvo izvajanja moči?

Panoptikon

Leta 1791 je angleški pravnik in filozof Jeremy Bentham predstavil načrt zapora Panoptikon. (V besedilu *Oko oblasti* Foucault pravi, da se je zamisel o Panoptikonu utrnila Benthamovemu bratu, ko je obiskal vojaško šolo (Foucault, 1991: 42)). Panoptikon je bil zamišljen kot krožna

zgradba, na obodu so celice, ki so med seboj ločene tako, da zaporniki med seboj ne morejo komunicirati. V središču zgradbe je prostor, v katerem je Inšpektor, med njim in celicami je vmesno območje.

Vsaka celica ima na zunanji strani okno, skozi katero pa ni mogoče videti ven, na notranji strani pa zamrežena vrata, ki Inšpektorju omogočajo opazovanje dogajanja v celici. Od Inšpektorja do celic lahko vodi ozka kositrna cev, ki Inšpektorju omogoča, da sliši vsak, tudi najmanjši šepet v celici. Inšpektor lahko vidi zapornike, sam pa ni viden. Bentham pravi, da je ključno, da se morajo ljudje, ki so nadzorovani, vedno čutiti pod nadzorom, zato govori o Inšpektorjevi "navidezni vsenavzočnosti". Poleg Inšpektorja je zapor odprt tudi za obiskovalce – ti nadzorujejo tako zapornike kot Inšpektorja. Gre pravzaprav za "stroj", ki je bil v osnovi zamišljen tako, da je vsakdo pod nadzorom, da torej temelji na nezaupanju: "*V Panoptikonu pa vsi ali večina nadzorujejo vsakogar – pač glede na mesto, ki ga zavzema. To je aparat, v katerem ni absolutne točke, zato je v njem cirkulacija nezaupanja popolna.*" (Foucault, 1991: 50). Vstop ali izstop iz zgradbe je mogoč samo po eni poti (Bentham, 1787/1995/2001).

Čeprav Panoptikon ni bil nikoli zgrajen in gre za utopijo, ki v realnosti verjetno nikoli ne bi delovala natanko tako, kot je bilo zamišljeno (Bentham je namreč pozabil na odpor posameznikov in je predpostavil, da so zaporniki povsem pasivna bitja (Foucault, 1991: 53)), pa je Benthamova zamisel po svoje revolucionarna. Na podlagi načrta Panoptikona se je namreč porodila zamisel o nadzoru kot tehnologiji oblasti. Tako je za Panoptikon značilno, da je v njegovem središču nadzornik, ki je neviden, vsi drugi pa so vidni. Gre torej za asimetrični nadzor, za oko, ki gleda, a ni videno: "*To, da oko vidi, ne da bi bilo videno – v tem je največja zvijača Panoptikona. Če lahko razločim pogled, ki me zalezuje, lahko obvladam nadziranje, lahko ga tudi sam zalezujem, ugotovim njegove premore in slabosti, preučim njegovo regularnost, ga izsledim. Če pa je Oko skrito, potem me gleda tudi takrat, kadar ne vidi. Oko, ki je potuhnjeno v senci, pomnoži vse svoje moči...*" (Miller, 1981: 18). Miller zato pravi, da skuša v Panoptikonu Bentham maksimirati videz in minimizirati resničnost (Miller, 1981: 22), s tem pa doseže funkcioniranje oblasti na mikroravni: "*Kdor je podrejen polju vidnosti in to ve, sam prevzame prisile oblasti; spontano jih uporablja na samem sebi; vase vtisne oblastno razmerje, v katerem igra hkrati obe vlogi: postane načelo svoje lastne podvrženosti*", pravi Foucault (Foucault, 1984: 202).

Revolucionarnost Benthamove ideje je v tem, da je, kot je ugotovil Foucault, načelo grajskih celic obrnil na glavo. Če je zaporniški sistem grajskih celic zapornika vrgel v temo (Foucault, 1991: 42), je zdaj zapornik izpostavljen svetlobi. Miller pravi, da je v Panoptikonu "*svetloba tista, ki dela iz nas ujetnike*" (Miller, 1981: 17). In ker je svetlobi oziroma nadzornemu očesu nemogoče uiti, Miller meni, da je "*Panoptikon stroj za proizvodnjo dozdevka Boga*" (Miller, 1981: 18). Zaradi tega miselnega preskoka v kaznovanju, preskoka od modela, ki je zapornika izvrgel, v model, v katerem je zapornik izpostavljen oblasti, ki gleda, Foucault Benthama označuje za "*enega najpomembnejših inovatorjev na področju tehnologije oblasti*" (Foucault, 1991: 48).

V Benthamovem Panoptikonu je mogoče vse preračunati, izmeriti vsak učinek in vzpostaviti polje popolne predvidljivosti. Ne samo mogoče, tudi potrebno, saj naj bi ravno s tem, ko bi upoštevali vse podrobnosti in obvladali vse vzroke, obvladali tudi učinke. Po mnenju Foucaulta zato Panoptikon deluje kot nekakšen laboratorij oblasti, Foucault pravi, da "*je privilegiran kraj,*

ki omogoča eksperimentiranje z ljudmi in docela zanesljivo analiziranje sprememb, ki bi jih lahko dosegli pri njih" (Foucault, 1984: 203).

To obvladovanje učinkov gre tako daleč, da skuša posameznika ne samo prisiliti, da se obnaša tako, kot je to od njega zahtevano, temveč mu celo želi odvzeti svobodno voljo, da ne bi sploh pomislil, da bi kaj storil narobe. Foucault pravi: "*Bentham je v svojem besedilu zelo jasno zapisal, kako pomembno je odvračanje. 'Zelo važno je', pravi, 'da ima Inšpektor zapornika neprestano na očeh; tako mu skorajda ne bo prišlo na misel, da bi storil kaj narobe'. S tem smo se znašli v srcu revolucionarnih prizadevanj: kako preprečiti ljudem, da bi storili kaj narobe, kako izničiti njihovo željo, da bi grešili. Skratka, kako jim odvzeti zmožnost in voljo.*" (Foucault, 1991: 47).

Benthamove zamisli o prosojnosti se niso ustavile samo pri zaporu. Bentham je menil, da je mogoče z njegovim izumom "*izboljšati moralo – ohraniti zdravje – okrepiti industrijo – ... – utrditi ekonomijo – ... – vse s preprosto idejo v Arhitekturi!*" (Bentham, 1787/1995/2001) in je zato predlagal, da bi njegov izum uporabili ne samo v zaporih, temveč tudi v bolnišnicah, norišnicah, šolah ter celo v politični skupščini. Oziroma kot ugotavlja Dolar: "*v naslednjem koraku, kako čim bolje izpostaviti pogledu celoten družbeni prostor, ga napraviti preglednega in dostopnega kontroli...*" (Dolar, 1991: XX). S tem Panoptikon postane šola človeštva (Miller, 1981: 20), nadzorovanje pa postane orodje izvajanja oblasti.

Panoptikon in disciplinarna oblast

Benthamov izum je tako v splošnem pravzaprav nova tehnologija oblasti, disciplinarna oblast. In čeprav Panoptikon sam ni bil nikoli zgrajen, se je zamisel o nadzoru kot tehnologiji oblasti pozneje močno zakoreninila v kaznovalnem sistemu. V 18. stoletju je namreč prišlo do odpora proti "spektaklu mučenja", s katerim se je obredno razkazovala oblast (Foucault, 1984: 59), zato je v drugi polovici tega stoletja prišlo do reforme v kazenskem pravu: "*kaznovala naj ne bi nič manj, temveč bolje; nemara naj bi kaznovala manj strogo, a zato naj bi kaznovala bolj univerzalno in bolj neogibno*" (Foucault, 1984: 83). "*Kazen se je iz umetnosti neznosnih občutkov spremenila v ekonomijo odvzetih pravic*" (Foucault, 1984: 17), prakso spektakularnega kaznovanja telesa je nadomestilo kaznovanje duše, ki učinkuje na voljo (Foucault, 1984: 22). Skratka, bistvo kazni postane, da popravlja in zdravi (Foucault, 1984: 16), pravzaprav da posameznike celo odvrača od nepravilnih ravnanj. Kot ugotavlja Foucault, je zato Benthamov Panoptikon odlično služil novemu tipu suverenosti. Novi mehanizem oblasti se tako usmeri na ljudi (Foucault pravi 'telesa') in njihovo delo, njegova najpomembnejša značilnost pa je, da se izvaja konstantno in s pomočjo nadzorovanja (Foucault, 1991: 37). Ta oblast je nesuverena (leži zunaj suverenosti), Foucault pa jo poimenuje disciplinarna oblast. Disciplina je po Foucaultu "*nekakšna vrsta oblasti, način, kako se izvaja, ki vsebuje cel skupek instrumentov, tehnik, postopkov, aplikacijskih ravni, tarč; je fizika ali anatomija oblasti, tehnologija*" (Foucault, 1991: 213). S pomočjo disciplinarne oblasti posameznike nadzorujemo in dresiramo, če je treba, tudi kaznujemo (Foucault, 1997/2003: 154), pri čemer kazen ni samo neposredna, fizična, temveč se je spremenila v ekonomijo odvzetih pravic, njen cilj pa je 'izdelati' discipliniranega posameznika. Nadzor je torej usmerjen

h konkretnemu posamezniku z namenom spremeniti in podrediti si ga. V 18. stoletju je bila torej 'Oblast' usmerjena k posamezniku. Potem pa je odkrila še populacijo.

Biopolitika: od oblasti, ki je usmrtila, do oblasti, ki omogoča življenje

Če je v 17. in 18. stoletju začelo prihajati do premika od klasičnih suverenih družb k disciplinskim družbam, v katerih se je oblast ukvarjala predvsem s posameznikom, pa je konec 18. stoletja in pozneje oblast "odkrila" populacijo. "*Prvič se je govorilo, da je nemogoče vladati državi brez poznavanja njene populacije*", pravi Foucault (Foucault, 1991: 67). Oblast pa je začela izvajati regulacijske ukrepe na ravni celotne populacije. O tej novi tehnologiji oblasti pravi Foucault takole:

> "*Discipline so imele dejansko opraviti s posameznikom in z njegovim telesom. Tisto, s čimer imamo opravka v novi tehnologiji oblasti, pa ni natanko družba (ali konec koncev družbeno telo, kot ga definirajo pravniki); še manj je to posameznik-telo. Gre za novo telo: multiplo telo s številnimi glavami, če že ne z neskončno mnogimi, pa vsaj s tolikimi, da jih ni nujno mogoče prešteti. To je pojem 'populacije'. Biopolitika ima opravka s populacijo... gre za kolektivne pojave, ki s svojimi ekonomskimi in političnimi učinki nastopijo ter postanejo umestni zgolj na ravni množice. Gre za pojave, ki so, če jih vzamemo same na sebi, torej posamezno, naključni in nepredvidljivi, vendar pa predstavljajo na kolektivni ravni konstante, ki jih je enostavno, vsekakor pa mogoče določiti.*" (Foucault, 1997/2003: 156).

Gre torej za statistično spremljanje pojavov, iskanje globalnih kazalcev in povprečnih vrednosti ter uvedbo regulacijskih mehanizmov na tej globalni ravni. Namen teh regulacijskih mehanizmov pa je ohranjanje globalnega ravnotežja, povprečja, pravzaprav namestitev varnostnih mehanizmov okrog naključnosti, ki se ji reče življenje (Foucault, 1997/2003: 156). Torej ne gre več za disciplino, temveč za regulacijo: "*Nikakor ne gre za priključitev na posamezno telo, kot stori disciplina. Potemtakem sploh ne gre za to, da bi posameznika zajeli na ravni detajlov, temveč nasprotno za to, da s pomočjo globalnih mehanizmov delujemo tako, da je doseženo globalno stanje ravnovesja, ustaljenosti; skratka za upoštevanje življenja, bioloških procesov človeka-vrste ter za to, da nad njimi ne zagotovimo neke discipline, temveč regulacijo*" (Foucault, 1997/2003: 156–157). Pri statističnem nadzoru gre torej za pridobivanje védenja zaradi upravljanja (kontrole), zato je bila statistika tradicionalno v službi države (Whitaker, 1999: 42). Inšpektor postane Birokrat, namesto posameznikov pa pregleduje družbo (Whitaker, 1999: 43). Whitaker pravi, da je 20. stoletje stoletje obveščevalne dejavnosti, pri čemer je zanj obveščevalna dejavnost "*avtomatsko in namensko pridobivanje, urejanje, nadomeščanje, analiza, interpretacija in zaščita informacij. ... sistematično organizirana birokratska dejavnost ... s svojo polavtonomno vlogo v globalni politiki*" (Whitaker, 1999: 5).

Vendar pa ta nova tehnologija oblasti, ki ravno tako temelji na nadzorovanju – tokrat pač na nadzorovanju populacije – ne izpodrine prejšnje disciplinske tehnologije. Nikakor, z njo deluje vzporedno. Foucault pravi, da nova regulacijska oblast disciplinsko: "*zaobseže, integrira, deloma spremeni, predvsem pa jo izkorišča za to, da se vanjo nekako vsadi, in se s pomočjo te predhodne disciplinarne tehnike dejansko utrdi. ... Povedano drugače: disciplina poskuša vladati množici ljudi, kolikor more, in mora ta množica razpasti na individualna telesa, ki jih je mogoče nadzorovati, dresirati, izkoriščati ter morebiti kaznovati. Nova tehnologija pa se naslavlja na množico ljudi, toda ne, kolikor so ti ljudje zvedeni na telesa, temveč nasprotno: kolikor ta tehnologija oblikuje neko globalno množico, ki jo zadevajo skupni procesi...*" (Foucault, 1997/2003: 153–154). S tem pa ta nova tehnologija oblasti prejšnjo celo nadgradi. Foucault govori o normalizacijski družbi, v kateri se sekata disciplina in regulacija (Foucault, 1997/2003: 161).

Po Foucaultu se torej za disciplinarno tehnologijo oblasti pojavi še biopolitika (Foucault zanjo uporablja tudi izraz tehnologija varnosti ali regulacijska oblast). Disciplinarna tehnologija se osredotoči na posameznika, na telo, biopolitika pa se osredotoči na življenje, na množico, poskuša nadzirati in regulirati "*niz naključnih dogodkov, ki se lahko proizvedejo v živi množici ... poskuša kontrolirati (morebiti spremeniti) njihovo verjetnost, vsekakor pa uravnovesiti njihove učinke ... stremi k nekakšni homeostazi, toda ne z individualno dresuro, temveč z globalnim ravnovesjem*" (Foucault, 1997/2003: 158–159), to pa ima posledice tudi za kaznovalno politiko. Whitaker namreč ugotavlja, da sodobna družba deluje "*na identifikaciji tveganja, ne nujno kaznivih dejanj kot takih*" (Whitaker, 1999: 22), zaradi česar krivda ali nedolžnost posameznika nista pomembni, pomembno je tveganje, ki ga skupina ljudi pomeni za organizacijo (Whitaker, 1999: 25–26).

V obeh primerih gre za tehnologiji telesa, vendar gre v prvem primeru za tehnologijo, kjer je telo individualizirano, v drugem primeru pa del neke širše skupnosti (Foucault, 1997/2003: 158–159); in ker ti dve tehnologiji nista na isti ravni, se med seboj ne izključujeta, prav nasprotno: dopolnjujeta se. "*Imamo torej dva niza: niz telo - organizem - disciplina - institucije; in niz populacija - biološki procesi - regulacijski mehanizmi - država*" (Foucault, 1997/2003: 159).[18]

Deleuze zato pravi, da smo posamezniki postali *dividuelni*: "*Disciplinarne družbe imajo dva pola: podpis, ki nakazuje individuuma, ter število ali matično številko, ki nakazuje njegovo mesto v množici. Tako prva kot druga nista bili za discipline nikoli nezdružljivi. Oblast hkrati pomasovi in oposamezni, se pravi vzpostavi telo tistih, nad katerimi se izvaja, oziroma ukalupi individualnost vsakega člena telesa (Foucault je izvor te dvojne skrbi videl v pastoralni oblasti duhovnika - črede in vsake izmed ovčk...) ... Nismo več med parom množica-posameznik. Individuumi so postali dividuelni.*" (Deleuze, 2002: 175).

[18] Tipičen primer za to sta medicina, ki je po Foucaultu "*vednost-oblast, ki se hkrati nanaša na telo in na populacijo, na organizem in na biološke procese in ki bo torej imela disciplinarne in regulacijske učinke*" (Foucault, 1997/2003: 161), ter seksualnost, ki ima, "*če je nedisciplinirana in nepravilna, vselej dve vrsti učinkov: ... učinek na telo ... [ter] določene učinke na ravni populacije*". (Foucault, 1997/2003: 161).

Pri prehodu iz disciplinskih v regulacijske družbe pa je viden še en prehod, prehod iz družbe suverenosti, ki je usmrtila ali pustila živeti, v regulacijsko družbo, ki omogoča življenje ali pa pusti umreti (Foucault, 1997/2003: 157). Oblast postane pastoralna, začne se "*uvajanje oblastnih aparatov, ki omogočajo ne le opazovanje, temveč tudi neposredni poseg in manipuliranje s tem pojavom [življenjem, m. op.]*" (Foucault, 1991: 99), začenja se oblast nad življenjem, oblast, ki tokrat deluje tako, da okrog naključnosti namešča varnostne mehanizme (npr. socialna zavarovanja, spremljanje epidemij itd.), ki ne delujejo na ravni posameznika, temveč na ravni populacije. Zato je danes nadzorovanje posameznikov ne samo sredstvo disciplinskega nadzora, marveč tudi sredstvo za zagotavljanje pravic družbene participacije; posamezniki smo že s samo participacijo v družbi (uveljavljanje državljanskih, zdravstvenih, zaposlitvenih in drugih pravic) izpostavljeni nadzoru, ta izpostavljenost pa je nujna za naše preživetje. "*Moderna država blaginje brez računalnikov in zbirk podatkov [torej nadzora, m. op.] ne more delovati*" pravi Mayer-Schönberger (Mayer-Schönberger, 2001: 222). S tem pa se spremeni tudi tehnologija kaznovanja – neprilagojenih posameznikov ni več treba neposredno kaznovati, dovolj je le, da jih izvržemo in "pustimo umreti".

Družba nadzora

Na vprašanje, kaj so družbe, v katerih sta na delu tako disciplina kot tudi regulacija, Deleuze odgovarja: "*... je pa dejansko Foucault tudi prvi opozoril, da so disciplinarne družbe nekaj, kar ravnokar zapuščamo, kar nismo več. Vstopamo v družbe nadzora, ki ne funkcionirajo s pomočjo zapiranja, temveč s pomočjo nenehnega nadzora in hipne komunikacije"* (Deleuze, 2002: 171). Za razliko od disciplinarnih družb, ki organizirajo velika okolja zapiranja, v katerih "dresirajo" posameznika (posameznik vedno prehaja iz enega v drugo: iz družine v šolo, iz šole v kasarno, iz kasarne v tovarno) (Deleuze, 2002: 173), gre zdaj za *"postopno razpršeno vzpostavitev novega režima gospostva*" (Deleuze, 2002: 177). Zgodil se je prehod iz družb začenjanja v družbe nekončanja: v disciplinskih družbah "*nismo nehali začenjati (od šole do kasarne, od kasarne do tovarne), v družbah nadzora pa nikoli ničesar ne končamo*" (Deleuze, 2002: 175). Ta prehod se na konkretni ravni kaže predvsem v izobraževanju, ki postaja permanentno, na ravni podjetja oziroma na delovnem mestu, ki postaja mesto nenehnega tekmovanja in nadzora in ki se z delom na domu širi tudi v zasebno sfero posameznika, ter pri marketingu, ki je "*postal središče ali 'duša' podjetja*" in o katerem Deleuze pravi, da "*je zdaj instrument družbenega nadzora in tvori nesramno raso naših gospodarjev*" (Deleuze, 2002: 176).

Skratka, v družbah nadzora je ključen nadzor, ki je "*kratkega roka in hitrega kroženja, toda tudi nenehen in brezmejen, medtem ko je bila disciplina dolgoročna, neskončna in diskontinuirana*" (Deleuze, 2002: 176), nadzor, ki ga Deleuze označuje kot pošast, ki jo je Foucault prepoznal kot našo bližnjo prihodnost (Deleuze, 2002: 174). Ta prehod v družbe nadzora Deleuze lepo povzame v enem stavku: "*Človek ni več zaprt, temveč zadolžen.*" (Deleuze, 2002: 176).

Ravno zaradi hkratnega delovanja discipline in regulacije se nadzor danes pojavlja v obliki nadziranja ljudi, ki se ga v glavnem poslužujejo države in nosilci oblasti, ter v obliki zbiranja podatkov o ljudeh (Lyon, 1994: 11). Webster ugotavlja, da sta "*organizacija in nadzorovanje*

siamska dvojčka, ki sta zrasla z razvojem modernega sveta" (Webster, 1995: 54). Beniger celo govori o *revoluciji nadzora* v 20. stoletju, ki jo primerja z industrijsko revolucijo 19. stoletja – pri njej gre predvsem za zmožnost izrabe informacij (Beniger, 1986: 427). Skratka gre za družbo, v kateri nadzor v njenem temelju ohranja ravnotežje (zaradi česar se sodobna družba boji odpraviti nadzorovanje in zaradi česar v tehtanju med pravico do zasebnosti in drugimi pravicami in ugodnostmi skoraj praviloma izgublja pravica do zasebnosti), ta nadzor pa je močno odvisen od tehnologije. In to ne od katerekoli tehnologije, temveč od informacijske tehnologije, zato Webster predlaga, da bi bilo morebiti namesto pojma *informacijska družba* bolje uporabljati pojem *družba nadzora*.

Tehnologija nadzorovanja

Vsekakor velja, da je nadzor tesno povezan s tehnologijo, predvsem z informacijsko tehnologijo, ki je namenjena zbiranju in obdelavi vseh vrst podatkov in informacij, ter s komunikacijsko tehnologijo, ki je po mnenju Thomasa okužila vse vidike človeške komunikacije, saj "*posreduje skoraj vsako obliko človeških odnosov*" (Thomas, 2000: 22). Kot je razvidno že iz razvoja pravne zaščite zasebnosti, so ravno tehnološke spremembe pomemben dejavnik, ki povečuje nadzor, in s tem tudi eden poglavitnih motivov za spremembo zakonodaje. Zaskrbljujoče je tudi to, da "*so se znanstvena tehnologija in klasične metode nadzorovanja združile in da so zato tehnična sredstva za nadzorovanje izredno izpopolnjena in se še izpopolnjujejo*" (Šelih, 1979: 157). Značilen zgled za to so telekomunikacijske tehnologije (primera *Katz*[19] in *Olmstead*[20] v ZDA) in tehnologije, ki omogočajo avtomatsko obdelavo podatkov (zakonodaja za zaščito osebnih podatkov v Evropi).

Vendar pa sodobna računalniška tehnologija ni namenjena samo spremljanju posameznikovih dejavnosti, temveč lahko celo tehnično omeji določena ravnanja posameznikov in jim tako fizično omeji možnosti (napačnega) delovanja. Deleuze pravi: "*V družbah nadzora pa bistveno ni več podpis ali število, temveč šifra: šifra je geslo, disciplinarne družbe pa urejajo ukazi ... Numerični jezik sestoji iz šifer, ki zaznamujejo dostop ali zavrnitev dostopa do informacije.*" (Deleuze, 2002: 175). Ne gre torej za to, da bi oblast s prepovedjo, ukazom posamezniku omejila dostop, gre za to, da posameznika opremi z geslom, ki mu dostop omogoča ali pa ga zavrne. Posamezniku se torej odvzema svobodna volja, le-to pa nadomeščata geslo in tehnologija: "*Ni pomembna zapornica, temveč računalnik, ki zabeleži dopustno ali nedopustno mesto vsakogar in izvaja občo modulacijo*" pravi Deleuze (Deleuze, 2002: 177).

Računalnik oziroma informacijsko-komunikacijska tehnologija se torej vzpostavlja kot osrednja tehnologija nadzora, saj ta tehnologija nadzorovanje poglablja in krepi. Ne samo, da ga omogoča, temveč ga tudi olajšuje, saj je že v osnovi zasnovana za zbiranje in hranjenje podatkov. Deleuze pravi, da "*stroji izražajo družbene oblike*" (Deleuze, 2002: 176) (čeprav velja, da niso določujoči): "*vsakemu tipu družbe očitno ustreza neki tip stroja: preprosti ali dinamični*

[19] Katz v. United States, 389 U.S. 347 (1967).
[20] Olmstead v. United States, 277 U.S. 438 (1928).

stroji družbam suverenosti, energetski stroji disciplinarnim družbam, kibernetični stroji ali računalniki družbam nadzora" (Deleuze, 2002: 172). Zato ne preseneča, da je sistematičen in množičen nadzor, kakršnega poznamo v sodobni družbi, nastal obenem z nastankom in rastjo vojaške organizacije, industrijskih mest, vladne administracije in kapitalističnega podjetništva, predvsem pa z nastankom informacijskih in mikroprocesorskih tehnologij, ne preseneča pa niti, da je zasebnost posameznikov postala resen problem prav v dvajsetem stoletju in da so se strahovi glede informacijske zasebnosti razvili kot neposreden odgovor na razvoj informacijske tehnologije (Cate, 1997: 44).

Nastanek interneta je probleme nadzorovanja in zasebnosti še okrepil. Po poročilu Privacy & Human Rights 1999 zasebnost ogrožajo trije pomembni pojavi: *globalizacija* (odstranjuje geografske omejitve pri pretoku podatkov), *konvergenca med tehnologijami* (le-te so med seboj čedalje bolj povezljive in medoperabilne) ter *multimedialnost* (podatki v neki obliki se lahko hitro spremenijo v drugo obliko) in za internet zagotovo velja, da predstavlja stično točko med temi tremi pojavi. Gre za medij, ki je globalen, multimedialen, na njem pa prihaja tudi do konvergence med različnimi tehnologijami, saj se v internet danes ne povezujemo samo z računalniki, temveč tudi z mobilnimi telefoni in celo drugimi napravami (npr. nadzornimi kamerami ('*nannycam*', Wi-Fi kamere itd.), televizorji in celo hladilniki). Ker se uporaba interneta hitro širi, je lahko ta medij posredno velika grožnja zasebnosti.

Benthamov načrt Panoptikona iz leta 1791 je predvideval optični nadzor, v informacijski družbi pa vidnost ni več samo optična, večina današnjega nadzora se pojavlja na območju digitalnih signalov in prometnih podatkov, ki se zbirajo in shranjujejo samodejno in vsaj nekaj časa tudi hranijo. Zato so zbirke podatkov eno poglavitnih orodij množičnega nadzora. James Rule ugotavlja, da predstavljajo omejitev sodobnih sistemov nadzora štirje dejavniki: velikost datotek, ki jih sistem lahko shranjuje, stopnja, do katere so lahko ti sistemi centralizirani (pri čemer je treba poudariti, da so tudi formalno ločeni, na videz decentralizirani nadzorni sistemi, ki so povezani prek komunikacijske tehnologije, lahko centralizirani (Lyon, 1994: 55)), hitrost pretoka podatkov in informacij med točkami v sistemu ter število stičnih točk med sistemom in subjektom (Lyon, 1994: 51). Po Benigerju se revolucija nadzora vzdržuje sama po sebi, to pa omogočajo trije dejavniki. Izraba energije, hitrost obdelovanja informacij in tehnologije nadzora sobivajo v pozitivni spirali – napredek enega dejavnika povzroči ali vsaj omogoči napredek preostalih. Poleg tega tehnološke inovacije sprožajo potrebe po novih in novih tehnoloških inovacijah (Beniger, 1986: 433–434); značilen zgled so tehnologije zbiranja podatkov, ki so s seboj prinesle potrebo po novih tehnologijah shranjevanja podatkov, povečane zmogljivosti pomnilniških sistemov pa ustvarjajo možnosti za še bolj izpopolnjene in ekstenzivne metode zbiranja podatkov.

Vendar pa je povečana moč nadzorovanja tudi v tem, da tehnologija omogoča povezovanje zbranih podatkov.[21] Ni torej nujno, da nadzor poteka v obliki enega orwellovskega Velikega brata, lahko je tudi *razpršen*. S povezavo razpršenih podatkov in njihovo obdelavo lahko pridemo do novih pomembnih podatkov in informacij. Pri tem je ključna uporaba informacijsko-komunikacijske tehnologije. Nove razsežnosti nadzora pa vzpostavljajo tudi napredne statistične tehnike, na primer tehnike izkopavanja podatkov (ang. *data mining*) in sistemi umetne inteligence. S tem se dogaja preskok na novo raven, na raven *preventive* in *predvidevanja*. Sodobna panoptična tehnologija tako ne čaka, da se nekaj zgodi, temveč ukrepa že vnaprej na podlagi zbranih podatkov in ocenjenih predvidevanj; posameznike razvršča v kategorije tveganja (Whitaker, 1999: 44), zaradi česar se odpirajo nove možnosti za različne oblike statistične diskriminacije, npr. diskriminacije potrošnikov.

Množični podatkovni nadzor postaja rutinski in je čedalje bolj namenjen profiliranju posameznikov, razvrščanju v kategorije. *Preventiva, predvidevanje* in *katalogiziranje* postajajo čedalje pomembnejše usmeritve v razvoju sodobnih nadzorovalnih sistemov.

Nove elektronske nadzorne tehnologije so nevidne oziroma težko opazne, neprostovoljne (oziroma posameznik nima možnosti, da bi se jim izognil), so bolj kapitalsko kot delovno intenzivne (zaradi česar so tudi razmeroma poceni in ekonomične) in niso usmerjene k obravnavi točno določenega posameznika, temveč h kategoriji posameznikov (Lyon, 1994: 68). Zaradi tehnologije postaja nadzorovanje čedalje bolj obsežno, nezaznavno, instrumentalizirano, neselektivno in preventivno, zaradi česar tudi čedalje bolj spodkopava človekove pravice in svoboščine. V kontekstu množične rabe tehnologij nadzora danes pa ne moremo mimo ugotovitve Šelihove, ki možnosti zlorabe ne vidi zgolj v neupravičeni ali nepooblaščeni uporabi tehnologij nadzora, temveč tudi v prepogosti rabi le-teh s strani tistih, ki so jih sicer upravičeni uporabljati (Šelih, 1979: 157).

Po ugotovitvah poročila Privacy and Human Rights 2003 je v skoraj vsaki državi, ki je po 11. septembru 2001 spreminjala kazensko in preiskovalno zakonodajo, opaziti dvoje teženj. Prva je povečan obseg pooblastil za nadzorovanje, ki obsega tudi povečan obseg podatkov, ki jih državni organi smejo zbirati. Druga težnja pa gre v smeri poenostavljanja oziroma zmanjševanja zahtev za odobritev takih posegov s strani sodišč in za zmanjšan nadzor nad delom preiskovalnih

[21] Kako povezovanje podatkov prek univerzalnih identifikatorjev pomnoži moč nadzorovanja, kaže primer rabe *Social Security Number* (SSN) v ZDA. Hkrati je uporaba SSN tudi primer tehnologije, ki čedalje bolj pridobiva vlogo izvajanja nadzora. SSN je bila v ZDA na začetku razvita kot identifikacijska številka za ameriški sistem socialne varnosti. Leta 1943 je ameriški predsednik Roosevelt ukazal, naj se SSN začne uporabljati v vladnih zbirkah podatkov, leta 1961 pa je ameriška davčna uprava SSN uporabila kot davčno številko. Pozneje se je SSN začela uporabljati kot osebna vojaška številka; to številko so uporabljali tudi v kartotekah vietnamskih veteranov, obvezno so jo morali oddati vsi kupci državnih obveznic, prejemniki starostne pomoči itd. Leta 1976 je ameriški Kongres dovolil uporabo SSN v zbirkah registriranih vozil in vozniških dovoljenj, po letu 1984 pa so morali vsi imetniki bančnih računov bankam sporočiti svoje številke SSN (Sykes, 1999: 51-52). Hkrati se je uporaba številke SSN razširila še v zasebnem sektorju. Sykes navaja, da jo kot identifikacijo uporabljajo univerze, trgovine, podjetja, delodajalci itd. Skratka, nenadoma je SSN postala univerzalni identifikator, na katerega se "lepijo" številne med seboj ločene zbirke podatkov in prek katerega je te zbirke podatkov mogoče natančno povezati v velik nacionalni dosje. Po 11. septembru 2001 se v ZDA dejansko čedalje bolj govori o povezovanju teh baz med seboj, verjetno pa ni naključje, da so med pomembnimi zagovorniki tudi predstavniki industrije, ki se ukvarja z zbirkami podatkov (npr. izvršni direktor Oracla Larry Ellison ter izvršni direktor Sun Microsystems Scott McNealy) (EFF, 2005b).

organov in tajnih služb (Laurant, 2003: 23–24). Prvi predlog protiteroristične zakonodaje v Kanadi je npr. predvideval, da preiskovalnim organom ne bi bilo več treba opravičiti zahtevka za pridobitev sodne odredbe za prisluškovanje (Laurant, 2003: 23). V ZDA so bili predlogi spremembe zakonodaje s stališča zaščite zasebnosti še bolj sporni, saj so se že kmalu po 11. septembru oglasile zahteve po prepovedi takih kriptografskih izdelkov, ki bi državnim organom onemogočali dostop do vsebine šifriranih sporočil (Harrison, 2001), in celo predlogi, naj ima policija pristojnost odrediti nadzor prometnih podatkov v internetnih komunikacijah brez odredbe sodišča za 48 ur (McCullagh 2001a, 2001b in 2001c); to se je v obliki t. i. *National Security Letter* (pisma o nacionalni varnosti, dokumenta, ki ga izda FBI in v katerem zagotovi, da je zadeva pomembna za nacionalno varnost) delno celo uresničilo. Po ameriškem USA PATRIOT Act[22] namreč lahko FBI v primerih nacionalne varnosti zahteva vpogled v finančne transakcije; novembra 2003 pa je ameriški Kongres sprejel zakon, s katerim je 'finančne institucije' definiral tako široko, da lahko FBI zahteva podatke od zavarovalnic, nepremičninskih agencij, pošte, potovalnih agencij, igralnic, zastavljalnic, ponudnikov dostopa do interneta, izposojevalnic avtomobilov in vseh drugih podjetij, "*katerih denarne transakcije imajo visoko uporabnost pri preiskovanju kriminala*" (Singel, 2003). Leta 2005 je FBI uporabil institut 9254-krat, in sicer proti 3501 posamezniku (EPIC, 2006a).

Če je pred nekaj leti veljalo, da zmožnosti tehnologije krepko prehitevajo pravni razvoj v smislu, da nadzora ne omejujejo tehnologije, temveč pravna pravila, se danes zdi, da pravna pravila temu razvoju tesno sledijo.

Nadzor državljana in nadzor potrošnika

Beniger pravi, da je obdelava informacij temeljna za vse dejavnosti, usmerjene k cilju (Beniger, 1986: 434), zato se praktično vse sodobne organizacije tako ali drugače ukvarjajo ali vsaj srečujejo z nadzorom. Po Foucaultu ima nadzor disciplinsko in regulacijsko funkcijo. Imamo torej dva niza: "*niz telo - organizem - disciplina - institucije; in niz populacija - biološki procesi - regulacijski mehanizmi - država*" (Foucault, 1997/2003: 159). Obe funkciji nadzora je mogoče zaznati tako v javnem kot v zasebnem sektorju.

Država disciplinski nadzor izvaja ob pomoči represivnih organov, regulacijskega pa prek državne statistike in tajnih služb (kolikor le-te zaznavajo stopnje določenih negativnih pojavov v družbi, seveda pa tajne službe lahko delujejo tudi disciplinsko). Zasebni sektor izvaja disciplinski nadzor na delovnem mestu, regulacijskega pa nad potrošniki z marketingom. Smo torej hkrati posamezniki-državljani, posamezniki-potrošniki in posamezniki-delojemalci, smo dividuelni.

[22] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001, 18 U.S.C. (2001).

Prvotno so države nadzor (v obliki prisluškovanja in prestrezanja pisem) uporabljale v diplomaciji in politiki. Na to kaže tudi zelo zgoden nastanek kriptografije - očitno zaradi želje po zaščiti zasebnosti in tajnosti (Kahn, 1973: 77). Leta 1653 je tako Lord Turloe v Angliji osnoval "*The Secret Office*" (Bamford, 1983: 500), leta 1657 pa je odpiranje pisem v Angliji postalo povsem zakonito, saj je bilo v poštnem pravilniku zapisano, da je "*pošta najboljše sredstvo za odkrivanje nevarnih in zlobnih dejanj proti državi*" (Kahn, 1973: 109). Pozneje se je na podlagi zakona o poštnih uradih iz leta 1711 celo izoblikoval sistem, v katerem so poštni uradniki smeli pošto odpirati le na podlagi odredb, te pa so si izdali kar sami (Kahn, 1973: 109). Angliji so sledile tudi druge države, ki so okrog leta 1700 kmalu ustanovile svoje "črne kabinete" (ang. *Black Chamber*); najbolj znan med njimi je bil dunajski, v katerem so prestrezali predvsem diplomatsko pošto (Kahn, 1973: 104). Pozneje so te kabinete začeli opuščati (v Angliji junija 1844, v Avstriji 1848, v Franciji v istem obdobju), razlog za to pa je bil razvoj človekovih pravic, ki ni dopuščal samovoljnega vladnega odpiranja pošte (Kahn, 1973: 111).

Države pa so nadzor uporabljale tudi v smislu regulacije, predvsem v obliki popisovanja posesti in preštevanja prebivalstva z namenom vzpostavitve pregleda ter utrjevanja moči. Eden najzgodnejših primerov sega v leto 1086, ko so v Angliji začeli voditi *Domesday Book*, v katero so zapisovali zakupna zemljišča, vsebovala pa je tudi obsežno zbirko podatkov o prebivalstvu in njegovem imetju, na podlagi katere so uvedli davčno reformo ter okrepili vojaško moč (Lyon, 1994: 22–23), čeprav so bili popisi prebivalstva znani že precej pred tem časom. Lyon pa ugotavlja, da se je nadzor bolj pospešeno razvil skupaj z demokracijo, natančneje skupaj z razsvetljensko zahtevo po enakosti (Lyon, 1994: 24) oziroma politični participaciji. Državni regulacijski nadzor pa je, kot ugotavlja Foucault, dobil pospešek konec 18. stoletja in pozneje, ko se začenja pojavljati biopolitika (Foucault, 1991: 67), ter z uvedbo tehnologije (Hollerithovih strojev pri ameriškem popisu prebivalstva leta 1890 (Black, 2002: 34), katerih uporaba se je hitro razširila v druge države in v zasebna podjetja).

Zgodovinsko gledano, je torej največja grožnja zasebnosti država, vendar pa lokomotiva tega procesa čedalje bolj postaja zasebni sektor. Nadzorovanje v zasebnem sektorju se je razvilo praktično z nastankom kapitalizma – menedžment je bil prvotno razvit za nadzor in discipliniranje delavcev (Lyon, 1994: 25) – kapitalizem pa je zelo hitro začel uporabljati nadzorne tehnologije ne samo za nadzor zaposlenih, temveč tudi za nadzor potrošnikov. Predvsem je problematično, ker ima danes zasebni sektor na voljo bistveno več sredstev za obdelavo osebnih podatkov kot država (Flaherty, 2001: 187), hkrati pa je za razliko od državnega zasebni nadzor, kot bo prikazano v naslednjih poglavjih, v ZDA skoraj povsem nereguliran, v Evropi pa se nadzorovalne prakse pogosto močno razlikujejo od predpisanega stanja.

Dodatni problem potrošniškega nadzorovanja pa je tudi ta, da si posamezniki ne morejo privoščiti in celo ne želijo "izstopiti". Nadzor jim namreč na videz prinaša dodatne ugodnosti (npr. popuste), včasih (v ZDA) pa je za izstop iz tega sistema treba celo plačati. Večinoma izstop niti ni mogoč, saj podjetja povezujejo uporabo svojih storitev z nadzorovanjem potrošnikov; potrošniki, ki želijo ohraniti svojo zasebnost, tako sploh ne morejo stopiti v poslovno razmerje ali uporabljati storitev podjetja. Tehnologije kot t. i. "zaupanja vredno računalništvo" ("Trusted

Computing") pa možnosti izstopa še omejujejo. Kljub temu da je nadzorovanje na videz prijazno do potrošnika, saj se mu prilagaja in ga "potiska", kamor si sam želi, oziroma ga zalaga z dobrinami in vsebinami, ki ustrezajo njegovemu izmerjenemu okusu in ocenjenim potrebam, pa je pravzaprav potrošnik tisti, ki je v podrejenem položaju, torej tisti, ki v resnici ni svoboden.

Posledice se kažejo v različnih oblikah statistične diskriminacije, tipično pa v poslovnem modelu dinamičnega določanja cen (ang. *dynamic pricing*), v katerem se potrošniku lahko zgodi, da bo zaradi svojih preteklih nakupnih navad za neki izdelek plačal več kot drugi ali pa morda ne bo deležen enakih popustov kot drugi. Dinamično določanje cen je določanje cen glede na ponudbo, povpraševanje in spreminjajoče se potrošniške preference (Srivastava, 2001: 1–2), ta model pa naj bi bil primeren predvsem za t. i. povezano ekonomijo (ang. *connected economy*) ter velike, fragmentirane in nestanovitne trge (Srivastava, 2001: 3), na katerih pa se uporablja informacijska tehnologija, ki omogoča zajemanje in analizo podatkov o potrošnikih (definicija pravzaprav opisuje tipično internetno okolje). Eden izmed poučnih primerov posledic uporabe takega modela za potrošnike se je zgodil konec leta 2000, ko so nekateri uporabniki spletne trgovine Amazon.com ugotovili, da za enake izdelke plačujejo več kot drugi. Amazon je pozneje priznal, da so preverjali vpliv cene na nakupne navade potrošnikov, vendar pa naj bi bilo to preverjanje omejeno, potrošniki pa naj bi bili izbrani povsem naključno in ne na podlagi potrošniških preferenc (Bicknell, 2000). Ne glede na zagotovila Amazona pa je zelo verjetno, da tovrstna statistična diskriminacija že obstaja, le da je potrošniki ne opazijo. Na to med drugim nakazuje tudi ocena analitikov organizacije Forrester Research, ki pravi, da bo "*poosebljeno določanje cen (zagotovo) del naravnega razvoja spleta*" (Bicknell, 2000).

Potrošniki in državljani tako živimo v svetu, v katerem se "moramo" odpovedati delu svoje zasebnosti v imenu večje funkcionalnosti in udobja, sodobni Panoptikon pa je zasnovan tako, da se posamezniki nadzoru podrejajo celo prostovoljno.

Ambivalentnost nadzora: nadzor oblasti

Če smo potrošniki in državljani izpostavljeni nadzoru, pa lahko posamezniki nadzor tudi izvajamo. Funkcija nadzora je namreč ambivalentna, saj lahko tudi državljani nadzorujejo oblast (oziroma v splošnem nosilce moči) in ne samo nasprotno. Če o nadzoru posameznikov govori zamisel Panoptikona, pa je zamisel nadzorovanja oblasti Bentham razvil v svojem delu *Of Publicity*.

Tako kot si je Bentham v Panoptikonu zamislil popolno transparentnost zapornikov, je v zamisli o nadzoru politične skupščine uporabil idejo o transparentnosti ob pomoči publicitete, ki predstavlja zakon za zagotavljanje javnega zaupanja (Bentham, 1791/1994: 581). Prepričan je bil, da odprta in svobodna politika ne predstavlja zaupanja in varnosti samo za ljudi, temveč tudi za voditelje: "*Dovolimo, da ne bo mogoče, da bi bilo narejeno karkoli, kar bi bilo ljudstvu neznano – dokažimo jim, da jih ne želimo niti ogoljufati, niti presenetiti – s tem jim odvzamete vsa orožja nezadovoljstva. Javnost vam bo poplačala s še večjim zaupanjem. Kleveta bo izgubila*

svojo moč... od dveh vlad, od katerih bo ena delovalo skrito in druga odprto, bo slednja imela moč, pogum in spoštovanje, in to jo bo napravilo močnejšo od druge" (Bentham, 1791/1994: 582–583). Še bolj konkretno: "*zakonito nasprotovanje* (Bentham je verjetno mislil *možnost* zakonitega nasprotovanja, m. op.) *nepriljubljenim ukrepom bo preprečilo zamisel nezakonitega odpora*" (Bentham, 1791/1994: 583).

Hkrati je po Benthamu publiciteta tudi "*pogoj za oblikovanje razsvetljene sodbe*" (Bentham, 1791/1994: 590): "*Prav tako, kot je za vladane pomembno poznati vodenje vladajočih, je za vladajoče pomembno, da poznajo želje vladanih*", navaja Bentham kot tretji razlog publicitete (Bentham, 1791/1994: 584). Poleg tega je "*publiciteta absolutno nujna, da volivci lahko delujejo na podlagi znanja*" (Bentham, 1791/1994: 585).

Publiciteta bo torej članom parlamenta pomagala spoznati potrebe ljudstva, ljudstvu pa bo pomagala v parlament izvoliti primerne zastopnike: "*Ljudstvo bo bolj varno pred zvijačami demagogov in prevarami goljufov; bolj bo spoštovalo velike nadarjene posameznike, lahkomiselnost bo zmanjšana na komaj zaznavno mero. Navadi razsojanja in debate bosta preželi vse družbene razrede*" (Bentham, 1791/1994: 583).

Še pomembnejša pa je nadzorna funkcija publicitete. Že takoj na začetku namreč kot prvi razlog za publiciteto Bentham navaja, da je z njo treba "*prisiliti člane skupščine opravljati njihovo dolžnost*" (Bentham, 1791/1994: 581). Po njegovem mnenju je namreč javnost "*tribunal, ki ima večjo moč kot vsi drugi tribunali skupaj; ... je nepodkupljiv; nenehno teži k temu, da postane razsvetljen, ...kazni, ki jih nalaga, so neizogibne*" (Bentham, 1791/1994: 581–582). Bentham tako neposredno razvije tezo, da izpostavljenost oblasti nadzoru javnosti le-to disciplinira (saj "*odpravlja nerazsvetljene sobane, v katerih se kotijo arbitrarna politična dejanja, kaprice monarhov, vraževernost, zarote duhovnikov in tiranov, epidemije in nevedne iluzije*" (Foucault, 1991: 46–47)); to je vidno tudi, ko govori o "sovražnikih publicitete", ki se želijo izogniti publiciteti: "*Sovražnike publicitete lahko razvrstimo v tri kategorije: hudodelec, ki poskuša ubežati roki pravice; tiran, ki skuša zadušiti javno mnenje, ker se boji slišati njegov glas; boječ ali len človek, ki se pritožuje nad splošno nesposobnostjo zato, da bi zakril svojo lastno.*" (Bentham, 1791/1994: 582). Zato Bentham meni, da tisti, ki bi se želel skriti pred publiciteto, "*ni niti dober niti pameten človek, ker se na dolgi rok nima ničesar bati, upa pa lahko na vse*" (Bentham, 1791/1994: 582). Kajti "*tajnost je instrument zarote; zato ne bi smela biti sistem normalnega vladanja*" (Bentham, 1791/1994: 591).

Zamisel o transparentnosti parlamenta je pravzaprav zelo podobna zamisli Panoptikona, v obeh primerih Bentham uporabi isto načelo, in sicer načelo nadzora, nadzor pa je orodje, s katerim naj bi nadzornik (v enem primeru gre za Inšpektorja, v drugem za ljudstvo) dosegel podreditev nadzorovanega – njegovo moralno vedenje. Oba sistema tudi temeljita na popolnem nezaupanju; v Panoptikonu je tudi Inšpektor nadzorovan (s strani obiskovalcev), parlament je nadzorovan s strani javnosti. V obeh primerih gre torej za stroj, ki naj bi bdel nad ravnanjem posameznikov, hkrati pa ne bi bil v lasti nikogar in ga torej ne bi bilo mogoče zlorabiti.

A razlika ni le v tem, da gre pri zamisli o Panoptikonu za nadzor večine s strani manjšine, pri zamisli o publiciteti parlamenta pa za nadzor manjšine (poslancev) s strani večine. V družbi nadzora smo nadzoru bistveno bolj izpostavljeni posamezniki kakor predstavniki

oblasti, tehnologija nadzorovanja posameznikov pa je bolj učinkovita in razvita kot tehnologija nadzorovanja oblasti. Hkrati je nadzorovanje posameznikov čedalje bolj netransparentno.

Poleg tega prihaja še do sprevračanja Benthamove zamisli o povezovanju netransparentnosti z nemoralnostjo. V *Of Publicity* je namreč Bentham razvil tezo, da netransparentnost, skrivanje oblasti kaže na njeno nemoralnost: "*Nezaupljivost se vedno povezuje s skrivnostjo. [Nezaupljivost] misli, da vidi zločin, kjer opazi spakovanje tajnosti; in redko se vara. Zakaj bi se skrivali, če nas ni groza, da bi bili vidni? Tako kot se nemoralnost zavija v temo, nedolžnost zakoraka v odprti dan...*" (Bentham, 1791/1994: 582). Čeprav je bila zamisel prvotno naperjena proti netransparentnosti oblasti, pa se pogosto uporablja kot argument proti zasebnosti posameznikov. Spreobrnjeno zamisel o netransparentnosti in nemoralnosti je provokativno prikazal avtor znamenitega šifrirnega programa PGP Phill Zimmermann: "*Če ste res državljan, ki spoštuje zakon in nimate ničesar skriti, zakaj potem ne pošiljate pošte na razglednici? Zakaj se na zahtevo takoj ne podvržete testiranju o vsebnosti drog v vašem telesu? Zakaj za policijsko preiskavo vaše hiše zahtevate sodno odredbo? Ali morda skušate kaj skriti? Ali pomeni, da ste prevratnik, trgovec z drogo ali morda paranoičen norec, če skrivate svojo pošto v kuverto? Ali imajo državljani, ki spoštujejo zakon, kakršnokoli potrebo po šifriranju svoje pošte?*" (Zimmermann, 1999).

Posamezniki, ki želijo zaščititi svojo zasebnost, so torej deležni očitkov o skrivanju in s tem nemoralnosti. "*Biti dober državljan... pomeni biti merljiv in predvidljiv potrošnik*" (Palmer, 2000: 92), pravi Gareth Palmer. Z drugimi besedami: biti dober državljan pomeni postati transparenten za oblast in družbo. In nasprotno – kdor je netransparenten, že po definiciji postane "slab" oziroma sumljiv.

Možnosti osvoboditve v družbi nadzora?

Glede na to, da nadzor v temelju sodobne družbe ohranja ravnotežje, in glede na to, da sodobni nadzor pravzaprav deluje precej prikrito in morda celo hinavsko, se upravičeno zastavlja vprašanje, ali je v družbi nadzora sploh še možna "osvoboditev", še posebej pa se to vprašanje zastavlja v primeru nadzora potrošnikov. Če namreč skuša država oceniti tveganje in ga izključiti, pa skušajo korporacije prepoznati priložnosti (morebitne potrošnike) in jih vključiti (Whitaker, 1999: 125). Whitaker pravi, da se slogan iz Orwellovega romana "*Veliki brat te opazuje! / Big Brother is watching you!*" spreminja v slogan "*Veliki brat skrbi zate / Big Brother is watching out for you*". Če je državni nenadzor pomenil, da te država pusti pri miru, pa potrošniški nenadzor zdaj pomeni, da je potrošnik izločen iz koristi (Whitaker, 1999: 142). "*Zgodnejši Panoptikoni so vedno povzročili odpor. Današnji Panoptikon pa je bolj fin, bolj prožen, bolj participativen, bolj konsenzualen*", pravi Whitaker, a nadaljuje: "*Toda popoln družbeni nadzor je mogoč samo v domišljiji.*" (Whitaker, 1999: 152).

Kot je opozoril že Foucault, je popoln nadzor (obnašanja posameznikov) slepilo, saj ljudje nismo pasivna bitja, temveč aktivno iščemo načine, kako se izmuzniti iz mreže. Deleuze pravi, da *"družbe nadzora delujejo s pomočjo ... informacijskih strojev in računalnikov, katerih pasivna nevarnost so motnje, aktivna pa piratstvo in vpeljava virusov"* (Deleuze, 2002: 176). Po njegovem

mnenju piratstvo in računalniški virusi postajajo *"stavke oziroma tisto, kar so v devetnajstem stoletju imenovali 'sabotaža' (cokla v stroju)"* (Deleuze, 2002: 172). Tehnologija torej ne samo zasužnjuje, temveč omogoča tudi osvoboditev. Če po eni strani drži, da je tehnologija ravnotežje med nadzorom in zasebnostjo praktično vedno pomikala proti nadzoru, pa ne smemo pozabiti, da jo je mogoče uporabiti tudi za varovanje zasebnosti. Za razvoj teh tehnologij, na primer šifrirnih sistemov, sistemov za anonimizacijo, sistemov za preprečevanje vdorov itd., so zaslužni številni posamezniki in nevladne organizacije, zaradi nevarnosti kiberkriminala pa ti sistemi niso uporabni zgolj za zaščito zasebnosti, temveč čedalje bolj postajajo nujni del vsakega informacijskega sistema. Danes se pospešeno razvija tudi trg informacijske varnosti, informacijska varnost postaja izdelek. Kljub temu je ta tehnologija pod velikim udarom, predvsem države in njenih represivnih organov. Uporaba kriptografije v civilne namene je bila vedno predmet številnih razprav in poizkusov omejitev, hkrati pa je bila njena uporaba v vojaške in obveščevalne namene popolnoma neomejena. Tehnologija sicer omogoča osvoboditev, a kaže, da le manjšemu številu posameznikov, ki si morajo uporabo tehnologije celo izboriti, pri tem pa tudi pristati na številne stroške, saj taka osvoboditev navadno pomeni tudi izločenost. Zato v družbi nadzora sicer so možnosti osvoboditve, vendar osvoboditev ni samoumevna, temveč si jo je treba izboriti. Žal se zdi, da si večina potrošnikov (in državljanov) tega niti ne želi.

PRAVICA DO ZASEBNOSTI

Ko govorimo o zasebnosti, mislimo predvsem na pravico do zasebnosti. Osrednja prvina pravice je možnost, da posameznik na določen način ravna, pravo pa pravice dodeljuje zato, da lahko posamezniki zadovoljujejo svoje interese. Cilj pravice je torej interes, pravo pa varuje tiste interese, ki so ovrednoteni kot pravno relevantni (Pavčnik, 1997: 116–117). Večina literature, pa tudi aktivistov, ki se ukvarjajo z zasebnostjo, o zasebnosti govori kot o pravici. Ta pravica pa je navadno negativno definirana.

Berlin negativno svobodo definira kot svobodo *od*, odsotnost vmešavanja (Berlin, 1992: 74), zato se negativno koncipirana svoboda nanaša na območje nadzora, ne na njegov vir (Berlin, 1992: 76). Gre torej za odsotnost prisile in vmešavanja drugih: "*Brez politične svobode oziroma prostosti si le, če ti človeška bitja preprečujejo doseči namen. Sama nesposobnost doseči namen še ni odsotnost politične svobode.*" (Berlin, 1992: 70). Gre torej za to, da "*neki del človeške eksistence mora ostati zunaj sfere družbenega nadzora. Zavzetje tega zatočišča, če je še tako majhno, bi bilo despotizem ... Moramo ohraniti minimalno območje osebne svobode, če nočemo 'degradirati in zanikati svoje narave' ... Kaj mora biti torej ta minimum? Tisto, čemur se človek ne more odpovedati, ne da bi prizadel bistvo svoje človeške narave. Kaj je to bistvo? ... To je bilo in najbrž vedno bo stvar neskončne razprave.*" (Berlin, 1992: 73). V Berlinovem razumevanju negativne svobode je mogoče potegniti vzporednice s pomenom zasebne oziroma intimne sfere po Arendtovi. Arendtova namreč poudarja pomen intimnega prostora pred vdorom družbenega v posameznika. To je po njenem pogoj političnega delovanja. "*Gre za nekakšen 'room of one's own', ki jo potrebujemo, da bi se zatopili v dialog v samim seboj takrat, kadar moramo misliti in razsojati*" (Jalušič, 1995: IL), pri čemer pa Arendtova tega prostora, v katerem naj bi posameznika pustili pri miru, ne dojema samo kot privilegij filozofov, temveč ga hoče omogočiti vsakomur, ki želi postati politično bitje (Jalušič, 1995: IL).

Seveda pa se zastavlja vprašanje, kako obsežno naj bo to območje osebne svobode. Berlin pravi, da če "*bi vstopali vanj [torej, če bi ga ožili, m. op.], bi se posameznik znašel na preozkem območju še za tisti minimalni razvoj svojih naravnih sposobnosti, ki nam edine omogočajo uveljavljati ali si sploh zamisliti različne cilje...*" (Berlin, 1992: 71). Zato je treba "*potegniti mejo med območjem zasebnega življenja in območjem javne oblasti*[23]" (Berlin, 1992: 71), a to zaradi človeške soodvisnosti ni enostavno. Iz tega sledi, da je vprašanje določitve meje, znotraj katere bi morali posamezniki biti nedotakljivi, povezano s pojmovanjem, "*kaj pomeni biti normalno človeško bitje*" (Berlin, 1992: 83). Kje torej potegniti mejo med zasebno in javno sfero? Na to vprašanje Berlin odgovarja, da je to "*stvar razprave, pravzaprav prepira*" (Berlin, 1992: 71). Zaradi tega je tudi obseg pravice do zasebnosti stvar nenehne razprave, nenehnega dogovarjanja in "prepiranja", ki se pod vplivom tehnološkega razvoja nadzorovalnih tehnologij le še stopnjuje.

---

[23] Berlin v tem kontekstu sicer postavlja vprašanje zasebnega območja le nasproti javni oblasti, ne pa tudi nasproti družbi, vendar je iz njegove koncepcije svobode razvidno, da si zastavlja tudi vprašanje omejevanja svobode s strani družbe, in ne samo države.

Vendar pa Berlin podobno kot Habermas in Arendtova, le mnogo bolj eksplicitno, ugotavlja, da "*občutek zasebnosti, prostora osebnih odnosov kot nečesa samoumevno svetega, izhaja iz pojmovanja svobode, ki navzlic svojim verskim koreninam v svoji razviti obliki ni veliko starejše od renesanse ali reformacije*" (Berlin, 1992: 76). Sicer je bila želja po tem, da se ne bi nihče vtikal vate, vedno znak visoke civiliziranosti (Berlin, 1992: 76), vendar pa "*pojma posameznikovih pravic ni bilo v pravnih koncepcijah Rimljanov in Grkov; zdi se, da isto velja za judovsko, kitajsko in vse druge doslej odkrite stare civilizacije. Prevlada tega ideala je bila prej izjema kot pravilo*" (Berlin, 1992: 75). Zasebna sfera v svoji eksplicitni obliki, zasebnost kot pravica in vrednota, se torej pojavi šele s kapitalizmom. Kapitalizem oziroma tržno usmerjena množična družba pa ta ideal čedalje bolj spodjeda in ob pomoči tehnološkega napredka tudi oži območje zasebnosti. "*Ideal svobodne izbire ciljev ... ter s tem povezani pluralizem vrednot je morda le pozni sad naše pojemajoče kapitalistične civilizacije: ideal, ki ga minule dobe in primitivne družbe niso priznavale, ideal, ki se mu bodo zanamci čudili, z njim morda simpatizirali, a ga bodo le slabo razumeli*" (Berlin, 1992: 89), pravi Berlin. Morda velja nekaj podobnega tudi za pravico do zasebnosti?

Izvor pravice do zasebnosti

Razpravljanje o pravici do zasebnosti zadeva predvsem obseg te pravice, včasih pa se nekateri celo sprašujejo, ali je zasebnost sploh pravica, ali ne gre morda le za interes. Wagner DeCewova tako meni, da je zasebnost *interes*, to pa odpira vprašanje, koliko naj bo ta interes zaščiten (Wagner DeCew, 1997: 27), oziroma ali je sploh mogoče določiti neki minimalen, vendar absoluten standard zaščite zasebnosti. Gre za vprašanje, koliko je možno 'trgovanje' z zasebnostjo. To vprašanje je še posebej zaostreno pri t. i. informacijski zasebnosti, izpostavljeno pa je tudi pri libertarni kritiki zasebnosti, ki zbiranje in obdelavo osebnih podatkov vidi zgolj kot izmenjavo informacij, skratka kot problem svobode trgovanja in ne kot problem poseganja v neko pravico posameznika. Pravica do zasebnosti je sicer pogosto določena kot "*meja, do katere družba lahko vdre v posameznikove zadeve*" (Laurant, 2003: 1), vendar je problem definicije veliko bolj večplasten, kot se zdi na prvi pogled.

Kot ugotavljajo številni avtorji (Wagner DeCew, Agre, Sykes, Bennett in drugi), je zasebnost zelo slabo definirana, dodaten problem pa predstavljajo še kolizije drugih pravic z zasebnostjo ter posledično vprašanje pod- in nadrejenosti posameznih pravic. Prav tako zasebnost prihaja v kolizijo z različnimi interesi (npr. poslovni interes, javna varnost...), zaradi česar zasebnost včasih ne more biti varovana zaradi pravnih in družbenih razlogov (Wagner DeCew, 1997: 28). Poleg tega je dojemanje zasebnosti s strani posameznika relativno – njeno dojemanje se razlikuje tako med posamezniki kot tudi glede na dani kontekst (Wagner DeCew, 1997: 29 ter Cate v Etzioni, 1999: 199).

Pomembno vprašanje je tudi, ali je zasebnost temeljna ali pa morda izvira iz drugih pravic. Nekateri, npr. William Parent, jo vidijo kot nekaj unikatnega in temeljnega oziroma nekaj, kar izvira iz naravnega prava (tega mnenja sta npr. Warren in Brandeis); drugi, ki zastopajo t. i. redukcionistični pogled (npr. Judith Thomson), pa zasebnost vidijo kot nekaj, kar izvira iz drugih

pravic, predvsem lastninske pravice in nedotakljivosti telesa (Wagner DeCew, 1997: 29), čeprav je slednji pogled v zadnjem času že močno presežen. Kljub temu je vprašanje pomembno, saj se zastavlja vprašanje, katera pravica je bolj temeljna in s tem prioritetna, kadar pride do kolizije. Zdi se, da ima redukcionistični pogled velik vpliv na zasebnost na delovnem mestu v ZDA; delodajalci namreč posege v komunikacijsko zasebnost zaposlenih pogosto opravičujejo s tem, da zaposleni uporabljajo opremo, ki je last podjetja, pravica razpolaganja z zasebno lastnino pa ima prednost pred pravico posameznika do zasebnosti. Redukcionisti sicer menijo, da je možno vsako izmed pravic zasebnosti razložiti na tak način, da zasebnost sploh ni omenjena (Wagner DeCew, 1997: 46), tako prepričanje pa verjetno izvira iz omejenega razumevanja zasebnosti, za katerega se zdi, da je značilno predvsem za ZDA. Ameriška ustava namreč pravice do zasebnosti ne omenja eksplicitno, zaradi česar je bilo priznanje obstoja pravice do zasebnosti v ameriški ustavi s strani Vrhovnega sodišča ZDA v obliki "sence" (ang. *penumbra*), torej kot pravice, ki ni izrecno definirana, temveč je zagotovljena le v konceptu, deležno številnih kritik in polemik o pravnem 'izumljanju'.

Seveda pa je mogoče tudi nasprotno sklepanje, da je namreč pravica do zasebnosti temeljna, vse druge človekove pravice pa predstavljajo le posamične vidike pravice do zasebnosti (Laurant, 2003: 1). Glede na pomen zasebne sfere po Arendtovi, glede na pomen tistega "*koščka sveta*", ki ga "*silno in nujno potrebujemo*" (Arendt, 1958/1995: 72), njeno povezanostjo s svobodo in avtonomijo posameznika, pa je tako razumevanje pravice do zasebnosti zagotovo bolj ustrezno. Tako razumevanje pravice do zasebnosti, ki to pravico postavlja kot temeljno in univerzalno, kot pravico, ki ima naravnopravne temelje, podpira tudi razumevanje pomena zasebnega prostora Hannah Arendt, prav tako pa po mnenju ameriških pravnih strokovnjakov razvoj pravice do zasebnosti v ZDA kaže predvsem na njene naravnopravne temelje (Turkington in Allen, 2002: 58). Ne nazadnje tako razumevanje potrjuje tudi dejstvo, da je zasebnost kmalu postala predmet varstva tudi v mednarodnem merilu, da gre za pravico, ki je v mnogih državah pridobila lastnost ustavno zavarovane vrednote, uživa pa tudi kazenskopravno varstvo, kar ji priznava visoko stopnjo na lestvici družbeno priznanih vrednot (Šelih, 1979: 149, 154 ter 179).

Problem definicije pravice do zasebnosti

Zasebnost se povezuje s številnimi pojmi in vrednotami. David Flaherty, eden prvih pooblaščencev za varstvo zasebnosti v Kanadi, je ugotovil, da se pravica do zasebnosti povezuje z naslednjimi pojmi: pravica do osebne avtonomije, pravica biti puščen pri miru, pravica do zasebnega življenja, pravica nadzorovati informacije o sebi, pravica omejiti dostopnost do sebe, pravica ekskluzivnega nadzora dostopa do zasebnega področja, pravica zmanjšati nadlegovanje na najmanjšo možno mero, pravica pričakovati zaupnost, pravica uživati osamljenost, pravica uživati intimnost, pravica uživati anonimnost, pravica uživati zadržanost ter pravica do tajnosti (Cate, 1997: 21). Zato so nekateri prepričani, da zasebnosti pravzaprav sploh ni, temveč gre le za pojem, za katerim se skrivajo različne bolj ali manj nepovezane pravice (Wagner DeCew, 1997: 46), oziroma da zasebnosti ni mogoče definirati, saj naj bi bil problem zasebnosti v

osnovi stvar vrednot, interesov in moči (Gellman, 2001: 194). Definiranje pravice do zasebnosti oziroma njenega obsega je torej lahko precej arbitrarno. Pravzaprav gre bolj za regulacijo posegov v zasebnost, kot pa za določitev neke absolutne meje, ki je ni dovoljeno prestopiti. Zato pravo vedno le sledi razvoju tehnologije, ki omogoča nove in nove posege v zasebnost (in nekatere posege sankcionira, druge pa dopušča), hkrati pa sledi tudi "razpoloženju v družbi", ki zasebnosti daje enkrat večjo, drugič manjšo težo (predvsem v okviru dileme zasebnost ali javna varnost); kljub manjšim nihanjem meje v to ali ono smer pa družba zasebnost praviloma zgolj oži. Lampe pravi: "*kdaj je interes 'drugih' po vdoru v posameznikovo zasebnost prevladujoč, analogno jezičku na tehtnici, proti posameznikovemu interesu, je vprašanje, na katerega išče odgovor pravo*" (Lampe, 2004: 40). Ne gre torej za določitev absolutne meje, temveč za iskanje ravnotežja, tehtanje interesov posameznika in drugih posameznikov oziroma družbe. Ker pa se družbena sfera širi, se ravnotežje dolgoročno pomika le v eno smer, in sicer tako, da se oži zasebni prostor posameznika. Vsekakor pa velja, da je zasebnost nujen element kakovostnega življenja v sodobni družbi (Cate, 1997: 101), varstvo zasebnosti pa eden izmed pomembnih elementov sodobne demokratične države, saj je nepogrešljiva v vsakem sodobnem konceptu svobode (Etzioni, 1999: 191).

Bellottijeva ugotavlja, da je mogoče pravico do zasebnosti definirati na dva načina – normativno in operacionalno (Bellotti, 2001: 66). Normativna definicija govori o tem, da so nekateri vidiki posameznikove narave in njegovih dejavnosti zasebni; to pomeni, da se jih ne sme razkriti drugim. Ta definicija je izrazito kulturno in kontekstualno pogojena. Zato enaka dejanja v nekaterih kulturah veljajo za poseg v zasebnost, v drugih pa so skoraj povsem neproblematična; enako velja za dejanja v različnih kontekstih, saj za poseg v zasebnost ni vseeno, ali se ljudje med seboj poznajo ali ne,[24] v katerem prostoru pride do spornega dejanja itd. Tipičen primer, ki ponazarja problematičnost normativne definicije zasebnosti, so identifikacijske kartice (osebne izkaznice) in videonadzor. V ZDA in Veliki Britaniji proti identifikacijskim karticam vlada velik odpor, češ da gre za prevelik poseg v zasebnost posameznika (čeprav je bilo v zadnjem času že nekaj opaznih poizkusov uvedbe le-teh), v celinski Evropi pa so osebne izkaznice nekaj povsem vsakdanjega. Po drugi strani javnost videonadzor na javnih mestih v Veliki Britaniji sprejema praktično povsem mirno, prav tako se posameznikom v drugih državah po 11. septembru 2001 uporaba videonadzora na nekaterih posebnih mestih (npr. letališčih) zdi čedalje manj sporna.

Druga definicija, ki jo uporablja Bellottijeva, pa je operacionalna in se nanaša na nadzor nad dostopom, se pravi zmožnost nadzora informacij o sebi oziroma zmožnost nadzora odtekanja (ang. *outflow*) informacij. Po tej definiciji je bistvena zmožnost posameznika, da se sam odloči, koliko informacij želi izmenjati z okolico in kdaj (Bellotti, 2001: 67–68). Taka definicija zasebnosti se Bellottijevi zdi bolj ustrezna, saj je situacijsko neodvisna in relacijsko specifična (torej jo določa posameznik sam, ne pa družba in kultura), podobnega mnenja pa je tudi Samarajiva, ki zasebnost definira kot "*zmožnost eksplicitnega ali implicitnega pogajanja*

[24] Pa tudi v kakšnih odnosih so ljudje; tipičen primer, ki to ponazarja, je vprašanje, ali gre za poseg v zasebnost, če npr. nekdo gleda svojega pomanjkljivo oblečenega intimnega partnerja, oziroma če gleda svojega pomanjkljivo oblečenega *nekdanjega* intimnega partnerja.

o mejnih pogojih družbenih odnosov", kar zajema nadzor nad odtokom in nadzor nad pritokom informacij ter tudi pobudo za začetek stika (Samarajiva, 2001: 283).

Kljub temu gre pri obeh definiranjih pravice do zasebnosti v osnovi za subjektivno presojo posameznika, kdaj se mu zdi, da nekdo posega v njegovo zasebnost, zaradi tega je težko postaviti univerzalne kriterije, ki bi bili splošno sprejemljivi.

Pravica do zasebnosti in svoboda ter avtonomija

Povezavo med pravico do zasebnosti in svobodo poudarjajo praktično vsi avtorji, ta povezava pa je tako močna, da gre po prepričanju nekaterih pri razsodbah ameriškega Vrhovnega sodišča, ki so povezane z zasebnostjo, v resnici za razsodbe, ki se nanašajo na avtonomijo in svobodo (Wagner DeCew, 26). To velja predvsem za prvi primer, v katerem se je Vrhovno sodišče ZDA sklicevalo na pravico do zasebnosti oziroma na zasebnost v zakonski zvezi (ang. *marital privacy*) ter na odločitve, ki so se nanašale na uporabo policijsko-preiskovalnih tehnik. Wagnerjeva poudarja, da je zasebnost bistvena za samospoštovanje in občutek identitete, saj zagotavlja zmožnost nadzora nad odločanjem (Wagner DeCew, 1997: 66): "*naše vzdrževanje samospoštovanja zahteva zasebnost in nadzor nad določeno sfero naših življenj, informacije o nas so bistvenega pomena, če želimo biti neodvisna človeška bitja, sposobna rasti, izpolnjevanja, neodvisno od pritiskov, čustvenega stresa, predsodkov ali izgube samospoštovanja in drugih vplivov, ki spremljajo izgubo zasebnosti*" (Wagner DeCew, 1997: 67).

Pri povezavi zasebnosti s svobodo gre po eni strani za svobodo nasproti državi, po drugi strani pa za svobodo nasproti drugim posameznikom in družbi, kar zajema avtonomijo in pravico odločanja o zasebnih stvareh neodvisno od družbenih prisil, kajti zasebnost preprečuje pritiske h konformnosti (Wagner DeCew, 1997: 77). Številni, večinoma ameriški avtorji v zvezi z zasebnostjo poudarjajo predvsem pomen odsotnosti državnega nadzora, vpliv družbe pa je pogosto zapostavljen. Razlogi za to zapostavljenost vpliva družbe so verjetno zgodovinski, saj je, zgodovinsko gledano, največjo grožnjo pravici do zasebnosti predstavljala država, predvsem totalitarna, v kateri je, kot pravi Sykes, za razliko od demokratične, "*vse ... odprto za preiskavo, celo najbolj trivialni vidiki življenja*" (Sykes, 1999: 19).

Charles D. Raab celo trdi, da sta odsotnost oblastnega nadzorstva posameznikov in varstvo zasebnosti *nujna pogoja* za liberalno in participativno demokracijo (Raab, 1997: 161). Berlin se s tem stališčem verjetno ne bi povsem strinjal, saj pravi, da "*med svobodo posameznika in demokratično vladavino ni nujne povezave*" (Berlin, 1992: 76), vsaj ne, če govorimo le o negativni svobodi. V primeru (ameriškega) razumevanja zasebnosti kot pravice, da me oblast pusti pri miru, se "*odgovor na vprašanje 'Kdo mi vlada?' logično razlikuje od vprašanja 'Koliko se oblast vtika vame?'*" (Berlin, 1992: 76), kajti tudi despot lahko svojim podložnikom dovoli veliko osebne svobode. To kaže na to, da zasebnost (ter svoboda) in demokracija nista nujno povezani.

Je pa Raab v svoji ugotovitvi izpostavil pomemben element – participativno demokracijo – ki bi ga lahko razumeli v smislu poudarjanja povezave med zasebnostjo in političnim delovanjem. V praksi je ameriško Vrhovno sodišče večkrat priznalo zasebnost kot bistveni element pri ohranjanju politične svobode – predvsem v primeru zavrnitve zakona, ki je prepovedoval

anonimne pamflete,[25] in v primeru zahtev za razkritje članov NAACP,[26] kjer so v razsodbi ugotovili močno povezanost med pravico do zasebnosti in svobodo združevanja (Sykes, 1999: 84–85).

Medosebni vidik pravice do zasebnosti

Zasebnost pa ima dvojno funkcijo, oziroma je povezana z nadzorom. Zasebnost po eni strani posamezniku omogoča, da drugim omeji dostop do sebe, po drugi strani pa mu onemogoča dostop v domeno zasebnega drugih posameznikov. Zasebnost po eni strani pospešuje individualnost, povezovanje z drugimi in izbiro življenjskega sloga, po drugi strani pa povečuje in ponotranja družbeni nadzor (Wagner DeCew, 1997: 68). Kot pravi Schoemann, pa se lahko nadzorna funkcija zasebnosti razvije v osvobodilno funkcijo. Nadzorna funkcija namreč pomaga ščititi človeško dostojanstvo in človeško emocionalno ranljivost. Deluje kot nekakšna protiutež drugim sistemom nadzora (Wagner DeCew, 1997: 70), saj posamezniku omogoča, da se umakne izpred oči drugih in s tem postane bolj avtonomen. Zasebnost tako z omejitvijo dostopa ne izolira ljudi, temveč jim omogoča, da se z drugimi združujejo avtonomno, s tem pa se povečuje zmožnost ustvarjanja novih in globljih odnosov.[27] Ali kot pravi DeCewova: zasebnost zagotavlja nadzor nad sprejemanjem odločitev ne samo s tem, kakšne informacije imajo drugi o posamezniku in za kakšne namene te informacije uporabljajo, temveč tudi katere osebne dejavnosti posameznik opravlja in kakšne odnose vzpostavlja brez vmešavanja drugih (Wagner DeCew, 1997: 66, 69). Podobnega mnenja je tudi Šelihova, ki pravi, da zasebnost posamezniku omogoča, da najde samega sebe, s čimer postaja avtonomen, to pa mu omogoča, da "*konstruktivno sodeluje z drugimi in se vključuje v družbo*" (Šelih, 1979: 176). Zato ne gre samo za vrednoto posameznika, temveč za vrednoto, ki je pomembna za celotno družbo. Po mnenju Šelihove se pri pravici do zasebnosti "*splošni interes kaže prav prek posameznikovega interesa*" (Šelih, 1979: 31).

Zasebnost je torej pomembna, ker povečuje zmožnost posameznika, da avtonomno in neodvisno od okolice vzpostavlja odnose z drugimi. Zato nekateri zasebnosti ne vidijo kot samo osebnostno pravico, temveč kot nekakšno družbeno pravico (Šelih, 1979: 151). S tem se razkrije še ena pomembna razsežnost zasebnosti, in sicer tista, ki jo DeCewowa imenuje dimenzija odnosnosti (ang. *relational dimension of privacy*). Ta dimenzija ima tudi politični pomen, saj v končni fazi lahko omogoča svobodo združevanja in svobodo političnega delovanja. Ta pogled poudarja nujnost medsebojne povezanosti. DeCewova pravi, da smo posamezniki svobodni takrat, ko imamo na voljo različne družbene skupine, ki jim pripadamo in od njih dobivamo podporo. Pri tem izrecno zavrača brezbrižnost do drugih in poudarja svobodo povezovanja z drugimi (Wagner DeCew, 1997: 71).

---

[25] Talley v. California, 362 U.S. 60 (1960).

[26] National Association for the Advancement of Colored People v. Alabama, 357 U.S. 449 (1958).

[27] Shoemann pravi, da zasebnosti ščiti zmožnost ustvarjanja "pomembnih odnosov" (ang. *meaningful relationship*).

Pravica do zasebnosti in pravica do umika v samoto ter nadzor nad publiciteto

Vidik pravice do zasebnosti, ki poudarja posameznikovo možnost, da se umakne v osamo, so izpostavljali predvsem Cooley ter Waren in Brandeis, ki zasebnost definirajo kot pravico biti sam, oziroma pravico biti puščen pri miru. Če je Arendtova govorila o prostoru, ki ga potrebujemo, da bi se zatopili v dialog v samim seboj, pa gre pri obravnavi zasebnosti kot pravici biti puščen pri miru tudi za vprašanje pravice do osebne imunitete oziroma neoskrunjenosti osebnosti (Wagner DeCew, 14, 15), ta vidik pa zajema tudi nadzor nad publiciteto. Ker ta vidik zasebnosti zadeva tudi svobodo medijskega poročanja, verjetno ni naključje, da se je tako gledanje na zasebnost v ZDA razvilo kot odgovor na čedalje bolj nadležen tisk. Razumevanje zasebnosti kot pravice biti puščen pri miru je tudi vzrok za razumevanje problema nezaželene elektronske pošte (t. i. smetja ali spama) na internetu in neposrednega trženja kot nečesa, kar vdira v zasebnost posameznikov, čeprav pri teh posegih v zasebnost ne gre za odtekanje informacij.

Pri pravici biti puščen pri miru gre predvsem za razumevanje zasebnosti kot negativne pravice, zgodovinsko gledano, naj bi posameznika pri miru pustila država. Iz tega razumevanja izvira angleška domneva o nedotakljivosti državljanovega doma oziroma nedotakljivost stanovanja, iz katere se je pozneje razvila tudi zasebnost komunikacij in upravičeno pričakovanje zasebnosti. Leta 1765 je britanski lord Camden protestiral, ker so preiskovalci želeli vstopiti v njegovo hišo in zaseči neke listine, parlamentarec William Pitt pa je o tem zapisal: "*Tudi najrevnejši človek se v svoji koči lahko upira Kroni. Lahko je slaboten, lahko se maje njegova streha, v kočo lahko piha veter, noter lahko prideta nevihta ali dež, toda kralj Anglije ne sme noter*." (Laurant, 2003: 5). Že pred tem je James Otis leta 1761 nasprotoval podaljšanju "*writs of assistance*", določil, ki so omogočala vladno preiskovanje domov posameznikov, češ da je "*človekova hiša njegov grad*", človek pa je v svoji hiši zaščiten kot "*princ v svojem gradu*" (njegovi pogledi so močno vplivali na ameriško *Deklaracijo o neodvisnosti* in amandmaje k ameriški ustavi (t. i. *Bill of Rights*) (Sykes, 1999: 84)).

Vendar pa se razumevanje pravice do zasebnosti kot *zgolj* pravice biti puščen pri miru (ter celo zgolj biti puščen pri miru s strani države), razumevanje, ki prevladuje predvsem v ZDA, pokaže za precej omejeno, brž ko začnemo govoriti o poseganju družbe v zasebno sfero (predvsem v primeru posegov zasebnih podjetij). Nekateri zasebnost razumejo kot okoliščino, v kateri ni dostopa do neobjavljenih osebnih informacij o drugem (Wagner DeCew, 1997: 28). Problem poudarjanja objavljenosti osebnih informacij (v smislu javne objave) pa je v tem, da po tem razumevanju pravice do zasebnosti zbiranje osebnih podatkov, ki so v različnih dosjejih, če le-ti niso javno dostopni (npr. medicinske kartoteke, potrošniški profili itd.), ne pomeni kršitve zasebnosti. Razumevanje zasebnosti kot pravice zgolj dovoliti ali zavrniti dostop do osebnih informacij in do človeka, bi pomenilo, da je zasebnost podrejena lastninski pravici. Po tem pogledu namreč zasebnost pomeni pravico drugim izključiti dostop do lastnine nekoga drugega, torej do sebe (Wagner DeCew, 1997: 54). To pa je pogled, ki je z razumevanjem zasebnosti kot osebnostne pravice v sodobnem času že močno presežen.

Ruth Gavison sicer meni, da lahko nekdo izgubi zasebnost že samo s tem, ko postane predmet pozornosti, pa čeprav pri tem niso pridobljene nobene nove informacije (Wagner DeCew, 1997: 33), Thomas Scanlon pa pravi: "*Če nekdo name pritisne z osebnimi vprašanji v položaju, ko je to navadno družbeno nesprejemljivo, lahko kadarkoli zavrnem odgovor. Vendar pa dejstvo, da ni bila pridobljena nobena informacija, ne pomeni, da ni bilo kršitve; do te pride ravno tako, kot v primeru, če nekdo kuka skozi okno moje kopalnice, pa me ne vidi, ker sem se umaknil*" (Scanlon v Wagner DeCew, 1997: 34). Kljub temu tudi tako razširjeno razumevanje pravice biti puščen pri miru še vedno ne preseže razumevanja pravice do zasebnosti kot zgolj podvrste lastninske pravice.

Pravica do zasebnosti in meje tajnosti podatkov

Predvsem informacijska in komunikacijska zasebnost se pogosto varuje s tajnostjo. Zato kriptografija velja za eno poglavitnih tehnologij zaščite zasebnosti (na internetu).
Vendar se pogosto zastavlja vprašanje, ali je upravičeno, da je vsaka zasebna stvar tudi tajna, iz česar izvirajo tudi poizkusi omejevanja kriptografije. Določena zasebna razmerja in zasebne informacije so namreč sicer lahko del zasebne sfere, a je včasih upravičeno, da "izstopijo" iz nje. Take izjeme veljajo predvsem v primerih, ko so ogroženi javni interesi (npr. varnost, javno zdravje) ali ko gre za varovanje pravic drugih posameznikov. Amitai Etzioni v *The Limits of Privacy* izpostavlja več takih primerov, npr. testiranje novorojenčkov za virus HIV ter Meganine zakone v ZDA.

Testiranje novorojenčkov za virus HIV ima številne prednosti. Študije so dokazale, da se velik delež otrok, ki so rojeni materam, okuženim z virusom HIV, in se rodijo neokuženi, lahko okuži z dojenjem, otrokom, ki se rodijo okuženi, pa je mogoče z ustreznim zgodnjim zdravljenjem povečati kakovost življenja. Vendar pa testiranje za HIV ne razkrije samo otrokove okuženosti, temveč tudi okuženost matere. Številne mame se bojijo, da bodo zaradi okužbe diskriminirane in bodo izgubile službo, prav tako ni dvoma, da so medicinski podatki načeloma zasebna stvar vsakega posameznika. Vendar ima v nekaterih primerih tajnost podatka o okužbi z nalezljivo boleznijo lahko za posledico nove okužbe, zato je verjetno upravičeno testiranje novorojenčkov brez privolitve njihovih mater (Etzioni, 1999: 17–42).

Podobno, morda še večjo dilemo pa predstavljajo Meganini zakoni (ang. *Megan laws*). Ti so bili v ZDA sprejeti kot reakcija na brutalno posilstvo in umor sedemletne deklice Megan Kanka v začetku 90. let. Pozneje je bilo ugotovljeno, da je zločin zagrešil sosed, ki je bil pred tem že obsojen na zaporno kazen zaradi dveh spolnih napadov na mladoletno osebo, njegovi novi sosedje (po prestani zaporni kazni se je preselil) pa o njegovi preteklosti niso nič vedeli. Ob dejstvu, da so študije dokazale veliko stopnjo povratništva v kriminal med tistimi, ki so že bili obsojeni za spolne delikte, so v ZDA sprejeli t. i. Meganine zakone, ki so od spolnih prestopnikov zahtevali, da se registrirajo v okrožju, v katerem živijo. Oblika Meganinih zakonov se sicer med državami razlikuje (kdo se mora prijaviti, kakšne so kazni, kako je z dostopnostjo do teh podatkov itd.), vendar se ob obvezni registraciji zastavlja vprašanje dvojnega kaznovanja.[28]

[28] Leta 2002 je Vrhovno sodišče ZDA presodilo, da določba Meganinih zakonov, ki zahteva objavo fotografij in naslovov spolnih prestopnikov na internetu, ne krši ameriške ustave (Laurant, 2003: 523).

Znani so primeri, ko so pod Meganine zakone zapadli tudi ljudje, ki jih sicer verjetno ne bi imeli za spolne delikvente – npr. v Kaliforniji so med njimi homoseksualci, ki so bili obsojeni še pred dekriminalizacijo homoseksualnosti, v Wisconsinu je v registru 18-letnik, ki se je želel poročiti s svojim nosečim 14-letnim dekletom, itd. (Etzioni, 1999: 54). Podobno se dogaja tudi v primeru objave osebnih podatkov in fotografij domnevnih pedofilov s strani spletnega projekta *perverted-justice.com*, ki lovi domnevne pedofile na internetu. Podatke objavijo tudi, kadar posamezniki še niso bili obsojeni za spolni napad in je šlo zgolj za poskus vzpostavitve stika z mladoletnikom; to sicer jasno zapišejo, kljub temu pa je očitno, da bodo domnevni pedofili v očeh javnosti veljali za krive ne glede na sporni postopek ugotavljanja njihove krivde.

Čeprav so se kritiki Meganinih zakonov ukvarjali predvsem z vprašanji, ali so le-ti pravični in učinkoviti in ne toliko z vprašanjem poseganja v zasebnost, je dejstvo, da se je ravno na tem primeru izpostavila dilema, kje potegniti mejo zasebnosti. Čeprav gre pri Meganinih zakonih za vprašanje pedofilije, se zastavlja vprašanje, ali je smiselno to načelo širiti in mejo zasebnosti ožiti še na drugih področjih. Pravzaprav se taka vprašanja zastavljajo vedno, kadar se zgodi kakšno kaznivo dejanje, ki zelo odmeva v javnosti. Tako je država pod vplivom družbe prisiljena ožiti zasebno sfero.

Dimenzije pravice do zasebnosti

Dosedanji prikaz pojmovanj zasebnosti kaže predvsem na to, da pravica do zasebnosti ni enodimenzionalen pojem. Pojmovanje pravice do zasebnosti v ZDA obsega izražanje posameznikove osebnosti, avtonomijo, zmožnost nadzora nad informacijami o sebi ter t. i. temeljne komponente zasebnosti, ki naj bi bile skrivnost, anonimnost in možnost umika v osamo (Cate, 1997: 19). Prav tako Wagner DeCewova meni, da je zasebnost skupinski pojem (ang. *cluster concept*), ki pokriva več zasebnostnih interesov (Wagner DeCew, 73). Pojem zasebnosti obsega nadzor nad informacijami o posamezniku, potrebo po neodvisnosti in samoizražanju ter avtonomnem oblikovanju socialnih vezi. Po mnenju avtorjev poročila Privacy & Human Rights 1999 je zasebnost temelj človeškega dostojanstva in drugih vrednot, kot npr. svobode združevanja in svobode govora, iz česar tudi izhaja razumevanje zasebnosti kot temeljne pravice, iz katere izhajajo preostale pravice v sodobni družbi – po njihovem mnenju je zasebnost postala ena najpomembnejših (pa tudi najbolj ogroženih) človekovih pravic v sodobni družbi. Sodobne klasifikacije pravice do zasebnosti le-to delijo glede na njene dimenzije, nekateri pa težijo tudi h klasifikaciji pravice do zasebnosti glede na možne vdore vanjo (Lampe, 2004: 49). Zato velja, da pravica do zasebnosti ni trdno definiran pojem, konec koncev pa ni niti enotne klasifikacije dimenzij zasebnosti.

Wagner DeCewova tako govori o treh vrstah zasebnosti, ki se med seboj mnogokrat prekrivajo: *informacijski zasebnosti*, *zasebnosti dostopnosti* ter *zasebnosti izražanja*. Informacijska zasebnost obsega varovanje informacij o posamezniku (t. i. osebne podatke), z njegovimi komunikacijami vred (Wagner DeCew, 1997: 75–78). Ogrožena pa je z zbiranjem in objavo osebnih podatkov brez soglasja posameznika, prisluškovanjem in opazovanjem ali pa tudi samo s poskusi teh

dejanj. Pri zasebnosti dostopnosti gre za možnost posameznika, da je sam; da nihče ni pozoren nanj in da nihče nima o posamezniku niti informacij niti fizičnega pristopa do njega (Wagner DeCew, 1997: 76). Zasebnost izražanja se nanaša na avtonomijo posameznika, da svobodno izbira stike, življenjski slog, načine delovanja, in da posameznika ščiti pred konformističnimi pritiski okolice.

Avtorji poročila Privacy & Human Rights 2003 ločijo naslednje vrste zasebnosti: *informacijsko zasebnost*, ki se navezuje na obdelavo osebnih podatkov, oziroma je znana tudi kot zaščita (osebnih) podatkov; *zasebnost telesa*, ki posameznika ščiti pred postopki, ki zadevajo njegovo fizično telo, npr. genskimi testi, pregledom telesnih odprtin ter testi telesnih tekočin (krvi, urina); *zasebnost komunikacij*, ki ščiti posameznikove komunikacije ne glede na obliko pred prestrezanjem s strani drugih; *prostorsko zasebnost*, ki ščiti posameznika v njegovih prostorih, kar zajema preiskovanje in opazovanje njegovih domačih, pa tudi službenih prostorov.

Podobno, čeprav manj razčlenjeno delitev uporablja tudi Čebulj, ki navaja tri sestavine zasebnosti: *zasebnost v prostoru* (možnost posameznika, da je sam), *zasebnost osebnosti* (svoboda misli, opredelitve, izražanja) in *informacijsko zasebnost* (možnost posameznika, da obdrži podatke in informacije o sebi, ker ne želi, da bi bili z njimi seznanjeni drugi) (Čebulj, 1992: 7). Lampe, ki izhaja iz 8. člena Evropske konvencije o človekovih pravicah,[29] pa pravico do zasebnosti deli na področje, ki pokriva zasebno in družinsko življenje (*odločitvena in duševna zasebnost*), dom (*prostorsko zasebnost*) in dopisovanje (*informacijsko zasebnost*) (Lampe, 2004: 49).

Vpliv tehnoloških sprememb na razvoj pravice do zasebnosti

Kot rečeno, je k razvoju pravice do zasebnosti precej pripomogel razvoj tehnologije. Tehnološke spremembe namreč prinašajo nove oblike in načine posegov v zasebnost, pravo pa je na te spremembe prisiljeno reagirati. Pravzaprav pravni sistem tem tehnološkim spremembam večinoma le sledi (Sykes, 1999: 250), zato gre pri razvoju pravice do zasebnosti za nenehno prilagajanje načel varstva zasebnosti tehnološkim spremembam, kar velja zlasti za 20. stoletje (Gellman, 2001: 203).

Eden prvih primerov, ki je to ponazoril, je odločitev ameriškega Vrhovnega sodišča v zadevi Olmstead (gre za enega prvih sodno dokumentiranih primerov vladnega prisluškovanja) in njegova revizija leta 1967 v primeru *Katz proti Združenim državam*.[30] Vrhovno sodišče ZDA je v zadevi *Olmstead proti Združenim državam*[31] razsojalo leta 1928, razsodili pa so (z večino

[29] Svet Evrope. 1950. Evropska konvencija o varstvu človekovih pravic in mednarodnih svoboščin, spremenjena s protokoli št. 3, 5 in 8 ter dopolnjena s protokolom št. 2, ter njeni protokoli št. 1, 4, 6, 7, 9, 10 in 11 (Convention on Human Rights and Fundamental Freedoms as amended by Protocols Nos. 3, 5 and 8 and amended by Protocol No. 2 and its Protocols Nos. 1, 4, 6, 7, 9, 10 and 11). Sprejel jo je Svet Evrope leta 1950. Uradni list RS, št. 33/1994, "Mednarodne pogodbe", št. 7/1994, 13. 6. 1994. Konvencijo je Državni zbor Republike Slovenije ratificiral 13. 6. 1994. Veljati je začela dne 28. 6. 1994.

[30] Katz v. United States, 389 U.S. 347 (1967).

[31] Olmstead v. United States, 277 U.S. 438 (1928).

5 proti 4), da četrti amandma ameriške ustave,[32] ki prepoveduje nepooblaščene preiskave in zasege, ne ščiti pred prisluškovanjem telefonu brez sodnega naloga. Sodnik Taft in z njim večina članov Vrhovnega sodišča ZDA so menili, da v primeru Olmstead ni šlo ne za preiskovanje (prostorov) ne za zaseg. "*Dokazi so bili pridobljeni s poslušanjem in samo s tem. Ni bilo vstopa v hiše ali prostore obtožencev*", je menil sodnik Taft (Turkington in Allen, 1999: 78). Agenti FBI so namreč prisluškovalno napravo namestili na telefonsko žico zunaj hiše obtoženega in leta 1928 je Vrhovno sodišče ZDA presodilo, da tako dejanje ne predstavlja nezakonite preiskave, saj ni bilo fizičnega vstopa v obtoženčevo hišo, prav tako ni šlo za zaseg komunikacije, temveč zgolj za poslušanje.

Odločitev Vrhovnega sodišča ZDA je bila revidirana v 60. letih (čeprav je znan primer iz leta 1931 *Rhodes proti Graham*,[33] v katerem je bila tožniku priznana odškodnina zaradi prisluškovanja, vendar v tem primeru ni šlo za vladno prisluškovanje, temveč je prisluškoval zasebnik, poseg v zasebnost pa je bil sankcionirana po odškodninskem pravu (Turtington in Allen, 2002: 537–538)), ko so priznali, da se pravica do zasebnosti ne nanaša samo na lastnino, marveč tudi na posameznikove komunikacije, njegove misli in njegovo osebnost sploh (Sykes, 1999: 85). Dokončno prelomnico pri razumevanju komunikacijske zasebnosti pa je prinesla odločitev v zadevi *Katz proti Združenim državam*,[34] v kateri je sodišče ugotovilo, da četrti amandma[35] varuje ljudi, in ne prostorov (Agre, 2001: 7), o čemer več v nadaljevanju.

Kljub temu je primer *Olmstead*[36] zelo pomemben za poznejše varstvo zasebnosti v ZDA. V tem primeru je namreč zelo pomembno ločeno negativno mnenje sodnika Brandeisa. V njem je zapisal, da je bil četrti amandma[37] sprejet v posebnih zgodovinskih okoliščinah, skozi čas pa so nastopile nove. "*Vlada ima na voljo subtilnejša in bolj daljnosežna sredstva za vdor v zasebnost. ... Napredek znanosti v opremljanju vlade s sredstvi za vohunjenje se ne bo ustavil pri prisluškovanju. Nekega dne bodo morda razviti načini, ko bo vlada lahko kopirala listine, ne da bi jih sploh odstranila iz skritega predala... Napredek v psihologiji in sorodnih znanostih bo lahko odkril načine za razkritje neizraženih prepričanj, misli in čustev*", je zapisal (Turkington in Allen, 1999: 79). Brandeis je potegnil tudi vzporednice s primerom *Ex parte Jackson*[38] iz leta 1877, v katerem je bilo razsojeno, da je zapečateno pismo, ki je oddano na pošto, zaščiteno z ustavnimi amandmaji: "*V bistvu ni nikakršne razlike med zaprtim pismom in zasebnim telefonskim pogovorom. Kot je rekel sodnik Rudkin: 'Seveda, eno je vidno, drugo nevidno, eno je otipljivo, drugo neotipljivo, eno je zapečateno, drugo je nezapečateno, vendar so to razločki brez razlike'.*" (Turkington in Allen, 1999: 79). Brandeis je opozoril na duh ustave, ki priznava pomen posameznikove duhovne narave, njegovih občutkov in intelekta: "*[Pisci ustave] so želeli zaščititi Američane v njihovih prepričanjih, mislih, čustvih in občutjih... Zaradi zaščite te pravice je vsak neupravičen poseg v zasebnost s strani*

[32] 4. amandma, Listina svoboščin (Bill of Rights), 1791.
[33] Rhodes v. Graham, 37 S.W.2d 46 (1931).
[34] Katz v. United States, 389 U.S. 347 (1967).
[35] 4. amandma, Listina svoboščin (Bill of Rights), 1791.
[36] Olmstead v. United States, 277 U.S. 438 (1928).
[37] 4. amandma, Listina svoboščin (Bill of Rights), 1791.
[38] Ex parte Jackson, 96 U.S. 727 (1877).

vlade ne glede na način, na katerega je storjen, treba razumeti kot kršitev četrtega amandmaja." (Turkington in Allen, 1999: 79). Brandeisove napovedi so se z razvojem tehnologije po svoje že uresničile in leta 2001 je Vrhovno sodišče ZDA v primeru *Kyllo proti Združenim državam*[39] razsodilo, da uporaba naprave za termoopazovanje (naprave, ki zazna in prikaže toploto, ki jo oddajajo npr. ljudje v zgradbi) brez sodnega naloga predstavlja kršitev (Laurant, 2003: 522).

Vpliv družbenih sprememb na razvoj pravice do zasebnosti

Leta 1890 sta Samuel D. Warren in Louis D. Brandeis objavila nadvse vpliven članek z naslovom *The Right to Privacy*, ki šteje za enega prvih mejnikov pri priznavanju pravice do zasebnosti. V članku sta posebej izpostavila nove poslovne metode, nove tehnične izume in različne tehnološke naprave, npr. fotoaparate, naprave za slikovno in zvočno snemanje ter preveč podjeten tisk, ki so povečali vdore v zasebno življenje: "*...sodobni izumi in podjetništvo so posameznike podvrgli duševnim bolečinam in stiski, ki je veliko večja, kot jo lahko povzroči telesna poškodba.*" (Turkington in Allen, 1999: 31). S tem sta jasno pokazala, da zasebnost ogroža tako razvoj tehologije kot tudi širjenje družbenega. Po nekaterih ugibanjih naj bi članku botrovalo tudi Warrenovo nezadovoljstvo zaradi publicitete poroke njegove hčerke (Wagner DeCew, 1997: 15), dejstvo pa je, da sta Warren in Brandeis v članku posebej (pravzaprav že kar čustveno) izpostavila tisk, ki prestopa vse meje spodobnosti in vljudnosti: "*...ponudba ustvarja povpraševanje. Vsaka požeta letina neprimernih govoric postane seme za nove govorice... to pa ima za posledico zniževanje družbenih standardov in morale*." (Turkington in Allen, 1999: 31).

Na začetku besedila sta Warren in Brandeis izpostavila dejstvo, da je naravo in obseg temeljnega pravnega načela, ki ščiti osebe in lastnino, nujno občasno na novo definirati. Po njunem mnenju politične, družbene in ekonomske spremembe zahtevajo priznavo novih pravic. Ena izmed njih je tudi pravica do zasebnosti. V uvodu sta tako izpostavila nekaj pravic, ki so nastale zaradi omenjenih sprememb – npr. načelo nedotakljivosti človeka in lastnine je v začetku prepovedovalo zgolj fizične kršitve, pozneje pa se je razširilo še na poskuse poškodbe in grožnje. Še pozneje se je zaščita razširila tudi na zaščito posameznika pred hrupom, smradom, prahom, dimom in vibracijami. Potem se je pojavilo še pravo, ki je posameznika ščitilo pred obrekovanjem in klevetami. "*Zdaj pravica do življenja pomeni tudi pravico do uživanja življenja*." (Turkington in Allen, 1999: 29–30). V tem kontekstu pravica do zasebnosti ni nekaj novega, temveč del naravnega razvoja prava.

Warren in Brandeis sta ugotovila, da je čas, da pravo prizna pravico, ki pravzaprav v družbi velja že dolgo, oziroma je pravica, ki izvira iz človeške narave. Gre torej za pogled, po katerem je zasebnost del t. i. naravnega prava, oziroma gre za neodtujljivo, "sveto" pravico posameznika. Po mnenju nekaterih je konceptualni okvir njunega članka Godkinov članek "*The Rights of the Citizen*", ki sta ga Warren in Brandeis dvakrat citirala. V njem Godkin pravi, da ima posameznik naravno pravico, da se odloči, koliko vedenja o njegovih osebnih zadevah ima lahko javnost

[39] Kyllo v. United States, 533 U.S. 27 (2001).

(Turkington in Allen, 1999: 39). Podobnega mnenja je bilo leta 1905 Vrhovno sodišče Georgije, ki je v primeru *Pavesich proti New England Life Insurance Co.*[40] (v tožbi je šlo za uporabo fotografije Paola Pavesicha za reklamo za življenjsko zavarovalnico brez njegovega soglasja) zapisalo, da "*pravica do zasebnosti ... izvira iz naravnega prava*" (Turkington in Allen, 1999: 56); s tem je Georgija postala prva ameriška zvezna država, ki je priznala pravico do zasebnosti.

Warren in Brandeis sta v svojem članku, v katerem sta utemeljila obstoj dotlej še ne uradno priznane pravice do zasebnosti, izpostavila tezo, da je posameznikom treba priznavati nove pravice in nove zaščite v smislu naravnega razvoja prava. Vendar pa njuna teza kaže tudi na to, kako je pravzaprav širjenje družbenega ožilo zasebno sfero, zaradi česar so posamezniki čutili potrebo po zaščiti svojih dotlej samoumevnih "naravnih" pravic (npr. zasebnosti), te potrebe pa so se potem izrazile skozi razvoj sodnega varstva.

Razvojni temelji pravice do zasebnosti

Pravica do zasebnosti ni trdno in univerzalno definirana, saj je dojemanje zasebnosti izrazito subjektivno. Poleg tega v pravu prevladuje pristop varstva in s tem definiranja pravice do zasebnosti prek poseganja vanjo (da torej pravo predvsem prepoveduje določene posege v zasebnost)[41] (Orehar-Ivanc, 2002: 382). Zato in zaradi pritiskov širjenja družbenega na območje zasebne sfere gre pri pravnem varstvu pravice do zasebnosti večinoma le za reakcijo na pritiske, ne pa toliko za vnaprejšnje postavljanje omejitev ali varstva. Literatura sicer kot poglavitni dejavnik, ki je povzročil zahteve po prilagajanju načel varstva zasebnosti v pravu, izpostavlja tehnološke spremembe[42] (Gellman, 2001: 203), nedvomno pa gre tudi za reakcijo na družbene pritiske (predvsem nadležen tisk).[43]

Začetki zakonodaje, ki ščiti zasebnost, segajo že v leto 1361, ko je v Angliji zakon *Justices of the Peace Act* predvidel kazni za tiste, ki so skrivaj opazovali druge posameznike ali jim prisluškovali. Nekje okrog leta 1400 pa so tudi na Zahodu začeli bolj šifrirati vsebino občutljivih pisem. Leta 1466 ali 1467 je Leon Batista Alberti napisal enega najstarejših znanih zahodnih esejev o kriptoanalizi (Kahn, 1973: 79, 91), kar kaže na to, da je bilo varovanje komunikacijske zasebnosti problem, s katerim so se resno ukvarjali že vsaj od petnajstega stoletja naprej.

---

[40] Pavesich v. New England Life Insurance Co., 122 Ga. 190, 50 S.E. 68 (1905).

[41] Npr. tak pristop pri definiranju pravice do zasebnosti so ubrali na konferenci nordijskih pravnikov leta 1967.

[42] Čebulj ugotavlja, je bila zasebnost posameznika sicer ogrožena že pred nastankom informacijsko-komunikacijskih tehnologij in računalniških zbirk podatkov, vendar so nove tehnologije ogroženost zasebnosti povečale (Čebulj, 1992: 16).

[43] Odziv na družbene pritiske nadzorovanja je tudi nedavno sprejeta odločitev Evropskega sodišča za človekove pravice v primeru *Von Hannover proti Nemčiji* iz junija 2004. Sodišče je v razsodbi na pritožbo princese Caroline Monaške zaradi večletnega nadlegovanja s strani tiska zapisalo: "*Javnost nima legitimnega interesa vedeti, kje je pritožnica in kako se obnaša v svojem zasebnem življenju, čeprav se pojavlja na mestih, ki jih ni mogoče opisati kot samotna, ne glede na to, da je javno dobro znana.*" (Von Hannover v. Nemčija, odločba z dne 24. 6. 2004). S tem je sodišče postavilo mejo varovanja zasebnosti javnih oseb, kadar ne opravljajo javne funkcije. Sociološko gledano pa gre za odziv prava na družbeni pritisk poseganja v zasebno, celo intimno sfero posameznika.

Začetki pravne regulacije vladnega preiskovanja zasebnih prostorov segajo okrog leta 1761 in 1765 (v Angliji in angleških kolonijah, poznejših ZDA). Leta 1776 pa nastanejo tudi zametki varovanja informacijske zasebnosti, saj je takrat švedski parlament sprejel *zakon o dostopnosti javnih zapisov*, ki je določal, da morajo biti vsi podatki, ki jih zbere država, uporabljeni zgolj za zakonite namene. Leta 1858 je Francija sprejela ostre kazni za objavo zasebnih dejstev (Laurant, 2003: 5–6). Prvi zakon za zaščito informacijske zasebnosti pa je bil sprejet leta 1970 v Nemčiji v zvezni državi Hesse. Razvoj sodobne pravice do zasebnosti se je začel predvsem v ZDA (tako glede regulacije zasebnosti komunikacij kot tudi zasebne avtonomije in testa upravičenega pričakovanja zasebnosti). Mednarodnopravne temelje varovanja zasebnosti v sodobnem času pa je postavila predvsem *Splošna deklaracija človekovih pravic*[44] iz leta 1948 v 12. členu ter *Evropska konvencija o varstvu človekovih pravic in mednarodnih svoboščin*[45] v 8. členu.

Ena izmed prvih omemb pravice do zasebnosti v ameriškem pravu je sicer Cooleyjeva definicija zasebnosti (v okviru odškodninskega prava – *tort law*) kot pravice biti sam iz leta 1880; prvič pa je bila zasebnost omenjena v razsodbi sodišča že leto za tem, leta 1881, v primeru *DeMay proti Roberts*.[46] Za Thomasa M. Cooleyja je bila to pravica do lastne osebnosti in osebne imunitete (Wagner DeCew, 1997: 14), v njegovem razumevanju zasebnosti pa je podobno kot v ameriškem odškodninskem pravu močno opazno lastninsko koncipiranje zasebnosti. Tudi pravno varstvo posameznikove osebne sfere je imelo v prvotnem ameriškem odškodninskem pravu naravo premoženjskih oziroma lastninskih tožb (Lampe, 2004: 54–63), na kar kaže tudi ime najstarejšega delikta (ang. *tort*) ameriškega občega prava (ang. *common law*) – *trespass*; gre za protipravno vmešavanje v osebnost, lastnino ali pravico nekoga (Lampe, 2004: 55), izraz pa se povezuje predvsem z nezakonitim prečkanjem ali vstopom na tujo lastnino.

Koncipiranje pravice do zasebnosti v ZDA kot lastninske pravice

Vsekakor velja, da pred letom 1890, torej pred objavo članka Warrena in Brandeisa, pravice do zasebnosti v ameriškem pravu kot specifične pravice praktično ni bilo. Tisti vidiki pravice do zasebnosti, ki so veljali dotlej, so izvirali iz lastninske pravice, za katero je veljalo, da je sveta in neodtujljiva. Škodovanje ugledu nekega posameznika se tako ni razumelo kot poseg v zasebnost,

---

[44] Generalna skupščina Združenih narodov. 1948. Splošna deklaracija o človekovih pravicah (Universal Declaration of Human rights), 10. 12. 1948.

[45] Svet Evrope. 1950. Evropska konvencija o varstvu človekovih pravic in mednarodnih svoboščin, spremenjena s protokoli št. 3, 5 in 8 ter dopolnjena s protokolom št. 2, ter njeni protokoli št. 1, 4, 6, 7, 9, 10 in 11 (Convention on Human Rights and Fundamental Freedoms as amended by Protocols Nos. 3, 5 and 8 and amended by Protocol No. 2 and its Protocols Nos. 1, 4, 6, 7, 9, 10 and 11), sprejel jo je Svet Evrope leta 1950. Uradni list RS, št. 33/1994, "Mednarodne pogodbe", št. 7/1994, 13. 6. 1994. Konvencijo je državni zbor Republike Slovenije ratificiral 13. 6. 1994. Veljati je začela dne 28. 6. 1994.

[46] DeMay v. Roberts, 46 Mich. 160, 9 N.W. 146 (1881). Šlo je za tožbo ge. Roberts, ki je rojevala, proti zdravniku Dr. DeMayu, ki je prišel pomagat pri porodu. S seboj je vzel kot pomočnika mladega neporočenega moškega, ki je bil popolnoma nevešč v medicini in za go. Roberts popoln neznanec. Dovolil mu je, da je ostal v hiši, čeprav je bilo očitno, da bo lahko slišal in videl vse, kar se bo dogajalo. Sodišče je razsodilo, da "*je imela tožnica v teh trenutkih zakonito pravico do zasebnosti v svojem stanovanju, in da ji pravo to pravico zagotavlja. ... Dogodek je bil za tožnico svet in nihče ni imel pravice biti zraven, razen če je bil povabljen ali če je za to bila resnična in nujna potreba,*" je bilo zapisano v razsodbi (Turkington in Allen, 1999: 670).

temveč kot poškodovanje nečesa, kar nekdo poseduje, v tem primeru poškodovanje njegovega ugleda (Etzioni, 1999: 189).

Waren in Brandeis sta v svojem prelomnem članku izpostavila predvsem tisti vidik zasebnosti, ki posamezniku daje moč absolutnega nadzora nad mejo publicitete o njem. Del pravice biti puščen na miru je po njunem mnenju tudi nedotakljivost osebnosti in pravica do posameznikove osebnosti. Kljub temu da sta zavrnila razumevanje pravice do zasebnosti kot lastninske pravice in izpostavila drug vidik, t. i. "neoskrunjenost osebe" (ang. *inviolate personality*), pa se zdi, da je vpliv lastninskega koncipiranja pravice do zasebnosti v ZDA še vedno močno čutiti. Leta 1960 je namreč v ZDA dekan Prosser objavil članek, v katerem je zagovarjal tezo, da je zasebnost skupek različnih interesov, ne pa samostojna vrednota; edino, kar je različnim interesom skupno, je kršitev pravice posameznika biti sam; kršitve zasebnosti pa je razdelil na štiri delikte (ang. *tort*): delikt motenja (ang. *Intrusion Upon Seclusion tort*), delikt javne objave zasebnih zadev (ang. *Public Disclosure Of Private Facts tort*), delikt spravljanja v slabo luč (ang. *False Light in the Public Eye tort*) ter delikt prisvojitve imena ali podobe (ang. *Appropriation Of The Name Or Likeness tort*).

Po Prosnerjevi klasifikaciji je zasebnost skupek interesov, povezanih z ugledom, čustvenim mirom ter nedotakljivostjo lastnine (npr. fizično motenje samote). Bloustein nasprotno trdi, da emocionalne bolečine, ki jih zaradi vdora v zasebnost pretrpi posameznik, niso temeljni predmet varstva, temveč le posledica napada na posameznikovo dostojanstvo. Kršitev pravice do zasebnosti je torej napad na človekovo dostojanstvo (Turtington in Allen, 2000: 59–61 ter Lampe, 2004: 71–72), kar kaže na konceptualni premik v razumevanju zasebnosti kot osebnostne pravice.

Kljub temu je tudi po Blousteinovi kritiki razumevanje zasebnosti kot vrste lastninske pravice še vedno navzoče, na kar kaže tudi to, da zasebnost javnih oseb[47] sicer varuje njihovo ime in podobo, a praviloma zgolj pred komercialno zlorabo. Ameriško pravo meni, da je za uporabo imena ali podobe posameznika v komercialne namene potrebna njegova privolitev – licenca (Lampe, 2004: 75), bistvo le-te pa je plačilo nadomestila. Na te temelje kaže tudi ime enega izmed štirih deliktov odškodninskega prava, delikt prisvojitve imena ali podobe (ang. *Appropriation Of Name and Likeness*), ki se je včasih imenoval *misappropriation* ali *commercial appropriation* (neupravičena prisvojitev ali komercialna prisvojitev).

Iz lastninskega razumevanja zasebnosti sledi, da lahko lastnik s svojo lastnino naredi karkoli, torej tudi proda in tako izgubi nadzor nad njo. V ZDA je takšno lastninsko razumevanje zasebnosti še vedno zelo razširjeno predvsem v polju informacijske zasebnosti – pri zbiranju osebnih podatkov. Podjetja, ki zbirajo osebne podatke, imajo namreč le-te za svojo last in ne last posameznikov, od katerih so bili podatki zbrani, iz tega pa sledi, da jih smejo tudi prodajati naprej ali jih javno objaviti. Prizivno sodišče desetega okrožja v ZDA (ang. *U. S. Court of Appeals of Tenth Circuit*) je tako leta 1999 v primeru *US West proti FCC*[48] odločilo, da zaščita potrošnikove

[47] Po ameriškem pojmovanju ima interes javnosti prednost pred zasebnostjo, če gre za poseg v zasebnost t. i. javne osebe. Sicer so zavarovani tudi podatki iz zasebnih življenj javnih osebnosti, ki nimajo nobene zveze z njihovim javnim življenjem, vendar pa v primerih javnih senzacij sodišča niso priznavala odškodnine (Lampe, 2004: 69).

[48] U.S. West v. F.C.C., 182 F.3d 1224 (1999).

zasebnosti krši svobodo govora telekomunikacijskega podjetja, ki izvira iz prvega amandmaja[49] ameriške ustave.[50] White ugotavlja, da je sodišče s tem zavrnilo razumevanje osebnih podatkov kot lastnine posameznika; osebni podatki, ki jih zbere podjetje, so potemtakem "*vrsta 'govora' in je zato uporaba potrošnikovih podatkov s strani tretje stranke v poslovnih transakcijah poslovni govor, ki je zaščiten s prvim amandmajem*" (White, 2003: 24). Poleg tega je sodišče menilo, da "*zasebnost ni absolutna dobrina, ker družbi nalaga resnične stroške*" (U.S. West v. F.C.C., 182 F.3d 1224 (1999), ter White, 2003: 24), s tem pa je jasno pokazalo, da ima v ZDA ekonomska pobuda prednost pred pravico posameznika do zasebnosti.

Ko posameznik odda svoje osebne podatke, tako v ZDA načeloma nima več praktično nikakršnega nadzora nad njimi, kar je Sykes podkrepil s citatom nekega ameriškega odvetnika: "*Podatki so kot prostitutka; ko so enkrat zunaj, ima vsakdo dostop do njih.*" (Sykes, 1999: 101). To dokazuje tudi odločitev v primeru *Conboy proti AT&T Corp.*[51] V primeru je šlo za pritožbo stranke, ki je imela tajno telefonsko številko, telekomunikacijsko podjetje AT&T pa je to številko posredovalo podjetju, ki je želelo preveriti kreditno sposobnost strankine sorodnice. Stranka se je pritožila, a ker ni mogla dokazati, da ji je bila povzročena škoda, je bila njena pritožba zavrnjena (White, 2003: 25).

Načelo upravičenega pričakovanja zasebnosti

Pomemben mejnik v razvoju pravice do zasebnosti predstavlja uveljavitev pojma upravičeno pričakovane zasebnosti (ang. *reasonable expectation of privacy*) v primeru *Katz proti Združenim državam* leta 1967.[52] Ameriško Vrhovno sodišče je namreč s tem postavilo pomemben standard pri ločevanju zasebnosti in lastninske pravice. Toda razsodba Vrhovnega sodišča ZDA se nanaša le na ravnanje države oziroma njenih represivnih organov, torej zajema ta odločitev zgolj negativni vidik pravice do zasebnosti. Poleg tega je razsodba dober primer, kako pravo sledi razvoju tehnologije.

Po primeru Olmstead leta 1928, v katerem je Vrhovno sodišče ZDA razsodilo, da četrti amandma[53] ameriške ustave ne ščiti pred prisluškovanjem telefonu brez sodnega naloga, saj pri prisluškovanju ne gre ne za preiskovanje ne za zaseg, v ZDA skoraj 40 let ni bilo ustrezne zakonodaje, ki bi regulirala enega večjih posegov v zasebnost, namreč prisluškovanje. Politiki ni uspelo doseči konsenza glede regulacije prisluškovanja (Gellman, 2001: 207). Še več, v tem času je Vrhovno sodišče ZDA leta 1942 v primeru *Goldman proti Združenim državam*[54] razsodilo, da uporaba diktafona za snemanje pogovora v sosednji pisarni ne pomeni kršitve četrtega

---

[49] 1. amandma, Listina svoboščin (Bill of Rights), 1791.

[50] Šlo je za zahtevo *Federal Commnication Comission*, da podjetje za zbiranje in uporabo osebnih podatkov v tržne namene (v konkretnem primeru je šlo za prometne podatke o opravljenih telefonskih klicih strank podjetja) od uporabnikov pridobi predhodno soglasje.

[51] Conboy v. AT&T, 84 F. Supp. 2d 492 (2000).

[52] Katz v. United States, 389 U.S. 347 (1967).

[53] 4. amandma, Listina svoboščin (Bill of Rights), 1791.

[54] Goldman v. United States, 316 U.S. 129 (1942).

amandmaja,[55] saj ni bilo fizičnega vstopa v tuji prostor v povezavi s prisluškovanjem. Leta 1952 pa je v primeru *On Lee proti Združenim državam*[56] prav tako presodilo, da snemanje pogovora v pralnici ne pomeni kršitve. Odmik od dotedanje prakse je sicer opaziti leta 1961, ko so razsodili, da je snemanje z mikrofonom, nataknjenim na dolgo palico, kršitev, vendar je bila odločitev sprejeta zgolj na podlagi dejstva, da je mikrofon segal na "*ustavno zaščiteno območje*" (torej gre še vedno za lastninsko dojemanje pravice do zasebnosti) (Turkington in Allen, 1999: 92–93).

Potem pa je leta 1967 ameriško Vrhovno sodišče obravnavalo primer *Katz proti Združenim državam*.[57] Primer je pomenil pravo revolucijo v odnosu zakonodaje do zasebnosti, saj je sodišče prvič uveljavilo načelo upravičenega pričakovanja zasebnosti (ang. *reasonable expectation of privacy*). Nedotakljivost stanovanja oziroma prostorska zasebnost namreč zgodovinsko izvira iz angleške domneve o nedotakljivosti državljanovega in državljankinega doma, čeprav Zupančič ugotavlja, da je šlo pri tem le za teritorialno zasnovo varstva stanovanja. Problem pa je, ker je zaradi razvoja nadzorovalne tehnologije teritorialno varstvo zasebnosti danes postalo bistveno manj pomembno (Zupančič, 2002: 387), kar je ugotovil že Brandeis v svojem znamenitem ločenem negativnem mnenju v primeru *Olmstead*[58] (Turkington in Allen, 1999: 79). Sodobna tehnologija namreč omogoča kršitev zasebnosti brez neposrednega fizičnega dostopa oziroma vdora v tuje prostore; kot ugotavlja Šelihova, je razvoj tehničnih sredstev omogočil, da se je npr. mogoče seznaniti z vsebino zaprtega pisma, ne da bi ga odprli (Šelih, 1979: 156, 173).

Katz je bil obtožen nedovoljenega sporočanja informacij o stavah po telefonu. FBI ga je ujel s prisluškovanjem v javni telefonski govorilnici, pri čemer je bila prisluškovalna naprava nameščena na zunanji strani telefonske govorilnice. Obtoženec je na sodišče naslovil dve vprašanji, in sicer: ali je javna telefonska govorilnica ustavno zaščiteno območje in ali je za obstoj kršitve nujen *fizični vdor* na to območje.

Čeprav je nasprotna stran trdila, da je bila telefonska govorilnica steklena in je bilo torej Katza mogoče videti med pogovorom, je sodišče menilo, da je za razumevanje kršitve bistveno to, da je šlo za prisluškovanje (v razsodbi so zapisali, da je bilo sporno "*nepovabljeno uho*", in ne "*nepovabljeno oko*"). Poudarilo je, da je Katz s tem, ko je *zasedel* telefonsko govorilnico, imel vso pravico pričakovati, da njegov pogovor ne bo prišel v javnost (Turkington in Allen, 1999: 89). S tem je utemeljilo načelo upravičenega pričakovanja zasebnosti, po katerem pravo ščiti zasebnost posameznikov v vseh prostorih, v katerih posameznik lahko razumno pričakuje zasebnost. "*Pravo ne ščiti zgolj prostorov, lastnine in lastnikov, temveč posameznike, ki v določenem trenutku, v določenem prostoru ali pri določenem ravnanju (upravičeno) pričakujejo svojo zasebnost!*" ugotavlja Klemenčič (Klemenčič, 2002: 401).

S tem je lastninsko koncipiranje pravice do zasebnosti v ameriški pravni teoriji dokončno preseženo, a to ne pomeni, da ga v praksi še vedno ni mogoče zaslediti. To velja predvsem za zasebni sektor, presenetljivo pa tudi na številnih področjih javnega sektorja. Če je namreč Vrhovno sodišče ZDA našlo upravičeno pričakovanje zasebnosti v zaprti pisemski ovojnici, v

[55] 4. amandma, Listina svoboščin (Bill of Rights), 1791.
[56] On Lee v. United States, 343 U.S. 747 (1952).
[57] Katz v. United States, 389 U.S. 347 (1967).
[58] Olmstead v. United States, 277 U.S. 438 (1928).

domačih in lastnih poslovnih prostorih in v telefonski govorilnici, pa z evropske perspektive presenetljivo ni našlo upravičeno pričakovane zasebnosti v nekaterih drugih primerih.

Tako so na primer presodili, da v primerih policijske preiskave, ko je posameznik pri nekom na obisku (razen, če ostane čez noč), posameznik ne more upravičeno pričakovati zasebnosti v prostoru, v katerem je (Sykes, 1999: 80). Podobno so presodili, da posameznik ne more upravičeno pričakovati, da sogovornik (v konkretnem primeru tajni policijski agent) ne snema pogovora s skritim mikrofonom, oziroma ni opremljen z oddajnikom, tudi če se to dogaja na 'ustavno zaščitenem območju', torej v posameznikovem domu – iz tega sledi, da policijski sodelavec ne potrebuje sodnega naloga za snemanje pogovora.[59] Kljub temu je bilo v tem primeru zelo zgovorno ločeno negativno mnenje sodnika Douglasa, ki je zapisal, da "*je to, kar je bilo včasih znano kot prisluškovanje, danes elektronski nadzor*", vendar sta ta dva pojma neprimerljiva med seboj, saj je to "*enako, kot če bi primerjali smodnik z jedrsko bombo*" (Turkington in Allen, 1999: 100). Ločeno negativno mnenje je izrazil tudi sodnik Harlan, ki je menil, da "*breme varovanja zasebnosti v svobodni družbi ne sme biti na državljanih, temveč mora vlada upravičiti potrebo po elektronskem prisluškovanju*" (Turkington in Allen, 1999: 104).

Prav tako so presodili, da posameznik ne more upravičeno pričakovati zasebnosti pri bančnih in drugih zapisih, ki jih upravlja tretja stranka (primer *Združene države proti Miller*[60]), kar je z vidika informacijske zasebnosti nadvse problematično, saj so zbirke osebnih podatkov v ZDA večinoma vse pod nadzorom oziroma v lasti tretjih oseb in podjetij (Cate, 1997: 74). Take težnje je opaziti po vsem svetu. Osebni podatki posameznikov pa tudi elektronska in glasovna pošta so čedalje pogosteje shranjeni (neposredno ali vsaj v obliki varnostne kopije) na pomnilniških medijih v lasti podjetij.[61] Podatke, ki so bili včasih pod neposrednim nadzorom posameznikov, tako zdaj nadzorujejo in upravljajo ponudniki storitev, to pa ima v ZDA lahko resne pravne posledice, saj preiskovalci lahko te podatke pri ponudnikih storitev v nekaterih primerih zasežejo brez sodne odredbe (če bi bili podatki shranjeni pri posamezniku, pa bi za dostop do njih potrebovali sodno odredbo) – to je še posebej problematično v primeru elektronske pošte, ki je shranjena pri ponudniku brezplačne elektronske pošte, o čemer več v nadaljevanju.

Na podlagi odločitve v primeru *Miller* so leta 1979 v primeru *Smith proti Maryland*[62] presodili, da prometni podatki o telefonskih pogovorih niso zaščiteni s četrtim amandmajem[63] (Turkington in Allen, 1999: 104–105); s tem so uvedli ločevanje prometnih podatkov od same

---

59 Gre za primer iz leta 1971 (*Združene države proti White* (United States v. White, 401 U.S. 745 (1971)), podlaga za presojanje pa je bil tudi primer *On Lee* iz leta 1952 (On Lee v. United States, 343 U.S. 747 (1952)). Po mnenju sodišča bi si lahko tajni policijski agent, ki je pogovor snemal, ta pogovor tudi zapomnil in ga pozneje zapisal, zato za takšno nadzorovanje po njihovem mnenju ni potrebna sodna odredba (Turkington in Allen, 1999: 99).

60 United States v. Miller, 425 U.S. 435 (1976).

61 Bruce Schneier pravi: "*Varnost večine naših podatkov ni več pod našim nadzorom. To je novo. Če je nekdo ducat let nazaj želel pregledati vašo pošto, je moral vdreti v vašo hišo. Zdaj lahko vdre k ponudniku dostopa do interneta. Pred desetimi leti je bila vaša glasovna pošta shranjena na telefonski tajnici v vaši hiši, zdaj je shranjena v računalniku telekomunikacijskega podjetja.*" (Schneier, 2005)

62 Smith v. Maryland, 242 U.S. 735 (1979).

63 4. amandma, Listina svoboščin (Bill of Rights), 1791.

vsebine komunikacije (v Sloveniji in evropski zakonodaji se prometni podatki sicer štejejo za integralni del komunikacije (Klemenčič, 2002: 396)). Drugačnega mnenja je sicer bilo Vrhovno sodišče New Jerseyja, a je v svoji odločitvi pokazalo precejšnjo pragmatičnost pri tehtanju med pravico do zasebnosti in drugimi pravicami. V primeru *Država proti Hunt*[64] iz leta 1982 so zapisali, da ima "*posameznik pravico predpostavljati, da bodo telefonske številke, ki jih kliče, zabeležene izključno za poslovne namene telefonske družbe... Številke, ki jih kliče, so zasebna stvar... zasebnost podatkov s (telefonskega) računa je del paketa zasebnosti.*" (Turkington in Allen, 1999: 117). Vendar pa je sodišče presenetljivo odločilo, da odločitev ni retroaktivna. Obtoženca Hunt in Pirilo zato kljub zanju sprejemljivi odločitvi nista mogla uveljavljati ničnosti nezakonito pridobljenih dokazov. Razlog za tako odločitev je bilo veliko število še nerešenih primerov, ko je policija pridobila prometne podatke brez sodnega naloga (Turkington in Allen, 1999: 118).

Ti primeri kažejo na to, da je v ZDA razumevanje upravičenega pričakovanja zasebnosti sicer našlo svoje mesto v definiranju zasebnosti, a se pri priznavanju pravice do zasebnosti še vedno kažejo ostanki starega lastninskega koncipiranja zasebnosti, ki v praksi v nekaterih primerih ponudi zaščito samo tistim "delom" zasebnosti, nad katerimi ima posameznik neposreden, celo fizični nadzor.

Pravica do zasebnosti v ZDA

Ustavni temelji pravice do zasebnosti v ZDA

V ameriški ustavi pravica do zasebnosti ni nikjer izrecno navedena (pravica do zasebnosti je sicer izrecno omenjena v ustavah vsaj osmih zveznih držav (Cate, 1997: 66)), vendar pa je Vrhovno sodišče ZDA leta 1965 v primeru *Griswold proti Conencticut*[65] priznalo obstoj ustavne pravice do zasebnosti. Pri tem se je izkazalo, da ameriška pravna praksa zasebnosti ne dojema zgolj kot komunikacijsko zasebnost in pravico biti sam, temveč jo povezuje tudi z avtonomijo posameznika.

V posameznih odločitvah je sodišče sicer že pred tem posredno priznalo pravico do zasebnosti, v primeru *Griswold* pa je zasebnost nedvoumno omenjena. Leta 1958 je npr. zavrnilo poizkus države Alabama, da bi prisilila NAACP[66] (združenje *National Association for the Advancement of Colored People*), naj razkrije seznam svojih članov. V odločitvi so izrecno poudarili, da prek "zasebnosti združevanja" (ang. *privacy in one's associations*) ščitijo svobodo združevanja (Sykes, 1999: 85). Leta 1960 so v primeru *Talley proti Kaliforniji*[67] odpravili prepoved objave anonimnih pamfletov. Že pred tem so v nekaterih primerih (leta 1923 *Pierce proti Society of Sisters*,[68] v kateri so zavrnili zakone, ki so od otrok zahtevali obiskovanje javnih šol, ter leta 1925 *Meyer proti*

[64] State v. Hunt, 91 N.J. 338, 450 A.2d 952 (1982).
[65] Griswold v. Conencticut, 381 U.S. 479 (1965).
[66] National Association for the Advancement of Colored People v. Alabama, 357 U.S. 449 (1958).
[67] Talley v. California, 362 U.S. 60 (1960).
[68] Pierce v. Society of Sisters, 268 U.S. 510 (1925).

Nebraski,[69] ko so razveljavili zakone, ki so prepovedovali učenje drugih jezikov razen angleščine) razsodili v prid avtonomiji posameznika; v tem nekateri avtorji tudi vidijo temelje priznavanja pravice do zasebnosti v ameriški ustavi (Sykes, 1999: 84 ter Turkington in Allen, 1999: 612).

Priznanje obstoja pravice do zasebnosti v ameriški ustavi je sicer izzvalo številke kritike in polemike o pravnem 'izumljanju', med drugim tudi zato, ker je sodišče našlo pravico v obliki "sence" (ang. *penumbra*), torej kot pravico, ki ni izrecno definirana, temveč je zagotovljena le v konceptu; številne kritike pa so šle tudi v smeri očitkov o vsiljevanju skrajne individualistične filozofije in moralnega relativizma (Sykes, 1999: 86). Primer *Griswold proti Conencticut*,[70] ki je bil podlaga za priznanje pravice do zasebnosti v ameriški ustavi, sta namreč sprožila izvršni in strokovni direktor združenja *Planet Parenhood League of Connecticut*, Estelle Griswold in Dr. C. Lee Buxton, ki sta bila zaradi nasveta o uporabi kontracepcije vsak posebej kaznovana z denarno kaznijo 100 dolarjev. Sodišče je ugotovilo, da gre v tem primeru za zakon, ki vpliva na intimno razmerje med možem in ženo, torej posega v njuno "zakonsko (poročno) zasebnost", in zato je zakon o prepovedi kontracepcije razveljavilo. V razsodbi so izrecno zapisali, da se "*ukvarjamo s pravico do zasebnosti, ki je starejša kot Listina svoboščin,*[71] *starejša kot naše politične stranke in starejša kot naš šolski sistem*" (Turkington in Allen, 1999: 63). Ustavnost pravice do zasebnosti je dodatno utemeljil še sodnik Goldberg v ločenem pritrdilnem mnenju. Po njegovem mnenju so sestavljavci ustave priznavali še obstoj drugih pravic, ki obstajajo ob pravicah, ki so zapisane v ustavi in ustavnih amandmajih.[72] Dokaz za to je videl predvsem v devetem amandmaju[73] , ki določa, da naštevanje pravic v ustavi ne sme biti tolmačeno tako, kot da drugih pravic ni, in pri tem izpostavil svoje strinjanje z ugotovitvijo sodišča, da je pravica do zasebnosti temeljna osebna pravica (Turkington in Allen, 1999: 63–64). Pozneje je Vrhovno sodišče ZDA v primeru *Whalen proti Roe*[74] priznalo še pravico do informacijske zasebnosti, o čemer več v nadaljevanju.

Fred H. Cate ameriško ustavno pravico do zasebnosti deli na štiri področja. Ta področja predstavljajo temelj za priznavanje obsega pravnega varstva zasebnosti v ZDA, hkrati pa tudi omejitve varovanja zasebnosti (predvsem v zvezi z informacijsko zasebnostjo). Prvo področje predstavljajo odločitve Vrhovnega sodišča ZDA, ki se navezujejo na svobodo izražanja, združevanja in religije. Drugo skupino odločitve Vrhovnega sodišča ZDA, ki se nanašajo na preiskavo in zaplembo s strani državnih organov. Tretjo skupino pa predstavljajo odločitve Vrhovnega sodišča ZDA, ki zadevajo temeljne odločitve posameznika. V četrto skupino spadajo odločitve Vrhovnega sodišča ZDA v zvezi z nerazkritjem (Cate, 1997: 52–65). Najbolj kontroverzne so bile odločitve iz skupine, ki zadevajo temeljne odločitve posameznika, kamor spada tudi primer *Griswold*. Pri teh odločitvah se je namreč sodišče pri tehtanju med 'javno moralo' in svobodo posameznika praviloma postavilo na stran posameznika, iz česar izvirajo

---

69 Meyer v. Nebraska, 262 U.S. 390 (1923).

70 Griswold v. Conencticut, 381 U.S. 479 (1965).

71 Listina svoboščin (*Bill of Rights*) je prvih deset amandmajev k ameriški ustavi. Sprejeti so bili v paketu leta 1791.[72] Ustava Združenih držav Amerike (Constitution of United States of America), 1798, ter Listina svoboščin (Bill of Rights), 1791.

73 9. amandma, Listina svoboščin (Bill of Rights), 1791.

74 Whalen v. Roe, 429 U.S. 589 (1977).

očitki o ideološki pristranskosti sodišča in moralnem relativizmu. Primeru Griswold je namreč leta 1972 sledil primer *Eisenstadt proti Baird*,[75] v katerem je sodišče razveljavilo še prepoved izdaje kontracepcije neporočenim parom. Primer je (poleg vnovične potrditve povezave med zasebnostjo in avtonomijo posameznika) pomemben zato, ker je sodišče v odločitvi izrecno ločilo zasebnost in zakonsko zvezo: "*Če pravica do zasebnosti kaj pomeni, potem je to pravica posameznika, poročenega ali samskega, da je neodvisen od nepooblaščenega vladnega vsiljevanja...*" (Turkington in Allen, 1999: 623). Podobno kontroverzen primer je tudi *Roe proti Wade*[76] iz leta 1973, v katerem je sodišče na podlagi pravice do zasebnosti razveljavilo prepoved abortusa v Teksasu (Turkington in Allen, 1999: 630–637). Je pa tudi ta primer pokazal, da ameriška ustavnosodna praksa zasebnost dojema v močni povezavi z osebno avtonomijo.

Ker je ameriška ustava zasnovana na predpostavki ščitenja posameznika pred državo, torej podeljuje t. i. negativne pravice, s katerimi določa, česa država ne sme storiti in s tem ustvarja prostor posameznikove svobode, je razumljiv razvoj varstva zasebnosti, ki ima za posledico širjenje avtonomije posameznika. Vendar pa ravno od tu in iz pravice do zasebnosti, ki je na nekaterih področjih še vedno lastninsko koncipirana, izvira tudi poglavitna pomanjkljivost varstva zasebnosti v ZDA, ki preprečuje učinkovito varovanje informacijske zasebnosti. Zakon o zasebnosti (ang. *Privacy Act*)[77] vsebuje omejitve pri razkrivanju osebnih podatkov, a te omejitve ne veljajo za Kongres in preiskovalne organe, pa tudi za druge vladne agencije ne, ko gre za njihovo t. i. rutinsko uporabo; za to se je v praksi izkazalo, da pomeni praktično katerokoli rabo (Cate, 1997: 78). Pravni okvir njenega varovanja predstavljata zakon o svobodi informacij (ang. *Freedom of Information Act*,[78] FOIA[79]) ter zakon o zasebnosti[80], ki pa veljata samo za javni sektor.[81] Ravno pri varovanju informacijske zasebnosti v zasebnem sektorju pa je nujno potrebna dejavna vloga države pri ščitenju pravic posameznika; tu so se ZDA skoraj popolnoma odpovedale regulaciji in zadeve prepustile trgu.

---

75 Eisenstadt v. Baird, 405 U.S. 438 (1972).

76 Roe v. Wade, 410 U.S. 113 (1973).

77 Privacy Act of 1974, 5 U.S.C. (1974).

78 Freedom of Information Act of 2002, 5 U.S.C. (2002).

79 Poglavitni namen FOIA je zagotavljati nadzor javnosti nad delovanjem vlade. Zakon določa, da ima vsakdo pravico dostopa do kateregakoli zveznega dokumenta, razen v nekaterih primerih, med drugim je omejen dostop do "*osebnih in medicinskih ali podobnih dosjejev, katerih razkritje bi pomenilo očiten nepooblaščen poseg v zasebnost posameznika*" ter v primeru kazensko-preiskovalnih zadev, ko je "*upravičeno pričakovati, da bi objava dokumentov povzročila nepooblaščen vdor v posameznikovo zasebnost*" (US Department of Justice, 1996).

80 Zakon o zasebnosti (Privacy Act of 1974, 5 U.S.C. (1974)) prav tako prepoveduje razkritje posameznikovih osebnih podatkov (zakon uporablja izraz zapis, '*record*'), poleg tega pa določa, da smejo vladne agencije zbirati samo nujne in relevantne osebne podatke, osebne podatke v največji možni meri zbirati neposredno od posameznika, skrbeti za točnost in popolnost osebnih podatkov ter zagotoviti administrativne in tehnične postopke za zaščito osebnih podatkov.

Zato je v ZDA prostorska, komunikacijska in informacijska zasebnost zunaj doma in zunaj konteksta vladnega preiskovanja in zaplembe slabo varovana (Cate, 1997: 65), pravna ureditev teh področij pa nesistematična in včasih že kar dvolična.[82] To je očitno predvsem pri problemu zasebnosti na delovnem mestu, pri regulaciji informacijske zasebnosti v zasebnem sektorju, pri regulaciji nezaželene elektronske pošte (smetja ali spama) in pri spoštovanju zasebnosti s strani množičnih medijev. Poseben problem predstavlja tudi t. i. sektorski pristop zaščite zasebnosti, kar pomeni, da v ZDA nimajo splošne zakonodaje za zaščito pravice do zasebnosti, imajo pa sprejete številne zakone in uveljavljene različne partikularne rešitve. Manko sektorskega pristopa je tudi v tem, da je treba z nastankom vsake nove tehnologije vidike zasebnosti, ki jih ta tehnologija prinaša, na novo urediti, zato je sledenje zakonodaje tehnološkim spremembam bistveno upočasnjeno. Zaradi vloge ameriške vlade in ameriških korporacij pri razvoju in upravljanju interneta se na njem močno pozna tudi ameriški pristop do varovanja zasebnosti.

Pravica do zasebnosti v ZDA na delovnem mestu

Delodajalci v ZDA večinoma nasprotujejo državni regulaciji zaščite zasebnosti na delovnem mestu in menijo, da zadostuje samoregulacija s strani podjetij. Podobno menijo podjetja tudi glede zaščite zasebnosti potrošnikov, čeprav je v 70. letih prejšnjega stoletja ameriški Kongres ustanovil *Federal Privacy Comission*, ta pa je v svoji raziskavi ugotovila, da je samoregulacija v zasebnem sektorju popolna napaka (Sykes, 1999: 142); kljub temu tako zasebni sektor kot tudi Bela hiša še naprej vztrajata, da je samoregulacija povsem zadostna in da sprejem novih zakonov ni potreben (Laurant, 2003: 529). Raziskava, ki jo je vodil David Linowes, je ugotovila, da delodajalci o zaposlenih zbirajo podatke v prevelikem obsegu ter ne zagotavljajo točnosti in zaupnosti podatkov. Pav tako zaposlenim niso niti omogočili, da bi napačne podatke lahko popravili. Raziskava je razkrila primere, ko so bili zaposleni odpuščeni ali pa jim je bilo onemogočeno napredovanje zaradi nepreverjenih govoric (npr. nekomu so onemogočili napredovanje, ker naj bi bilo znano, da ima težave z drogo, podatek pa je izviral od soseda, ki je delodajalčevim preiskovalcem povedal, da je slišal, da naj bi zaposleni nekoč poizkusil marihuano itd.) (Sykes, 1999: 141–142). V ZDA na delovnem mestu delodajalec od zaposlenih lahko zahteva oddajo telesnih tekočin (za preverjanje drog ali test nosečnosti). Do leta 1988, ko je bil sprejet *Employee Polygraph Protection Act*,[83] ki tako početje prepoveduje (razen, če delodajalec t. i. "upravičeno sumi"), so lahko izvajali tudi poligrafsko testiranje zaposlenih (Sykes, 1999: 144). Sykes navaja, da so do tega leta izvedli okrog 2 milijona poligrafskih testiranj na leto. Vendar pa zakon ne preprečuje delodajalcem, da bi zaposlene smeli spraševati tudi najosebnejša vprašanja. Sicer je

---

[81] Evropske ureditve pri varovanju informacijske zasebnosti ne ločujejo med državnimi in zasebnimi upravljavci osebnih podatkov. Je pa po drugi strani res, da je v ZDA ameriška vlada največji posamični upravljavec podatkov in zbirk podatkov, verjetno pa tudi na svetu (Cate, 1997: 76), zato ne moremo trditi, da je to področje povsem neregulirano.

[82] Na to kažeta v nadaljevanju obravnavana zakona *Video Privacy Protection Act* (Video Privacy Protection Act of 1988, 18 U.S.C. (1988)) in *Driver's Privacy Protection Act* (Driver's Privacy Protection Act of 1994, 18 U.S.C. (1994)).

[83] Employee Polygraph Protection Act of 1988, 29 U.S.C. (1988).

ameriško Vrhovno sodišče leta 1977 v primeru *Whalen proti Roe*[84] priznalo, da ustava priznava dve vrsti zasebnosti – zasebnost, ki se veže na posameznikovo neodvisnost in avtonomijo, ter informacijsko zasebnost (pravico posameznika, da se izogne razkritju osebnih zadev) (Cate, 1997: 62–63 ter Sykes, 1999: 251); vendar pa se odločitev zaradi negativne koncepcije ustavnih pravic nanaša samo na državo, ne pa tudi na zasebni sektor. V primeru *Whalen* je skupina pacientov, ki je zakonito (na podlagi recepta) uživala nevarna zdravila, sprožila ustavni spor glede predloga zakona, na podlagi katerega je država New York želela ustvariti centralno računalniško evidenco vseh bolnikov, ki uživajo taka zdravila. Sodišče je sicer presodilo, da zakon ni v nasprotju z ustavo, vendar je odločitvi botrovalo to, da je zakon določal stroge administrativne in tehnične ukrepe za varovanje teh podatkov. Glede informacijske zasebnosti je zelo zgovorno mnenje sodnika Brennana, ki je menil, da je "*v tem primeru problematično predvsem centralno računalniško hranjenje tako zbranih podatkov... Centralno shranjevanje in enostaven dostop do podatkov močno povečujeta možnost zlorabe in nisem pripravljen reči, da nekoč v prihodnosti ne bo treba te tehnologije nekako obrzdati.*" (Turkington in Allen, 1999: 69–70).

Varstvo pravice posameznika, da se izogne razkritju osebnih zadev, je precej nesistematično urejeno v zasebnem sektorju. O tem zgovorno pričata dva primera, ki se nanašata na zastavljanje občutljivih vprašanj s strani delodajalca. Primer *Walls proti City of Petersburg*[85] iz leta 1990 je sprožila mestna uslužbenka, ki je bila zaradi zavrnitve odgovora na vprašanje (iz uradnega vprašalnika, ki so ga morali izpolniti vsi zaposleni), ali je imela kdaj spolne odnose s predstavnikom istega spola, izgubila službo. Pritožbeno sodišče četrtega okrožja (*Court of Appeals for the Fourth Circuit*) je presodilo, da vprašanje ne posega v njene pravice, ker ne sprašuje o zadevi, za katero ima tožnica pravico, da jo obdrži zase (Cate, 1997: 64). Sodišče je odločilo na podlagi ugotovitve, da ni pravice do homoseksualnosti (v originalni dikciji: '*to* engage *in homosexual acts*'), zaradi česar tudi ni ustavne pravice nerazkritja takih dejstev.

Podoben primer, ki je bil razrešen povsem drugače, se je zgodil v Kaliforniji. Pri tem ni nepomembno to, da je Kalifornija ena izmed redkih ameriških zveznih držav, v katerih je zasebnost zagotovljena v ustavi zvezne države (Cate, 1997: 67). Spor je sprožil iskalec zaposlitve Sibi Soroka, ki je moral izpolniti psihološki test. V njegovem primeru je vprašalnik, ki je bil podlaga za ugotavljanje sposobnosti za službo, vseboval zelo osebna vprašanja o veroizpovedi, spolni usmerjenosti, spolnem življenju in zdravstvenih podatkih. Sodišče je razsodilo njemu v prid, saj je menilo, da so posegi v zasebnost pod določenimi pogoji upravičeni, a samo v primeru t. i. nujnega interesa (ang. *compelling interest*), ki mora biti tesno povezan z dejansko naravo zaposlitve (Sykes, 1999: 144–146).

[84] Whalen v. Roe, 429 U.S. 589 (1977).
[85] Walls v. City of Petersburg, 895 F.2d 188, 192 (1990).

Če za državne organe velja, da ne smejo preiskovati in prisluškovati brez sodnega naloga (razen v že omenjenih primerih), pa v ZDA to ne velja za delodajalca. V primeru *O'Connor proti Ortega*[86] je Vrhovno sodišče ZDA leta 1987 presodilo, da je preiskava vladnega uslužbenca upravičena, če je opravljena v povezavi z njegovim delom in ni pretirano vsiljiva (Turkington in Allen, 1999: 162). V tem primeru je šlo za zdravnika, ki je bil na delovnem mestu že 17 let in je imel na svoji delovni mizi tudi osebne stvari, zaradi česar je sodišče sicer menilo, da uslužbenec v tem primeru upravičeno pričakuje zasebnost na delovnem mestu, vendar tudi v konkretnem primeru niso ugotovili, da bi bila preiskava neupravičena.

Podobno velja tudi za prisluškovanje telefonom, elektronski pošti in uporabi interneta, čeprav je res, da se Vrhovno sodišče ZDA o prestrezanju elektronske pošte še ni izreklo (Klemenčič, 2003: 137). Leta 1992 se je v Kaliforniji zgodil primer *Shoars proti Epson America Inc.*.[87] Ko je administratorka elektronskega poštnega sistema podjetja Epson ugotovila, da eden izmed direktorjev prebira elektronsko pošto zaposlenih in ga soočila s tem odkritjem, je bila odpuščena. Alana Shoars je vložila tožbo, vendar se je podjetje branilo, da je sistem za elektronsko pošto v njihovi lasti in imajo zato pravico, da ga upravljajo in nadzorujejo, ali se uporablja samo v delovne namene ali ne. Shoarsova je bila prepričana, da bo tožbo dobila, vendar kalifornijsko sodišče njenim argumentom, da je njena zasebnost zaščitena s kalifornijsko ustavo, ni pritrdilo, češ da ustava ščiti samo informacije, ki so osebne, ne pa tudi poslovnih komunikacij,[88] poleg tega je uporabljala opremo, ki je bila v lasti podjetja (Sykes, 1999: 140). Še več, izkazalo se je, da je leta 1986 sprejeti *Electronic Communication Privacy Act*[89] (ECPA), ki uravnava prisluškovanje elektronskim komunikacijam, precej pomanjkljiv. ECPA namreč v prvem poglavju, znanem tudi pod imenom *Wiretap Act*, prepoveduje prestrezanje elektronskih telekomunikacij, pri čemer je 'prestrezanje' definirano kot "*zaznavanje izžarevanja [signala] (ang.* aural*) ali druga pridobitev vsebine žice oziroma elektronske ali ustne komunikacije, ki poteka s pomočjo uporabe kakršnekoli elektronske, mehanične ali druge naprave*".[90] Gre torej za to, da mora prestrezanje potekati hkrati s prenosom. Vendar pa za nadzorovanje elektronske pošte ni treba uporabljati sočasnega prestrezanja. Če delodajalec dostopa do strežnika, v katerem je shranjeno elektronsko sporočilo, s tem zaobide prepoved sočasnega prestrezanja. ECPA namreč v drugem poglavju, znanem pod imenom *Stored Communications Act*, ki prepoveduje dostop do shranjenih elektronskih sporočil brez soglasja nadzorovane osebe, iz prepovedi eksplicitno izključuje "*osebe, ki zagotavljajo (ang. to provide) žično ali elektronsko komunikacijsko storitev*", torej so iz prepovedi izvzeti delodajalci, ki imajo v lasti komunikacijsko opremo podjetja (Sinrod, 2004). Vsekakor je treba ločevati med interno in zunanjo elektronsko pošto (predvsem dohodno), saj v primeru prestrezanja dohodne

---

86 O'Connor v. Ortega, 480 U.S. 709 (1987).

87 Shoars v. Epson America Inc., No. (SWC) II2749 (Cal App. Dep't. Super. Ct. Dec 8, 1992)

88 Na razliko v primerjavi z evropsko prakso kaže tudi razsodba Evropskega sodišča za človekove pravice v primeru *Niemietz proti Nemčiji* iz leta 1992, ko je le-to zapisalo: "*Poleg tega se zdi, da ni načelnega razloga, zakaj bi ta pojem 'zasebnega življenja' izključeval profesionalne ali poslovne dejavnosti [posameznika]...*" (Niemietz v. ZR Nemčija, odločba z dne 16. 12. 1992).

89 Electronic Communication Privacy Act of 1986, 18 U.S.C. (1986).

90 Electronic Communication Privacy Act of 1986, 18 U.S.C. (1986).

pošte delodajalec ne bere le pošte zaposlenega, temveč tudi tretjih oseb. Vendar pa ECPA delodajalcem v vsakem primeru dovoljuje nadzor komunikacij, ki zadevajo poslovanje podjetja, iz česar sledi, da lahko delodajalec npr. posluša pogovor vsaj nekaj časa, da lahko ugotovi, ali gre za poslovni ali zasebni pogovor (ACLU, 2003). Za razliko od telefonskega pogovora pa je dostop do elektronske pošte popoln (ne delen ali časovno omejen), zato je nadzor elektronske pošte laže upravičiti. V vsakem primeru pa velja, da lahko kot pogoj za zaposlitev delodajalci zahtevajo soglasje za nadzor v kakršnemkoli obsegu in v tem primeru je nadzor zaposlenega povsem zakonit. To se je izkazalo tudi v primeru *Bonita P. Bourke, et. al. proti Nissan Motor Corporation*,[91] ko je leta 1993 kalifornijsko prizivno sodišče razsodilo, da vpogled v elektronsko sporočilo, ki ga je uslužbenka poslala po omrežju podjetja, ne pomeni neupravičenega vdora v njeno zasebnost, ker je uslužbenka predhodno podpisala izjavo, v kateri se je zavezala, da bo elektronsko pošto uporabljala zgolj v službene namene (Klemenčič, 2003: 137). Še dlje pa je šlo isto sodišče z razsodbo v primeru *McLaren proti Microsoft*[92] iz leta 1999. V tem primeru je šlo za to, da je podjetje pregledalo šifrirano elektronsko pošto zaposlenega (ki so jo pred tem seveda dešifrirali), shranjeno v računalniku v mapi "*Osebni imenik*"; zaposleni je zato sprožil sodni spor. Sodišče je v razsodbi dalo prav delodajalcu, in sicer z obrazložitvijo, da je interes delodajalca, da prepreči pošiljanje neprimerne elektronske pošte, nad interesom zaposlenega do zasebnosti (Klemenčič, 2003: 137). Kaj je neprimerno, pa je pogosto stvar presoje delodajalca; na to kaže primer zaposlenega v podjetju Pillsbury. Zaposleni Michael Smyth je namreč leta 1994 enemu izmed sodelavcev poslal elektronsko sporočilo, v katerem je zapisal, da so njegovi predpostavljeni "*zahrbtne barabe*". Ker so le-ti spremljali komunikacijo svojih zaposlenih, so ga odpustili z obrazložitvijo, da so bili njegovi komentarji neustrezni in neprofesionalni. Smyth se je pritožil na sodišče in trdil, da so mu v podjetju zagotovili zasebnost komunikacij, podjetje pa je trdilo nasprotno. Zvezno sodišče je primer zavrglo (in s tem dalo prav delodajalcu) z obrazložitvijo, da tudi če bi podjetje zaposlenemu res obljubilo tajnost komunikacij, sporno dejanje ne posega v oškodovančevo zasebnost na nepošten način (Sykes, 1999: 141). Na podlagi ECPA je 29. junija 2004 ameriško prizivno sodišče prvega okrožja v primeru *U. S. proti Councilman*[93] najprej celo razsodilo, da ponudniki brezplačne elektronske pošte lahko zakonito berejo elektronsko pošto svojih uporabnikov brez njihovega soglasja oz. celo brez njihove vednosti. Ta odločitev je bila sicer avgusta 2005 revidirana in nadzor elektronske pošte v takih primerih ni dovoljen.

Organizacija ACLU ugotavlja, da se elektronsko nadzorovanje zaposlenih pogosto sprevrže v vohunjenje za zaposlenimi. V podkrepitev svojih ugotovitev navajajo različne primere nadzorovanja, npr. videonadzor v prostorih, ki so jih zaposleni uporabljali za preoblačenje. Po njihovi oceni delodajalci na leto prisluškujejo 400 milijonom klicev zaposlenih itd. (ACLU, 2003). Raziskava *American Management Association* iz leta 2001 o nadzoru na delovnem mestu v ZDA pa je pokazala, da 43 % podjetij nadzoruje uporabo telefona, 37 % uporablja video nadzor, 36 % pregleduje datoteke v računalnikih zaposlenih, 47 % pregleduje elektronsko pošto

[91] Bonita P. Bourke, et. al. v. Nissan Motor Corporation, No. 68-705 (Cal.Ct.App.1993).
[92] McLaren v. Microsoft, No. 05-97-00824 (Tex. Ct. App. 28. maj, 1999).
[93] United States of America v. Bradford C. Councilman, No. 03-1383 (1st Cir., June 29, 2004).

zaposlenih, 63 % podjetij spremlja uporabo interneta, 19 % pa spremlja uporabo računalnika (kdaj se zaposleni prijavi v sistem, kako tipka itd.). Raziskava je sicer ugotovila, da je nadzor večinoma občasen (t. i. '*spot check*'), vendar se njegov obseg povečuje, hkrati pa postaja tudi čedalje bolj rutinski (Schulman, 2001a). Kot je namreč ugotovil Schulman, je razlog za premik nadzorovanja posameznikov proti nadzoru celotne polulacije zaposlenih ta, da je zdaj celotna delovna sila sumljiva, saj so organizacije čedalje bolj zaskrbljene zaradi t. i. 'internih groženj' (Schulman, 2001b). Podjetja v ZDA se z nadzorom želijo zaščititi tako pred odtekanjem različnih poslovnih skrivnosti kot tudi pred odškodninskimi tožbami zaradi neprimernega ravnanja zaposlenih. V zvezi s slednjim je največkrat navajan primer podjetja Chevron, ki je moralo štirim ženskam plačati 2,2 milijona dolarjev odškodnine, ker jim je njihov zaposleni pošiljal elektronsko pošto z žaljivo vsebino (Sykes, 1999: 141). Res pa je, da takih primerov ni veliko, a se kljub temu uporabljajo kot izgovor za uvajanje čedalje obsežnejšega nadzora zaposlenih.

Zaradi tega se zaposlene čedalje bolj obravnava kot kos opreme (inventar) in ne kot avtonomne posameznike. Uporaba t. i. aktivnih značk, elektronskih identifikacijskih kartic, ki jih nosijo zaposleni in omogočajo njihovo natančno lociranje (ACLU, 2003), je tudi zunanji znak take obravnave. Prav tako posegi v telesno zasebnost (urinski, krvni in genski testi) s strani delodajalca, ki ima nad zaposlenimi ekonomsko moč, odpirajo vprašanja človekovega dostojanstva in avtonomije na delovnem mestu. Ni tudi odveč vprašanje, ali je povečevanje nadzora ustrezen način zmanjševanja internih groženj v podjetju. Etzioni namreč meni, da vohunjenje za elektronsko pošto zaposlenih uničuje občutek skupnosti na delovnem mestu (Whitaker, 1999: 105), to pa verjetno vpliva tudi na lojalnost podjetju. Kljub vsemu delodajalci v ZDA redno posegajo v zasebnost svojih zaposlenih, to pravico pa jim domnevno daje lastništvo nad delovno opremo. Odločitve ameriških sodišč kažejo, da država njihovo početje legitimira, tehnološki razvoj pa omogoča uporabo novih in čedalje cenejših nadzornih naprav. Kot bomo videli pozneje, so zaposleni v ZDA glede svoje zasebnosti na delovnem mestu v bistveno slabšem položaju, kot velja za evropske delojemalce.

Varstvo informacijske zasebnosti v ZDA v zasebnem sektorju

Podobno stanje, kot velja na področju zasebnosti na delovnem mestu, v ZDA velja tudi na področju informacijske zasebnosti (in zasebnosti nasploh) v zasebnem sektorju, v katerem je še vedno zelo razširjen lastninski koncept pravice do zasebnosti. Ravno tako kot za delodajalca velja, da lahko posega v zasebnost svojih zaposlenih bistveno bolj, kot vlada lahko posega v zasebnost svojih državljanov (Sykes, 1999: 147), velja za upravljavce osebnih podatkov, da lahko osebne podatke posameznikov zbirajo skoraj brez vsakršnih omejitev.

Načeloma namreč v ZDA na zvezni ravni za zasebni sektor ne veljajo skoraj nikakršne omejitve pri zbiranju in obdelavi osebnih podatkov, saj *Privacy Act*[94] velja samo za javni sektor. Nekatere države, npr. Massachusetts, Havaji, Minesota, Kalifornija in Georgija, imajo sicer urejene nekatere vidike varstva zasebnosti tudi na področju zasebnega sektorja (Laurant, 2003: 529). Problem pa je, ker v ameriški ustavi zasebnost ni omenjena kot pozitivna pravica, hkrati pa prvi amandma[95] govori o svobodi govora. Primer *US West proti FCC* ,[96] v katerem je prizivno sodišče desetega okrožja presodilo, da so osebni podatki, ki jih zbere podjetje, "*vrsta 'govora' in je zato uporaba potrošnikovih podatkov s strani tretje stranke v poslovnih transakcijah poslovni govor, ki je zaščiten s prvim amandmajem*" (White, 2003: 24), kaže na omejitve, ki jih ameriški pravni sistem postavlja posameznim zveznih državam, ki želijo regulirati obdelavo osebnih podatkov. Previsoka stopnja zaščite informacijske zasebnosti v zasebnem sektorju na ravni posamezne zvezne države bi namreč lahko bila v nasprotju s prvim amandmajem.[97] To pomeni, da ameriški sistem že v samem temelju otežkoča izenačitev varstva informacijske zasebnosti v javnem in zasebnem sektorju, ki sicer velja v Evropi.

Prav tako je informacijska zasebnost precej neustrezno zaščitena skozi odškodninsko pravo (*tort law*). *Restatement of The Law of Torts*[98] priznava štiri škodljiva dejanja proti zasebnosti, vendar je njihova aplikacija na informacijsko zasebnost mogoča le v delnem obsegu, pa še v teh primerih posamezniki s tožbo redko uspejo (Cate, 1997: 89–90), kar velja posebej v primerih vdorov v zasebnost posameznikov s strani množičnih medijev. Cate namreč ugotavlja, da kadar nastopi kolizija med zasebnostjo in svobodo izražanja, skoraj vedno prevlada slednja (Cate, 1997: 99), zato ne presenečajo primeri medijskega vdiranja v zasebnost posameznikov, ki jih v knjigi *The End of Privacy* navaja Charles J. Sykes, pri katerih so sodišča pritrdila medijem. Presenečajo le obrazložitve sodišč. Sykes med drugim navaja primer, ko je časopis v Georgiji objavil fotografijo napol razpadlega trupla umorjene 14-letnice, starši pa so proti časopisu vložili tožbo. V razsodbi je sodišče iz Georgije zahteve staršev zavrnilo in sicer z obrazložitvijo, da so bile objavljene fotografije "*vredne objave*" (ang. *newsworthy*). Podobno obrazložitev je na Floridi leta 1982 doživela žrtev ugrabitve, ki jo je policija povsem golo rešila iz rok ugrabitelja. Lokalni časopis je naslednji dan objavil fotografijo policijskega reševanja, na kateri je bila ženska pomanjkljivo zakrita z brisačo. S tožbo proti časopisu pa ni uspela, saj je bilo sodišče mnenja, da je bila njena ugrabitev in teror nad njo "*tipična čustveno razburljiva drama, ki privlači novinarje in druge*" (Sykes, 1999: 81).

Ko nekdo zbere osebne podatke, so ti njegova last in lahko z njimi počne praktično karkoli; to pomeni, da ni nikakršnih omejitev za njihovo nadaljnjo prodajo. Nekaj omejitev velja le za nekatere vrste osebnih podatkov, in sicer za finančne zapise, zdravstvene informacije, kreditna poročila, podatke o izposoji video kaset, kabelski TV, internetnih dejavnostih otrok, mlajših

---

94 Privacy Act of 1974, 5 U.S.C. (1974).
95 1. amandma, Listina svoboščin (Bill of Rights), 1791.
96 U.S. West v. F.C.C., 182 F.3d 1224 (1999).
97 1. amandma, Listina svoboščin (Bill of Rights), 1791.
98 Restatement of the Law (2d) of Torts, 1964.

od 13 let, podatke o šolanju in izobrazbi, podatke o lastnikih motornih vozil ter podatke, ki jih uporablja telemarketing (Laurant, 2003: 526–527). Kot bomo videli v nadaljevanju, je regulacija obdelave osebnih podatkov v ZDA v najboljšem primeru podobna gašenju požara (razen podatkov o šolanju in izobrazbi in v zadnjem času tudi zdravstvenih podatkov), oziroma se ameriška zakonodaja regulacije tega področja loteva izrazito kampanjsko, navadno kot reakcija na kak razvpit primer zlorabe.

Eden izmed značilnih zgledov je *Driver's Privacy Protection Act*[99] iz leta 1994. Zakon so sprejeli kot odziv na umor igralke Rebecce Schaeffer, ki ga je zagrešil njen preveč vneti oboževalec. Ta je namreč podatke o njej (naslov itd.) dobil s pomočjo zasebnega detektiva iz kalifornijskega *Urada za motorna vozila*. Zakon, ki je bil sprejet kot odziv na ta dogodek, prepoveduje oddajo osebnih podatkov, vendar pa določa štirinajst širokih izjem, ki prvotni namen zakona praktično povsem izničijo, saj med drugim prepoved ne velja za zasebne detektive (Cate, 1997: 79).[100]
Podobno je tudi na področju prisluškovanja elektronskim komunikacijam ter tajnem snemanju pogovorov. Prisluškovanje brez soglasja ali brez sodnega naloga je prepovedano, vendar le, če ga izvaja tretja oseba. ECPA[101] iz leta 1986 namreč določa izjemo, da je razkritje vsebine komunikacij dovoljeno že, če se z razkritjem strinja ena stran (Cate, 1997: 84). Podobno je Vrhovno sodišče ZDA razsodilo, da je dovoljeno tajno snemanje pogovora, ki ga ima nekdo z drugo osebo, tudi brez sodnega naloga. Odmeven primer se je zgodil leta 1998, ko je imel ameriški predsednik Bill Clinton razmerje s svojo pomočnico Monico Lewinsky, podatki o tem razmerju pa so prišli na dan tako, da je prijateljica Monice Lewinsky Linda Tripp snemala pogovor, v katerem se ji je Lewinskyjeva zaupala. Na podlagi teh določil delujejo različne vigilantske skupine, na primer člani spletne strani *perverted-justice.com*, ki se na lastno pest borijo proti pedofiliji. Člani *perverted-justice* se namreč na internetu prek forumov in spletnih klepetalnic izdajajo za mladoletnike in iščejo domnevne pedofile ter se z njimi dogovorijo za srečanje. Pogovore z njimi snemajo in ko domnevne pedofile zvabijo na kraj srečanja, jih fotografirajo in identificirajo, njihove podatke in zapis pogovora (ki navadno poteka v zasebni klepetalnici ali pa gre za izmenjavo povsem zasebnih sporočil) pa objavijo na spletni strani.

Podobno nekonsistentno stanje vlada tudi na področju zaščite osebnih podatkov. Ker se *Privacy Act*[102] ne nanaša na transakcijske podatke, so ponudniki telekomunikacijskih storitev do leta 1996 lahko zbirali in obdelovali te osebne podatke brez omejitev. Leta 1996 pa je Kongres sprejel *Telecommunications Act*,[103] ki je zaščito zasebnosti razširil tudi na transakcijske podatke (ne pa tudi na podatke iz telefonskega imenika); vendar pa zakon v členu 551f ponudnikom

---

99 Driver's Privacy Protection Act of 1994, 18 U.S.C. (1994).

100 Spremembo na tem področju pa sicer nakazuje primer Amy Boyer, ki jo je 15. oktobra 1999 ustrelil obsedenec Liam Youens. Youens je naslov delovnega mesta svoje žrtve dobil od podjetja Docusearch, ki se ukvarja z iskanjem osebnih podatkov in njihovim posredovanjem le-teh naročnikom preko interneta. Sodelavci podjetja Docusearch so od Boyerjeve s pomočjo lažnega predstavljanja pridobili podatke o naslovu njenega delovnega mesta in jih posredovali Youensu. Leta 2003 je Vrhovno sodišče zvezne države New Hampshire presodilo, da so v takšnih primerih trgovci z osebnimi podatki in zasebni preiskovalci lahko odgovorni za škodo, ki jo povzročijo s svojim ravnanjem (EPIC, 2006b).

101 Electronic Communication Privacy Act of 1986, 18 U.S.C. (1986).

102 Privacy Act of 1974, 5 U.S.C. (1974).

103 Telecommunications Act of 1996, 47 U.S.C. (1996).

storitev dovoljuje zbiranje teh podatkov, če je to potrebno, da zaščitijo svoj poslovni interes (to spet kaže na dojemanje pravice do zasebnosti kot podrejene lastninski pravici).

Zgovorna je tudi regulacija zaščite podatkov o izposoji in nakupih videokaset. Leta 1988 je bil sprejet *Video Privacy Protection Act*,[104] in sicer kot odgovor na sramotenje sodnika Roberta Borka, ki je kandidiral za člana Vrhovnega sodišča ZDA. Med njegovimi kongresnimi zaslišanji je namreč prišlo na dan, katere videokasete si je izposojal (Cate, 1997: 86). A podobno kot pri podatkih o lastnikih vozil, so tudi tu določene široke izjeme, med drugim ta, da se sme podatke o uporabnikovih potrošnih navadah razkriti v marketinške namene, če ima uporabnik možnost odjave (ang. *opt-out*). Možnost odjave v tem primeru ne pomeni, da mora uporabnik dati vnaprejšnje soglasje, temveč da se lahko naknadno odloči, da podatkov ne dovoli več uporabljati. Če je bil leta 1988 vsaj opravljen poskus zaščititi podatke o izposojenih videokasetah, pa je skoraj neverjetno, da so bili medicinski podatki, ki so bistveno bolj občutljivi, do leta 2001 na federalni ravni praktično povsem nezaščiteni[105] (z izjemo pogovorov med pacientom in psihiatrom, ki so od razsodbe Vrhovnega sodišča ZDA v primeru *Jaffee proti Redmond*[106] iz leta 1996 povsem zaupni). Šele tega leta so namreč stopili v veljavo *Standards for Privacy of Individually Identifiable Health Information* (znani tudi pod imenom *HIPAA Privacy Rule*[107]), ki so jih začeli pripravljati šele leta 1999. HIPAA Privacy Rule določa pogoje za obdelavo in shranjevanje osebnih podatkov pacientov, vendar ne prepoveduje uporabe teh podatkov za marketinške namene (Laurant, 2003: 528). Omejitve dostopa do teh podatkov sicer lahko sprejmejo posamezne zvezne države, vendar je to zaenkrat storila le peščica ameriških zveznih držav, saj imajo zdravstvene zavarovalnice velik ekonomski interes za te podatke. Zato je veliko vprašanje, ali ne bo tudi v tem primeru ekonomika zdravstvenega varstva prevladala nad pravicami pacientov.[108]

Fair Credit Report Act[109] iz leta 1970 je določal, da morajo podjetja, ki pripravljajo kreditna poročila, poskrbeti za vse razumne ukrepe za zagotovitev čim večje točnosti podatkov (Cate, 1997: 81). Kljub temu so raziskave pokazale, da v kreditnih poročilih mrgoli napak. Raziskava iz leta 1988 je na primer pokazala, da je bilo napačnih kar 43 % poročil, 19 % poročil pa je vsebovalo tako hude napake, da je bil zaradi njih posameznik lahko neupravičeno prikrajšan za posojilo, zaposlitev ali zavarovanje (Etzioni, 1999: 134). Zaradi tega je konec leta 1996 Kongres sprejel *Consumer Credit Reporting Reform Act*,[110] ki je odpravil številne pomanjkljivosti prvotnega zakona (Cate, 1997: 82–84). Kljub temu je spremenjeni zakon namenjen praktično zgolj reševanju 'tehničnih' problemov, samega zbiranja ali vsaj obsega zbiranja osebnih podatkov pa

---

104 Video Privacy Protection Act of 1988, 18 U.S.C. (1988).

105 Posamezne države so sicer lahko sprejele zaščitno zakonodajo, niso pa je bile dolžne sprejeti.

106 Jaffee v. Redmond, 518 US 1 (1996).

107 Standards for Privacy of Individually Identifiable Health Information (HIPAA Privacy Rule), Department of Health and Human Services, 2001.

108 Je pa res, da je zakonodajo za zaščito medicinskih kartotek, podobno kot zakonodajo za zaščito podatkov o izposojenih videokasetah, spodbudil napad na zasebnost člana ameriške elite. Leta 1980 je namreč Kongres tak zaščitni zakon zavrnil, potem pa je dve leti pozneje neki novinar na podlagi FOIA (Freedom of Information Act of 2002, 5 U.S.C. (2002)) zahteval seznam zdravil, ki jih je predpisoval uradni kongresni zdravnik – in senator Howard Baker je v senatu takoj izjavil, da je popolna zaupnost medicinskih podatkov izjemno pomembna (Sykes, 1999: 116).

109 Fair Credit Report Act of 1970, 15 U.S.C. (1970).

110 Consumer Credit Reporting Reform Act of 1996, 15 U.S.C. (1997).

ne problematizira. Zakon tako uveljavlja ukrepe za preprečevanje pojavljanja napak v podatkih, omejuje posredovanje nekaterih občutljivih podatkov (npr. medicinskih podatkov brez soglasja posameznika ni dovoljeno posredovati delodajalcem in zavarovalnicam) in določa obveznosti podjetij, da posameznike obveščajo o njihovih pravicah.

Sredi 70. let 20. stoletja je Vrhovno sodišče ZDA podprlo *Bank Secrecy Act*,[111] ki je od bank zahteval shranjevanje podatkov o bančnih komitentih do šest let, podatki pa morajo biti dostopni vladnim ustanovam. Sodnik Douglas je na odločitev podal ločeno negativno mnenje, v katerem je zapisal, da so "*posamezniki definirani s čeki, ki jih pišejo*" in da bi bilo za kazensko preiskavo zagotovo zelo 'koristno', če bi vlada imela dostop do podatkov o izposojenih knjigah, nakupih in zdravilih, ki jih nekdo jemlje (Sykes, 1999: 59); s tem je hotel opozoriti na pomen zasebnosti transakcijskih podatkov. Leta 1976 pa je Vrhovno sodišče ZDA v primeru *Združene države proti Miller*[112] razsodilo, da posamezniki nimajo pravice do zasebnosti bančnih računov, in sicer z obrazložitvijo, da za bančni račun skrbi tretja stran (Sykes, 59 ter Cate, 1997: 58).

Primeri kot npr. *US West proti FCC*[113] (ugotovitev sodišča, da zaščita potrošnikove zasebnosti krši svobodo govora telekomunikacijskega podjetja) in *Conboy proti AT&T Corp.*[114] (zavrnitev pritožbe stranke, ki je imela tajno telefonsko številko, telekomunikacijsko podjetje pa je to številko posredovalo naprej), kažejo, da so sodišča zaščiti informacijske zasebnosti v ZDA prej nenaklonjena kot ne. Kljub temu je bilo v ZDA nekaj odmevnih odločitev *Federal Trade Comission* (FTC), ki so zelo vplivale na varstvo informacijske zasebnosti. FTC namreč preganja nepoštena in varljiva ravnanja podjetij, torej lahko ukrepa v primerih, ko podjetja strankam zagotavljajo zasebnost in varovanje njihovih podatkov, v resnici pa se teh zagotovil ne držijo. Njihova vloga je torej podobna vlogi organov za varstvo osebnih podatkov v Evropi, a s to razliko, da FTC ne more ukrepati v primerih, ko podjetje stranke seznani s posledicami oddaje osebnih podatkov, pa čeprav je v izjavi zapisano, da bodo podatki uporabljeni v katerekoli namene.

Vprašanje obdelave osebnih podatkov v zasebnem sektorju v ZDA torej ni predvsem vprašanje (informacijske) zasebnosti, temveč svobode trgovanja in svobode komercialnega govora. Namesto poseganja v pravice se postavlja zgolj vprašanje trgovanja med posameznikom in organizacijo, ki zbira osebne podatke. Posameznik ima načeloma sicer možnost, da svojih podatkov ne proda, toda v praksi te možnosti največkrat dejansko nima, če se ne želi izključiti iz družbe. Sistemska neregulacija tega področja v zasebnem sektorju s strani ZDA tako posameznike glede informacijske zasebnosti sili v položaj, ko se svoji informacijski zasebnosti odrekajo na videz prostovoljno.

---

111 Bank Secrecy Act of 1970, 31 U.S.C. (1970).
112 United States v. Miller, 425 U.S. 435 (1976).
113 U.S. West v. F.C.C., 182 F.3d 1224 (1999).
114 Conboy v. AT&T, 84 F. Supp. 2d 492 (2000).

Obdelava in izmenjava osebnih podatkov v ZDA – nove grožnje zasebnosti

Dodatno grožnjo informacijski zasebnosti predstavlja obdelava in nadaljnja uporaba zbranih osebnih podatkov, ki v ZDA za zasebni sektor ni regulirana. Razlogi za neregulacijo so gotovo ekonomski interesi t. i. trgovcev z zasebnostjo (ang. *privacy merchant*). Po nekaterih ocenah imajo tri podjetja, ki se ukvarjajo s kreditnimi poročili, Equifax, TRW (pozneje preimenovana v Experian) in Trans Union Corporation, osebne podatke o 90 % odraslih Američanov (Etzioni, 1999: 128). Podjetje Abacus Alliance iz ZDA je leta 1997 združevalo podatke o nakupih potrošnikov, ki so tisto leto opravili več kot dve milijardi transakcij (Batagelj, 1997). Istega leta je podjetje Axciom posedovalo podatke o 196 milijonih Američanov (Whitaker, 1999: 132), zaradi sodelovanja s pošto pa so bili njihovi podatki vedno ažurni (Američani se namreč pogosto selijo). Po drugi strani pa neregulaciji tega področja precej botruje tudi miselnost, ki jo zelo dobro povzema libertarna kritika zasebnosti. Virginia Postrel tako pravi, da sta zbiranje in izmenjava informacij bistvena za svobodno družbo (Sykes, 1999: 229). Omejitev obdelave in izmenjave osebnih podatkov naj bi bila tako napad na svobodno novinarstvo, svobodno podjetništvo in svobodo komuniciranja, pri čemer ni mišljeno samo tržno komuniciranje, temveč tudi pravica, da se posamezniki učimo drug o drugem in širimo informacije. Vendar pa libertarci pozabljajo na razliko med medsosedskim opazovanjem ter zbiranjem podatkov v velikih brezosebnih zbirkah. Zakonska neregulacija tega področja v ZDA je privedla do tega, da je edino jamstvo za nerazkritje osebnih podatkov iz zbirk samo dobra volja in etika različnih nadzornih sistemov, pravna zaščita večinoma ni možna, mogoči so le neformalni pritiski javnosti. Eden takih uspešnih primerov se je zgodil leta 1990, ko sta podjetji *Lotus Development Corporation* in *Equifax* želeli na CD-ju izdati zbirko podatkov z osebnimi podatki o več kot sto milijonih ljudi iz ZDA (z osebnim dohodkom, starostjo, poročnim statusom itd. vred), a so zaradi burnega nasprotovanja javnosti izdajo CD-ja opustili. Dogodek je vsekakor pokazal, da javnost v ZDA lahko razmeroma visoko ceni zasebnost. Nekateri pa ta primer celo štejejo za ponazoritev, kako lahko samoregulacija učinkovito zaščiti zasebnost (Turtington in Allen, 2000: 427), čeprav je dokazov o neučinkovitosti samoregulacije verjetno bistveno več. Pomen državne regulacije se je zelo dobro pokazal na primeru registra ljudi, ki ne želijo biti kontaktirani s strani marketinških podjetij. To storitev, imenovano *Mail Preference Service,* je Direct Marketing Association brezplačno ponujala od leta 1971. Vendar so se določil o nekontaktu morala držati samo podjetja, ki so bila člani DMA. Do konca 90. let 20. stoletja se je nanj vpisalo samo 2 % odraslih Američanov (Cate, 1997: 105). Potem pa je FTC junija 2003 vzpostavil državni *Do Not Call Register* in napovedal, da bo proti kršiteljem, ki bodo klicali potrošnike, prijavljene na seznam, tudi ukrepal (Federal Trade Comission, 2003). V dobrega pol leta se je v register prijavilo 57 % odraslih Američanov. Da je državna regulacija učinkovitejša kot sistem samoregulacije, pa je pokazala raziskava podjetja Harris Interactive, saj je 92 % tistih, ki so se prijavili v register, izjavilo, da so prejeli manj marketinških klicev, 25 % pa sploh ni prejelo nobenega takega klica (Federal Trade Comission, 2004).

Državna regulacija tako pomeni nekakšno zunanjo spodbudo (največkrat negativno) podjetjem, da se držijo pravil. Pri samoregulaciji take vzpodbude ni (razen moralne zavezanosti potrošnikom) in ko se poveča konkurenca, je podjetjem pomemben samo dobiček (Sykes, 1999: 72). Pri tem nemalokrat pride do neetičnega ravnanja oziroma zavajanja s strani podjetij, ki zbirajo osebne podatke, do zlorab pri obdelavi osebnih podatkov ter do prodaje zbirk osebnih podatkov državnim organom, ki se tako izognejo prepovedi vzpostavljanja lastnih zbirk osebnih podatkov.

Primerov neetičnega ravnanja je kar nekaj. Leta 1998 je FTC kaznovala internetno podjetje Geocities zaradi zavajanja strank. Podjetje Geocities je namreč kljub izrecnim zagotovilom o varovanju zasebnosti zbiralo podatke o igralcih spletnih iger in jih prodajalo naprej (Sykes, 1999: 72). Podobna zgodba je prišla na dan istega leta, vpleteno pa je bilo podjetje Sun Microsystems, ki naj bi prodajalo elektronske naslove članov ene svojih spletnih strani. Stvar je bila posebej resna med drugim tudi zato, ker je bil Sun član *Online Privacy Alliance*, ki se zavzema za samoregulacijo, ki naj bi bila alternativa državni zakonodaji za zaščito zasebnosti (Glave, 1998).

Leta 2002 je FTC ukrepal proti podjetju, ki je od študentov zbiralo osebne podatke z zagotovilom, da bodo podatki posredovani zgolj izobraževalnim ustanovam in za izobraževalne namene, v resnici pa so jih prodali marketinškim podjetjem (Federal Trade Comission, 2002a). Istega leta so ukrepali tudi proti farmacevtskemu podjetju Eli Lilly, katerega uslužbenec je leta 2001 669 članom spletne strani *Prozac.com* poslal elektronsko sporočilo, in to vsem hkrati in tako, da so lahko vsi prejemniki videli druge prejemnike sporočila (Federal Trade Comission, 2002b). Odmevnejši primer je bil tudi ukrep proti Microsoftu oziroma njegovi storitvi MS Passport in MS Wallet, v okviru katere je Microsoft med drugim zbiral tudi številke kreditnih kartic. Med drugim je namreč zbiral več osebnih podatkov, kot je bilo navedeno v izjavi, namenjeni uporabnikom njihovih storitev (Federal Trade Comission, 2002c). Ni pa nujno, da je mogoče vse primere prodaje osebnih podatkov tudi preganjati. Organizacije, kot sta Blue Cross in Blue Shield, podatke iz medicinskih kartotek povsem legalno uporabljajo za obveščanje bolnikov (npr. sladkornim bolnikom pošiljajo obvestila o obolenju oči kot posledici diabetesa in brezplačni kupon za pregled), to pa se lahko sprevrže tudi v neposredno trženje. AT&T zbira podatke o uporabi telefona z namenom identifikacije tistih uporabnikov, ki zaradi finančnih koristi pogosto menjajo operaterje. Celo revija Playboy je leta 1998 pripravila načrt zbiranja in izmenjave podatkov o kupcih svoje revije (Sykes, 1999: 64–65).

Zlorabe pri obdelavi osebnih podatkov so mogoče iz več razlogov. Enega večjih problemov v zadnjem času povzroča t. i. *outsourcing* – oddaja del zunanjim podizvajalcem. Ameriška podjetja čedalje več del – predvsem razna manj zahtevna programerska dela, vnašanje podatkov ali prepisovanje po posnetem nareku (npr. ugotovitve zdravnika med pregledom pacienta) – 'izvažajo' v Indijo, Pakistan in podobne države, kjer je delovna sila dovolj izobražena, a bistveno cenejša kot v ZDA. Pri tem podjetja pogosto posredujejo v tujino občutljive podatke in pri tem se lahko zaplete. Leta 2003 je tako Lubna Baloch, prepisovalka iz Indije, zagrozila, da bo na internetu objavila medicinske kartoteke, če ji ameriško podjetje, ki ji je delo posredovalo, ne bo plačalo obljubljene 3 cente na vrstico (pozneje se je izkazalo, da si je delo posredovalo

več zunanjih izvajalcev, prvi zunanji izvajalec pa naj bi dobil 18 centov na vrstico). Ker so v medicinskih kartotekah pogosto tudi drugi občutljivi podatki, npr. številke bančnih računov, številke kreditnih kartic, številka zdravstvenega zavarovanja (SSN) itd., in ker ob morebitni zlorabi zunaj ZDA posamezniki nimajo na voljo pravnih sredstev za ukrepanje, je to vsekakor resen problem (Zetter, 2004a).

Še morda nekoliko resnejše posledice pa je leta 1997 izkusila Beverly Dennis iz Ohia, ki je prejela opolzko pismo neznanca, iz katerega je bilo razvidno, da pozna tudi njene pretekle naslove, vse o njeni ločitvi in osebnih navadah, celo znamko šampona, ki ga uporablja. Dennisova je na svoje presenečenje odkrila, da je bilo pismo poslano iz teksaškega zapora, poslal pa ga je zapornik, ki je za podjetje Metromail obdeloval osebne podatke (Sykes, 1999: 62–63), podjetje pa je podatke dobilo iz nagradnih anket, ki jih je Dennisova sama izpolnila. Izkazalo se je, da ni najemanje zapornikov za obdelavo osebnih podatkov nič nenavadnega – taka je bila namreč praksa v 27 državah, zaporniki v federalnih zaporih pa so vnašali celo podatke za davčni urad. Ko so zaradi dogodka v Teksasu prepovedali obdelavo osebnih podatkov zapornikom, ki so bili obsojeni zaradi spolnih deliktov, je direktor zapora potožil, da so zdaj izgubili najboljše programerje – pedofile (Sykes, 1999: 63).

Tretjo nevarnost pri prodaji osebnih podatkov pa predstavlja možnost, da te podatke od komercialnih posrednikov kupijo preiskovalni organi in tajne službe. Ker so bili predlogi, da bi FBI smel imeti neomejen dostop do vseh nacionalnih zbirk podatkov, oziroma predlogi o vzpostavitvi ene velike zbirke podatkov o vseh državljanih neuspešni (Whitaker, 1999: 131), se zastavlja vprašanje, ali neobstoj omejitev pri prodaji osebnih podatkov ne predstavlja možnosti, da se FBI omenjeni prepovedi izogne. Vprašanje so si številni strokovnjaki in aktivisti gibanja za zasebnost že večkrat zastavili (glej npr. Etzioni, 1999: 128, Whitaker, 1999: 132 ter Sykes, 1999: 60). David Banisar pa trdi, da se to že dogaja – FBI, DEA in IRS po njegovih trditvah skrivaj kupujejo komercialne zbirke podatkov in jih povezujejo s svojimi preiskovalnimi zbirkami (Sykes, 1999: 60). Utemeljenih sumov za to je kar nekaj.

Leta 1996 je podjetje Lexis-Nexis za deset dni omogočilo popoln dostop do številk socialnega zavarovanja (SSN se v ZDA uporablja kot enolični identifikator, podobno kot v Sloveniji EMŠO) kar po internetu. Zaradi pritiska javnosti so spletno stran zaprli in to je zaustavilo tudi načrte uprave *U. S. Social Security*, ki je nameravala po internetu – brez gesla – ponuditi podatke o osebnih dohodkih in pokojninah vseh imetnikov SSN (Whitaker, 1999: 99).

Podobno so uradniki več zveznih držav prodali osebne podatke skupaj s fotografijami iz voziških dovoljenj zasebnemu podjetju, za katerega se je pozneje izkazalo, da je od *U. S. Secret Service* dobilo približno 1,5 milijona dolarjev in izdatno tehnično pomoč z namenom, da ustvari nacionalno zbirko s fotografijami prebivalstva (Sykes, 1999: 60–61).

Leta 1996 je podjetje Aptex komercialno ponudilo sistem za opazovanje in profiliranje uporabnikov interneta SelectCast. Sistem je bil razvit s strani podjetja HNC Software, ki se ukvarja z razvijanjem programske opreme AI[115] (Glave, 1996), podjetje NHC pa je bilo leta

[115] AI - ang. *Arificial Inteligence*, umetna inteligenca.

1986 ustanovljeno za raziskovanje in razvoj na področju obrambe in varnosti (Heritage Media Corporation, 1999), ima pa še vedno močne povezave z ameriškimi tajnimi službami (Sykes, 1999: 68–69).

Če velja, da zaradi obsega in narave zbranih podatkov ločnica med marketingom in vohunjenjem čedalje bolj izginja, povezovanje trgovcev z zbirkami podatkov s tajnimi službami in državnimi organi to ločnico še dodatno briše. Pri tem je posebej zaskrbljujoča ugotovitev Davida Flahertyja, ki je zapisal, "*moj vtis je, da si javni sektor ni mogel privoščiti takšne programske opreme in sredstev za povezovanje osebnih podatkov, kakršne upravljajo v neposrednem trženju (posebej v ZDA)*" (Flaherty, 2001: 187).

* * *

Zakaj je pri zaščiti informacijske zasebnosti v ZDA prišlo do takšnih pomanjkljivosti, je vsekakor zanimivo vprašanje. Odgovor leži v ostankih lastninskega koncipiranja pravice do zasebnosti ter v libertarni ideologiji, ki zbiranje in obdelavo osebnih podatkov vidi zgolj kot izmenjavo informacij, kot problem svobode trgovanja, ne pa kot problem poseganja v zasebnost posameznika. Problem je tudi ameriška ustava, ki posameznikom podeljuje negativne pravice, zaradi česar informacijska zasebnost v zasebnem sektorju ostaja večinoma neregulirana. Nekateri vidijo pri vprašanju informacijske zasebnosti celo poskus ameriške države, da bi ustregla korporacijam, pa četudi so pri tem omejene pravice posameznikov. Ustanovitelj organizacije Junkbusters Jason Cattler se sprašuje: "*Zakaj za distribucijo korporacijske programske opreme brez dovoljenja uporabljamo izraz 'piratstvo', za distribucijo osebnih podatkov posameznikov brez dovoljenja pa izraz 'razdeljevanje' (ang. sharing)?*" (The Pew Internet & American Life Project, 2000: 11).

V primerjavi z regulacijo prisluškovanja Gellman ugotavlja, da je v ZDA po primeru *Olmstead*[116] leta 1928 do primera *Katz*,[117] torej 39 let, status quo ustrezal preiskovalcem, zato Kongresu v tem času ni uspelo sprejeti zakona, ki bi urejal to področje. Po primeru *Katz*, ki je postavil omejitve preiskovalcem, pa je bil zakonodajni konsenz hitro dosežen. Podobno je pri problemu informacijske zasebnosti, saj trenutno stanje ustreza korporacijam, regulacija na tem področju pa bo skoraj zagotovo prinesla samo omejitve (Gellman, 2001: 207). Zato Burkert ne ugotavlja brez razloga, da "*je videti, kot da sta oglaševanje in trženje med najbolj konservativnimi industrijskimi vejami, če bi sodili po količini denarja, ki sta ga ti dve industriji porabili za izogibanje regulacijskim spremembam*" (Burkert, 2001: 134). Ker sta zbiranje in obdelava osebnih podatkov sprejeta kot nekaj vsakdanjega in imata očitne poslovne prednosti, so zagovorniki omejitev pod velikim pritiskom, da dokažejo upravičenost svojih predlogov (Gellman, 2001: 211). Poleg tega pri prisluškovanju posamezniki veliko jasneje razumejo posledice kot pri zlorabi osebnih podatkov, zakonodaja o prisluškovanju regulira dejavnost majhne skupine vladnih agentov, medtem ko

[116] Olmstead v. United States, 277 U.S. 438 (1928).
[117] Katz v. United States, 389 U.S. 347 (1967).

bi imela regulacija področja informacijske zasebnosti velik vpliv na ekonomijo in veliko število zaposlenih (Gellman, 2001: 207–208). Nadzor je neopazen, potrošniki pa niti nimajo nasprotnih pričakovanj, namreč da bi bilo mogoče življenje tudi brez takega nadzora, saj gre pri teh posegih za ustaljeno prakso (Gellman, 2001: 211). Kljub temu se zdi, da bo razvoj varstva informacijske zasebnosti v Evropi tudi ZDA prisilil k spremembam na tem področju.

Pravica do zasebnosti v Evropi

Za razliko od ZDA je v večini evropskih držav zasebnost ustavna kategorija. Države, ki zasebnosti nimajo omenjene v ustavi, so Avstrija, Francija, Norveška in San Marino. Vendar pa imajo v Avstriji poseben zakon o varstvu osebnih podatkov, katerega del ima ustavni status, v Franciji in na Norveškem pa je ustavno sodišče presodilo, da je pravica do zasebnosti v ustavi omenjena implicitno. Velika Britanija, ki nima pisne ustave, je leta 1998 zaradi skladnosti z *Evropsko konvencijo o človekovih pravicah*,[118] ki so jo sprejele praktično vse evropske države, sprejela *Human Rights Act,*[119] v katerem je omenjena tudi pravica do zasebnosti.

Evropske države, članice Sveta Evrope, razen San Marina, so sprejele tudi *Konvencijo o varstvu posameznikov glede na avtomatsko obdelavo osebnih podatkov.*[120] To pomeni, da imajo večinoma tudi poseben zakon o varstvu osebnih podatkov in vzpostavljen nadzorni organ, ki bdi nad varstvom informacijske zasebnosti. Sicer je res, da se v praksi zakonodaja, predvsem tista, ki zadeva varovanje informacijske zasebnosti, mnogokrat ne upošteva, vendar imajo potrošniki in državljani v Evropi vsaj možnost pritožbe, popravka napačnih podatkov in uporabe drugih pravnih sredstev, to pa v ZDA v zasebnem sektorju ni vedno pravilo.

Poleg tega evropske nadnacionalne institucije (EU, Svet Evrope) težijo k poenotenju varstva zasebnosti v okviru nacionalnih zakonodaj na območju celotne Evrope. Za razliko od ZDA pa se v Evropi vzpostavljajo tudi enotna merila tako za javni kot za zasebni sektor. Zaradi določb Direktive EU 95/46/EC o zaščiti posameznikov glede na avtomatsko obdelavo osebnih podatkov in o svobodnem pretoku teh podatkov[121] iz leta 1995, ki dovoljujejo iznos osebnih podatkov samo v tiste države, v katerih je zagotovljeno ustrezno varstvo osebnih podatkov tudi za tuje državljane, pa se je ustvaril tudi pritisk na druge države, ki niso članice EU, naj sprejmejo ustrezno zaščitno zakonodajo.

---

[118] Svet Evrope. 1950. Evropska konvencija o varstvu človekovih pravic in mednarodnih svoboščin, spremenjena s protokoli št. 3, 5 in 8 ter dopolnjena s protokolom št. 2, ter njeni protokoli št. 1, 4, 6, 7, 9, 10 in 11 (Convention on Human Rights and Fundamental Freedoms as amended by Protocols Nos. 3, 5 and 8 and amended by Protocol No. 2 and its Protocols Nos. 1, 4, 6, 7, 9, 10 and 11), sprejel jo je Svet Evrope leta 1950. Uradni list RS, št. 33/1994, "Mednarodne pogodbe", št. 7/1994, 13. 6. 1994. Konvencijo je državni zbor Republike Slovenije ratificiral 13. 6. 1994. Veljati je začela dne 28. 6. 1994.

[119] Human Rights Act, 1998, Velika Britanija.

[120] Svet Evrope. 1981. Konvencija Sveta Evrope o varstvu posameznikov glede na avtomatsko obdelavo osebnih podatov (Convention for the Protection of Individuals with Automatic Processing of Personal Data), sprejel jo je Svet Evrope 28. 1. 1981. Uradni list RS, Mednarodne pogodbe, št. 3/1994. Konvencijo je državni zbor Republike Slovenije ratificiral dne 25. 1. 1994. Veljati je začela dne 1. 3. 1994.

[121] Direktiva 95/46/EC o varstvu posameznikov pri obdelovanju osebnih podatkov in svobodnem pretoku teh podatkov (Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data), sprejeta 24. oktobra 1995. Official Journal L 281, 23/11/1995 p. 0031 - 0050.

Verjetno je k razvoju varstva informacijske zasebnosti v Evropi (za razliko od ZDA) pripomogla tudi negativna izkušnja totalitarnih režimov, ki je ZDA ni nikoli izkusila tako zelo in na tak način kot Evropa. V knjigi *IBM and the Holocaust* Black prikaže povezavo med tehnologijo, informacijsko zasebnostjo in totalitarizmom. Razvrščanje, katalogizacija in preštevanje podatkov je bilo pred izumom računalnika zelo dolgotrajna naloga, saj je bilo treba vse analize opravljati ročno. Konec 19. stoletja je Herman Hollerith izumil posebno napravo za obdelavo podatkov, ki jo je poimenoval Hollerithov stroj (ang. *Hollerith machine*) in velja za predhodnika računalnika. Hollerithov stroj so najprej uporabili za analizo podatkov v ZDA pri popisu prebivalstva leta 1890. Raba naprave je bila silno učinkovita – ne samo, da so proces obdelave osebnih podatkov skrajšali, temveč so ga celo pocenili, saj so izračuni pokazali, da so pri popisu prihranili okrog pet milijonov dolarjev (Black, 2002: 34). Vendar pa hitrejša in cenejša analiza ni prinesla samo prednosti, temveč tudi nove nevarnosti, ki se jih pred nastankom te tehnologije ni nihče dobro zavedal. Dvanajstega aprila 1933 so namreč v tretjem rajhu začeli popisovati prebivalstvo in si pri tem pomagali s Hollerithovimi stroji. Eden izmed namenov popisa je bil tudi identifikacija judovskega prebivalstva in izdelava načrta za učinkovitejše deportacije in zaplembe premoženja (Black, 2002: 70, 77). Black je v svoji študiji dokazal, da so ob pomoči Hollerithovih strojev nacisti upravljali preskrbo vojske, koncentracijska taborišča, nadzorovali prebivalstvo in vodili skoraj celotno ekonomijo. Zgovorna je tudi primerjava Francije in Nizozemske pod nacistično zasedbo: v obeh državah so nacisti izvedli popis prebivalstva, katerega namen je bil identifikacija judovskega prebivalstva. Vendar so popisovalci v Franciji izvedbo popisa, predvsem pa delovanje Hollerithovih strojev, sabotirali (Hollerithovi stroji so kot nosilce podatkov uporabljali posebne luknjičaste kartice, ki so morale biti iz posebnega papirja in zelo natančno preluknjane, da se stroji niso zaustavljali in mašili). Na Nizozemskem pa je bilo sodelovanje z okupacijskimi oblastmi celo več kot zgledno, saj so na predlog nizozemskega statistika Jacobusa Lambertusa Lentza uvedli celo prve osebne izkaznice na svetu, take s fotografijo, prstnim odtisom in lastnoročnim podpisom posameznika ter oznako, ali je Jud ali ne. Uporaba oziroma neuporaba tehnologije sama po sebi ni edini vzrok za razliko v deležu deportacij judovskega prebivalstva, vendar so številke precej zgovorne: na Nizozemskem so deportirali okrog 73 % Judov, v Franciji pa okrog 25 % (Black, 2002: 372–423). Podobnega mnenja je tudi komisar Flaherty, ki pravi, da je bila v ozadju priprav evropske zakonodaje za zaščito informacijske zasebnosti implicitna želja po preprečitvi vnovičnega vzpona totalitarnih režimov, ki so želeli nadzorovati populacijo, čeprav je bil ta strah le redko izrečen v formalnih razpravah (Cate, 1997: 44).

V Evropi je večina držav podpisala in ratificirala mednarodne akte, ki urejajo varstvo zasebnosti. Najpomembnejši med njimi so *Splošna deklaracija človekovih pravic*,[122] *Mednarodni pakt o državljanskih in političnih pravicah*[123] ter *Evropska konvencija o varstvu človekovih pravic in*

[122] Generalna skupščina Združenih narodov. 1948. Splošna deklaracija o človekovih pravicah (Universal Declaration of Human rights), 10. 12. 1948.

[123] OZN. 1966. Mednarodni pakt o državljanskih in političnih pravicah (International Covenant on Civil and Political Rights), sprejeta v OZN 1966. Uradni list SFRJ, št. 7/1971. Pakt je ratificiral Zvezni zbor skupščine SFRJ 30. 1. 1971. Veljati je začel 12. 2. 1971.

mednarodnih svoboščin.[124] *Splošna deklaracija človekovih pravic* v 12. členu določa, da se "*nikogar ne sme nadlegovati s samovoljnim vmešavanjem v njegovo zasebno življenje, v njegovo družino, v njegovo stanovanje ali njegovo dopisovanje in tudi ne z napadi na njegovo čast in ugled. Vsakdo ima pravico do zakonskega varstva pred takim vmešavanjem ali takimi napadi.*" Enako se glasi tudi dikcija 17. člena *Mednarodnega pakta o državljanskih in političnih pravicah*. *Evropska konvencija o varstvu človekovih pravic in mednarodnih svoboščin* (EKČP), ki velja za najpomembnejši dokument s področja varovanja človekovih pravic in temeljnih svoboščin v Evropi, v 8. členu pravi, da ima vsakdo pravico do spoštovanja svojega zasebnega in družinskega življenja, doma in dopisovanja; posegi v to pravico so možni samo, če je tako določeno z zakonom in nujno v demokratični družbi zaradi državne ali javne varnosti ali ekonomske blaginje države, da se prepreči nered ali zločin, zavaruje zdravje ali morala ali da se zavarujejo pravice in svoboščine drugih ljudi. EKČP pa je sicer pomembna predvsem zato, ker je osnova, po kateri deluje Evropsko sodišče za človekove pravice. Z njegovimi odločbami se ustvarja sodna praksa, ki zelo vpliva na poenotenje obravnavanja človekovih pravic v Evropi, med drugim tudi pravice do zasebnosti.

Da natančne definicije pojma zasebnosti ni mogoče podati, je Evropsko sodišče za človekove pravice poudarilo v primeru *Niemietz proti Nemčiji* leta 1992: "*Sodišče ne smatra, da je mogoče ali nujno poizkusiti podati izčrpno definicijo 'zasebnega življenja'*".[125] To pa ne pomeni, da se sme zasebnost razlagati restriktivno; prav nasprotno, saj je sodišče poudarilo, da se pojma zasebnosti ne zdi smiselno omejiti zgolj na 'notranji krog' posameznika in ob tem popolnoma izključiti vidik vzpostavljanja in razvijanja odnosov z drugimi. To dokazuje, da se tudi v evropski pravni tradiciji zasebnost razume v povezavi z avtonomijo oziroma, da je sodišče v zasebnosti prepoznalo dimenzijo odnosa (ang. *relational dimension of privacy*). Zasebnost torej posamezniku zagotavlja mir pred zunanjim svetom, hkrati pa ščiti razmerja, ki jih ima z drugimi. Orehar Ivančeva pravi, da gre pri pravici do zasebnosti za "*element intimnosti, namenjen svobodnemu razcvetu osebnosti*" (Orehar Ivanc, 2002: 373).

Podobno kot v ZDA tudi v Evropi ESČP meni, da se država v temeljne odločitve posameznika – če seveda ne posegajo v pravice drugih in ne ogrožajo zdravja ali morale – ne sme vpletati, saj so te del zasebnosti. Tako so v primeru *Dudgeon proti Veliki Britaniji*[126] leta 1981 presodili, da je spolno življenje, ki se ne odvija v javnosti (torej ni kršena javna morala), del zasebnosti, in da torej država ne sme prepovedovati homoseksualnosti. Leta 2000 pa so v primeru *A. D. T. proti Veliki Britaniji*[127] presodili, da je vseeno, ali se homoseksualna praksa odvija med dvema ali več posamezniki, saj gre v vsakem primeru zgolj za zasebno ravnanje. Prav tako je sodišče

---

[124] Svet Evrope. 1950. Evropska konvencija o varstvu človekovih pravic in mednarodnih svoboščin, spremenjena s protokoli št. 3, 5 in 8 ter dopolnjena s protokolom št. 2, ter njeni protokoli št. 1, 4, 6, 7, 9, 10 in 11 (Convention on Human Rights and Fundamental Freedoms as amended by Protocols Nos. 3, 5 and 8 and amended by Protocol No. 2 and its Protocols Nos. 1, 4, 6, 7, 9, 10 and 11), sprejel jo je Svet Evrope leta 1950. Uradni list RS, št. 33/1994, "Mednarodne pogodbe", št. 7/1994, 13. 6. 1994. Konvencijo je državni zbor Republike Slovenije ratificiral 13. 6. 1994. Veljati je začela dne 28. 6. 1994.

[125] Niemietz v. ZR Nemčija, odločba z dne 16. 12. 1992.

[126] Dudgeon v. Velika Britanija, odločba z dne 22. 10. 1981.

[127] A. D. T. v. Veliki Britaniji, odločba z dne 31. 07. 2000.

menilo, da je del zasebne sfere tudi odločitev, ali bo posameznik svoje spolne aktivnosti snemal z videokamero (*Modinos proti Cipru*,[128] 1993) (Orehar Ivanc, 2002: 373–374).[129]

Hkrati ESČP pravico do zasebnosti v smislu biti puščen pri miru razume zelo široko – tudi v primerih povzročanja smradu (*Lopez Ostra proti Španiji*,[130] 1994), izpostavljenosti toksičnim emisijam (*Guerra in drugi proti Italiji*,[131] 1998) in hrupu (*Hatton in drugi proti Veliki Britaniji*,[132] 2001). Glede medijskih posegov v zasebnost pa je zelo pomembna odločitev v primeru *Von Hannover proti Nemčiji*[133] iz junija 2004, ko je sodišče razsodilo, da "*javnost nima legitimnega interesa vedeti, kje je pritožnica in kako se obnaša v svojem zasebnem življenju, čeprav se pojavlja na mestih, ki jih ni mogoče opisati kot samotna, ne glede na to, da je javno dobro znana*". Pri tem ESČP ni izpostavilo samo prepovedi, da se država ne sme vmešavati v zasebno življenje posameznika, temveč je poudarilo tudi pozitivno dolžnost države, da posameznika in njegovo zasebnost aktivno zaščiti. S tem se v Evropi vzpostavljajo povsem drugačni temelji varovanja zasebnosti kot v ZDA. Drugačnost evropskega pristopa pri varovanju zasebnosti pa je v primerjavi z ZDA razvidna predvsem na področju varstva informacijske zasebnosti.

Varstvo informacijske zasebnosti v Evropi

V ZDA se je pravica do zasebnosti sprva oblikovala ob sodni praksi, pozneje pa so sprejeli zakone, ki so v posameznih sektorjih urejali varstvo zasebnosti (t. i. sektorski pristop). Sicer je bil zakon, ki ureja varstvo osebnih podatkov, v ZDA sprejet že leta 1977, vendar velja le za javni sektor. V Evropi pa so ubrali povsem drugačen pristop, saj je prvi zakon za zaščito informacijske zasebnosti na svetu, ki je bil sprejet leta 1970 v Nemčiji (v zvezni državi Hesse), postavil enotna merila za javni in zasebni sektor.

Razlogi za sprejem take zakonodaje so bile obsežne družbene reforme, do katerih je v Evropi prišlo po drugi svetovni vojni. Evropske države so začele čedalje bolj postajati države blaginje in to je prineslo s seboj potrebo po pregledu in načrtovanju, vse skupaj pa veliko potrebo po zbiranju in analizi čedalje več podatkov. "*Moderna država blaginje brez računalnikov in zbirk podatkov ne more delovati*", pravi Mayer-Schönberger. Enako je veljalo tudi za povojna podjetja (Mayer-Schönberger, 2001: 222). Zato so v 70. letih 20. stoletja v Evropi nastali

---

128 Modinos v. Cipru, odločba z dne 22.04.1993.

129 Pri tem je zanimivo, da je v primeru *Bowers proti Hardwick* leta 1986 (Bowers v. Hardwick, 478 U.S. 186 (1986)) Vrhovno sodišče ZDA najprej podprlo zakon države Georgije, ki prepoveduje homoseksualne spolne odnose (ang. *anti-sodomy laws*, zakon jih prepoveduje ne glede na to, ali se odvijajo med homoseksualnimi ali heteroseksualnimi pari), leta 2003 pa je v zvezi s svobodo spolnega življenja očitno sprejelo stališče, ki ga je ESČP zavzelo že dobro desetletje pred tem, saj je v primeru *Lawrence proti Texas* (Lawrence v. Texas, 539 US 558 (2003)) presodilo, da so zakoni, ki vsebujejo take prepovedi, v nasprotju z ustavo (Laurant, 2003: 524). Problem vmešavanja države v zasebno oziroma intimno sfero posameznika je zelo dobro povzel Laurence Tribe v debati okrog primera *Bowers proti Hardwick*: "*... ni vprašanje, kaj je Michael Hardwick počel v zasebnosti svoje lastne spalnice, temveč kaj je država Georgija počela tam.*" (Wagner DeCew, 1997: 112).

130 Lopez Ostra v. Španiji, odločba z dne 9. 12. 1994.

131 Guerra et. al. v. Italija, odločba z dne 19. 2. 1998.

132 Hatton in drugi v. Veliki Britaniji, odločba z dne 2. 10. 2001.

133 Von Hannover v. Nemčija, odločba z dne 24. 6. 2004.

načrti za centralizacijo, povezovanje in nastanek velikih zbirk podatkov. Take načrte so imeli že leta 1960 na Švedskem (po tem načrtu naj bi združili zbirke podatkov iz popisa, centralni register prebivalstva ter davčne zbirke, zakon o zaščiti osebnih podatkov pa je bil sprejet leta 1973), pa tudi v nemški zvezni državi Hesse leta 1970 (zaradi odpora proti temu načrtu je bil v tej zvezni državi sprejet tudi prvi zakon o zaščiti informacijske zasebnosti na svetu) in na Bavarskem leta 1972 (računalnike z olimpijskih iger so nameravali uporabiti za vzpostavitev obsežnega informacijskega sistema). Zaradi negativnih izkušenj iz obdobja druge svetovne vojne je bil odpor proti tem načrtom razumljiv, a se je zakonodaja v začetku ukvarjala predvsem z računalniško obdelavo podatkov (Mayer-Schönberger, 2001: 223) in zagotavljanjem točnosti zbranih podatkov (Mayer-Schönberger, 2001: 226). Problem torej ni bil posameznik in njegove pravice, temveč podatki in uporaba računalniške tehnologije.

Toda razvoj tehnologije se je obrnil v drugo smer. Leta 1963 je DEC je razvil prvi miniračunalnik PDP-1 (Digital Equipment Corporation, 1963), ki je bil precej razširjen po univerzah, leta 1975 pa je nastal prvi poceni (stal je 397 dolarjev) miniračunalnik Altair, ki so ga v ZDA prodajali v trgovinah na drobno, zaradi česar je postal široko dostopen (Delaney, 1995).

Z razvojem mikroprocesorskih tehnologij uporaba velikih računalniških sistemov ni bila več ekonomsko upravičena. Nastanek množice majhnih, poceni, a zmogljivih računalnikov je razpravo o zaščiti informacijske zasebnosti obrnil v povsem drugo smer, saj je bilo novo, razpršeno tehnologijo veliko teže nadzirati kot omejeno število kompleksnih in dragih sistemov (katerih upravljanje je povrh vsega za razliko od nove generacije računalnikov zahtevalo večje število visoko specializiranih ljudi). Zaradi nove tehnologije so se v Evropi odločili, da je treba zaščitno zakonodajo razširiti tudi na zasebni sektor, z majhnimi podjetji vred (Mayer-Schönberger, 2001: 225).

Poleg tega so v drugi fazi razvoja informacijske zasebnosti v ospredje stopile pravice posameznika ali, kot pravi Mayer-Schönberger, "*zaščita podatkov kot poskus regulacije tehnologije se je spremenila v individualno svoboščino posameznikov*" (Mayer-Schönberger, 2001: 227). Počasi je postajalo jasno, da niso podatki tisti, ki potrebujejo zaščito, temveč da zaščito potrebuje posameznik. Zato so uvedli nekatere nove pravice: zbiranje podatkov je bilo mogoče le na podlagi zakona ali soglasja posameznika (na Norveškem so npr. v zakon izrecno zapisali, da ima posameznik pravico zavrniti oddajo osebnih podatkov, ki bodo uporabljeni v namene neposrednega trženja ali tržnih raziskav), posamezniki so morali biti obveščeni o namenu zbiranja, imeli so pravico zahtevati spremembo ali celo izbris netočnih podatkov. Hkrati so se pojavili tudi posebni pooblaščenci, katerih naloga je bila skrbeti za izvajanje te zakonodaje, informacijska zasebnost pa je postala ustavna kategorija v Avstriji, Španiji in na Portugalskem (Mayer-Schönberger, 2001: 226–227).

Obenem je prišlo še do enega premika. V 60. in 70. letih 20. stoletja je bila informacijska zasebnost problem večinoma znotraj nacionalnih držav. V 80. letih in pozneje pa je zaradi razvoja in povečane dostopnosti tehnologije informacijska zasebnost postala izrazito mednaroden izziv (Bennett, 2001: 103). Zato je *Organizacija za ekonomsko sodelovanje in razvoj* (OECD) 23.

septembra 1980 sprejela *Smernice za zaščito zasebnosti in čezmejni pretok osebnih podatkov*.[134] V *Smernicah* je izrecno navedeno, da veljajo tako za javni kot za zasebni sektor, uveljavljajo pa načela za pošteno in zakonito ravnanje z osebnimi podatki. Ta so bila pozneje povzeta tudi v drugih mednarodnih dokumentih. *Smernice* v 17. točki tudi izrecno določajo, da je omejitev čezmejnega pretoka podatkov mogoča, kadar država, v katero so namenjeni podatki, ne spoštuje teh *Smernic*. Zaradi tega so *Smernice* ustvarile pritisk na poenotenje oziroma sprejem ustrezne zaščitne zakonodaje in to se je kmalu pokazalo – zaradi 17. člena *Smernic* je namreč leta 1984 Velika Britanija sprejela zakonodajo za zaščito osebnih podatkov (Mayer-Schönberger, 2001: 237). Res pa je, da nekateri kritiki trdijo, da je zasebnost tisto, kar je s *Smernicami* po eni strani pridobila (minimalne standarde varstva), po drugi strani s čezmejnim pretokom osebnih podatkov izgubila (Gutwirth, 2002: 89), saj je bil eden izmed namenov *Smernic* ravno poenotenje zakonodaje zaradi odstranitev ovir čezmejnega pretoka podatkov.

Leto dni pozneje je Svet Evrope sprejel enega najpomembnejših dokumentov s področja varovanja informacijske zasebnosti – *konvencijo o varstvu posameznikov glede na avtomatsko obdelavo osebnih podatkov*.[135] Konvencija, ki je bila pripravljena na podlagi *Smernic OECD*, je jasno izpostavila povezavo med varstvom osebnih podatkov in zaščito zasebnosti posameznika ter problematičnost tehnologije (avtomatska obdelava osebnih podatkov), hkrati pa je določila pravila za zbiranje in obdelavo osebnih podatkov ter izenačila zbirke osebnih podatkov v javnem in zasebnem sektorju.

Konvencija določa, da se smejo osebni podatki uporabljati in shranjevati samo za zakonite namene in pošteno (ang. *fairly*); zbirati se smejo samo podatki, ki so ustrezni in skladni z dosegom namena, za katerega se zbirajo; prepovedano je čezmerno zbiranje osebnih podatkov; upravljavec zbirke osebnih podatkov pa mora zagotoviti njihovo točnost in posodobljenost in jih ne sme hraniti dlje, kot je nujno potrebno za dosego namena, zaradi katerega se zbirajo. Konvencija zahteva tudi obstoj ukrepov, ki bodo zagotovili, da bodo osebni podatki shranjeni za določene in zakonite namene in da se bodo obdelovali le podatki, ki so primerni, ustrezni in niso pretirani glede na namen zbiranja (Čebulj, 2002: 411). Poleg tega konvencija daje posameznikom pravico do seznanitve z obstojem in vsebino osebnih podatkov, ki jih zadevajo, ob morebitnih napakah pa pravico zahtevati popravek ali izbris osebnih podatkov.[136] Podobno

---

[134] OECD. 1980. Smernice za zaščito zasebnosti in čezmejni pretok osebnih podatkov (The OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data), sprejete 23. septembra 1980.

[135] Svet Evrope. 1981. Konvencija Sveta Evrope o varstvu posameznikov glede na avtomatsko obdelavo osebnih podatov (Convention for the Protection of Individuals with Automatic Processing of Personal Data), sprejel jo je Svet Evrope 28. 1. 1981. Uradni list RS, Mednarodne pogodbe, št. 3/1994. Konvencijo je državni zbor Republike Slovenije ratificiral dne 25. 1. 1994. Veljati je začela dne 1. 3. 1994.

[136] Enako pravico sicer daje posameznikom tudi 8. člen EKČP – tako je namreč razsodilo ESČP v primeru *Gaskin proti Veliki Britaniji* iz leta 1989 (Gaskin v. Velika Britanija, odločba z dne 27. 3. 1983; v primeru je šlo za pritožbo Gaskina, ki je bil po smrti matere nastanjen v sirotišnici, pozneje pa mu niso omogočili dostopa do njegove celotne sirotišnične kartoteke), ko je odločalo o pravici posameznika do seznanjanja s tem, kakšni podatki se o njem zbirajo in z vsebino teh podatkov (Čebulj, 2002: 411), vendar to ne velja v vseh primerih. V primerih državne varnosti je namreč mogoča tudi omejitev te pravice. ESČP je leta 1987 v primeru *Leander proti Švedski* (Leander v. Švedska, odločba z dne 26. 03. 1987) obravnavalo pritožbo Thorstena Leanderja, ki ga niso želeli zaposliti v vojaškem muzeju, ker ni prestal varnostnega preverjanja. Leander se je želel seznaniti z vsebino varnostnega preverjanja oziroma z eno izmed informacij, ki jih je vrhovnemu poveljniku švedskih oboroženih sil o njem posredoval *National Police Board*, zaradi katere ni mogel dobiti službe. Sodišče je presodilo, da ne gre za kršitev 8. člena, kar je tudi v skladu s konvencijo Sveta Evrope, ki dopušča določene izjeme, ki pa morajo biti predpisane v zakonu.

kot pri *Smernicah OECD* pa kritiki tudi tu izpostavljajo dejstvo, da namen poenotenja varstva zasebnosti ni toliko varstvo človekovih pravic kot zagotovitev neoviranega pretoka osebnih podatkov (Gutwirth, 2002: 90).

Toda razvoj zaščite informacijske zasebnosti se tu ni ustavil. Naslednji pomemben mejnik je razsodba nemškega ustavnega sodišča iz leta 1983, ki je izpostavila načelo informacijskega samoodločanja (ang. *information self-determination*), sodišče pa je tudi poudarilo, da mora država pojasniti, zakaj potrebuje podatke in kakšne so posledice zavrnitve oddaje osebnih podatkov (Mayer-Schönberger, 2001: 229). Pravica informacijskega samoodločanja je posameznikom tako dala možnost, da se sami odločajo, kako bodo sodelovali v družbi: "*Ni vprašanje, ali nekdo želi sodelovati v družbenih procesih, temveč kako*" (Mayer-Schönberger, 2001: 229). Vendar pa je v praksi začelo prihajati do pojavov, ko so podjetja posameznikom vsiljevala 'bianco soglasje' za kakršnokoli nadaljnjo uporabo osebnih podatkov. Ker je bilo to soglasje pogosto tudi del poslovne pogodbe in brez njega ni bilo mogoče dobiti storitev podjetja, posamezniki pa se nevarnosti take oddaje osebnih podatkov niso zavedali, v praksi pogosto ni bilo prave možnosti izbire. Zato je šlo varstvo informacijske zasebnosti v to smer, da so določena področja informacijske zasebnosti absolutno zaščitena in jih ni mogoče odtujiti. To pomeni, da se posameznik v pogodbi ne more odreči določenim pravicam, prav tako je prepovedano ali vsaj močno omejeno obdelovanje nekaterih občutljivih vrst osebnih podatkov (Mayer-Schönberger, 2001: 232–233). Poleg tega se v zadnjem času – predvsem na podlagi direktiv EU – širijo tudi pristojnosti in pooblastila ter zagotavlja neodvisnost pooblaščencev za varstvo osebnih podatkov. V prihodnosti pa bo verjetno najbolj občutljivo področje, s katerim se bodo ukvarjale evropske države, tehtanje med pravico do zasebnosti in pravico do dostopa do informacij javnega značaja.

S temi dilemami se od sprejetja zakona o dostopu do informacij javnega značaja leta 2003 in posledično uvajanja večje transparentnosti državnih dokumentov spopada tudi Slovenija, tudi na internetu. Prvi odmevnejši primer se je zgodil oktobra 2004, ko je Banka Slovenije na podlagi zakona o plačilnem prometu na svoji spletni strani objavila podatke o vseh imetnikih transakcijskih računov, tudi fizičnih osebah. Podatki – šlo je za ime, priimek in naslov osebe (brez hišne številke), številko računa ter evidenco o neporavnanih obveznostih – so bili dostopni brez omejitev, mogoče je bilo uporabiti tudi iskalnik. Kljub razburjenju, ki ga je povzročila v javnosti objava teh podatkov, pa ta s stališča zakona o varstvu osebnih podatkov[137] ni bila sporna, saj je imela pravno podlago v zakonu o plačilnem prometu. Inšpektor za varstvo osebnih podatkov je kljub temu izdal odločbo, s katero je prepovedal dostop do teh podatkov, saj z neomejeno objavo na internetu ni mogoče zagotoviti sledljivosti posredovanja osebnih podatkov, kot to določa 11. člen ZVOP[138] (Inšpektorat za varstvo osebnih podatkov, 2004). Primer jasno kaže, kakšne dileme prinaša kolizija dveh pravic in kakšne dileme prinaša uporaba novih tehnologij – interneta.

---

[137] Zakon o varstvu osebnih podatkov (ZVOP), Uradni list RS, št. 52/99, 57/01, 59/01-popr., 52/02-ZDU-1 in 73/04-ZUP-C.

[138] Zakon o varstvu osebnih podatkov (ZVOP), Uradni list RS, št. 52/99, 57/01, 59/01-popr., 52/02-ZDU-1 in 73/04-ZUP-C.

Vpliv direktiv EU na varstvo informacijske zasebnosti v Evropi

Kljub temu da je Konvencija Sveta Evrope prvi resnejši poskus poenotenja nacionalnih standardov za zaščito informacijske zasebnosti (načela, ki jih vsebuje ta konvencija, so v taki ali drugačni obliki povzeta tudi v drugih pravnih dokumentih, med drugim tudi v ZDA v *ITF Working Group Principles* (Cate, 1997: 91)), pa je v praksi naletela na nekaj težav. Ena večjih je odsotnost definicije, kaj je ustrezna stopnja zaščite osebnih podatkov (Cate, 1997: 35). Ta problem je skušala rešiti Evropska unija s svojimi direktivami.

Namen direktiv EU o zasebnosti je harmonizacija oziroma uskladitev zakonodajnega varstva zasebnosti v vseh državah članicah. Leta 1995 je EU sprejela *Direktivo o zaščiti osebnih podatkov* 95/46/EC.[139] Prvi osnutek direktive je bil pripravljen že leta 1990, vendar je predvideval drugačno obravnavo osebnih podatkov v javnem in zasebnem sektorju. Leta 1992 pa je evropski parlament sprejel dopolnilo, s katerim je osebne podatke v javnem in zasebnem sektorju izenačil, direktiva pa je bila dokončno sprejeta leta 1995.

Pomen direktive je sicer tudi v tem, da je jasno izpostavila povezavo med zaščito osebnih podatkov in temeljnimi pravicami in svoboščinami posameznika – Cate celo meni, da so stroški izpolnjevanja zahtev direktive (ki se prenašajo na državljane in potrošnike) pravzaprav nekakšen davek, ki je opravičen z visoko vrednostjo, ki jo ima zasebnost (Cate, 1997: 43). Vendar je po drugi strani iz direktive jasno razvidna želja zagotoviti neoviran pretok osebnih podatkov med državami, saj druga točka prvega člena jasno določa, da "*države članice ne smejo omejevati ali prepovedati prostega pretoka osebnih podatkov med državami članicami zaradi razlogov*" zaščite zasebnosti (2. točka 1. člena direktive 95/46/EC[140]).

Ta direktiva ima nekaj pomembnih določil, med drugim se ne nanaša samo na živeče posameznike, dovolj široko definira obdelavo osebnih podatkov, posebno pozornost namenja obdelavi občutljivih osebnih podatkov, predvsem pa v 28. členu zahteva ustanovitev neodvisnega nadzornega organa, ki skrbi za spoštovanje zakonodaje za zaščito zasebnosti. V Sloveniji ima to nalogo *Informacijski pooblaščenec* oz. državni nadzorniki za varstvo osebnih podatkov v okviru tega organa[141] in drugod po Evropi to delo opravljajo specializirane agencije, pooblaščenci (komisarji) ali posebni ombudsmani, ki morajo imeti določeno stopnjo pooblastil. Ta obsegajo predvsem dolžnost vlade, da se s tem organom posvetuje v vseh primerih, ki zadevajo spremembo zakonodaje s področja zasebnosti; ta organ ima pravico do vseh informacij, ki so relevantne za njegove preiskave, lahko prepove obdelavo osebnih podatkov ali uniči nezakonito vzpostavljeno

---

[139] Direktiva 95/46/EC o varstvu posameznikov pri obdelovanju osebnih podatkov in svobodnem pretoku teh podatkov (Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data), sprejeta 24. oktobra 1995. Official Journal L 281, 23/11/1995 p. 0031 - 0050.

[140] Direktiva 95/46/EC o varstvu posameznikov pri obdelovanju osebnih podatkov in svobodnem pretoku teh podatkov (Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data), sprejeta 24. oktobra 1995. Official Journal L 281, 23/11/1995 p. 0031 - 0050.

[141] To velja od sprejetja Zakona o Informacijskem pooblaščencu (ZInfP), Uradni list RS, št. 113/2005. Pred tem je to nalogo opravljal inšpektorat za varstvo osebnih podatkov.

zbirko osebnih podatkov, sprejema in obravnava pritožbe ter pripravlja redna poročila. S tem je EU vzpostavila celovit pravni okvir varovanja informacijske zasebnosti, posledica pa je tudi vzpostavitev opazovanja (monitoringa) tega področja. Ker direktiva prepoveduje iznos osebnih podatkov v države, v katerih ni ustrezne zaščite informacijske zasebnosti, zelo vpliva tudi na zakonodaje držav, ki niso članice EU. Direktiva tako za večino držav, v katerih je to področje neurejeno, pomeni pomemben motiv za sprejem ustreznih zakonov (Laurant, 2003: 15), to pa ne velja povsem za ZDA, ki so ta določila kritizirale, češ da so neprimerno nadležna ter nezdružljiva s postopki v resničnem svetu (EPIC, 2001). Po slovenskem *Zakonu o varstvu osebnih podatkov*[142] iznos osebnih podatkov v ZDA na podlagi starega 24. člena[143] oziroma novega 63. člena (ZVOP-1[144]) ni dovoljen, saj so bile ZDA še v začetku leta 2004 na seznamu držav z neustrezno stopnjo zaščite osebnih podatkov, ki ga je po starem zakonu vzdrževalo slovensko zunanje ministrstvo (Ministrstvo za zunanje zadeve, 2004)). Evropska komisija se ni sicer nikoli formalno izrekla o ne/ustreznosti zaščite informacijske zasebnosti v ZDA, vendar je najela dva ugledna ameriška profesorja prava, Schwartza in Reidenberga, ki sta pripravila analizo zakonodajne zaščite zasebnosti v ZDA. Analiza je pokazala precej pomanjkljivosti (Laurant, 2003: 16).

Iznos osebnih podatkov iz Evropske unije v ZDA

Ker bi take omejitve pretoka osebnih podatkov utegnile škodovati ameriškemu gospodarstvu, so ZDA Evropski uniji predlagale poseben sporazum *Safe Harbor Agreement*. Ta predvideva, da se bodo ameriška podjetja prostovoljno odločila spoštovati načela o zaščiti zasebnosti, ki sta jih pripravila ameriško trgovinsko ministrstvo ter uprava za interni trg Evropske komisije. Tako overjena podjetja bi lahko prejemala osebne podatke iz Evropske unije (Laurant, 2003: 17). Sporazum je bil kljub številnim kritikam julija 2000 sprejet, novembra istega leta pa so ameriškim podjetjem že začeli izdajati certifikate (Laurant, 2003: 17). Kritiki so izpostavljali predvsem to, da sporazum predvideva samo-certificiranje, saj je t. i. "*status safe harbor*" podeljen že s tem, ko se podjetje obveže, da bo spoštovalo načela o zaščiti zasebnosti. Problematična je torej samoregulacija in odsotnost zagotavljanja izpolnjevanja in sistematičnega pregleda izvajanja sprejetih obveznosti (Laurant, 2003: 18).

Čeprav je evalvacijsko poročilo o uspešnosti sporazuma pokazalo, da je sporazum uspešen,[145] pa kot kaže vprašanje pretoka osebnih podatkov med EU in ZDA še ni dokončno rešeno. Dodatno se je namreč zaostrilo z zahtevo ZDA po sporočanju podatkov o letalskih potnikih v ZDA, delno pa tudi z zahtevo ZDA po uvedbi biometričnih potnih listov. Evropska unija je na posredovanje podatkov o letalskih potnikih s posebnim sporazumom med EU in ZDA kljub

---

142 Zakon o varstvu osebnih podatkov (ZVOP-1), Uradni list RS, št. 86/04.

143 Zakon o varstvu osebnih podatkov (ZVOP), Uradni list RS, št. 52/99, 57/01, 59/01-popr., 52/02-ZDU-1 in 73/04-ZUP-C.

144 Zakon o varstvu osebnih podatkov (ZVOP-1), Uradni list RS, št. 86/04.

145 Commission of the European Communities. 2002. Commission Staff Working Paper - The application of Commission Decision 520/2000/EC of 26 July 2000 pursuant to Directive 95/46 of the European Parliament and of the Council on the adequate protection of personal data provided by the Safe Harbour Privacy Principles and related Frequently Asked Questions issued by the US Department of Commerce, 13. 02. 2002.

nasprotovanju Evropskega parlamenta najprej pristala, potem pa je Evropsko sodišče presodilo, da je ta sporazum nezakonit. Na podlagi pozneje razveljavljenega sporazuma je EU v ZDA pošiljala imena in naslove letalskih potnikov ter podatke o njihovih kreditnih karticah; letalska podjetja so ZDA 15 minut po vzletu letala poslala več kot 30 osebnih podatkov o posameznem letalskem potniku. Evropsko sodišče je presodilo, da zaščita osebnih podatkov v ZDA ni ustrezna, zato sporazum nima ustrezne pravne podlage, do konca septembra 2006 pa naj bi EU poiskala ustrezno pravno podlago za tak sporazum (BBC News, 2006a).

Taka odločitev Evropskega sodišča ni presenetljiva, saj je glede sporočanja podatkov o letalskih potnikih *Data Protection Working Party* 29. januarja 2004 izdala mnenje[146], v katerem je izpostavila številne probleme, za katere ameriška stran še ni našla zadovoljivih rešitev. Med drugim so opozorili na to, da namen zbiranja teh podatkov ni dovolj jasno definiran, da ZDA želi zbirati preveč podrobne osebne podatke (med drugim tudi, kakšen obrok hrane potnik naroči na letalu, iz tega pa je v nekaterih primerih mogoče sklepati na religijo), da je predvideni čas shranjevanja podatkov predolg (prvotni predlog za shranjevanje do osem let so pozneje skrajšali na tri leta in pol). Hkrati so opozorili tudi na to, da ameriška stran potnikom ne zagotavlja ustreznih pravic informacijske zasebnosti (vpogled v podatke itd.) ter izrazili negativno stališče do uporabe podatkov v sistemu CAPPS II.[147]

Še hujši pa so bili predlogi glede uporabe biometrije na meji. *Electronic Privacy Information Center* je v zvezi z varovanjem osebnih podatkov tujih državljanov ameriškemu *Ministrstvu za domovinsko varnost* posredoval precej pripomb na program ADIS (*Arrival Departure Information System* – gre za del sistema US-VISIT). EPIC v svoji analizi ugotavlja, da se bo v okviru programa ADIS zbiralo veliko število osebnih podatkov, ti podatki pa ne bodo varovani v skladu z mednarodnimi standardi varovanja informacijske zasebnosti; poleg tega je predvidena doba hranjenja teh podatkov sto let, to pa ni v skladu z zahtevo, da se podatki ne smejo hraniti dlje časa, kot je treba za dosego namena, zaradi katerega so bili obdelovani. EPIC je opozoril predvsem na naslednja neskladja s sprejetimi mednarodnimi standardi: *Ministrstvo za domovinsko varnost* posameznikom, ki niso državljani ZDA, ne bo omogočilo vpogleda v njihove osebne podatke, posameznik ne bo mogel zahtevati popravka napačnih podatkov, ministrstvo pri zbiranju podatkov ne bo omejeno samo na zbiranje tistih osebnih podatkov, ki jih potrebuje za izvajanje svojih zakonskih nalog, temveč bo lahko zbiralo praktično katerekoli podatke. Prav tako ministrstvo ne bo dolžno posamezniku razkriti seznama ustanov in posameznikov, ki jim je posredovalo njegove osebne podatke.

Ker je stopnja varstva informacijske zasebnosti ljudi, ki bodo obravnavani s programom ADIS, bistveno nižja od stopnje varovanja zasebnosti ameriških državljanov, EPIC ugotavlja, da je ta program tudi v neskladju s *Splošno deklaracijo človekovih pravic*,[148] pa tudi z leta 1980 sprejetimi

---

[146] Data Protection Working Party. 2004. Opinion 2/2004 on the Adequate Protection of Personal Data Contained in the PNR of Air Passengers to Be Transferred to the United States' Bureau of Customs and Border Protection (US CBP). 10019/04/EN WP 87.

[147] Sporazum je bil na koncu kljub kritikam sprejet 28. maja 2004 (IDABC, 2004).

[148] Generalna skupščina Združenih narodov. 1948. Splošna deklaracija o človekovih pravicah (Universal Declaration of Human rights), 10. 12. 1948.

Smernicami OECD za zaščito zasebnosti in čezmejni pretok osebnih podatkov[149] ter *Smernicami o avtomatiziranih zbirkah osebnih podatkov*,[150] ki jih je leta 1990 sprejela OZN (EPIC, 2004a).

Komunikacijska zasebnost v Evropi

8. člen EKČP vsakomur priznava tajnost pisem in drugih občil, ki se razlagajo zelo široko, torej kot telefonske komunikacije, elektronska pošta, sporočila SMS itd., saj oblika in vsebina sporazumevanja ni pomembna. Kljub temu imajo v nekaterih državah še težave s prilagajanjem zakonodaje razvoju tehnologije. Na Nizozemskem npr. status elektronske pošte v zvezi s pravico do tajnosti komunikacij ni povsem jasen, zato so leta 2000 začeli pripravljati spremembe ustave (glede na poročilo Privacy & Human Rights 2003 jih parlament še ni obravnaval), po katerih naj bi bila pravica do tajnosti občil zapisana bolj neodvisno od tehnologije[151] (Laurant, 2003: 363).

Seveda pa pravica do komunikacijske zasebnosti ni absolutna, saj je Evropsko sodišče za človekove pravice v primeru *Klaas in drugi proti Nemčiji*[152] leta 1978 zapisalo, da je tajni nadzor telekomunikacij nujno potreben element zagotavljanja nacionalne varnosti (Klemenčič, 2002: 398). Seveda je za to potrebna sodna odredba oziroma zakonska podlaga, vendar je ta v primeru tajnih služb lahko precej široka. V Nemčiji npr. tajna služba Bundesnachrichtendienst (BND) po razsodbi nemškega ustavnega sodišča iz leta 1999 sme prisluškovati mednarodnim komunikacijam avtomatsko in brez sodnega naloga (t. i. *metoda screening*)[153] v primerih preprečevanja terorizma in nezakonite trgovine z orožjem in drogami (Laurant, 2003: 249). Pri vprašanju, ali so zaščitena samo komunikacijska sredstva, ki so v lasti posameznika, ali tudi druga sredstva, pa je sodišče leta 1998 v primeru *Lambert proti Franciji*[154] jasno poudarilo, da ni razlike med lastnim telefonskim priključkom ali telefonskim priključkom tretje osebe; istega leta pa v primeru *Kopp proti Švici*[155] tudi, da so prav tako zaščiteni klici iz poslovnih prostorov ter v poslovne prostore. Prav tako so pred posegi delodajalca zaščitena tudi komunikacijska sredstva, ki jih na delovnem mestu uporablja zaposleni; o tem več v nadaljevanju.

---

[149] OECD. 1980. Smernice za zaščito zasebnosti in čezmejni pretok osebnih podatkov (The OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data), sprejete 23. septembra 1980.

[150] Resolucija Generalne skupščine OZN A/RES/45/95. 1990. Smernice o avtomatiziranih zbirkah osebnih podatkov. (Guidelines for the Regulation of Computerized Personal Data Files), sprejeta v Generalni skupščini OZN 14. decembra 1990.

[151] Zdajšnja dikcija 13. člena nizozemske ustave, ki govori o tajnosti komunikacij, namreč prepoveduje posege v "*zasebnost telefona in telegrafa*".

[152] Klaas et. al v. ZR Nemčija, odločba z dne 6. 9. 1978.

[153] Vendar pa morajo biti iskalni pojmi, ki jih uporabljajo avtomatski iskalniki, odobreni s strani t. i. komiteja G10 (Temporary Committee on the ECHELON Interception System, 2001: 23).

[154] Lambert v. Francija, odločba z dne 24. 8. 1998.

[155] Kopp v. Švica, odločba z dne 25. 3. 1998.

Leta 1997 je bila v EU sprejeta *Direktiva o zasebnosti telekomunikacij* 97/66/EC,[156] leta 2002 pa *Direktiva o zasebnosti in elektronskih komunikacijah* 2002/58/EC.[157] Obe direktivi sta nekoliko bolj konkretizirali varstvo zasebnosti na področju telekomunikacij in elektronskih komunikacij.

Direktiva o zasebnosti in elektronskih komunikacijah 2002/58/EC, na podlagi katere sta bila v Sloveniji sprejeta *Zakon o elektronskih komunikacijah (ZeKOM)*[158] in novela *Zakona o varstvu potrošnikov (ZVPot-A*[159]*),* določa, da komunikacij in z njimi povezanih prometnih podatkov ni dovoljeno shranjevati brez soglasja uporabnika, razen za potrebe prenosa ali upravljanja prometa ter zaračunavanja storitev. Izjema je shranjevanje komunikacij za potrebe dokazovanja komercialnih transakcij, pri čemer pa morajo biti uporabniki predhodno obveščeni o shranjevanju, namenu shranjevanja in trajanju hranjenja. 5. točka 6. člena pa pravi, da smejo prometne podatke obdelovati samo tisti, ki delujejo pod oblastjo ponudnikov storitev; to je posebej pomembno pri oddaji del zunanjim izvajalcem.

Pomembno novost predstavlja tudi razumevanje terminalske opreme uporabnikov kot dela zasebne sfere (24. točka), s čimer direktiva uporabnikovi terminalski opremi daje status zasebnega prostora, v katerem lahko posameznik upravičeno pričakuje zasebnost. 24. točka pa celo govori o vohunskih programih (ang. *spyware*), spletnih hroščih (ang. *web bugs*) in drugih skritih identifikatorskih napravah, ki lahko vstopijo (direktiva uporabi izraz *vstopiti* (ang. *to enter*), kar tudi kaže na razumevanje terminalske opreme kot zasebnega virtualnega prostora, v katerega se vstopa) v uporabniški terminal brez njegove vednosti; pri tem direktiva izrecno poudarja, da smejo biti te naprave (v bistvu gre za računalniške programe) uporabljene le v legitimne namene in z vednostjo uporabnika. Direktiva posebej izpostavlja problem spletnih piškotkov (ang. *cookies*), o katerih več v nadaljevanju; zanje določa, da jih mora imeti uporabnik možnost zavrniti, hkrati pa mora biti seznanjen s tem, kakšne informacije spletni strežnik ob pomoči piškotka shranjuje na njegovi terminalski opremi. S tem je EU skušala vzpostaviti pravni okvir varovanja zasebnosti tudi na internetu.

Iz direktive je viden tudi t. i. evropski pristop pri varovanju informacijske zasebnosti. Direktiva namreč določa, da obdelovanje osebnih podatkov, ki jih zbere ponudnik javno dostopne elektronske komunikacijske storitve za namene trženja brez soglasja uporabnika, ni dovoljeno (torej uveljavlja t. i. pristop *opt-in*), ponudniki storitev pa morajo uporabnike vedno obvestiti o tem, katere podatke obdelujejo, s kakšnim namenom in kakšen je čas shranjevanja teh informacij. 30. točka izpostavlja načelo čim manjšega obsega zbiranja osebnih podatkov, pri čemer je v direktivi zapisano, da morajo biti sistemi za zagotavljanje storitev *zasnovani* tako,

---

[156] Direktiva 97/66/EC o obdelavi osebnih podatkov in varstvu zasebnosti v telekomunikacijskem sektorju (Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector), sprejeta 15. decembra 1997. Official Journal L 024, 30/01/1998 p. 0001 - 0008.

[157] Direktiva 2002/58/EC o obdelovanju osebnih podatkov in varstvu zasebnosti na področju elektronskih komunikacij (Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector), sprejeta 12. julija 2002. Official Journal L 201, 31/07/2002 p. 0037 - 0047.

[158] Zakon o elektronskih komunikacijah (ZeKOM), Uradni list RS, št. 43/04 in 86/04 – ZVOP-1.

[159] Novela Zakona o varstvu potrošnikov (ZVPot-A), Uradni list RS št. 110/02.

da zbiranje osebnih podatkov zmanjšajo na minimum; z drugimi besedami, sistemi morajo biti zasnovani za ščitenje zasebnosti. Tak pristop bi, če bi bil resno upoštevan, utegnil imeti precej daljnosežne posledice, podobno kot so jih imeli ameriški CALEA Act,[160] evropska *Resolucija o zakonitem prestrezanju telekomunikacij* ter poročilo *Delovne skupine za policijsko sodelovanje* iz leta 1995, ki so spodbudili tak razvoj digitalnih telefonskih komunikacijskih naprav, ki so zasnovane za nadzor.

Pomemben korak pa predstavlja tudi odnos do osebnih podatkov, ki se zbirajo in so objavljeni na javno dostopnih imenikih. Direktiva, ki sicer govori o imenikih naročnikov na elektronske komunikacijske storitve, je očitno pisana z mislijo na javne telefonske imenike (v 38. točki celo konkretno omenja telefonsko številko), kljub temu pa je definicija dovolj široko zastavljena, da je mogoče kot javni imenik razumeti ne samo telefonski imenik, temveč tudi imenik elektronske pošte ali pa morda imenik drugih osebnih (kontaktnih) podatkov.

Precej kritik so bila deležna tudi določila o obsegu zbiranja in obveznem shranjevanju prometnih podatkov. Pri tem ne gre za problem varstva in zaupnosti teh podatkov, saj je Evropsko sodišče za človekove pravice leta 1984 v primeru *Malone proti Veliki Britaniji*[161] zapisalo, da so prometni podatki integralni elementi telefonskih komunikacij[162] (iz česar sledi, da jih sme operater telekomunikacij posredovati državnim organom samo na podlagi sodne odredbe ali pristanka naročnika) (Klemenčič, 2002: 403), temveč za načelno vprašanje zapisovanja osebnih podatkov ljudi, ki niso ničesar osumljeni, ob dejstvu, da je mogoče te podatke pozneje uporabiti tudi v morebitnem postopku proti njim.

Novembra 1996 je bila v evropskem uradnem listu objavljena *Resolucija o zakonitem prestrezanju telekomunikacij* (ang. *Resolution on the Lawful Interception of Communications*). V njej je zapisano, da je "*z zakonom podprto prestrezanje telekomunikacij pomembno orodje za zaščito nacionalnega interesa, nacionalne varnosti in preiskovanje resnih kaznivih dejanj*"; podana pa je tudi zbirka podrobnih zahtev, ki jih bodo morala izpolnjevati telekomunikacijska podjetja. Izstopa predvsem to, da resolucija od telekomunikacijskih podjetij zahteva zbiranje velikega števila (osebnih) podatkov, med drugim tudi podatke o lokaciji uporabnika mobilnega telefona. (Council Resolution, 1996: 1–6). Leta 1996 je torej Evropska unija določila nabor prometnih podatkov, ki jih telekomunikacijska podjetja morajo zapisovati v primeru sodne odredbe.

---

160 Communications Assistance for Law Enforcement Act (Digital Telephony Act) of 1994, 47 U.S.C. (1994).

161 Malone v. Velika Britanija, odločba z dne 02. 08. 1984.

162 Na prometne podatke imajo v ZDA nekoliko drugačen pogled, saj so leta 1979 v primeru *Smith proti Maryland* (Smith v. Maryland, 242 U.S. 735 (1979)) presodili, da prometni podatki o telefonskih pogovorih niso zaščiteni s četrtim amandmajem (4. amandma, Listina svoboščin (Bill of Rights), 1791) (Turkington in Allen, 1999: 104-105). S tem so uvedli ločevanje prometnih podatkov od same vsebine komunikacije. Do take obravnave prometnih podatkov v zadnjem času sicer prihaja tudi v Evropi.

Direktiva o zasebnosti in elektronskih komunikacijah[163] iz leta 2002 pa je v 15. členu državam članicam že omogočila shranjevanje prometnih podatkov za določen čas. Na podlagi tega člena so imele države članice EU možnost operaterjem mobilne telefonije predpisati rok obveznega shranjevanja prometnih podatkov.[164] Hraniti so se smeli tudi podatki o lokaciji uporabnika, ki se štejejo med prometne podatke, čeprav nekateri pravni strokovnjaki opozarjajo, da bi t. i. lokacijska zasebnost zaslužila enako pravno varstvo kot sama vsebina komunikacije (Možina, 2002: 5).

Kmalu po sprejemu direktive 2002/58/EC pa so se razširile ideje o obvezni hrambi prometnih podatkov. EU je pri tem izhajala iz bojazni, da "*se zaradi spremembe tehnologije, poslovnih modelov in ponujenih storitev (npr. enotne tarife za uporabo storitev (ang. flat rate, predplačniške in brezplačne elektronsko komunikacijske, storitve elektronska pošta, sporočila SMS in MMS) ... nekateri prometni podatki ne shranjujejo v takem obsegu kot v preteklih letih. Ti prometni podatki zato niso dostopni oblastem, kadar jih potrebujejo.*" (DG Information Society and DG Justice and Home Affairs, 2004).

Sprejemanje *Direktive o obvezni hrambi prometnih podatkov*[165] so spremljali številni protesti in zapleti, saj sta direktivi nasprotovala tako posebna *Alvarova komisija*, ki je predlog zavrnila (Alvaro, 2005), kot tudi Evropski parlament. Kljub temu je bila *Direktiva o obvezni hrambi prometnih podatkov*[166] decembra 2005 sprejeta, aprila 2006 pa tudi objavljena v uradnem listu EU. Če je bilo v prejšnjih direktivah shranjevanje prometnih podatkov prepovedano, oziroma dovoljeno le kot izjema, pa je direktiva 2006/24/ES to pravilo povsem obrnila na glavo. Zahteva namreč obvezno hrambo prometnih podatkov telefonskih in internetnih komunikacij (z naslovi elektronske pošte vred) ter podatkov o lokacijah mobilnih telefonov; čas hrambe traja od 6 do 24 mesecev, v nekaterih primerih pa tudi več, poleg tega direktiva ne omejuje, za katera kazniva dejanja je mogoče shranjene podatke uporabiti.

---

163 Direktiva 2002/58/EC o obdelovanju osebnih podatkov in varstvu zasebnosti na področju elektronskih komunikacij (Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector), sprejeta 12. julija 2002. Official Journal L 201, 31/07/2002 p. 0037 - 0047.

164 V Sloveniji je zaznavanje lokacije mobilnih telefonov od leta 2003 zahteval *Pravilnik o programski opremi in vmesnikih za zakonito prestrezanje komunikacij* (4. člen, 6. točka), ki je bil 13. avgusta 2003 objavljen v Uradnem listu RS št. 73/03. *Pravilnik o opremi in vmesnikih za zakonito prestrezanje komunikacij*, ki je bil sprejet leta 2006 in ki je nadomestil starejši pravilnik, pa glede zaznavanja lokacij vsebuje enake določbe.

165 Direktiva 2006/24/ES Evropskega parlamenta in Sveta z dne 15. marca 2006 o hrambi podatkov, pridobljenih ali obdelanih v zvezi z zagotavljanjem javno dostopnih elektronskih komunikacijskih storitev ali javnih komunikacijskih omrežij, in spremembi Direktive 2002/58/ES (Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC), sprejeta 14. 12. 2005. Official Journal L 105, 13/04/2006, p. 0054 - 0063.

166 Direktiva 2006/24/ES Evropskega parlamenta in Sveta z dne 15. marca 2006 o hrambi podatkov, pridobljenih ali obdelanih v zvezi z zagotavljanjem javno dostopnih elektronskih komunikacijskih storitev ali javnih komunikacijskih omrežij, in spremembi Direktive 2002/58/ES (Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC), sprejeta 14. 12. 2005. Official Journal L 105, 13/04/2006, p. 0054 - 0063.

Že iz direktive 2002/58/EC je bilo moč razbrati tudi poskus monopolizacije nadzornih sistemov s strani držav in omejevanje predvsem nadzora, ki ga izvajajo zasebna podjetja. Direktiva je namreč vključevala ukrepe za zavarovanje telekomunikacijskih omrežij ter zagotavljanje tajnosti komunikacij (npr. prepoveduje uporabo vohunskih programov (ang. *spyware*) brez soglasja, sledenje mobilnim telefonom, razen kadar te informacije potrebujejo reševalne službe ali policija itd.). Ti ukrepi večinoma zadevajo zasebni sektor, saj je za izvajanje takega nazora potrebno soglasje posameznika. Po drugi strani pa je od operaterjev telekomunikacij v primeru zakonitega prestrezanja komunikacij zahtevala zbiranje in shranjevanje podatkov na lastne stroške (podobno je tudi v Sloveniji, 130. člen *Zakona o telekomunikacijah*[167] od operaterjev zahteval, naj na lastne stroške zagotovijo ustrezno programsko opremo in primerne vmesnike za nadzor telekomunikacijskega prometa, po uveljavitvi *Zakona o elektronskih komunikacijah*[168] leta 2004 pa je tako določilo zapisano v 107. členu). To pomeni, da se stroški zakonitega prestrezanja komunikacij prenašajo na zasebne operaterje.[169] Vprašanje stroškov hrambe prometnih podatkov je bilo pomembno vprašanje tudi pri sprejemanju *Direktive o obvezni hrambi prometnih* podatkov,[170] na koncu pa je obveljalo, da povračilo stroškov operaterjem, nastalih zaradi obvezne hrambe prometnih podatkov, ureja vsaka država po svoji presoji.

Zasebnost na delovnem mestu

Glede pravice do zasebnosti na delovnem mestu v evropski pravni ureditvi sicer vlada še nekaj nejasnosti (predvsem manjka določitev najnižje zahtevane stopnje varstva zasebnosti, podobno kot pri informacijski zasebnosti). Vsekakor pa je zasebnost na delovnem mestu v razvitih evropskih državah precej bolje zaščitena kot v ZDA, saj načeloma velja obveznost delodajalca, da zaposlene vsaj obvesti o možnosti nadzora na delovnem mestu, poleg tega je v primeru nadzora komunikacij dovoljen samo tisti nadzor, ki se nanaša na delo.

---

167 Zakon o telekomunikacijah (ZTel), Uradni list RS, št. 30/01, 52/02-ZJA, 110/02-ZGO-1 in 43/04-ZEKom.

168 Zakon o elektronskih komunikacijah (ZeKOM), Uradni list RS, št. 43/04 in 86/04 – ZVOP-1.

169 Tako prenašanje stroškov na pleča operaterjev med le-temi razumljivo povzroča veliko nezadovoljstvo, tudi v Sloveniji. Prenašanje stroškov za zakoniti nadzor na operaterje je v razsodbi z dne 27. februarja 2003 problematiziralo tudi avstrijsko zvezno ustavno sodišče, ki je razsodilo, da je avstrijski zakon, ki od ponudnikov telekomunikacijskih storitev zahteva, da državi omogočijo prestrezanje komunikacij na lastne stroške. neustaven (Schröder in Laurant, 2005). O tem problemu nekoliko več v nadaljevanju.

170 Direktiva 2006/24/ES Evropskega parlamenta in Sveta z dne 15. marca 2006 o hrambi podatkov, pridobljenih ali obdelanih v zvezi z zagotavljanjem javno dostopnih elektronskih komunikacijskih storitev ali javnih komunikacijskih omrežij, in spremembi Direktive 2002/58/ES (Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC), sprejeta 14. 12. 2005. Official Journal L 105, 13/04/2006, p. 0054 - 0063.

Prav tako so delodajalci omejeni tudi pri zastavljanju osebnih vprašanj. ESČP je leta 1999 obravnavalo dva primera odpusta homoseksualcev iz britanske vojne mornarice. Za Lustig-Preana je leta 1994 Royal Navy Special Investigations Branch ugotovila, da je homoseksualec, zato so ga poklicali na zaslišanje. Tam je svojo spolno usmeritev priznal, zato je bil po nadaljnji preiskavi proti njemu leta 1995 odpuščen. Enako se je zgodilo Beckettu, ki je svojemu duhovniku priznal svojo spolno usmeritev, pozneje pa je bil o tem vprašanju poklican na zaslišanje k poveljniku. Sodišče je v primeru *Lustig-Prean in Beckett proti Veliki Britaniji*[171] presodilo, da spraševanje delodajalca o spolni usmeritvi zaposlenega predstavlja poseg v zasebnost. Podobno sicer velja tudi v ZDA (tam je v vojski uveljavljeno načelo "*ne sprašuj, ne povej*" – "*don't ask, don't tell*"), vendar je Vrhovno sodišče ZDA v primeru *Able proti Združenim državam*[172] leta 1998, ko je posameznik na svojem delovnem mestu sam izjavil, da je homoseksualec, in so ga zato odpustili, menilo, da je vojska ravnala zakonito. Ameriško Vrhovno sodišče je obrazložilo, da je "*bistvo vojaške službe podrejanje želja in interesov posameznikov potrebam vojske*", prepoved homoseksualnosti pa ni sporna, ker "*pospešuje kohezivnost enote, povečuje zasebnost in zmanjšuje seksualne napetosti*" (Turkington in Allen, 1999: 739); s tem so zavzeli skoraj povsem nasprotno stališče kot ESČP.

V Evropi so torej sodišča, kar zadeva zasebnost komunikacij na delovnem mestu, bolj naklonjena zaposlenim kot v ZDA (Klemenčič, 2003: 137). V zvezi z nadzorom na delovnem mestu sta verjetno najpomembnejši odločitvi Evropskega sodišča za človekove pravice *Halford proti Veliki Britaniji*[173] iz leta 1997 v zvezi s kršitvijo 8. člena EKČP ter odločitev Kasacijskega sodišča Francije v primeru *Societe Nikon France, SA v. Onof* iz leta 2001. V primeru *Halford proti Veliki Britaniji*, v katerem je policija nadzorovala službeni telefon svoje uslužbenke (z namenom, da bi zbrala gradivo za svojo obrambo v postopku zaradi diskriminacije), je ESČP izrecno zapisalo, da zaposleni na delovnem mestu upravičeno pričakuje zasebnost.

Tudi v Sloveniji se je Ustavno sodišče RS večkrat postavilo na stran pravice do zasebnosti. Na zasebnost na delovnem mestu pa bo verjetno zelo vplivala tudi odločba Up-472/02 iz oktobra 2004, s katero je Ustavno sodišče RS sicer odločalo o snemanju pogovora s strani zasebnika in uporabi tega posnetka v poznejšem civilnem sodnem postopku. Sodišče je zapisalo: "*Poseg v pravico do zasebnosti bi bil pod določenimi pogoji dopusten, vendar bi morale biti v pravnem postopku za izvedbo dokaza, pridobljenega s kršitvijo pravice do zasebnosti, posebej utemeljene okoliščine. Izvedba takega dokaza bi morala imeti poseben namen za izvrševanje neke ustavno zavarovane pravice. V takem primeru mora sodišče upoštevati načelo sorazmernosti in skrbno prisoditi, kateri pravici je treba dati prednost.*"

Po mnenju sodišča namreč: "*Posnetka oziroma tonskega zapisa telefonskega pogovora tudi ni mogoče enačiti z zapiski o pogovoru. Gre namreč za bistveno kakovostno razliko... Kot je bilo že poudarjeno, daje tonski zapis oblast nad tujo osebo oziroma njeno osebno dobrino, ker omogoča*

---

171 Lustig-Prean in Beckett v. Velika Britanija, odločba z dne 27. 09. 1999.
172 Able v. United States, 155 F.3d 628 (1998).
173 Halford v. Velika Britanija, odločba z dne 25. 6. 1997.

ponovitev (vnovično predvajanje). Če je torej to storjeno brez vednosti prizadete osebe, je s tem poseženo v izključno pravico osebe, da sama razpolaga s svojo besedo oziroma z glasom.".[174] S tem je tudi slovenska sodna praksa poudarila obstoj kvalitetnega preskoka, ki ga je v nadzorovanje prinesla tehnologija, in s tem pomena pravic posameznika v visoko tehnološki družbi.

Odločitev francoskega Kasacijskega sodišča v primeru *Societe Nikon France, SA v. Onof*, št. 99-42.942 z dne 2. 10. 2001 pa izrecno pravi, da "*delodajalec, ki bere sporočila, ki jih zaposleni pošilja ali sprejema prek službenega računalnika, krši temeljne pravice delavca, kot jih določa 8. člen Evropske konvencije o človekovih pravicah... To velja ne glede na to, ali je bil delavec vnaprej seznanjen, da službenega računalnika ne sme uporabljati v neslužbene namene... Podjetje ali druge ustanove ne smejo biti mesta, na katerih bi delodajalci arbitrarno in brez omejitev izvajali svoje diskrecijske pravice; ne smejo postati okolja totalnega nadzora, v katerih temeljne človekove pravice nimajo veljave... Menimo, da je splošna popolna prepoved uporabe e-pošte v neslužbene namene nerealna in krši pravno načelo sorazmernosti.*" (Klemenčič, 2002: 402.)

Klemenčič tako ugotavlja, da "*se domet pravice do komunikacijske zasebnosti ne ustavi zgolj pri zagotavljanju zaupnosti vsebine sporočanja in podatkov, povezanih z njo, ampak hkrati prepoveduje tudi nesorazmerne prepovedi komuniciranja z zunanjim svetom*" (Klemenčič, 2002: 395). Priporočilo Sveta Evrope št. R(89) 2[175] namreč določa, da imajo zaposleni na delovnem mestu pravico do vzpostavljanja osebnih in socialnih stikov. Podobnega mnenja je bilo tudi ESČP v primeru *Niemietz proti Nemčiji*[176] leta 1992, ko je zapisalo da *"spoštovanje zasebnega življenja mora vsebovati tudi določeno stopnjo pravice do vzpostavljanja in razvijanja odnosov z drugimi človeškimi bitji"* in *"Poleg tega se zdi, da ni načelnega razloga, zakaj bi ta pojem 'zasebnega življenja' izključeval profesionalne ali poslovne dejavnosti [posameznika]..."*

Poleg tega bi nadzor s strani delodajalca lahko kršil tudi interes tretjih oseb, ki komunicirajo z zaposlenim in morda niti ne vedo, da gre za službeno komunikacijsko sredstvo in da delodajalec nadzoruje komunikacije zaposlenega, s katerim so v stiku (Klemenčič, 2001: 188–189). Ta problem je zelo očiten pri morebitnem nadzorovanju službenih mobilnih telefonov, kjer je možnosti za razlikovanje med službenim in zasebnim komunikacijskim sredstvom še manj. Tudi tu se je slovenska sodna praksa postavila na stran posameznika, saj je Upravno sodišče RS sprejelo odločitev, s katero je zaposlenemu priznalo pravico do varstva zasebnosti pri uporabi službenih mobilnih telefonov (Klemenčič, 2003: 137).

Zaradi zgoraj neštetih razlogov bi tudi vsak poseg države, ki bi nesorazmerno prepovedal uporabo kriptografije ali anonimnih poštnih strežnikov, lahko pomenil poseg v ustavno zajamčeno komunikacijsko zasebnost (Klemenčič, 2002: 395). To je ugotovitev, ki je v kontekstu ameriških poizkusov omejevanja uporabe kriptografije za Slovenijo še kako pomembna.

---

[174] Odločba Ustavnega sodišča RS, št. Up-472/02, Uradni list RS, št. 114/2004.

[175] Svet ministrov Sveta Evrope. 1989. Priporočilo Sveta Evrope št. R(89) 2 o varstvu osebnih podatkov, uporabljanih za zaposlovanje (Recommendation No. R (89) 2 on the protection of personal data used for employment purposes), sprejeto 18 januarja 1989.

[176] Niemietz v. ZR Nemčija, odločba z dne 16. 12. 1992.

Boj za pravico do zasebnosti

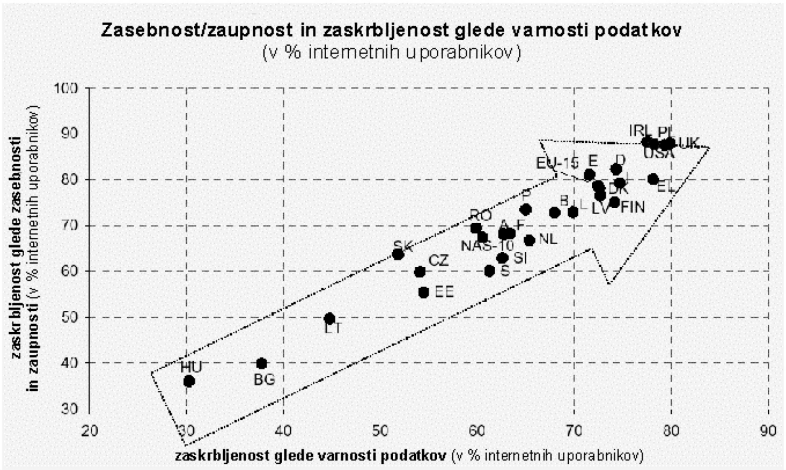
Zaradi težavnosti definicije zasebnosti in hitrega tehnološkega razvoja je predvsem v ZDA opaziti številne pomanjkljivosti in nedoslednosti pri zakonodajni zaščiti zasebnosti (Agre, 2001: 6); še težje pa je z usklajevanjem mednarodnega varstva zasebnosti. Bennett ugotavlja, da je ogroženost zasebnosti težje merljiva kot ogroženost okolja, zato se države tudi težje sporazumejo o še sprejemljivem nivoju ogrožanja zasebnosti na podoben način, kot se lahko sporazumejo o še sprejemljivem nivoju strupov v okolju. Res pa je, da se to utegne spremeniti, saj direktive EU predstavljajo pomemben korak k usklajevanju zaščite zasebnosti na meddržavni ravni. Zaradi nemotene čezmejne izmenjave osebnih podatkov se tudi na ZDA ustvarja pritisk za povečanje stopnje varstva informacijske zasebnosti v zasebnem sektorju. Kljub temu je samo na podlagi sprejete zakonodaje in uveljavljenih politik zaščite zasebnosti težko ugotoviti, kakšna je dejanska stopnja zaščite zasebnosti v posamezni državi (Bennett, 2001: 119). Razlog za to je predvsem globalizacija pretoka podatkov, ki jih omogočajo sodobne informacijske tehnologije, pa tudi subjektivno dojemanje zasebnosti, ki se v različnih kulturah razlikuje.

Ker je zasebnost pravica, in to pogosto pravica posameznika nasproti državi, ne preseneča, da se z zasebnostjo ukvarjajo tudi nevladne in aktivistične organizacije. Vprašanje zasebnosti je bilo resno politično vprašanje v 70. letih 20. stoletja (Davies, 2001: 148). Takrat se je v Evropi dvignilo močno gibanje proti popisu prebivalstva, ki je bilo najmočnejše na Nizozemskem (to glede na izkušnjo s popisom in posledicami popisa, ki so ga izvajali med nacistično okupacijo, verjetno ni naključno). Iz tega gibanja se je v poznih osemdesetih letih oblikovala organizacija *Privacy Alert* (*Stichting Waakzaamheid Persoonregistratiie*), ki je za dvajset let postala največja nevladna organizacija za varstvo zasebnosti v svetovnem merilu. Vendar pa je leta 1994 organizacija nehala delovati, in to ravno v času, ko je Nizozemska začela uvajati schengenski sistem nadzora meja, osebne izkaznice in identifikacijske številke za prebivalstvo (Davies, 2001: 154). Podobno se je zgodilo tudi drugim organizacijam, npr. *New Zealand Privacy Foundation*, *Australian Privacy Foundation* in *Canadian Privacy Council*, ki je propadel že praktično takoj po ustanovitvi (Davies, 2001: 154–155). Edina izjema je pravzaprav *Electronic Privacy Information Center* (EPIC) iz Washingtona, ki še deluje in trenutno združuje strokovnjake in aktiviste s področja zasebnosti z vsega sveta. (Sodeluje tudi s *Privacy International*, katere vpliv pa je bistveno manjši, in z *Electronic Frontier Foundation* ter *American Civil Liberties Union*, ki pa se ukvarjata tudi z drugimi temami.)

Pravzaprav gre za gibanje, ki je večinoma neistitucionalizirano (gre bolj za mrežo posameznikov, ki med seboj komunicirajo po internetu) in se aktivira le občasno, ob kriznih dogodkih, ki ogrožajo zasebnost; zato se zdi, da gibanje zamira. Razlogi za to so številni, izpostaviti pa je treba nekaj dejstev. Najprej se zdi, da zasebnost ni več resno politično vprašanje, saj se praviloma ne pojavlja v volilnih programih političnih strank, poleg tega v razmerju zasebnost proti varnosti po 11. septembru 2001 prevladuje strah pred terorizmom. Drugi razlog je verjetno tudi institucionalizacija varstva zasebnosti. Evropske države pa tudi nekatere druge, ki sprejemajo evropski model (npr. Kanada), so uvedle posebne pooblaščence oziroma varuhe

pravic zasebnosti, ki se s področjem varstva zasebnosti ukvarjajo profesionalno, prav tako se z varstvom zasebnosti na določenem segmentu ukvarjajo profesionalno tudi strokovnjaki za informacijsko varnost. Verjetno največji problem pa je odnos posameznikov do zasebnosti.

Številni avtorji (Sykes, 1999: 11, Davies, 2001: 147, Agre, 2001: 6 itd. ...) so ugotovili, da je stopnja podpore zasebnosti v javnomnenjskih anketah v ZDA in Avstraliji precej visoka. Raziskava GVU iz leta 1997 je pokazala, da v ZDA anketiranci med najbolj kritičnimi vprašanji interneta postavljajo na prvo mesto zasebnost (Georgia Tech Research Corporation, 1997b). Leto prej je bila zasebnost na drugem mestu (Georgia Tech Research Corporation, 1997a). Raziskava PEW Internet & American Life iz leta 2000 je prav tako pokazala, da so Američani zelo zaskrbljeni zaradi vdorov v zasebnost (The Pew Internet & American Life Project, 2000: 10), podobno kažejo tudi ankete v Evropi. Primerjalna evropska raziskava SIBIS je pokazala, da so prebivalci evropskih držav na splošno precej zaskrbljeni zaradi zasebnosti, čeprav je strah pred vdorom v zasebnost v celinski Evropi manjši kot v Veliki Britaniji, na Irskem in v ZDA (Empirica, 2003: 29). Podobno stanje je v Sloveniji pokazala raziskava RIS 98 - WWW, po kateri je bila po mnenju anketirancev zasebnost na petem mestu med najbolj perečimi, kritičnimi vprašanji, s katerim se spopada internet, na drugem mestu pa je bila varnost transakcij.



Graf 1: Zaskrbljenost posameznikov glede zasebnosti in zaupnosti na internetu ter zaščite podatkov po posameznih državah (vir: Vehovar, Jovan in Kragelj, 2003: 31).

Videti je torej, da so posamezniki precej zaskrbljeni glede zasebnosti in da jim zasebnost pomeni neko vrednoto. Vendar se izkaže, da to velja samo na načelni ravni. Praksa namreč pokaže skoraj popolno odsotnost mobilizacije za zaščito zasebnosti ter odsotnost zaščitnih praks oziroma takega ravnanja posameznikov, ki bi čim bolj zmanjšalo možnost vdorov v zasebnost. Očitno se posamezniki sicer zavedajo ogroženosti zasebnosti na načelni ravni, vendar na te grožnje oziroma na nadzor pristajajo in se niti ne poskušajo zaščititi – pogosto tudi na škodo udobja in zaradi neznanja. Ker večina nadzora danes poteka skrito, hkrati pa je nadzor nujen za, kot pravi Foucault, "omogočanje življenja", torej za participacijo v sodobni družbi in državi blaginje, ga posamezniki sprejemajo. Problematiziran je le, ko pride do zlorabe, pri čemer pa mora biti povezava med nadzorom in zlorabo očitna.

Jeffrey Rosen[177] je ta učinek v intervjuju za Wired News opisal takole: "*To, kar ljudi skrbi, ni zasebnost kot taka, temveč nadzor nad okoliščinami njihovega razkritja. Isti ljudje, ki pravijo, da so zaskrbljeni zaradi možne zlorabe njihovih marketinških podatkov, so si popolnoma voljni namestiti spletno kamero (ang. webcam) ali pisati dnevnik na internetu (ang. blog). In isti ljudje, ki se upirajo nadzornim kameram, bodo morda precej voljni zaupati svoje osebne podatke neposrednemu trženju na podlagi predpostavke, da bodo za to dobili ustrezno nagrado. To je navidezen občutek nazora... Pogosto se nevarnosti oddaje svojih osebnih podatkov zavedo šele, ko pride do zlorabe, takrat pa je že prepozno.*" (Zetter, 2004b).

Danes se aktivisti gibanja za elektronsko zasebnost ukvarjajo predvsem s tistimi vprašanji varstva zasebnosti, ki niso institucionalizirana, torej s področji zlorab, ki jih ne preganjajo državni organi (zaradi pomanjkljive zakonodaje ali pa zaradi omejitev, ki izhajajo iz teritorialne pristojnosti zakonodaje), in s problemi informacijske varnosti ter z nevarnostmi, ki jih prinašajo nove tehnologije. Povezujejo se in sodelujejo prek interneta (tipičen primer je EPIC, ki izdaja letno poročilo o zasebnosti, pripravljajo pa ga strokovnjaki z vsega sveta, ki med seboj komunicirajo praktično samo po internetu), ukvarjajo pa se tako s spremembami zakonodaje kot s spremljanjem nevarnosti, ki jih prinašajo nove tehnologije. Zato se čedalje bolj ukvarjajo tudi s problemi zasebnosti na internetu. Ključna točka boja za zasebnost na internetu oziroma boja za komunikacijsko zasebnost na splošno pa je boj za svobodno uporabo kriptografije. Pravzaprav se je problem zasebnosti na internetu vzpostavil ravno ob vprašanju kriptografije. Dileme, ki so se ob tem zastavile, pa so povzročile nastanek gibanja za elektronsko zasebnost.

[177] Jeffrey Rosen je leta 2004 napisal knjigo *The Naked Crowd*, v kateri je analiziral odnos Američanov do zasebnosti v razmerju do varnosti po 11. septembru 2001.

KRIPTOGRAFIJA IN GIBANJE ZA ELEKTRONSKO ZASEBNOST

Kot že rečeno, sodobna informacijsko-komunikacijska tehnologija omogoča številne posege v zasebnost, saj je pogosto že zasnovana za nadzor. Vendar pa tehnologija posameznikom tudi omogoča, da se izognejo nadzorovanju. A podobno kot pri primerjavi Benthamove ideje Panoptikona in načela publicitete v delovanju politične skupščine, lahko tudi pri tehnologiji ugotovimo, da je ta večinoma uporabljena za nadzor posameznikov, ne pa toliko za njihovo zaščito pred nadzorom. Uporabo tehnologij, ki onemogočajo nadzor, skušajo države in njeni represivni organi sistematično omejevati, zato je ta tehnologija dostopna le manjšemu številu posameznikov, ki si uporabo teh tehnologij uspejo izboriti. Ena takih tipičnih tehnologij je kriptografija, katere uporabo so skušale države pravno in dejansko omejevati, njeni zagovorniki pa so bili deležni številnih očitkov oziroma družbenih pritiskov, češ da kriptografija pomaga pri skrivanju kriminalcev in teroristov. Primer kriptografije in gibanja za elektronsko zasebnost tako kaže, da je uporaba tehnologij, ki posamezniku omogočajo, da se izogne nadzoru, v praksi zelo omejena in celo velja za družbeno nezaželeno, vendar to ne velja za tehnologije, namenjene nadzoru. Uporaba teh je zelo razširjena in navadno velja za družbeno povsem sprejemljivo.

Kriptografija

Informacije, ki potujejo po internetu in elektronskih omrežjih (npr. telefonskem omrežju) ali so shranjene na internetu, so zaradi narave samega kiberprostora, v katerem ni fizičnih ovir in ki v osnovi ni odporen proti prestrezanju, bolj izpostavljene različnim zlorabam, kot so informacije v fizičnem prostoru. Poglavitni razlog za to je globalizacija interneta in povečana dostopnost, o čemer več v nadaljevanju. Tem nevarnostim se je mogoče izogniti z uporabo kriptografije.

Kriptologija (beseda izvira iz grškega izraza *kryptos logos*, ki pomeni skrita beseda, prvi pa jo je v angleščini uporabil sir Thomas Browne leta 1658 (Kahn, 1973: 432)), je veda o tajnosti, šifriranju, zakrivanju vsebine sporočil (kriptografija) in o razkrivanju šifriranih podatkov (kriptoanaliza). S kriptografijo ne moremo preprečiti prestrezanja, lahko pa preprečimo, da bi prisluškovalec prišel do vsebine sporočila, s tem pa prestrezanje postane neuporabno.

V kriptografiji imenujemo temeljno sporočilo čistopis (ang. *cleartext*, *plaintext*), zašifrirano pa šifropis ali tajnopis (*kriptogram*, *ciphertext*). Čistopis po nekem postopku (algoritmu, metodi) spremenimo v tajnopis, pri tem pa uporabimo neke vrednosti za parametre v šifrirnem algoritmu. Tem vrednostim pravimo ključ ali geslo. Sogovornika se morata torej dogovoriti o algoritmu in o ključu, da si lahko pošiljata šifrirana sporočila.

Z vidika šifrirnega in dešifrirnega ključa poznamo dve vrsti kriptografije: *simetrično*, ki za šifriranje in dešifriranje sporočila uporablja isti ključ (isto geslo), in *asimetrično*, pri kateri je ključ za šifriranje različen od ključa za dešifriranje. Asimetrični šifrirni algoritem namreč predvideva, da imata pošiljatelj in prejemnik vsak svoj par ključev, javnega, ki je javno objavljen, in zasebnega, ki ga obdržita v tajnosti. Za pošiljanje šifriranega sporočila potrebuje pošiljatelj naslovnikov javni ključ in svoj zasebni ključ, prejemnik pa potrebuje pošiljateljev javni ključ in

svoj zasebni ključ. Javni ključi so torej javno objavljeni (pravzaprav to morajo biti), zasebne ključe pa posamezniki obdržijo zase; s tem odpade potreba po t. i. varnih kanalih za prenos šifrirnih ključev, kar je potrebno pri simetrični kriptografiji.

Poleg simetričnih in asimetričnih algoritmov poznamo tudi zgostitvene algoritme (ang. *hash algorithms*, včasih tudi *message digests* ali *fingerprints*),[178] ki poljubno dolg niz znakov preslikajo v število fiksne dolžine. To pomeni, da izračunajo t. i. prstni odtis (ang. *fingerprint*) tega niza znakov, kar je osnova za digitalni podpis (ang. *digital signature*) oziroma za zagotovilo, da sporočilo med prenosom ni bilo spremenjeno. Z uporabo kombinacije kriptografskih metod, metod za digitalno podpisovanje in z uporabo potrdil (ang. *certificate*), ki vsebujejo npr. čas nastanka, podatke o lastniku, rok veljavnosti ipd., lahko zagotovimo zaupnost (ang. *confidentiality*), celovitost (ang. *integrity*) in overjanje (ang. *authentication*) sporočila.[179] Vse te matematično-računalniške tehnike lahko danes služijo za učinkovito zaščito zasebnosti oziroma za tajnost komuniciranja. Je pa šifriranje mogoče uporabljati tako za skrivanje vsebine elektronskih sporočil kot tudi vsebine datotek in celotnih pomnilniških medijev (npr. diskov). Navadno se šifriranje uporablja pri prenosu sporočil in podatkov prek telekomunikacijskih omrežij, mogoče pa ga je uporabljati tudi za zaščito podatkov in sporočil znotraj samega računalniškega sistema; s tem se izognemo kraji ob nepooblaščenem dostopu.

Pri uporabi šifriranja je najpomembneje, katero kriptografsko metodo in kako velik ključ uporabljamo. Večji ključ načeloma pomeni večjo varnost (varnost je sicer odvisna tudi od uporabljenega algoritma), vendar je šifriranje procesorsko in časovno bolj zahtevno. Prav tako je treba vedeti, da je praktično vse kriptografske metode mogoče z uporabo kriptoanalize razbiti in tako sporočilo dešifrirati brez ključa, vprašanje je le v kolikšnem času. Edina do zdaj znana izjema je metoda *one-time pad* (nekateri jo imenujejo tudi *one-time tape* ali *one-time letter pad*), ki sta jo leta 1917 odkrila Gilbert S. Vernam iz AT&T ter vodja kriptografskih raziskav ameriške vojske med prvo svetovno vojno, major Joseph Mauborgne.[180] Kot bo prikazano v nadaljevanju, so bile nekatere kriptografske metode razvite s 'pomočjo' tajnih služb (predvsem ameriške *National Security Agency*) in zato morda niso tako varne, kot se zdi na prvi pogled. Včasih so kriptografske metode razvila tudi neznana podjetja ali pa so bile metode razvite v tajnosti. Pri tem se pogosto uporablja napačen argument, da tajnost metode zagotavlja njeno varnost. To označujemo tudi z izrazom "varnost skozi skrivanje" (ang. *security through obscurity*), ki pa v kriptografiji ne deluje. Eden prvih takih primerov se je zgodil leta 1924, ko je Alexander von Kryha začel prodajati šifrirno napravo, katere kriptogram je štirim ameriškim kriptoanalitikom uspelo razbiti v dveh urah in 41 minutah. Kljub temu se je naprava še naprej uspešno prodajala, nemška diplomacija pa naj bi jo uporabljala še do 50. let 20. stoletja (Dupuis, 1999).

---

[178] Najbolj znana algoritma za implementacijo digitalnih prstnih odtisov sta MD5 in SHA.

[179] Poleg tega mora celovita varnostna aplikacija zagotoviti še preprečevanje tajenja (ang. *nonrepudiation*) in nadzor nad dostopom (ang. *access control*) do podatkov.

[180] Metoda velja za edino, ki je dokazano ni moč razbiti, vendar le, če je pravilno uporabljena. Ameriška agencija NSA v knjižici *The Venona Story*, objavljeni na svoji spletni strani, navaja, da jim je okrog leta 1946 uspelo razbiti kriptograme sovjetske tajne službe KGB, ki so nastali s pomočjo metode *one-time pad*. Vendar pa do razbitja ni prišlo zaradi pomanjkljivosti algoritma, temveč zaradi nemarnosti sovjetske tajne službe, ki je dele šifrirnih ključev uporabila večkrat. *One-time pad* namreč zahteva, da se vsak ključ uporabi samo enkrat, ključ pa mora biti povsem naključno generiran (Benson, 2005: 27). Res pa je, da je to metodo precej nepraktično uporabljati, zato se večinoma ne uporablja.

Zato prej navedeni "argumenti" pogosto pomenijo le to, da metoda ni bila javno preizkušena, ali pa, da celo sploh ni bila preizkušena. V kriptologiji se je namreč izoblikovalo načelo, da morajo biti vse kriptografske metode javno objavljene in da jih morajo preizkusiti vodilni kriptoanalitiki, saj le to zagotavlja njihovo kakovost. Dobro izbrana in preizkušena metoda namreč potencialnemu napadalcu onemogoča izvajanje znanih in učinkovitih napadov (npr. frekvenčno analizo). To pomeni, da lahko napadalec uporabi praktično samo metodo grobe sile (ang. *brute force attack*, preizkušanje vseh možnih kombinacij gesel), ta pa je zaradi svoje zahtevnosti razmeroma neučinkovita.[181] Seveda je mogoče, da bo proti metodi izveden kak neznan ali pa vsaj javno neznan napad, a je ta nevarnost veliko manjša, če je bila metoda javno preizkušena.

Nastanek javno dostopne kriptografije

Kriptografija ni nekaj, kar bi nastalo skupaj z računalniki, temveč je znana že skoraj 4000 let. Prvi primer zapisane kriptografije naj bi bili egiptovski nestandardni hieroglifi, ki so nastali okrog leta 1900 pr. n. š. (Kahn, 1973: 68). Kriptografijo so v zgodovini uporabljali večinoma za vojaške in politične namene npr. Rimljani. (Znan je npr. *Cezarjev algoritem*, s katerim so v času Cezarja sporočila šifrirali tako, da so posamezno črko v sporočilu zamenjali s črko, ki je bila v abecedi nekaj mest za njo ali pred njo.) Kahn pa ugotavlja, da se je sodobna zahodna kriptografija razvila kot posledica sodobne diplomacije; to se vidi predvsem na primeru Benetk, v katerih je Giovanni Soro leta 1506 in 1510 opravil prve večje uspešne kriptoanalize šifriranih sporočil (Kahn, 1973: 83). Leta 1861 so v ZDA prijavili prvi kriptografski patent. Leta 1923 je Arthur Scherbius začel izdelovati šifrirne stroje Enigma, katerih izboljšane različice so pozneje med drugo svetovno vojno v vojaške namene uporabljali Nemci. V 30. letih 20. stol. pa je kriptografija začela postati mehanizirana (Bamford, 1983: 427). Sprva so za šifriranje in razbijanje šifer uporabljali mehanske naprave (ena prvih je bila naprava za razbijanje Enigme, imenovana Bombe, razvili so jo že v 30. letih prejšnjega stoletja poljski kriptografi in jo tik pred napadom Nemčije na Poljsko julija 1939 posredovali Veliki Britaniji in Franciji (Bamford, 1983: 485–486)), pozneje pa računalnike s procesorji. Vsekakor je sodobno kriptografijo ustvaril telegraf. Z nastankom radia, ki je omogočal enostavno nepooblaščeno prisluškovanje, pa se je razvila sodobna kriptoanaliza (Kahn, 1973: 155).

---

[181] Metoda grobe sile namreč zahteva veliko procesorske moči, vendar pa je treba opozoriti, da je procesorsko moč mogoče dobiti tudi s porazdejeno obdelavo podatkov. Obstajajo namreč volonterski projekti, eden bolj znanih je npr. *RC5 Challenge* iz leta 1997, ko uporabniki na svojem računalniku v času, ko ta ni v uporabi, obdelujejo podatke, ki jih dobijo iz omrežja. Obdelane podatke potem pošljejo nazaj v osrednji strežnik. Tako darujejo nekaj svojega prostega procesorskega časa in če je takih uporabnikov veliko, dobimo velikansko procesorsko moč. S projekti razbijanja šifriranih sporočil z metodo grobe sile se med drugim ukvarja organizacija distributed.net (<http://www.distributed.net>). Znano je tudi, da je mogoče šifrirano sporočilo RSA razbiti s faktorizacijo. To je poseben matematični postopek iskanja praštevilčnih faktorjev danega števila. Napadalec, ki bi mu uspelo izpeljati faktorizacijo, bi lahko na podlagi tega postopka odkril zasebni ključ in tako dešifriral sporočilo. Marca 1994 so Atkins, Graff, Lenstra in Leyland v članku "*The Magic Words Are Squeamish Ossifrage*"opisali faktoriziranje 129-mestnega (426-bitnega) števila. Faktoriziranje je s pomočjo 600 prostovoljcev na 1600 računalnikih trajalo osem mesecev. Avgusta 1999 je Lenstru in Rieleju uspelo faktorizirati 155-mestno (512-bitno) število po sedmih mesecih. Ocenjujejo, da bi bilo s porazdeljeno obdelavo podatkov prek interneta ta čas mogoče skrajšati na nekaj dni (RSA Laboratories, 2000: 48 in 52).

Revolucijo v kriptografiji pa je povzročilo odkritje asimetrične kriptografije oziroma javna objava tega odkritja leta 1977 v obliki algoritma RSA, pri čemer ni zanemarljiv nastanek povečane dostopnosti računalnikov navadnim državljanom. Po nekaterih ugibanjih naj bi asimetrično kriptografijo že pred tem verjetno odkrili v ameriški NSA v 60. letih (Whitaker, 108), zagotovo pa nekoliko pozneje tudi v britanski tajni službi *Government Communications Headquarters* (GCHQ[182]) (Schneier, 1998)[183], vendar svojih odkritij niso nikoli javno objavili, verjetno se tudi niso zavedali posledic svojega odkritja. Leta 1976 sta matematika Whitfield Diffie in Martin E. Hellman v reviji *IEEE Transactions on Information Theory* objavila članek z naslovom "*New Directions In Cryptography*". V članku sta opisala protokol za varno izmenjavo šifrirnih ključev prek nezaščitenega medija, znan tudi kot sistem šifriranja z javnimi ključi. Leto pozneje se je Ronald L. Rivest domislil novega šifrirnega algoritma, ki bi temeljil na sistemu javnih ključev, omogočal pa bi tudi digitalno podpisovanje. Algoritem je skupaj z Adijem Shamirjem in Leonardom M. Adlemanom opisal v članku, ki ga je septembra 1977 objavila revija *Scientific American*. V članku so avtorji zapisali, da bodo tehnične podrobnosti algoritma brezplačno poslali vsakomur, ki jim bo poslal kuverto z znamko. Prejeli so na tisoče zahtevkov z vsega sveta in leto zatem so v reviji *Communications of the ACM* objavili šest strani dolg članek z naslovom "*A Method for Obtaining Digital Signatures and Public-Key Cryptosystems*". V njem je bil opisan celotni algoritem, ki so ga po začetnicah avtorjev poimenovali RSA (RSA Laboratories 2000, 12). Izkazalo se je, da je algoritem RSA kriptografsko izjemno močan (Vidmar, 1997: 181), kar pomeni, da je sporočila, zašifrirana z njim, izjemno težko razbiti.

Štirinajst let za tem, leta 1991, je računalniški programer Philip R. Zimmermann napisal računalniški program PGP (*Pretty Good Privacy*), namenjen šifriranju elektronskih sporočil in računalniških datotek. PGP je za šifriranje uporabljal algoritem RSA. Program je tekel na popolnoma običajnih računalnikih PC in ga je bilo za tedanje standarde uporabniške prijaznosti razmeroma enostavno uporabljati, predvsem pa je bil zelo učinkovit. Program se je pozneje razvijal naprej in danes omogoča digitalno podpisovanje, izmenjavo javnih ključev prek t. i. strežnikov javnih ključev (ang. *keyserver*), šifriranje datotek in diskov, nepovratno brisanje datotek, zelo domiseln sistem za preverjanje zaupanja javnim ključem, nove šifrirne algoritme itd.; predvsem pa je zelo prijazen do uporabnika in je (oziroma je bil v preteklosti) brezplačen. Danes je na voljo je tudi njegov popolnoma brezplačen odprtokodni klon GPG. Zimmermann je bil prepričan o trdni povezanosti med demokracijo in zasebnostjo in o tem, da je "*edini način za zaščito zasebnosti močna kriptografija*" (Zimmermann, 1993). Ker je tega leta ameriški senat

[182] GCHQ je nastala iz organizacije, znane kot Room 40, ki je bila leta 1914 v Veliki Britaniji ustanovljena za razbijanje vojaških šifer (Bamford, 1983: 481).

[183] Asimetrično kriptografijo (Ellis jo je poimenoval '*non-secret cryptography*') naj bi v 60. letih v GCHQ odkril James Ellis. Algoritem, podoben RSA, naj bi leta 1973 odkril tudi Clifford Cocks, M. J. Williamson pa leta 1974 algoritem, podoben Diffie-Helmanovemu algoritmu. Ni povsem znano, ali je NSA do podobnih odkritij prišla neodvisno že pred tem ali pa se je z njimi seznanila prek britanske tajne službe, zelo verjetno pa se v tajnih službah niso zavedali pomena tega odkritja. Prva vojaška naprava, ki je uporabljala sistem kriptografije z javnimi ključi, je namreč nastala šele sredi 80. let 20. stoletja; šlo je za vojaški telefon STU-III. Schneier zato pravi, da "*če so morda res odkrili matematiko, pa je jasno, da nikoli niso razumeli pomena tega odkritja*" (Schneier, 1998).

obravnaval zakon, ki bi krepko omejil uporabo kriptografije v civilne namene, je Zimmermann, ki je želel izničiti učinke tega zakona, program javno objavil na internetu in dovolil njegovo brezplačno kopiranje (Zimmermann, 1999). Zimmermann sicer ni imel dovoljenja za uporabo patentiranega algoritma RSA v svojem programu, zato mu je lastnik patenta RSADSI zagrozil s tožbo. Pozneje je Zimmermann sklenil dogovor z RSADSI in potem skupaj z MIT leta 1994 izdal povsem zakonito različico programa PGP (Phillips, 2001: 265). V razmeroma kratkem času se je program razširil po vsem svetu. V dveh letih je postal dejanski standard za učinkovito zaščito podatkov in elektronske pošte (Zimmermann, 1993), zato so februarja 1993 na Zimmermanova vrata potrkali agenti FBI zaradi suma, da je omogočil nezakonit izvoz vojaške tehnologije (Gimon, 1995). V ZDA kriptografijo namreč štejejo za vojaško tehnologijo,[184] katere izvoz je mogoč samo z dovoljenjem. Januarja 1996 je bila preiskava ustavljena brez obtožbe, saj proti osumljencu niso našli dokazov za kaznivo dejanje. Je pa ostal grenak priokus, da je šlo v Zimmermanovem primeru za poskus zastraševanja.

Pomen kriptografije

Kriptografija je ena izmed najbolj znanih in učinkovitih tehnik zaščite zasebnosti, saj omogoča zakrivanje informacij in komunikacij. Poleg tega uporaba kriptografskih tehnik omogoča vsaj deloma anonimno širjenje informacij (npr. poročila o kršitvah človekovih pravic) ter omogoča zagotavljanje integritete sporočil. V praksi to pomeni, da lahko s kriptografskimi tehnikami tudi preprečimo, da bi kdo sporočila v elektronski obliki (npr. poročila organizacij za zaščito človekovih pravic ali pa osebno korespondenco) spreminjal (Madsen in Banisar, 2000: 5).

Po eni strani so tradicionalni uporabniki kriptografije države in njeni organi, po drugi strani pa kriptografija lahko rabi tudi navadnim državljanom. Po mnenju organizacij za elektronsko zasebnost bomo v prihodnosti za medsebojno komuniciranje uporabljali predvsem elektronske komunikacije. Te je mogoče nadzorovati neopazno in v velikem obsegu. Kriptografija je po njihovem mnenju instrument, ki zagotavlja zasebnost, zasebnost pa je temeljna človekova pravica, zato pravico do uporabe kriptografije te organizacije enačijo s pravico do zasebnosti. Čeprav se zavedajo nevarnosti zlorabe kriptografije, so prepričane, da bi njena prepoved povzročila večjo škodo kot to, da je dovoljena (Zimmermann, 1993). Zimmermann pravi, da "*skuša kriptografija izenačiti odnose moči med vlado in njenimi državljani*", zato je "*kriptografija zelo politična tehnologija*" (Hoffman, 1996). Leta 1996, sredi najhujših bitk glede uporabe kriptografije v ZDA, je izjavil, da se bo lahko zgodilo, da bo neka prihodnja vlada tehnologijo, ki bo optimizirana za nadzor posameznikov, začela izrabljati. Zimmermann je to izjavil v kontekstu odgovorov na kritike šifrirnega čipa Clipper (pri katerem je šlo za to, da so v ZDA želeli uzakoniti tako kriptografijo, ki bi državnim organom omogočila dostop do nešifriranega besedila). Zagovorniki Clipperja so namreč trdili, da se z uvedbo tega sistema ne bo nič spremenilo, saj bo FBI za

[184] Izvoz kriptografskih izdelkov v ZDA urejata dva zakona: *Arms Export Control Act* in *Export Administration Act*. Na podlagi teh dveh zakonov se večina kriptografskih izdelkov šteje za municijo in zato se jih sme izvoziti samo s posebnim dovoljenjem (Allard in Kass, 1997: 574).

prisluškovanje še vedno potreboval sodni nalog, Zimmermann pa je želel opozoriti na to, da ni nujno, da bodo tudi vse prihodnje vlade demokratične. Po njegovem mnenju se namreč lahko zgodi, da bo tehnologija, ki bo oblikovana za nadzorovanje, zares zlorabljena šele, ko bo na oblast prišla nedemokratična vlada ("*...če bo slaba vlada nekoč prišla na oblast, bo to morda zadnja vlada, ki jo bomo izvolili*" (Hoffman, 1996)). Na nekem drugem mestu je izjavil, da "*če ne bomo storili nič, bodo nove tehnologije dale državi moč nadzora, o kakršni je Stalin lahko samo sanjal*" (Zimmermann, 1993). Podobnega mnenja je bil tudi Rivest, ki je v polemiki okrog uvedbe čipa Clipper zagovornici Clipperja Denningovi zapisal, da "*samo zato, ker si spoznala trenutne predstavnike različnih državnih agencij in čutiš, da jim lahko zaupaš, to še ne pomeni, da takšno zaupanje lahko prenesemo na njihove naslednike. Treba je vzpostavljati institucionalne varovalke zavor in ravnotežij (ang. checks and balances), ki premagajo občasne moralne spodrsljaje enega ali več trenutnih imetnikov oblasti... Korumpirani predsednik lahko (za kopije šifrirnih ključev) ukaže, da se uporabijo za neustrezne namene*" (Rivest, 1994).

Šifrirni program PGP uporabljajo številni politični aktivisti po svetu – npr. organizacije za zaščito človekovih pravic, tibetanska vlada v izgnanstvu itd. V nekem intervjuju je Zimmermann povedal, da uporabo njegovega programa poučujejo tudi odporniške skupine v Burmi, vendar uporaba kriptografije ni omejena samo na politične oporečnike. Konec 60. let je IBM zaradi nevarnosti računalniškega kriminala začel razvijati šifrirni algoritem Lucifer. Po Zimmermanovem mnenju "*navaden posameznik potrebuje šifriranje za učinkovito funkcioniranje v informacijski dobi*" (Hoffman, 1996). Številne raziskave so namreč pokazale, da je pomemben dejavnik, ki zavira opravljanje elektronskih transakcij in plačevanja po internetu, strah pred krajo številke kreditne kartice ali osebnih podatkov. Proti temu pa se je mogoče zavarovati s šifriranjem. Na pomen uporabe kriptografije kaže tudi ugotovitev Rotenberga, ki pravi, da bo zasebnost za informacijsko ekonomijo naslednjega stoletja tisto, kar je bila zaščita potrošnikov in skrb za okolje za industrijsko družbo v dvajsetem stoletju (Cate, 1997: 3).

* * *

Zaradi želje po neoviranem nadzorovanju so si države in njihovi organi vedno prizadevali nadzorovati in monopolizirati kriptografijo. "*Vlada, ljubosumna na svoje skrivnosti, skuša odkriti naše,*" je zapisal Sykes (Sykes, 1999: 155). Ni torej presenetljivo, da je odkritje *učinkovite* kriptografije v ameriški državni administraciji sprožilo preplah, predvsem med njenimi represivnimi organi. Do odkritja algoritma RSA je bilo namreč večino javno dostopnih kriptografskih metod mogoče razbiti, do objave računalniškega programa PGP pa kriptografija ni bila dostopna navadnim posameznikom. Monopol nad kriptografijo so torej *de facto* imele vojska in tajne službe, deloma pa je bila kriptografija dostopna tudi v akademskih krogih in velikim podjetjem. Z razvojem informacijsko komunikacijske tehnologije, ki je omogočila nastanek in javno objavo kakovostnih in poceni ali celo brezplačnih šifrirnih programov, pa se je to spremenilo. Ker je bil državni *de facto* monopol na področju kriptografije odpravljen, ga je država poskusila vsiliti – najprej z zakonodajo, ko ji to ni uspelo, pa še na druge načine.

Vojna ameriške vlade proti kriptografiji in elektronski zasebnosti

Leta 1952 je ameriški predsednik Harry S. Truman ustanovil NSA – *National Security Agency*. Obstoj agencije je bil dolga leta državna skrivnost, prav tako je ukaz o njeni ustanovitvi še vedno tajen. Naloga NSA je prestrezanje in kriptoanaliza tujih komunikacij ter razvoj rešitev za zaščito ameriških državnih komunikacij in informacijskih sistemov (Phillips, 2001: 255). Kljub temu da so obveščevalne naloge NSA omejene na obveščevalno spremljanje tujih komunikacij, pa NSA zelo vpliva tudi na razvoj in omejevanje kriptografije znotraj ZDA, saj nastopa kot svetovalec *Bureau of Export Administration* (BXA), zaradi česar ima vpliv na to, katere kriptografske izdelke bodo ameriška podjetja smela izvažati. Sodeluje tudi z *National Institute of Standards and Technology* (NIST) pri pripravi varnostnih standardov, ki veljajo za državne računalniške in komunikacijske sisteme (RSA Laboratories 2000, 175–177). Glede na to, da ima NSA na voljo velika finančna sredstva in da je velik poslovni partner podjetij, ki se ukvarjajo z varnostnimi rešitvami, lahko na ta podjetja izvaja tudi poslovne pritiske, s katerimi lahko doseže opustitev proizvodnje določenih rešitev (RSA Laboratories 2000, 177). Hkrati NSA veliko vlaga tudi v raziskovanje in razvoj, leta 1979 je bila največji zaposlovalec v ameriškem obveščevalnem sektorju (Phillips, 2001: 255), zato številnim raziskovalcem in podjetjem omogoča delo in poslovanje in ima nad njimi ekonomsko moč. Eden najbolj poučnih primerov vojne NSA proti javno dostopni kriptografiji je primer algoritma DES.

DES

Konec 60. let 20. stoletja so v IBM spoznali, da je zaradi čedalje večje razširjenosti računalniške tehnologije v bančništvu nastala nevarnost računalniškega kriminala. Zato so znotraj podjetja ustanovili posebno raziskovalno skupino, ki naj bi se ukvarjala z razvojem kriptografije za komercialne namene. Raziskovalna skupina je pod vodstvom Horsta Feistla leta 1971 končala razvoj šifrirne naprave, imenovane Lucifer. Šlo je za poseben algoritem, ki je bil implementiran v majhnem čipu, in v tistem času je bila to najmanjša šifrirna naprava na svetu. Nastanek Luciferja je pomenil prvo resno konkurenco šifrirnim algoritmom in napravam, ki jih je razvijala NSA. Bamford je zapisal: "*Prvič v zgodovini se je NSA soočila s konkurenco na lastnem ozemlju. Zunanji konkurenti pa niso bili ljubitelji, temveč visoko izobraženi profesionalci z neomejenimi sredstvi...*" (Bamford, 1983: 435).

Leta 1973 je ameriški *National Bureau of Standards* (NBS; iz njega je pozneje nastal NIST) želel pripraviti standard za šifriranje civilnih komunikacij. Ravno v tem času je IBM razvil šifrirni algoritem Lucifer, o čemer je bila NSA obveščena, saj Bamford navaja, da so uslužbenci NSA redno obiskovali IBM in spremljali njihov napredek (Bamford, 1983: 435). Lucifer, ki ga je uporabljala tudi vojska, je uporabljal 128-bitni šifrirni ključ, vendar je NBS v sodelovanju z NSA Lucifer za civilno rabo priredila. 128-bitni šifrirni ključ so skrajšali na 64 bitov, pri čemer pa je bilo 8 bitov kontrolnih in je bila torej dejanska dolžina ključa samo 56 bitov, poleg tega so priredili še nekatere matematične postopke v samem algoritmu. (Spremenili so t. i. *S-boxe*,

v katerih potekajo permutacije.) Tako modificiran algoritem je nato NBS januarja 1977 potrdil kot standard *Data Encription Standard* (DES), in sicer potem, ko je revizija NSA ugotovila, da naj bi v njem ne bilo nobenih statističnih ali matematičnih slabosti (Bamford, 1983: 436).

Bamford celo trdi, da je IBM algoritem skupaj z NSA priredil, še preden so ga sploh prijavili NBS, dejstvo pa je, da teoretično ozadje algoritma nikoli ni bilo povsem pojasnjeno, zaradi česar je obstajal sum, da ameriška vojska pozna bližnjico za razbijanje civilne inačice DES (Vidmar, 1997: 179). NSA tega nikoli ni hotela komentirati, češ da je njihova politika, da ne razpravljajo o prednostih in slabostih šifrirnih tehnik, saj bi s tem lahko sovražnikom razkrili slabosti ameriških šifrirnih sistemov ali jih opozorili na slabosti njihovih (Phillips, 2001: 256).

Preden je spremenjeni Lucifer postal standard, je bil deležen številnih kritik. Najvidnejša nasprotnika DES sta bila akademska kriptologa Martin E. Hellman in Whitfield Diffie. Izračunala sta, da bi bilo mogoče s posebnim računalnikom za 20 milijonov dolarjev 56-bitni DES v povprečju razbiti v manj kot pol dneva, vsaka rešitev (razbitje kriptograma) pa bi stala 5000 dolarjev. Poleg tega sta ugotovila, da se stroški računalniške moči zmanjšujejo, zato sta ocenila, da bi tak računalnik v desetih letih stal samo 200.000 dolarjev, vsaka rešitev pa le 50 dolarjev. Na podlagi dejstva, da bi ob enakih pogojih in 128-bitnem ključu vsaka rešitev stala 200,000,000,000,000,000,000,000,000 dolarjev, sta bila kritika prepričana, da je DES namenoma oslabljen. NBS je v odgovor kritikam pripravil dve delavnici na temo DES, na katerih so ugotovili, da bi razbijanje DES trajalo 17.000 let (Bamford, 1983: 438), seveda pa so upoštevali zgolj možnost napada z grobo silo. A izkazalo se je, da je bila civilna različica algoritma resnično prirejena, saj naj bi IBM že med razvojem algoritma odkril matematično bližnjico za razbijanje civilne različice DES, vendar je zaradi zahtev ameriške NSA to odkritje ostalo tajno. V letih 1990 in 1991 sta izraelska kriptografa Eli Biham in Adi Shamir predstavila novo vrsto kriptoanalize, ki sta jo poimenovala diferencialna kriptoanaliza (ang. *differential cryptanalysis*). Porodil pa se je sum, da je bila civilna različica DES namerno prirejena tako, da je bila učinkovitost dotlej neznanega napada z diferencialno kriptoanalizo povečana (sci.crypt, 1994).

Leta 1993 je Michael Wiener na konferenci o kriptografiji predstavil načrt za napravo za razbijanje 56-bitne različice DES po metodi grobe sile. Naprava bi po njegovih izračunih stala milijon dolarjev in bi DES lahko razbila povprečno v treh urah in pol. Phil Zimmermann je izračunal, da bi nekoliko kompleksnejši napravi za 100 milijonov dolarjev uspelo razbiti šifrirano sporočilo povprečno v dveh minutah, na pričanju pred podkomitejem ameriškega senata leta 1996 pa je izjavil, da NSA s svojim proračunom lahko razbije sporočilo, zašifrirano s civilno različico DES, v hipu (Zimmermann, 1993). Julija 1998 je John Gillmore iz fundacije *Electronic Frontier Foundation* predstavil napravo DES Cracker, ki je z metodo grobe sile (ang. *brute-force*) in ob pomoči porazdeljene obdelave podatkov prek interneta razbila DES v 22 urah (RSA Laboratories 2000, 63). Istega leta je skupina kriptografov predstavila tudi DES Cracker za 250.000 dolarjev, ki je DES razbil v manj kot treh dneh (Sykes, 1999: 173). Od takrat naprej je znano, da DES ni več varen, NSA pa ima zelo verjetno na voljo ustrezno tehnologijo za njegovo razbijanje.

Kljub temu se je DES močno uveljavil v bančništvu in pozneje nasploh v civilni sferi, saj je bilo napisanih veliko računalniških programov, ki uporabljajo DES, poleg tega so ta algoritem poučevali praktično na vseh univerzah. Razlogov za njegovo uveljavitev je več, kljub temu da je bil ta standard za nevladne organizacije neobvezen. Banke so po eni strani s sprejetjem tega standarda pokazale, da po svoji najboljši moči skrbijo za varnost in se vedejo odgovorno, po drugi strani pa je uporaba standarda omogočila skupno uporabnost informacijskih sistemov in neovirano izmenjavo podatkov, obenem pa so se banke izognile razvoju lastnih šifrirnih sistemov, s čimer so se izognili tako stroškom kot tudi odgovornosti za njihovo morebitno neustreznost. S tem so odgovornost prenesle na državo, to pa je bil verjetno tudi eden poglavitnih vzrokov za hitro širitev DES.

Leta 1987 je National Bureau of Standards DES znova pregledal in se po nasvetu NSA, ki je bila kljub slabostim DES zaskrbljena zaradi njegove razširjenosti po svetu (Diffie in Landau, 1999: 65), odločil, da standarda zaradi zastarelosti in verjetnosti, da bo kmalu javno razbit, ne bo podaljšal. Ker pa niso pripravili novega standarda in ker je nanje pritisnila finančna industrija, so DES spet potrdili; enako se je zgodilo tudi leta 1993 (Phillips, 2001: 258). DES oziroma njegove inačice, npr. *Triple DES*, ki je sicer močnejši, vendar še vedno temelji na algoritmu DES, so tako v rabi še danes. Ker pa je po Wienerjevi predstavitvi DES Crackerja leta 1993 in njegovi dejanski izdelavi leta 1998 postalo jasno, da DES ni več ustrezen in ne more biti več standard, je NIST začel pripravljati AES – *Advanced Encryption Standard*.[185]

Dokler je bila javnosti oziroma civilni sferi dostopna le kriptografija, ki so jo ameriške tajne službe znale razbiti, ameriške državne institucije niso čutile potrebe po omejevanju kriptografije. Z razvojem znanosti in tehnologije pa je nastopila nevarnost, da bo močna kriptografija postala dostopna vsem. Dodatno nevarnost je predstavljalo to, da bi lahko močna kriptografija postala dostopna ne samo domači, ameriški javnosti, temveč tudi tujim državam. Zato je NSA skušala omejevati znanstveno raziskovanje in izvoz kriptografskih izdelkov onkraj meja ZDA ter vsiljevati svoje kriptografske standarde.

Omejevanje svobode govora

Bamford v knjigi *The Puzzle Palace* pravi, da je NSA kmalu po ustanovitvi oblikovala desetčlanski znanstveno-svetovalni odbor (*National Security Agency Scientific Advisory Board*); leta 1957 pa je znotraj agencije nastalo poročilo Bakerjevega komiteja (vodil ga je William O. Baker), v katerem so ugotovili, da je treba zagotoviti dotok znanja in znanstvenikov iz akademskih krogov. Čeprav so leta 1965 odprli *National Cryptologic School* (Bamford, 1983: 153), pa si v NSA niso želeli odprtega sodelovanja, saj niso želeli, da kriptološki izsledki postanejo javno znani. Bamford pravi, da se je NSA že pred tem lotila projekta *Lightening*, ki je potekal med letoma 1956 in 1962, pri njem pa so sodelovale ameriške univerze. V okviru projekta sta potekali

[185] Končni algoritem za AES so izbirali med več algoritmi, konec leta 2000 pa so izbrali algoritem *Rijndael* avtorjev Joana Daemena in Vincenta Rijmena. Vsi algoritmi, ki so kandidirali za standard AES, so bili javno objavljeni, preizkusili pa so jih vodilni svetovni kriptoanalitiki.

dve poletni šoli, in sicer *Summer Campus Advanced Mathematics Program* ter *Advanced Language Program*, ki so se ju udeležili številni znanstveniki. Tako je nastalo več kot 160 člankov, vloženih je bilo 320 patentnih prošenj in napisanih 71 doktoratov (*university theses*). Projekt *Lightning* naj bi tako rabil za zagon raziskav na področju kriptografije (Bamford, 1983: 430). To je agenciji sicer koristilo, a duh je bil spuščen iz steklenice. NSA je namreč skušala po eni strani spodbujati razvoj kriptografije, po drugi strani pa sadove tega razvoja obdržati le zase, to pa se je izkazalo za nezdružljivo.

Prvi v javnosti vidnejši poskusi omejevanja kriptografije so se zvrstili že kmalu po objavi algoritma RSA septembra 1977 v reviji Scientific American. Rivest, eden izmed izumiteljev algoritma, je bil namreč povabljen na konferenco *Institute of Electrical and Electronics Engineers* (IEEE), na kateri naj bi predstavil svoje delo. Toda organizator konference je prejel pismo nekega J. A. Meyerja z opozorilom, da bo Rivestovo predavanje verjetno kršitev zakona *International Traffic in Arms Regulations* (ITAR), saj bodo na konferenci navzoči tudi tuji državljani (Diffie in Landau, 1999: 61–62). Ker je imel IEEE sklenjen sporazum o sodelovanju tudi s Sovjetsko zvezo, je bila nevarnost, da bodo kopije govorov poslane tudi tja (Bamford, 1983: 444).
Izkazalo se je, da je bil Meyer uslužbenec NSA. Ker pa je NSA zanikala povezavo z Meyerjevim pismom (šlo naj bi za zasebno pismo, saj je bil Meyer tudi član IEEE) in zaradi prvega amandmaja ameriške ustave,[186] ki govori o svobodi govora, je bil prispevek na konferenci vseeno predstavljen (Diffie in Landau, 1999: 61–62).

Sprva je NSA želela preprečiti vsakršno javno razpravo o kriptografiji. Direktor NSA Bobby Ray Inman je v javnem govoru marca 1979 dejal, da "*je zelo realna in kritična nevarnost, da bo neomejena javna razprava o kriptoloških zadevah resno ogrozila zmožnost vlade, da opravlja obveščevalne dejavnosti (ang. signals intelligence – SIGINT), in zmožnost vlade, da zaščiti informacije v zvezi z nacionalno varnostjo pred tujimi sovražnimi izrabami*" (EFF, 2001). Zato je zahteval, naj raziskovalci in NSA sklenejo kompromis, sicer bo zahteval sprejem zakonov o omejevanju objave kriptografskih raziskav (Diffie in Landau, 1999: 63). Toda že prej se je izkazalo, da bo zaradi svobode govora raziskovalcem praktično nemogoče preprečiti javno objavo svojih odkritij (kljub temu je Inman še leta 1983 naročil študijo o omejitvi akademskega raziskovanja na tem področju (Sykes, 1999: 174)), zato se je NSA odločila na raziskovalce pritisniti s finančnimi ukrepi.

Finančni pritiski na raziskovalce

NSA je od svojih raziskovalcev lahko zahtevala tajnost njihovih odkritij. Pravno formalno tega ni mogla zahtevati od velikih podjetij. Ker pa je bila ameriška država za podjetja, npr. AT&T in IBM, vedno pomembno tržišče, je NSA prek ekonomskih pritiskov lahko dosegla njihovo sodelovanje. Zapletlo pa se je pri svobodnih in akademskih raziskovalcih. A ne za dolgo.

[186] 1. amandma, Listina svoboščin (Bill of Rights), 1791.

Izkazalo se je namreč, da večino svobodnih raziskovalcev financira *National Science Foundation* (NSF).

Leta 1977 sta dva uslužbenca NSA[187] obiskala direktorja NSF Fredericka Weingartna in ga obvestila, da verjetno krši zakon, ker financira kriptografske raziskave *Massachusets Institute of Technology* (Diffie in Landau, 1999: 62). NSA je namreč želela postati edina ustanova, ki bi financirala tovrstne raziskave, saj bi tako dobila neposreden nadzor nad večino raziskovalcev s področja kriptografije.

NSA se je sklicevala na predsedniško direktivo, ki daje NSA pooblastilo, da se edina ukvarja s kriptografijo, vendar je Weingarten podobne obtožbe slišal že dve leti prej, junija 1975. Takrat jih je NSF preverila in ugotovila, da takšnega ukaza ni. Weingarten je zato svoja obiskovalca s tem seznanil in ker NSA ni uspelo z grožnjami, je ubrala spravljivejše tone. NSF so predlagali sodelovanje pri recenziranju predlaganih projektov. Ker je imela NSA veliko strokovnjakov s področja kriptografije, se je Weingarten s tem strinjal, vendar je poudaril, da bo sprejel le nasvete, ki se bodo nanašali na tehnično in znanstveno plat prijavljenih projektov, poleg tega naj bi bile NSA-jine recenzije javne (Bamford, 1983: 442–443).

Leta 1981 je posebna delovna skupina *American Council of Education* predlagala, naj se uvede prostovoljen sistem predhodnega pregleda (ang. *prepublication review*) znanstvenih publikacij s področja kriptografije. Kljub pomislekom so se odločili za dveletno preskusno obdobje. Preskus se je izkazal za razmeroma uspešnega, saj je NSA le v nekaj primerih predlagala manjše popravke ali zahtevala, naj avtor članka ne objavi. V enem primeru pa je celo pomagala trem izraelskim znanstvenikom, Feigeju, Fiatu in Shamirju, ki so želeli v ZDA patentirati nekatera svoja odkritja, ameriška vojska pa jih je želela označiti kot zaupna, kljub temu da so imeli o tematiki že več javnih predavanj (Diffie in Landau, 1999: 63). Shamirjevega odvetnika je namreč poklical anonimni upokojeni uslužbenec NSA in mu natančno povedal, na koga naj se obrne, da bo ukaz o zaupnosti umaknjen. Shamir se je pozneje NSA javno zahvalil za pomoč (Diffie in Landau, 1999: 254).

Kljub vsemu je NSA pozneje predlagala, da bi v okviru sodelovanja z NSF kriptografske raziskave financirali oni, raziskovalci pa bi bili prisiljeni sprejeti financiranje NSA. Leta 1980 je Leonard Adleman z MIT želel prijaviti projekt s področja kriptografije, a ga je NSF obvestila, da njegovega projekta ne more financirati. Istega dne ga je poklical direktor NSA in mu sporočil, da bi njegov projekt želela financirati NSA. Ker se je Adleman bal, da mu bo NSA postavila pogoje glede objave njegovih odkritij, je financiranje s strani NSA zavrnil (Bamford, 1983: 455). Pozneje je bil ta sistem zavrnjen in sprejeta je bila odločitev, da se smejo raziskovalci sami odločiti, čigavo finančno pomoč bodo sprejeli (Diffie in Landau, 1999: 63).

[187] Bamford navaja, da naj bi bila to direktor COMSEC sektorja Cecil Corry in njegov pomočnik David C. Boak, vendar ne navaja, kje je dobil ta podatek (Bamford, 1983: 441-442).

Omejevanje patentiranja

NSA je želela preprečiti vsako javno razkritje kriptografskih odkritij tudi na druge načine. V povojnih letih je večino kriptografskih patentov imela v lasti NSA, plačevanje licenčnine pa je celo povzročalo manjše napetosti med NSA in GCHQ (Bamford, 1983: 491). Ko pa so se s kriptografijo začeli ukvarjati tudi v akademskih krogih, so prošnje za patente začeli vlagati tudi neodvisni izumitelji. Leta 1977 sta samostojni raziskovalec Carl Nikolai in profesor z University of Wisconsin George Davida neodvisno želela prijaviti vsak svoj patent s področja kriptografije. Nicolai je izumil šifrirni telefon, ki ga je imenoval *Phasorphone* in ga je nameraval prodajati po zelo dostopni ceni okrog 100 dolarjev. Davida pa je želel patentirati tokovni šifrirnik (ang. *stream cipher device*, naprava za šifriranje toka podatkov, npr. zvoka) (Bamford, 1983: 449). Oba izumitelja sta iz patentnega urada dobila ukaz, da je njun izum postal tajen in da o njem ne smeta govoriti.

Izkazalo se je, da je leta 1951 sprejeti *Invention Secrecy Act*[188] NSA omogočal, da izumiteljem prepove govoriti o izumu, kar zajema tudi predstavitve na znanstvenih konferencah. Izumitelja sta se na to odločitev pritožila in o vsem skupaj obvestila revijo Science. Nicolai je za Science izjavil, da gre po njegovem mnenju za načrt NSA, kako omejiti zasebnost Američanov, in da se argument o nacionalni varnosti uporablja samo kot krinka (Bamford, 1983: 449). Zadeva je v javnosti sprožila precejšnje razburjenje.

Zaradi tega je direktor NSA Inman privolil v prvi javni intervju. V njem je povedal, da je šlo v primeru Nicolaia za nestrinjanje med ocenjevalci, zaradi česar je prišlo do napake, prav tako naj bi do birokratske napake prišlo tudi v primeru Davide (Bamford, 1983: 450–51). NSA je tajni ukaz umaknila (Sykes, 1999: 173), pozneje pa je ameriško pravosodno ministrstvo presodilo, da so takšne omejitve neustavne (Phillips, 2001: 256–257). Vendar pa je bilo ravnanje Davide in Nicolaia prej izjema kot pravilo, saj takšni tajni ukazi podjetjem navadno koristijo, ker se s tem čas patentne zaščite poveča, velika podjetja pa izgubo dobička, ki nastane zaradi tega, lahko morda uporabijo tudi kot argument pri sklepanju poslov z vlado.

Omejevanje izvoza kriptografskih izdelkov

Znanstveni članki o kriptografiji so suhoparno gradivo, ki ga razumejo le posamezniki z določenim predznanjem iz kriptografije in matematike, prav tako se konferenc o tej tematiki udeležuje le ozek krog posameznikov. Da bi bila kriptografija zares uporabna in dostopna vsem posameznikom, je treba kriptografske zamisli preliti v tehnično rešitev. Ta je lahko kos strojne opreme, še pogosteje pa gre za računalniški program. Najprej so se oglasili predlogi, naj se v ZDA dovoli samo uporaba šibke kriptografije, kar bi ustrezno opremljenim državnim organom omogočilo, da v nujnih primerih (npr. ugrabitvah) hitro razbijejo zaščito (Denning, 1997: 184).

[188] Invention Secrecy Act of 1951, 35 U.S.C. (1951).

Žal takšna kriptografija uporabniku ne daje ustrezne zaščite, saj lahko šifropis razbije vsakdo, ki ima zmogljivejši računalnik in ustrezno računalniško znanje, poleg tega bi bile take omejitve zelo verjetno v nasprotju s svobodo govora, zato so v javnosti takoj naletele na velik odpor.

NSA se je zategadelj odločila, da bo skušala zaustaviti širjenje računalniških programov in kriptografskih naprav (čipov, kartic itd.) onkraj meja ZDA. Pri tem se je oprla na zakon *International Traffic in Arms Regulations* oziroma *US Export Regulations*, s katerim omejuje izvoz kriptografskih proizvodov iz ZDA, ter uporabila poslovne pritiske, s katerimi je od podjetij zahtevala, naj opustijo določene kriptografske produkte ali pa naj vanje vgradijo t. i. 'stranska vrata'.

Eden bolj znanih poizkusov omejevanja izvoza računalniških kriptografskih izdelkov je že omenjeni Zimmermanov *Pretty Good Privacy* iz leta 1991. V tem primeru se je izkazalo, da je omejevanje z izvoznimi dovoljenji v obdobju interneta povsem neučinkovito. Predpostavka izvoznih predpisov je, da podjetja programsko opremo prodajajo in da torej podjetja svoje izdelke nadzirajo, Zimmermann pa je svoj program dal v prosto rabo in je s tem izgubil ves nadzor nad njim. Pozneje se je sicer izkazalo, da ameriški izvozni predpisi prepovedujejo samo izvoz kriptografske programske opreme v elektronski obliki, in to so izkoristili člani organizacije PGP International, ki so leta 1997 izvorno programsko kodo programa PGP 5.0 natisnili v 12 knjigah (na več kot 6000 straneh) in jo povsem zakonito izvozili v Evropo. V Evropi je nato več kot 70 prostovoljcev to knjigo s pomočjo digitalnega skenerja in optičnega prepoznavanja znakov pretvorilo nazaj v digitalno obliko in iz nje naredilo binarno različico programa (PGP International, 2005). Pozneje se je oblikovala celo spletna stran www.cryptoscan.org z nasveti, kakšna orodja uporabiti, da bi zaobšli izvozne predpise. Po letu 1999 so ZDA opustile izvozna dovoljenja, razen za peščico držav.

Ne samo, da izvozni predpisi niso bili učinkoviti, deležni so bili tudi številnih kritik zaradi finančne škode, ki so jo povzročali ameriškim podjetjem. Ameriški izdelovalci bi bili namreč prisiljeni za zunanje trge izdelati take kriptografske izdelke, da bi zanje lahko dobili izvozna dovoljenja. To v praksi pomeni, da morajo biti izdelki ustrezno oslabljeni (npr. dovoljen je bil izvoz takih izdelkov z algoritmom RSA, ki uporabljajo samo 40-bitni ključ). Po eni strani bi bila torej podjetja prisiljena izdelovati dve vrsti izdelkov (enega za domači in enega za tuji trg), po drugi strani pa bi pridobitev izvoznega dovoljenja za podjetje pomenila priznanje, da njihovi izdelki niso dovolj varni. Znan je vsaj en primer, ko je imelo podjetje zaradi tega poslovno škodo. Phillips namreč navaja, da je podjetje DEC zaradi teh omejitev in očitkov, da prodaja varnostno nezanesljive izdelke, opustilo vsaj eno računalniško rešitev za varno izmenjavo podatkov med računalniki (Phillips, 2001: 257). Da je argument o finančni škodi resen, dokazuje tudi to, da se je Francija konec 90. let odločila liberalizirati svojo politiko do kriptografije (ki je bila ena najbolj omejujočih na svetu), in sicer z argumentom, da bi "*liberalizacija šifrirne tehnologije omogočila francoskim podjetjem poln vstop na trg elektronske trgovine, ki ga trenutno obvladujejo podjetja iz ZDA*" (izjava francoskega ministra za industrijo Christiana Pierreta 29. avgusta 1997 (GILC, 1998)).[189]

[189] Leta 1999 so v Franciji dejansko začeli sproščati uporabo šifrirne tehnologije (Madsen in Banisar, 2000: 55).

Vsiljevanje kriptografskih standardov in sistem depozita šifrirnih ključev

Ker zaradi globalizacije in hitre širitve interneta izvozne omejitve niso bile učinkovite, se je NSA skupaj z FBI lotila drugačne taktike. Naloga *National Bureau of Standards* oziroma njegovega naslednika *National Institute of Standards and Technology* je priprava državnih standardov za civilno sfero. Za kriptografske standarde velja, ki se jih morajo držati vse državne agencije, za podjetja pa niso obvezni, razen če sodelujejo z državnimi agencijami. Kljub temu se jih podjetja prostovoljno držijo zaradi večje združljivosti in povezljivosti.

Zamisel NSA in FBI je bila, da kot standard postavijo take kriptografske izdelke, ki bi državnim organom omogočali dostop do šifriranih podatkov. Drugi kriptografski pripomočki, ki tem standardom ne bi ustrezali, ne bi dobili licence, njihova uporaba pa bi bila omejena. Pri tem se je pogosto uporabljal argument, da se bo sicer močno kriptografijo uporabljalo v kriminalne namene. Čeprav se na prvi pogled zdi, da bi bila taktika vsiljevanja s strani države odobrenih kriptografskih standardov lahko celo uspešna, je v luči omenjenega argumenta nesmiselnost takega predloga očitna, saj je pričakovati, da kriminalci ne bodo uporabljali programske opreme s tako državno licenco (Denning, 1996: 216).

Ena izmed različic tega predloga je celo predvidevala zakonsko prepoved uporabe nekaterih (močnih) kriptografskih metod, ki ne bi bile v skladu s standardi. Po tem predlogu bi posamezniki sicer še vedno lahko razvijali svoje lastne kriptografske metode, vendar samo za osebno rabo in izobraževanje, brez dovoljenja pa jih ne bi smeli prosto širiti (Denning, 1997: 187–188). Drugi predlog je predvideval, da bi močno šifriranje dovolili samo v zaprtem omrežju. Gre za uporabo t. i. mrežnega šifriranja oziroma šifriranja povezav znotraj zaprtega omrežja (ang. *link encryption*), pri čemer podatki sistem zapustijo nešifrirani in to državnim organom omogoča prestrezanje pri izhodu iz sistema (Denning, 1997: 184 ter Denning in Baugh, 2000: 119). Podoben sistem uporabljajo v omrežju mobilne telefonije GSM za govor, ki se prenaša po radijskih povezavah od telefona do bazne postaje.[190]

Leta 1982 je *National Bureau of Standards* začel pripravljati standard za kriptografijo z javnimi ključi (asimetrično kriptografijo). Podjetje RSA Data Security, ki so ga ustanovili izumitelji algoritma RSA, je bilo seveda zelo zaniteresirano za to, da RSA postane ameriški zvezni standard, NSA pa je temu nasprotovala (Diffie in Landau, 1999: 64). Ker je NBS medtem že ugotovil, da šifrirni algoritem DES zaradi starosti in verjetnosti, da bo kmalu razbit, ni več ustrezen (prvotno ga celo niso hoteli znova potrditi kot standard (Phillips, 2001: 258)), so na podlagi leta 1987 sprejetega *Computer Security Act*[191] skupaj z NSA začeli razvijati standarde za javno dostopno kriptografijo, za zaščito občutljivih, a ne tajnih informacij. Projekt se je

[190] Glede mobilne telefonije GSM je treba opozoriti, da so šifrirne algoritme GSM že razbili, a to ne preseneča, saj so bili tako kot DES razviti s 'pomočjo' NSA. Telefoni GSM za šifriranje zvoka do bazne postaje uporabljajo algoritma A5/1 (močnejši) in A5/2 (šibkejši), za generiranje šifrirnih ključev pa algoritem A8. A8 sta Ian Goldberg in David Wagner razbila aprila 1998, prav tako sta avgusta 1999 dokazala, da je razbitje A5/2 mogoče v realnem času. Prvi uspešni napad na algoritem A5/1 je izvedel Jovan Golić maja 1999. Biryukov in Shamir pa sta dokazala, da ga je mogoče razbiti v manj kot sekundi z uporabo računalnika z vsaj 128 Mb RAM ter dvema 73 Gb diskoma (Schneier, 1999).

[191] Computer Security Act of 1987, 40 U.S.C. (1987).

imenoval *Capstone*, v okviru tega projekta pa naj bi razvili standarde za šifriranje podatkov, digitalno podpisovanje, izmenjavo ključev ter zgostitvene funkcije (za zagotavljanje integritete podatkov).

Pred sprejetjem zakona je bil Kongres postavljen pred vprašanje, katera agencija naj skrbi za razvoj civilne kriptografije. NSA se je kongresnike trudila prepričati, da bi morala to vlogo prevzeti ona. Direktor NSA William Odom je izpostavil, da ima NSA že dolgoletne izkušnje s kriptografijo in veliko strokovnjakov. Njegovi argumenti, da bi šlo v primeru, če to vlogo prevzame NBS, samo za dvojno birokracijo, pa Kongresa niso prepričali. Člani *House Government Operations Committee* so namreč zapisali, da se je NSA v preteklosti trudila zaustaviti ali pa omejevati raziskave v kriptografiji (Diffie in Landau, 1999: 68). Kljub temu je zakon določal, da se mora NIST pri izdelavi računalniško-varnostnih in kriptografskih standardov posvetovati z NSA.

Bitke pa še ni bilo konec. NIST je dobil nove naloge, ni pa dobil ustreznega financiranja za njihovo izvedbo. V primerjavi z NSA, ki je imela leta 1987 na *netajnem* računalniško-varnostnem programu 300 zaposlenih in proračun v vrednosti 40 milijonov dolarjev, je bil NIST finančno in kadrovsko silno podhranjen, saj je imel istega leta na voljo le 1,1 milijona dolarjev in 16 zaposlenih, do leta 1990 pa se je njegov proračun povečal na 1,9 milijona dolarjev, število zaposlenih pa na 33. Poleg tega sta NIST in NSA podpisala poseben memorandum, v katerem se je NIST zavezal, da se bo o vseh vprašanjih, povezanih s kriptografijo, posvetoval z NSA (Diffie in Landau, 1999: 70). S tem si je NSA zagotovila, da bo še naprej igrala pomembno vlogo pri omejevanju javno dostopne kriptografije. Neposredna posledica sodelovanja z NSA je bila vnovična zavrnitev algoritma RSA za državni standard v okviru projekta Capstone, čeprav naj bi ga tokrat uporabili za digitalno podpisovanje dokumentov. Po seriji neuspešnih sestankov med letoma 1989 in 1990 pa je namesto njega NSA ponudila svoj algoritem, a je bil počasen in oslabljen (Diffie in Landau, 1999: 72–73).

Septembra 1992 je podjetje AT&T napovedalo novo napravo, namenjeno šifriranju telefonskih komunikacij, imenovano *Surity 3600*. Stala naj bi 1100 dolarjev in naj ne bi uporabljala šifrirnih algoritmov, odobrenih s strani NSA. To je med ameriškimi državnimi organi povzročilo preplah in AT&T so najprej zagrozili s pravnimi posledicami (Sykes, 1999: 175). Aprila 1993 pa je ameriška vlada objavila predlog novega standarda za obdelavo podatkov (*Federal Information Processing Standard*), ki bi ga morale upoštevati vse vladne agencije in podjetja, ki z njimi sodelujejo. Predlog je predvideval uporabo *Escrowed Encrypted Standarda*. Gre za sistem depozita šifrirnih ključev (t. i. sistem *key escrow*), ki bi dopuščal uporabo močnih kriptografskih algoritmov, od posameznikov pa bi zahteval, da svoje ključe deponirajo pri pooblaščeni agenciji. To bi državnim organom omogočilo dostop do teh ključev (EPIC, 1998c in EPIC, 1998d).

Kmalu je nastala izvedba tega sistema za telefone, imenovala se je čip Clipper. To je bil poseben čip, namenjen vgradnji v telefone, v vsakega pa sta bili vgrajeni dve edinstveni nespremenljivi številki – serijska številka in rezervno geslo. Na podlagi teh dveh številk se tvori posebno polje LEAF (*Law Enforcement Access Field*), ki hrani sejni ključ (na začetku vsakega telefonskega pogovora se generira nov šifrirni ključ, ki velja za čas trajanja komunikacije – seje, od tod ime sejni ključ), tega pa je mogoče dobiti ob pomoči omenjenih številk. Predlog je predvideval, da

bi ti dve številki hranili ločeni depozitni agenciji in ju v primeru sodne odredbe posredovali preiskovalnim organom.

Pravosodno ministrstvo, ki ni želelo, da AT&T pošlje na trg svojo različico šifrirnega telefona, je kmalu po javni predstavitvi Escrowed Encrypted Standarda pri AT&T naročilo 9000 telefonov[192] s čipom Clipper (Phillips, 2001: 264), poleg tega so začeli pritiskati na vse izdelovalce kriptografskih produktov, naj 'prostovoljno' sprejmejo njihovo rešitev.

Toda predlog je bil deležen številnih kritik, med drugim tudi zato, ker je Clipper uporabljal šifrirni algoritem Skipjack, ki ga je razvila NSA in je bil do junija 1998 tajen (RSA Laboratories 2000, 114). Porodil se je tudi dvom o neodvisnosti depozitnih agencij,[193] poleg tega pravosodno ministrstvo ni predvidelo sankcij za primer, da bi agencije komu izročile ključe brez sodne odredbe (Sykes, 1999: 175). Pozneje je FBI poizkušal uveljaviti podoben zakon, ki bi zahteval obvezen depozit šifrirnih ključev, tokrat pri agenciji, neodvisni od vlade (ta sistem so prav tako poimenovali 'key escrow', zanj pa se uporablja tudi izraz 'key recovery' ali 'trusted third parties'); to je Marc Rotenberg iz EPIC označil za "*Clipper z veselim obrazom*" (Sykes, 1999: 177). Predlog je bil pozneje zavrnjen.

Po nekaterih zamislih naj bi sistem Clipper ne bil omejen samo na ZDA. NSA je šla celo tako daleč, da je začela kampanjo pri tujih državah, da bi sprejele standard Clipper, a pri tem seveda ni bila preveč uspešna (Sykes, 1999: 176). Celo dve leti po uradni opustitvi projekta je leta 1996 NSA vložila prošnjo za patentiranje sistema key-escrow; ugodeno ji je bilo aprila 2004.[194] Istega leta so ZDA začele pritiskati na OECD, naj sprejme kriptografske smernice, po katerih bi sistem depozita šifrirnih ključev postal mednarodni standard.

Piko na i je postavil raziskovalec Matt Blaze iz AT&T, ki je maja 1994 dokazal, da je mogoče polje LEAF pokvariti tako, da ga bo čip Clipper sprejel, polje pa ne bo vsebovalo sejnega ključa. To je celotno zamisel o sistemu depozita gesel povsem izničilo. Dva meseca zatem je podpredsednik ZDA predlog javno umaknil (Phillips, 2001: 264).

* * *

Ameriška vlada je torej uporabo kriptografije vztrajno skušala omejevati, čeprav so se praktično vsi poskusi omejevanja kriptografije v ZDA izkazali za neuspešne. Po eni strani zato, ker bi prepoved kriptografije omejevala svobodo govora, po drugi strani pa zato, ker so bile v kriptografske izdelke, ki jih je želela odobriti država, vgrajene resne varnostne pomanjkljivosti. Verjetno edini pravno sprejemljivi predlog je predvideval višjo kazen za uporabo kriptografije pri storitvah kaznivih dejanj. Če bi si posameznik pri kaznivem dejanju pomagal s kriptografijo, bi se mu kazen podvojila.[195]

---

[192] Naročilo je bilo vredno 8 milijonov dolarjev (Denning, 1994).

[193] Kopije ključev naj bi hranila *Treasury Department* in NIST.

[194] Kopija patenta št. 6,724,893 z dne 20. aprila 2004 je dostopna na spletni strani Cryptome.org (<http://cryptome.org/pat6724893.pdf>).

[195] Omenjeni predlog za podvojitev kazni je bil predlagan v ameriškem trgovinskem parlamentarnem odboru (EPIC, 1998a).

Ne glede na nevarnosti zlorabe kriptografije v kriminalne namene pa je *National Research Council* v svojem poročilu *Cryptography's Role in Securing the Information Society* leta 1996 zapisal, da NSA po njihovem mnenju ni prava agencija, ki naj bi bila odgovorna za razvoj kriptografije za zasebni sektor (Dam in Lin, 1996: 338), ter izrazil močno podporo uporabi kriptografije. Uporaba kriptografije bi po njihovem mnenju povečala zaupnost in varstvo osebnih podatkov posameznikov in podjetij ter zmanjšala ekonomsko vohunjenje s strani tujih podjetij. V poročilu so tudi zapisali, da se zavedajo nevarnosti, ki jih prinaša uporaba kriptografije, vendar je po njihovem mnenju na dolgi rok uporaba kriptografije neizbežna, koristi pa pretehtajo nad stroški (Dam in Lin, 1996: 339). Kaže, da so do tega spoznanja prišli tudi v ameriški administraciji, saj so leta 2000 ZDA precej sprostile (ne pa tudi povsem odpravile) izvozna dovoljenja za kriptografske izdelke (Madsen in Banisar, 2000: 118).

Poleg tega je maja 1999 zvezno pritožbeno sodišče iz Kalifornije v primeru *Bernstein proti Department of Justice*[196] razsodilo, da so izvozne omejitve v *Export Administration Regulations*, ki omejujejo distribucijo kriptografije, neustavne, ker omejujejo znanstveno izražanje (ang. *scientific expression* – sodišče je menilo, da je računalniški program, zapisan v programskem jeziku, oblika govora) in ker vladnim uradnikom podeljujejo neomejeno diskrecijsko pravico, s čimer je kršen prvi amandma,[197] ki zagotavlja svobodo govora.

Kljub temu ameriški državni organi še vedno izrabijo vsako priložnost za poiskus omejiti uporabo kriptografije ali povečati svoje pristojnosti pri prisluškovanju in prestrezanju elektronskih sporočil. ZDA so praktično edina demokratična država, ki skuša regulirati uporabo kriptografije znotraj svojih meja (Whitaker, 1999: 110). Tako so se že kmalu po 11. septembru v ZDA oglasile zahteve po prepovedi kriptografskih izdelkov, ki bi državnim organom onemogočali dostop do vsebine šifriranih sporočil (Harrison, 2001), in celo predlogi, naj ima policija pristojnost odrediti nadzor internetnih komunikacij brez odločbe sodišča za 48 ur (McCullagh, 2001a, 2001b in 2001c).

Mednarodni poskusi omejevanja kriptografije

Očitno je, da ugotovitve *National Research Council* držijo – širjenje kriptografije je neizbežno. K temu prispevajo tako tehnični napredek, potreba po varnem elektronskem poslovanju kot tudi to, da večina držav svojim državljanom ne omejuje uporabe kriptografije. Poleg tega, kot ugotavlja poročilo *Cryptography and Liberty 2000*, čedalje več držav izrecno zavrača omejevanje kriptografije; nekatere države (npr. Belgija leta 1994 in Francija leta 1999), ki so uporabo kriptografije prepovedovale, pa svoj odnos do tega vprašanja liberalizirajo (Madsen in Banisar, 2000: 7).

[196] Bernstein v. United States Department of Justice, 176 F.3d 1132 (1999).
[197] 1. amandma, Listina svoboščin (Bill of Rights), 1791.

Vendar pa se raba kriptografije širi predvsem v sferi ekonomije (npr. na področju varovanja poslovnih transakcij in zaščite avtorskih pravic), ne pa toliko na področju varovanja zasebnosti (npr. običajnih medčloveških komunikacij). Zato je uporaba šifriranja pri npr. elektronskem bančništvu povsem enostavna in globoko integrirana v sam sistem bančnega poslovanja, šifriranje elektronske pošte pa je v primerjavi s tem še vedno razmeroma zapleteno opravilo, poleg tega tudi ni standardizirano.

Ključno vlogo pri odpravljanju omejevanja kriptografije je odigrala EU. Evropska komisija je namreč oktobra 1997 pripravila poročilo "*Towards an European Framework for Digital Signatures and Encryption*", v katerem je zapisala, da je "*šifriranje bistveno orodje za zagotavljanje varnosti in zaupanja v elektronske komunikacije*" in da "*omejevanje uporabe šifriranja lahko prepreči podjetjem in državljanom, ki spoštujejo zakon, da bi se zaščitili pred napadi s strani kriminala*" (EPIC, 1997). Poročilo je tudi jasno zavrnilo uporabo sistema depozita šifrirnih ključev, med drugim tudi iz razloga proste konkurence, ter predlagalo, da se dovoli uporaba digitalnega podpisovanja brez vključenih identifikacijskih podatkov, kar omogoča varne anonimne transakcije (EPIC, 1997).

Kljub temu so ZDA skupaj z Veliko Britanijo na mednarodni ravni skušale doseči omejitve kriptografije. ZDA so – večinoma neuspešno – pritiskale na OECD, EU, G7 in G8 ter Svet Evrope, poizkusile pa so doseči tudi sklenitev mednarodnega dogovora Wassenaar Arrangement. Na drugi strani so jim nasprotovale večinoma Nemčija in skandinavske države (Madsen in Banisar, 2000: 19).

Wassenaarski sporazum

Wassenaarski sporazum je dokument o prepovedi izvoza tehnologije dvojne rabe (ang. *dual use technology*) v nekatere nedemokratične države. Ker je mogoče kriptografijo uporabljati tako za civilne kot tudi za vojaške namene, velja za tehnologijo dvojne rabe.

Leta 1998 je Wassenaar Secretariat predstavil nov seznam tehnologije dvojne rabe, na katerem so se znašli tudi nekateri kriptografski proizvodi. Ti izdelki, ki so ostali tudi na revidiranem seznamu iz leta 2003, so simetrični algoritmi, ki uporabljajo šifrirne ključe, daljše od 56 bitov, rešitve za faktorizacijo celih števil, večjih od 512 bitov, ter rešitve za izračun nekaterih diskretnih algoritmov. Izločeni pa so tisti izdelki, ki šifriranje uporabljajo za zaščito avtorskih pravic in intelektualne lastnine (npr. regijska zaščita na ploščah DVD) ter nekateri izdelki, ki se uporabljajo v bančništvu (Wassenaar Secretariat, 2003).

Na podlagi teh določil štejejo za tehnologijo dvojne rabe tudi spletni brskalniki, ki omogočajo več kot 56-bitno šifriranje, ter spletni strežniki SSL (*Secure Socket Layer*), ki se uporabljajo v elektronskem bančništvu in elektronskem poslovanju.

Vendar pa Wassenaarski sporazum nima statusa mednarodne pogodbe; bolj gre za telo, ki služi za izmenjavo informacij in stališč o mednarodni trgovini s tehnologijo dvojne rabe, njegova priporočila pa niso obvezna. Nekatere države (Kanada, Nemčija in Švica) so zato leta 1998 napovedale, da ne bodo upoštevale teh kriptografskih omejitev.

Kriptografske smernice OECD

ZDA so leta 1996 prek pravosodnega ministrstva (oziroma posebnega odposlanca za kriptografijo Davida Aarona), FBI in NSA začele pritiskati na OECD, naj sprejme kriptografske smernice. S tem bi sistem depozita šifrirnih ključev postal mednarodni standard. Predlog sta poleg ZDA podpirali še Velika Britanija in Francija, nasprotovali pa so mu predstavniki Japonske, Kanade, Nemčije in Danske (Madsen in Banisar, 2000: 19). Toda OECD je marca 1997 sprejela *Smernice o kriptografski politiki*,[198] v katerih je podprla neomejen razvoj in uporabo kriptografskih izdelkov (seveda pa so razlogi za to predvsem ekonomski, ne toliko človekove pravice). V *Smernicah* so zapisali, da je "*kriptografija dragoceno orodje za zaščito zasebnosti, tako tajnosti podatkov in komunikacij kot tudi za zaščito identitete posameznikov. Kriptografske metode prav tako ponujajo nove možnosti za zmanjšanje zbiranja osebnih podatkov s tem, ko omogočajo varna, a anonimna plačila, transakcije in interakcije*".[199] *Smernice* izpostavljajo osem načel, med njimi pravico posameznika, da uporablja tiste kriptografske metode, ki najbolj ustrezajo njegovim potrebam; državam pa priporočajo, da kar najbolj spoštujejo svobodo izbire: "*razvoj in nabava kriptografskih metod sme biti omejena samo s trgom v odprtem in konkurenčnem okolju*". Če so šla prizadevanja ZDA v smeri, da se omeji javno rabo močne kriptografije, pa so *Smernice OECD* izpostavile nasprotno načelo: "*Za zaščito priznanega javnega interesa, npr. zaščito osebnih podatkov ali elektronskega poslovanja, lahko države sprejmejo kriptografske politike, s katerimi zahtevajo uporabo takih kriptografskih metod, ki bodo zagotavljale zadostno stopnjo zaščite*".[200] Te *Smernice* je podprla tudi G8 na vrhunskem zasedanju v Denverju leta 1997 (Madsen in Banisar, 2000: 23).

Svet Evrope

Nekoliko drugačna stališča pa je leta 1995 sprejel Svet Evrope. Septembra 1995 so namreč sprejeli Priporočilo Sveta Evrope št. R(95) 13 glede problemov kazensko procesnega prava, povezanega z informacijskimi državami.[201] V njem so zapisali, da "*morajo imeti preiskovalni organi pooblastilo, da osebam, ki imajo nadzor nad podatki v računalniških sistemih, ukažejo, naj jim omogočijo dostop do računalniškega sistema in podatkov*" (10. člen). Poudarili so, da imajo operaterji javnih telekomunikacijskih storitev posebno dolžnost izvesti vse tehnične ukrepe, ki omogočajo zakonito prestrezanje telekomunikacij ter identifikacijo uporabnikov (11. in 12. člen). Glede uporabe šifriranja pa 14. člen priporoča sprejem ukrepov, ki bodo zmanjšali negativne učinke uporabe kriptografije, pri čemer pa ti ukrepi "*ne smejo prizadeti legitimne uporabe kriptografije bolj, kot je nujno potrebno*".

V tem stališču je že mogoče razbrati novo taktiko, s katero so si želeli preiskovalni organi zagotoviti možnost nadzorovanja.

---

198 OECD. 1997. Smernice o kriptografski politiki (Guidelines on Cryptography Policy), sprejete 27. marca 1997.
199 OECD. 1997. Smernice o kriptografski politiki (Guidelines on Cryptography Policy), sprejete 27. marca 1997.
200 OECD. 1997. Smernice o kriptografski politiki (Guidelines on Cryptography Policy), sprejete 27. marca 1997.
201 Svet ministrov Sveta Evrope. 1995. Priporočilo Sveta Evrope št. R(95) 13 glede problemov kazensko procesnega prava, povezanega z informacijskimi državami (*Recommendation No. R(95) 13, Concerning Problems of Criminal Procedure Law Connected with Information states*), sprejeto 11. septembra 1995.

Vrnitev k izvoru problema: zagotavljanje možnosti za nadzorovanje

Vodilno vlogo pri prizadevanjih za prepoved ali vsaj omejevanje kriptografije v ZDA je imela sprva NSA, FBI pa se je kljub izkušnji iz časa prohibicije v dogajanje vpletel šele pozneje, sredi 90. let 20. stoletja. Susan Landau je ugotovila, da je bil FBI sprva povsem nezainteresiran za sodelovanje z NIST in NSA pri postavljanju kriptografskih standardov. Svetovalec direktorja NSA Clinton Brooks ji je v pogovoru povedal, da v FBI dolgo časa niso dojeli, da komunikacije postajajo digitalne, zato so se jim zdela vprašanja kriptografije futuristična (Diffie in Landau, 1999: 75). Danes FBI velja za enega najbolj vnetih nasprotnikov kriptografije (EPIC, 1998b).

Vendar pa tajne službe in preiskovalni organi kriptografiji ne nasprotujejo zaradi nje same. To je vidno predvsem iz odnosa FBI do tega vprašanja. Problem predstavlja kriptografija skupaj z digitalizacijo in globalizacijo oziroma predvsem z dostopnostjo tehnologije vsem posameznikom. Kriptografija je problem zato, ker skupaj z drugimi tehnologijami onemogoča nadzor. In to ne nadzora majhne skupine posameznikov, temveč nadzor kogarkoli, ki bi mu bila kriptografija dostopna.

In ker jim s prepovedjo kriptografije ni uspelo, so se preiskovalni organi vrnili nazaj k bistvu problema. To pa je: kako si zagotoviti možnosti za nadzorovanje. To se je najbolj jasno pokazalo na primeru *Digital Telephony Act*. Clinton Brooks je namreč Landauovi med enem izmed pogovorov povedal, da je bilo celotno prizadevanje okrog sprejema *Digital Telephony Act* leta 1994 (uradno se imenuje *Communications Assistance for Law Enforcement Act*[202]) rezultat srečanj med NSA, FBI in NIST (Diffie in Landau, 1999: 76).

Operacija 'Root Canal' in vgrajevanje 'stranskih vrat'

Pred nastankom digitalne tehnologije je prisluškovanje potekalo tako, da so preiskovalni agenti na žice osumljenčevega telefona priključili prisluškovalno napravo; tak je bil tudi prvi sodno dokumentiran primer vladnega prisluškovanja, Olmstead,[203] v ZDA leta 1928. Pozneje so agenti prišli do operaterja telefonskega omrežja in se v njegovih prostorih priključili na želeni telefonski priključek, operater pa jim je moral omogočiti dostop do svojih naprav. Pri tem je bila vloga operaterjev pasivna, poleg tega so preiskovalni organi v prostore operaterja lahko vstopili samo s sodnim nalogom.

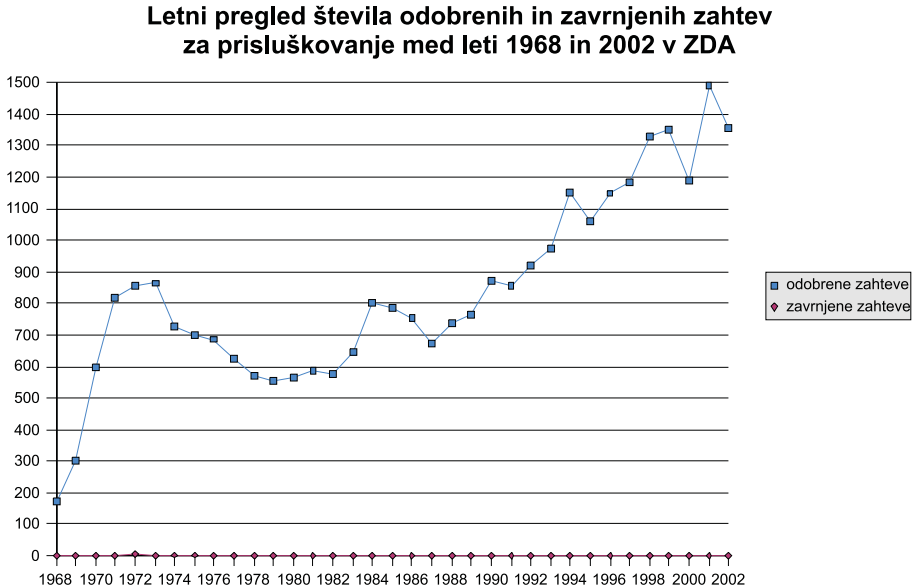
Konec 80. let 20. stoletja je FBI začel izvajati operacijo Root Canal (*Operation Root Canal*), v okviru katere je želel telefonske operaterje prepričati, naj v svoje telefonske centrale vgradijo tehnične zmožnosti za enostavnejše prisluškovanje (na daljavo), hkrati pa bi morali preiskovalnim organom omogočiti tudi dostop do nešifrirane komunikacije v primeru, da se komunikacija šifrira.[204] FBI je leta 1991 Kongresu tako predlagal sprejem določila, ki bi od izdelovalcev in ponudnikov elektronskih komunikacijskih sistemov zahteval, naj v svoje izdelke vgradijo tako tehnologijo, ki bo državnim organom omogočila dostop do nešifrirane komunikacije (Phillips,

---

[202] Communications Assistance for Law Enforcement Act (Digital Telephony Act) of 1994, 47 U.S.C. (1994).
[203] Olmstead v. United States, 277 U.S. 438 (1928).
[204] Gre za zamisel o mrežnem šifriranju (ang. *link encryption*), o kateri je bil govor v enem izmed prejšnjih poglavij.

2001: 263). Z drugimi besedami, predlog je predvideval, da bi morali izdelovalci v svoje kriptografske izdelke vgraditi posebno bližnjico za dostop oziroma t. i. 'stranska vrata' (ang. *trap door, back door*), skozi katera bi imeli državni organi dostop do telekomunikacijskega omrežja.

Telekomunikacijska podjetja so zahteve FBI zavrnila v glavnem zaradi visokih stroškov, ki bi jih imela s prilagajanjem svoje opreme tem zahtevam[205], pa tudi zato, ker bi taka stranska vrata lahko izkoristil kdorkoli, prav tako pa so predlogu nasprotovale tudi številne nevladne organizacije. Vendar pa je po nekaj letih lobiranja in po tem, ko je vlada telekomunikacijskim podjetjem ponudila pol milijarde dolarjev za pokritje stroškov, leta 1994 Kongres sprejel *Communications Assistance for Law Enforcement Act* (CALEA),[206] znan tudi pod imenom *Digital Telephony Act* (EPIC, 2004c).



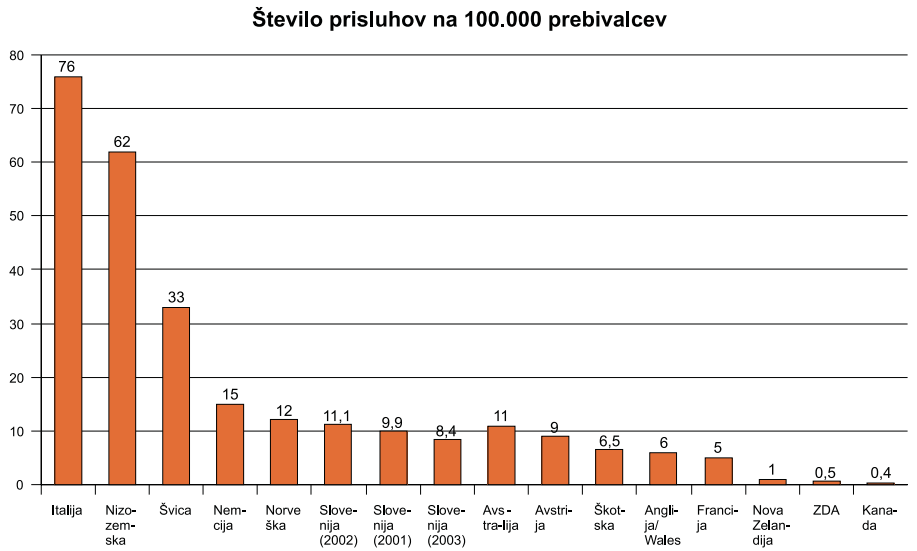
Graf 2: Letni pregled števila odobrenih in zavrnjenih zahtev za prisluškovanje med leti 1968 in 2002 v ZDA. Vir: Title III Wiretap Orders 1968-2002 (EPIC, 2002a).

[205] Podobno Etzioni piše o tem, da sta FBI in FTC želela prepričati mobilne operaterje, naj razvijejo tehnologijo, ki bi omogočala lociranje uporabnikov mobilnih telefonov. Podjetja so sodelovanje zavračala in to so utemeljevali z razlogi ščitenja zasebnosti svojih uporabnikov. Ko pa je trg sam začel zahtevati lokacijske storitve, so podjetja pozabila na zasebnost in začela razvijati tovrstno tehnologijo, ki naj bi se uporabljala v komercialne namene. Seveda jo je mogoče uporabiti tudi v preiskovalne namene (Etzioni, 1999: 130). To kaže na to, da je skrb za zasebnost pogosto zgolj krinka, s katero je mogoče uveljaviti drugačne interese.

[206] Communications Assistance for Law Enforcement Act (Digital Telephony Act) of 1994, 47 U.S.C. (1994).[207] Freedom of Information Act of 2002, 5 U.S.C. (2002).

Organizacija CPSR je na podlagi zahtevka FOIA[207] dobila 185 strani obsežno dokumentacijo o dejavnostih FBI, ki je razkrila, da je FBI v okviru operacije Root Canal sprožil usklajeno javno kampanjo za sprejem ustrezne zakonodaje. Predstavniki FBI so namreč poudarjali, da se je zaradi razvoja tehnologije zagotavljanje spoštovanja zakonov (ang. *law enforcement*) znašlo v krizi, saj naj za preganjanje kriminala ne bi bilo več mogoče uporabljati prisluškovanja. To zadnje sicer ni držalo, saj so člani CPSR ugotovili, da dokumenti FBI dokazujejo, da FBI ni imel nikakršnih tehničnih težav s prisluškovanjem. Kopije teh dokumentov so objavljene v knjigi *The Electronic Privacy Papers* (Schneier in Banisar, 1997: 135–219). Še več. Kot je razvidno iz analize odobrenih in zavrnjenih zahtev za prisluškovanje med letoma 1968 in 2002, ki so jo opravili v EPIC, se je število odobrenih prisluhov od 80. let praktično vztrajno večalo, enako naraščanje števila prisluhov velja tudi za prisluškovanje NSA po zakonu *Foreign Intelligence Surveillance Act*[208] (EPIC, 2006c).

Ob tem tudi ni zanemarljiv podatek, da je v mednarodnem merilu prisluškovanja v ZDA razmeroma malo (podatki so na voljo seveda samo za uporabo metode prisluškovanja s strani policije, ne pa tudi tajnih služb). Razlog pa je v tem, da lahko policija v ZDA enostavneje uporabi druge prikrite metode in sredstva za zbiranje podatkov kot npr. v evropskih državah.



Graf 3: Primerjava števila prisluhov na 100.000 prebivalcev po 14 državah za leto 2002 (Vir: Albrecht, Dorsch in Krüpe, 2003: 104 ter Policija, 2004).

[208] Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. (1978).

Sicer je res, da se je povečala tudi uporaba telekomunikacijskih naprav, vendar kritiki opozarjajo, da je resen problem tudi enostavnost prisluškovanja, ki jo omogoča sodobna tehnologija. CALEA[209] od telefonskih operaterjev namreč zahteva, da preiskovalnim organom omogočajo prestrezanje vseh komunikacij v realnem času oziroma v času njihovega prenosa. Zakon zahteva, da morajo biti prestrežene komunikacije v taki obliki, da jih je mogoče prenesti na oddaljena sredstva preiskovalnih organov. Z drugimi besedami: vloga operaterjev je zdaj postala aktivna, saj zakon zahteva, da na zahtevo preiskovalnih organov prestreženo komunikacijo le-tem tudi dostavijo po telekomunikacijskem omrežju, oziroma da v svoje telefonske centrale vgradijo zmožnosti za prisluškovanje na daljavo (t. i. *remote wiretapping port*), kar je preiskovalcem močno olajšalo delo. Tako agentom FBI ni več treba hoditi v prostore telekomunikacijskih podjetij, temveč lahko prisluškujejo iz svojih pisarn. Odtod izraz "prijazno prisluškovanje" (ang. *to wiretap friendly*), ki pomeni predvsem to, da je prisluškovanje prijazno oziroma preprosto za prisluškovalca (Laurant, 2003: 49). Seveda je jasno, da bi bilo zelo težko zagotoviti prisluškovanje prav vsem naročnikom telekomunikacijskih storitev hkrati, zato CALEA[210] določa, da javno tožilstvo določi, kakšna mora biti maksimalna zmogljivost hkratnih prisluhov, ki jih morajo telekomunikacijska podjetja zagotoviti. FBI je leta 1995 predlagal, naj bi operaterji zagotovili zmogljivosti za hkratno prisluškovanje do enemu odstotku komunikacij v posamezni regiji (FBI, 1995).

Vendar pa se ti predlogi niso ustavili samo v ZDA, pa tudi v že omenjenem priporočilu Sveta Evrope št. R(95) 13[211] ne. FBI je namreč že leta 1991 začel lobirati pri EU, naj sprejme podobno zakonodajo, ki bo od operaterjev telekomunikacij zahtevala tesnejše sodelovanje z organi pregona. Na srečanju Sveta ministrov EU decembra 1991 v Treviju je bilo odločeno, da je treba narediti študijo o učinkih razvoja prava, tehnologije in trga v telekomunikacijskem sektorju na različne možnosti prestrezanja. Junija leta 1993 so nato ministri na sestanku v Kobenhavnu sprejeli t. i. 'vprašalnik o telefonskem prisluškovanju', ki je bil poslan vsem državam članicam in na podlagi katerega je novembra istega leta Svet ministrov sprejel že omenjeno resolucijo o zakonitem prestrezanju telekomunikacij (*Resolution on the Lawful Interception of Telecommunications*). Resolucija je bila v evropskem uradnem listu z nekaj dopolnili objavljena leta 1996 (Statewatch, 1997).

Iz osnutka resolucije, katerega dele je v svojem poročilu objavila Statewatch in so sicer zaupni[212], je razvidno, da je imel na njen nastanek in oblikovanje veliko in neposredno vlogo prav FBI. Končno besedilo resolucije tako pripisuje prestrezanju telekomunikacij velik poudarek: "*Z zakonom podprto prestrezanje telekomunikacij je pomembno orodje za zaščito nacionalnega*

---

209 Communications Assistance for Law Enforcement Act (Digital Telephony Act) of 1994, 47 U.S.C. (1994).

210 Communications Assistance for Law Enforcement Act (Digital Telephony Act) of 1994, 47 U.S.C. (1994).

211 Svet ministrov Sveta Evrope. 1995. Priporočilo Sveta Evrope št. R(95) 13 glede problemov kazensko procesnega prava, povezanega z informacijskimi državami (*Recommendation No. R(95) 13, Concerning Problems of Criminal Procedure Law Connected with Information states*), sprejeto 11. septembra 1995.

212 Gre za dokument *Interception of communications*, report to COREPER, ENFOPOL 40, 10090/93, Confidential, Brussels, 16.11.93, katerega del je objavljen v Statewatch, 1997.

interesa, nacionalne varnosti in preiskovanje resnih kaznivih dejanj". Duha CALEA iz leta 1994 pa je mogoče razbrati iz drugega dela resolucije, kjer je med zahtevami, ki jih bodo morala izpolnjevati telekomunikacijska podjetja, navedeno, da morajo preiskovalnim organom na njihovo zahtevo omogočiti nepretrgan in trenuten dostop do podatkov, ki jih prenašajo, ter spremljajoče prometne podatke. Če telekomunikacijsko podjetje uporablja šifriranje ali stiskanje podatkov, pa se od njega zahteva, da preiskovalnim organom priskrbi podatke v nešifrirani obliki (Council Resolution 1996, 1–6).

Hkrati je komite K4 (poseben organ, ustanovljen na podlagi Maastrichtske pogodbe, ki koordinira predvsem pravno in policijsko sodelovanje držav članic EU) pripravil poseben memorandum, namenjen državam nečlanicam EU,[213] s katerim je skušala EU k sporazumu o prestrezanju telekomunikacij pritegniti še druge države. S tem je EU na pobudo FBI dosegla harmonizacijo zakonodaje, predvsem pa tehničnih karakteristik telekomunikacijske opreme. V leta 1995 nastalem poročilu *Delovne skupine za policijsko sodelovanje* (*Police Cooperation Working Group*) je namreč zapisano, da mora biti v naslednji generaciji satelitskih telekomunikacijskih sistemov vgrajena zmožnost nadzorovanja posameznikov (ang. "*next generation of satellite-based telecommunications systems ... should be able to 'tag' each individual subscriber in view of a possibly necessary surveillance activity.*") Po njihovem mnenju novi telekomunikacijski sistemi predstavljajo "*globalen problem, ki je lahko rešljiv le z globalnim sodelovanjem*" (Statewatch, 1997); to kaže na to, da se nadzor globalizira. Statewatch je v svojem poročilu zapisala: "*Kot kaže, je strategija najprej zagotoviti, da se bo 'zahodni svet' (EU, ZDA in njuni zavezniki) sporazumel o 'pravilih' in 'postopkih', potem pa bodo te izdelke [telekomunikacijske naprave, m. op.] prodali državam tretjega sveta...*" (Statewatch, 1997).[214]

Potem ko se je izkazalo, da razvoja kriptografije ni mogoče zaustaviti, je šel razvoj sodobnega nadzorovanja v smeri pravnih zahtev za omogočanje neoviranega dostopa do komunikacij. Po eni strani to kaže na težnjo po preventivnem obravnavanju vseh posameznikov kot kriminalcev in prenašanju stroškov nadzora na zasebna podjetja in s tem posredno na njihove stranke. Po drugi strani pa je prišlo tudi do pomembnega premika v razumevanju pooblastil države. Ne samo, da vlada lahko zahteva dostop do komunikacije, temveč, kot so zapisali predstavniki ACLU v odprtem pismu kongresniku Brooksu 22. septembra 1994, predlog CALEA[215] "*ustvarja predpostavko, ki je nevarna in brez primerjave, da namreč vlada ... lahko od zasebnikov zahteva, da ustvarijo poseben dostop (ang. create special access)*". To je po njihovem mnenju primerljivo z "*zahtevo, da bi vsi graditelji morali v nove hiše vgraditi nadzorne kamere, ki bi jih lahko uporabljala vlada*" (ACLU, 1994).

---

213 Gre za *Memorandum of Understanding on the Legal Interception of Telecommunications*.

214 Danes so v vse nove telefonske centrale že vgrajene tehnične možnosti za prisluškovanje in to predstavlja nov problem, saj so telefonske centrale z vsemi tehničnimi zmožnostmi za nadzorovanje vred danes dostopne tudi zasebnikom (npr. podjetjem), nad katerimi pa se izvaja precej manj strog nadzor kot nad operaterji javne telefonije.

215 Communications Assistance for Law Enforcement Act (Digital Telephony Act) of 1994, 47 U.S.C. (1994).

EPIC-ovo odprto pismo pa je bilo še jasnejše: "*Prvič se bo zgodilo, da bo zakonodaja zahtevala, da morajo biti naša sredstva za komuniciranje oblikovana tako, da olajšajo vladno prestrezanje. Če smo vedno priznali potrebo preiskovalcev, da dobijo preiskovalne informacije na podlagi sodnega naloga, pa nikoli nismo sprejeli stališča, da mora biti uspeh take preiskave zagotovljen... Načelo, ki je uveljavljeno v predlogu zakona, bo lahko enostavno uporabljeno za vse nove tehnologije, ki nastajajo, in bo vključeno v načrt Nacionalne informacijske infrastrukture*" (EPIC, 1994).
Leta 1994 so med nove, nastajajoče tehnologije šteli internet. Šest let po EPIC-ovem odprtem pismu so se njihovi strahovi popolnoma uresničili.

Carnivore

Junija 1996 je Phil Zimmermann nastopil pred podkomitejem ameriškega senata. V svojem pričanju je posvaril pred prestrezanjem elektronskih sporočil. Opozoril je namreč na to, da je elektronska sporočila mogoče prestrezati in analizirati bistveno enostavneje, kot to velja za govorne komunikacije, saj tehnologija omogoča, da je to narejeno "*preprosto, rutinsko, avtomatsko in neopazno ter v velikem obsegu*" (Zimmermann, 1993). Zimmermann je opozoril na to, da je tehnologija Velikega brata v internet na neki način že vgrajena. Manjkala je samo aplikacija, ki bi to tehnologijo v praksi tudi izvajala.[216]

Sredi leta 2000[217] so začeli v javnost prihajati podatki, da FBI pripravlja poseben sistem za nadzor interneta, imenovan Carnivore. EPIC je po FOIA[218] od FBI zahteval vpogled v dokumentacijo o programu, vendar je do dokumentov prišel šele s pomočjo tožbe (EPIC, 2005a). Dokumentacija, ki jo je prejel, je razkrila, da gre za poseben računalniški sistem (uradno se imenuje DCS1000), ki ga državni organi namestijo na povezave ponudnika dostopa do interneta, namenjen pa je prestrezanju in filtriranju celotnega internetnega prometa, ki poteka prek te povezave.[219] Neodvisno raziskovalno poročilo iz decembra 2000 je pokazalo, da je sistem sestavljen iz priključka v 'ethernetno'[220] omrežje, računalnika za filtriranje in zbiranje podatkov, ki sta nameščena pri ponudniku dostopa do interneta, ter nadzornega računalnika, na katerega se lahko po varni telefonski povezavi navežejo agenti FBI in po njej lahko upravljajo

---

[216] Za razliko od telefonije ni enotnega standarda za prestrezanje internetnih komunikacij. *IETF Network Working Group* je celo ugotovila, da je prestrezanje na internetu zelo težko izvesti in to je privedlo do špekulacij, da bodo državne organizacije opustile poizkuse uvedbe nadzora nad internetom (Branch, 2003). Seveda se to ni zgodilo.

[217] Obstoj Carnivora je prvi javno omenil Robert Corn-Revere v svojem pričanju pred parlamentarnim pododborom za ustavo 6. aprila 2000 (Corn-Revere, 2000).

[218] Freedom of Information Act of 2002, 5 U.S.C. (2002).

[219] Podoben sistem "črne škatle" so leta 1998 uvedli v Rusiji. Imenuje se SORM-2, vendar so za razliko od ZDA v Rusiji zahtevali, da njegovo namestitev in vzdrževanje plačujejo sami ponudniki dostopa do interneta. (V Rusiji morajo namreč ponudniki dostopa do interneta pridobiti državno licenco za opravljanje dejavnosti). Po dveh ustavnih pritožbah je bil z nekaj manjšimi spremembami sistem kmalu uveden po vsej Rusiji, civilnega nadzora nad njegovim delovanjem pa ni (Laurant, 2003: 54, 420). Podoben sistem uporabljajo v Ukrajini, a so tam zahtevo za kritje stroškov namestitve sistema podprli večji operaterji, ki pričakujejo, da bodo s tem onemogočili konkurenco manjših operaterjev (Laurant, 2003: 509).

[220] Ethernet je tehnologija prenosa podatkov, ki se uporablja v krajevnih omrežjih. V 70. letih prejšnjega stoletja jo je razvil Robert Metcalfe.

prestrezno napravo in pregledujejo podatke. Prek nadzornega računalnika lahko agenti FBI nastavljajo filtre, sprožijo začetek zbiranja podatkov ali zbiranje zaustavijo ter podatke prenesejo do svojih pisarn. Carnivore ima dva načina delovanja, t. i. omejeni način (ang. *pen mode*), v katerem se zbirajo samo naslovni (prometni) podatki (ang. *addressing information* – naslovi IP in uporabniška imena pošiljatelja in prejemnika elektronske pošte itd.), ter polni način (ang. *full mode*), v katerem se zbira celotna vsebina komunikacij (vsebina elektronskih sporočil, vsebina prenesenih datotek, spletnih strani itd.) (IIT Research Institute, 2000: ix-x).

Nastanek Carnivora je odprl več vprašanj. Prvi problem je v tem, da je sistem zasnovan tako, da spremlja dejavnosti *vseh* uporabnikov, podatke o osumljencih, za katere je izdan sodni nalog, pa je nato mogoče pridobiti s pomočjo filtriranja. Načeloma bi torej sistem lahko zapisoval ves promet vseh uporabnikov. Čeprav poročilo navaja, da naj bi bil Carnivore opremljen z modemom zmogljivosti prenosa 56k bps (IIT Research Institute, 2000: 3–12), pa nekateri opozarjajo, da so te naprave (zanje se uporablja tudi izraz črna škatla, ang. *black box*) povezane z računalniki preiskovalnih organov s hitrimi povezavami (Laurant, 2003: 53). Nekateri podatki celo kažejo na to, da so bile že v začetku to povezave vrste T1, ki omogočajo prenos do 1,5 Mb/s (McCullagh, 2001d).

Poleg tega javnosti ni dostopna izvorna koda programa. FBI trdi, da izvorne kode ne sme razkriti, ker mu to prepovedujejo licenčni pogoji (program je namreč razvilo zasebno podjetje); poleg tega bi bilo s pomočjo izvorne kode mogoče v programu najti napake, katerih zloraba bi onemogočila nadzorovanje (IIT Research Institute, 2000: 4–8). Toda brez izvorne kode ni mogoče ugotoviti, ali morda program ne vsebuje kakšnih skritih funkcij, ki omogočajo zlorabe. Revizorji so v poročilu zapisali, da je nevarnost, da bi s pomočjo Carnivora kdo namerno ali nenamerno nepooblaščeno prestrezal internetne komunikacije. Avtorji poročila sicer ugotavljajo, da je verjetnost, da bi to počel kdo mimo FBI, resda minimalna, in poudarjajo pomen sodnega nadzorstva nad delom preiskovalcev, so pa zapisali, da ugotavljanje nevarnosti nepooblaščenih namernih kršitev presega namen poročila (IIT Research Institute, 2000: 4–10).

Na še en pomemben vidik te tehnologije pa je opozoril Phillip Branch s *Swinburne University of Tehnology*. Po njegovem mnenju zakonito prestrezanje v internetu poleg povečane možnosti zlorab že po definiciji ogroža omrežno varnost. Posebej problematične so lahko napake in varnostne pomanjkljivosti naprav za prestrezanje internetnega prometa, kar bi v končni fazi lahko celo omogočilo nezakonite zlorabe s strani kiberkriminala. Da taki pomisleki niso neutemeljeni, kaže prisluškovalna afera v Grčiji leta 2006. Februarja tega leta je namreč razvedelo, da je nekdo od obdobja pred olimpijskimi igrami leta 2004 do marca 2005 nezakonito prisluškoval okrog 100 mobilnim telefonom grških politikov, med drugim tudi predsedniku vlade. Pozneje se je izkazalo, da so napadalci prisluškovali s pomočjo zlorabe slabo dokumentiranega modula za zakonito prisluškovanje (Schneier, 2006f). Te naprave lahko vplivajo tudi na stabilnost omrežja in zanesljivost internetnih storitev (Branch, 2003). Poleg tega je Branch opozoril na še en pomemben problem, ki za ZDA sicer ni preveč relevanten, za druge države, ki bi tak sistem kupile od ZDA, pa zelo. Opozoril je namreč na vsaj teoretično možnost, da so v prestrezne naprave morda namerno vgrajene tudi take tehnologije, ki bi tujim tajnim službam omogočale

nezakonit dostop do naprave in s tem do internetnih komunikacij.

Na nevarnost zlorabe s strani FBI pa je pokazala ugotovitev IIT Research Institute, da Carnivore nima vgrajenega sistema individualne odgovornosti, saj se vsi agenti v sistem prijavijo z istim uporabniškim imenom in geslom (IIT Research Institute, 2000: 5–2). V primeru zlorab bi bilo torej zelo težko ugotoviti, kdo je zanje odgovoren, zato je bilo v študiji zapisano priporočilo, naj se to popravi. Do konca leta 2003 sistem Carnivore ni bil popravljen (Laurant, 2003: 533), januarja 2005 pa se je izkazalo, da je FBI sistem Carnivore nehal uporabljati leta 2002 (FBI, 2003a in FBI, 2003b), namesto njega pa uporablja neimenovano komercialno programsko opremo.

Predstavnik ACLU Barry Steinhardt je 24. julija 2000 v pričanju pred kongresnim odborom izjavil, da "*noben preiskovalni organi ni nikoli pred tem zahteval pooblastila za dostop do vseh komunikacij, ki potekajo prek omrežja ponudnika storitve, na temelju nenadzorovane obljube, da ne bo zablodil onkraj meja svojih pooblastil.*" (Steinhardt, 2000).

Dodaten problem je predstavljala namera FBI, da Carnivore namesti na vse ponudnike dostopa do interneta. To je sprožilo huda nasprotovanja ameriških uporabnikov interneta, pa tudi ponudnikov dostopa do interneta. (Organizirana je bila tudi odmevna kampanja pod imenom StopCarnivore.) Najodmevnejša je bila zavrnitev enega največjih ameriških ponudnikov dostopa do interneta, podjetja Earthlink. To je namreč imelo zaradi namestitve Carnivora tehnične težave, poleg tega je trdilo, da je razvilo svojo rešitev za spoštovanje odredb sodišča, s katero preiskovalnim organom lahko omogoči dostop do vseh informacij, ki jih zahtevajo s sodnim nalogom (StopCarnivore.org, 2000). Kljub temu so 4. februarja 2004 prejeli sodno odredbo, ki jim je nalagala namestitev Carnivora. To je edina znana sodna odredba, ki od ponudnika dostopa do interneta zahteva namestitev Carnivora.[221] Zato so takrat ocenjevali, da bo sistem v letu ali dveh kljub odporu nameščen v vse ponudnike interneta v ZDA, a je do tega prišlo še hitreje. FBI je namreč teroristične napade 11. septembra 2001 hitro izkoristil za povečanje nadzora na internetu (McCullagh, 2001d ter Tech Law Journal, 2001). Spletni časopis Wired News je že 12. septembra 2001 poročal, da so samo nekaj ur po terorističnih napadih agenti FBI začeli obiskovati ponudnike dostopa do interneta in elektronske pošte z zahtevami po namestitvi sistema Carnivore. Ponudili so jim plačilo stroškov in obljubili, da bo namestitev trajala le kratek čas. Zaradi tega in zaradi učinka terorističnih napadov so pri tem naleteli na malo nasprotovanja (McCullagh, 2001d).

Ob sprejemanju CALEA[222] je FBI trdil, da se s sprejemom tega zakona ne bo nič spremenilo. Agentje bodo še vedno potrebovali sodni nalog, zakon pa bi le znova vzpostavil ravnovesje med pravicami in varnostjo, ki je veljalo v času pred nastankom digitalne tehnologije in ga je nastanek digitalizacije in kriptografije porušil (Sykes, 1999: 164).

---

[221] Kopijo sodne odredbe je objavil EPIC na naslovu: <http://www.epic.org/privacy/carnivore/cd_cal_order.html>.

[222] Communications Assistance for Law Enforcement Act (Digital Telephony Act) of 1994, 47 U.S.C. (1994).

Vendar pa zakonodaja, ki je bila sprejeta po terorističnih napadih 11. septembra 2001, preiskovalnim organom omogoča, da dobijo dovoljenje za prisluškovanje po enostavnejši poti, če dokažejo, da preiskujejo zadeve, povezane z nacionalno varnostjo. V manj kot tednu dni po napadih je bil vložen predlog USA PATRIOT Act[223] in bil sprejet po hitrem postopku in praktično brez razprave (EPIC, 2005b). USA PATRIOT Act[224] dovoljuje zbiranje prometnih podatkov (t. i. *pen register*) na podlagi potrdila tožilca, da bodo pridobljeni podatki in uporaba prestrezanja verjetno relevantni za preiskavo (*Sec. 216: Modification of authorities relating to use of pen registers and trap and trace devices*). 216. člen je definicijo prometnih podatkov, ki je bila prej napisana za telefonijo, razširil tako, da velja za tudi internet, vendar je po mnenju EPIC problematična zato, ker je mogoče iz naslovov URL, ki zapadejo pod definicijo 216. člena, odkriti veliko več informacij kot iz podatka o klicani telefonski številki.

V okviru FISA (*Foreign Intelligence Surveillance Act*[225]) so dovoljena t. i. klateška prisluškovanja (ang. *roving wiretap*, uporablja se tudi izraz *multipoint wiretaps*), kar pomeni, da lahko FBI in CIA na podlagi ene odredbe prisluškujeta več različnim napravam, ki jih *morda* uporablja osumljenec (*Sec. 206: Roving surveillance authority under the Foreign Intelligence Surveillance Act of 1978*). Kritiki opozarjajo, da takšne splošne odredbe FBI omogočijo prestrezanje komunikacij vseh uporabnikov javnega internetnega dostopa (npr. v knjižnicah, univerzah ali kiberkavarnah), saj lahko FBI domneva, da jih bo uporabil tudi osumljenec.

Federalna sodišča lahko ne glede na svojo krajevno pristojnost izdajajo prisluškovalne odredbe, ki veljajo za celotno državo (*Sec. 220: Nationwide service of search warrants for electronic evidence*).

V nekaterih primerih je mogoče celo prestrezanje brez sodne odredbe ali pa lahko preiskovalni organ od ponudnika elektronskih storitev zahteva, da podatke na podlagi sodnega poziva predloži sodišču (t. i. *subpoena*), torej za njihovo pridobitev ni potrebna sodna odredba. 217. člen namreč določa, da je mogoče prestrezanje komunikacij računalniškega prestopnika (ang. *computer trespasser*) brez sodne odredbe, če lastnik ali operater zaščitenega računalnika, na katerega je prestopnik vdrl, to dovoli. Kritiki opozarjajo, da je 'zaščiteni računalnik' definiran tako, da lahko 217. člen velja za praktično katerikoli vdor kamorkoli na internetu (*Sec. 217: Interception of computer trespasser communications*). 210. člen določa amandmaje k ECPA,[226] ki preiskovalnim organom omogočajo, da od ponudnika storitev zahtevajo, da sodišču predloži (na podlagi sodnega poziva (t. i. *subpoena*)) osebne podatke naročnika, prometne podatke o njegovih storitvah (podatke o klicih, čas klicev, vrste uporabljenih storitev itd.) ter način plačila storitev, skupaj s številkami kreditnih kartic in bančnih računov, od koder je bila storitev plačana (*Sec. 210: Scope of subpoenas for records of electronic communications*); 212. člen pa razširja definicijo nujnih primerov, v katerih ponudnik elektronskih storitev lahko preiskovalcem razkrije podatke

[223] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001, 18 U.S.C. (2001).

[224] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001, 18 U.S.C. (2001).

[225] Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. (1978).

[226] Electronic Communication Privacy Act of 1986, 18 U.S.C. (1986).

o naročniku ali vsebino komunikacij, če grozi neposredna nevarnost za življenje ali telo (*Sec. 212: Emergency disclosure of electronic communications to protect life and limb*). *The Homeland Security Act*[227] pa je pozneje to določbo razširil tudi na primere, ko preiskovalni organ to v dobri veri domneva.

USA PATRIOT Act ima še druga določila, ki povečujejo možnosti za elektronsko nadzorovanje (EPIC, 2005b, EFF, 2003 ter USA PATRIOT Act[228]), zato ne preseneča dejanski razmah elektronskega nadzorovanja v ZDA. Po navedbah poročila Privacy and Human Rights 2003 je bilo leta 2002 v ZDA odobrenih 1228 zahtevkov za prisluškovanje po *Foreign Intelligence Surveillance Act*,[229] največ dotlej. Uporaba elektronskega nadzorovanja se je v ZDA v desetih letih več kot potrojila, pri čemer so preiskovalci zaznali uporabo kriptografije le v 18 primerih in jim je v vseh uspelo podatke dešifrirati (Laurant, 2003: 531). Težnje po širjenju pooblastil preiskovalnih organov pa so vidne tudi drugod po svetu. *Konvencija o kibernetski kriminaliteti*,[230] ki jo je leta 2001 sprejel Svet Evrope, tako v 17. členu od podpisnic predvideva sprejetje ukrepov, ki bodo zagotovili takojšnje zavarovanje podatkov o prometu ter razkritje zadostne količine podatkov, ki omogočajo ugotovitev istovetnosti ponudnika storitev; poseben problem pa predstavlja prestrezanje internetnih komunikacij, o čemer več v nadaljevanju.

Tako so se trditve FBI, da bo CALEA[231] le znova vzpostavil ravnovesje med pravicami in varnostjo, ki je veljalo v obdobju pred nastankom tehnologije in kriptografije, izkazale za neresnične. Pravna načela, ki jih je uvedel CALEA in ki so botrovala nastanku Carnivora, so v ZDA skupaj z USA PATRIOT Act[232] tehtnico izrazito prevesile stran od pravice do zasebnosti. Barry Steinhardt, direktor ACLU, je v intervjuju za Wired News konec leta 2001 opisal vpliv USA PATRIOT Acta takole: "*Odličen primer tega [da je zakonodaja sodišča izločila iz procesa nadzora nad nadzorovanjem] je v USA Patriot Actu uporaba zakonodaje za prisluškovanje v internetu, kjer imate naslove internetnih protokolov in URL-je. Vloga sodišč ne bi mogla biti bolj omejena. So samo še podpisovalci [sodnih odredb, m. op.] (ang. they are rubber-stamping). Vse, kar morajo storiti preiskovalci, je, da se prikažejo in rečejo, da opravljajo preiskavo, sodišče pa mora to požigosati*" (Polen, 2001). Podobno velja tudi za druge države, ki so po 11. septembru 2001 spreminjale kazensko in preiskovalno zakonodajo. Poročilo privacy & Human Rights 2003 namreč ugotavlja, da je povsod po svetu mogoče opaziti povečan obseg pooblastil za nadzorovanje in obseg podatkov, ki jih državni organi smejo zbirati, poenostavljanje postopkov za odobritev takih posegov s strani sodišč ter zmanjšan nadzor nad delom preiskovalnih organov in tajnih služb (Laurant, 2003: 23–24).

---

227 The Homeland Security Act of 2002, 6 U.S.C. (2002).

228 Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001, 18 U.S.C. (2001).

229 Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. (1978).

230 Svet Evrope. 2001. Konvencija o kibernetski kriminaliteti (Convention on Cybercrime), sprejel jo je Svet Evrope 23. novembra 2001. Uradni list RS, Mednarodne pogodbe, št. 17/2004. Konvencijo je državni zbor Republike Slovenije ratificiral dne 20. 5. 2004. Veljati je začela dne 1. 1. 2005.

231 Communications Assistance for Law Enforcement Act (Digital Telephony Act) of 1994, 47 U.S.C. (1994).

232 Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001, 18 U.S.C. (2001).

Da ta premik od pravice do zasebnosti ni naključen, kaže tudi leta 1986 sprejeti ECPA,[233] ki v sekciji 2703 določa, da smejo preiskovalci dobiti vsebino elektronske pošte na podlagi sodne odredbe. Vendar to določilo za javne sisteme elektronske pošte velja samo, če so elektronska sporočila v sistemu shranjena manj kot 180 dni. Če so v javnem sistemu shranjena dlje časa, namreč pridobijo status navadne zbirke podatkov in jih preiskovalci lahko pridobijo po lažji poti – na podlagi sodnega poziva (t. i. *subpoena*) ali na podlagi odredbe brez obvestila (ang. *warrant without notice*) (Banisar, 1994).

* * *

Iz poročil o uporabi Carnivora za leti 2002 in 2003, ki jih je FBI na podlagi zahtevka FOIA[234] posredoval EPIC, pa je razvidno, da je leta 2002 FBI brez sodne odredbe (po 216. sekciji USA PATRIOT Act[235]) zbiral prometne podatke v treh primerih, leta 2003 pa v šestih. Te preiskave so trajale do 60 dni, razen v enem primeru, ko je nadzor potekal več kot osem mesecev (od 10. januarja do 26. avgusta 2002). Nadzor prometnih podatkov se je izvajal v primerih goljufivih e-poštnih sporočil, prodaje prepovedanih substanc, posredovanju gradiv za podporo terorizmu, obscenih in nadlegovalskih telefonskih klicev ter izsiljevanju, požigu in širjenju navodil za izdelavo uničevalnih naprav. Pri nadzoru internetnega prometa s sodno odredbo pa je FBI v poročilu navedel zgolj to, da so imeli leta 2002 in 2003 dva taka primera (skupaj torej štiri). Konkretnejših podatkov o primerih pa FBI ni želel dati, saj naj bi šlo za "*občutljive preiskave*". Poleg tega se podatki, ki jih je posredoval FBI, nanašajo zgolj na tiste primere, v katerih je FBI uporabil svojo lastno prisluškovalno opremo, v poročilu pa so izpuščeni primeri, ki so zaobsegali vohunstvo in mednarodni terorizem. Prav tako so na voljo samo podatki za FBI, ne pa tudi za druge agencije, pa tudi ne primeri, ko so ponudniki dostopa do interneta (po ukazu FBI) izvajali nadzor z lastno opremo (FBI, 2003a ter FBI, 2003b). Zato ne preseneča, da je število navedenih primerov pravzaprav presenetljivo majhno.

Na to, da je obseg tovrstnega nadzora v polju obveščevalne dejavnosti verjetno precej večji, pa kaže serija razkritij o dejavnosti NSA po terorističnih napadih 11. septembra 2001. Najprej je konec leta 2005 prišlo na dan, da je NSA na podlagi ukaza predsednika ZDA Georgea Busha brez sodnih odredb ter brez vednosti Kongresa (zelo verjetno pa tudi v nasprotju z zakonom (*Foreign Intelligence Surveillance Act*[236]) prisluškovala Američanom (Schneier, 2006a). Sredi leta 2006 je prišlo na dan, da je NSA zbirala tudi prometne podatke o telefonskih klicih več deset milijonov Američanov ter na zbranih podatkih izvajala statistične analize izkopavanja podatkov (t. i. data mining) (Page, 2006). Zaradi teh razkritij je EFF s skupino potrošnikov proti telekomunikacijskemu podjetju AT&T januarja 2006 vložila tožbo zaradi domnevno

[233] Electronic Communication Privacy Act of 1986, 18 U.S.C. (1986).
[234] Freedom of Information Act of 2002, 5 U.S.C. (2002).
[235] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001, 18 U.S.C. (2001).
[236] Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. (1978).

nezakonitega omogočanja dostopa do telefonskih klicev in elektronske pošte tajni službi NSA. V okviru sodnega postopka je prišlo na dan, da je imela NSA v dogovoru s podjetjem AT&T (ki ima okrog tretjinski tržni delež na področju širokopasovnega dostopa do interneta v ZDA) v mestu Bridgeton, kjer ima AT&T glavno vozlišče za lokalni in mednarodni promet, ter v AT&T-jevem vozlišču v San Franciscu posebne nadzorne centre, od koder lahko nadzoruje omrežnipromet (Harris, 2006). Po nekaterih podatkih naj bi množično tajno nadzorovanje Američanov potekalo že sedem mesecev pred terorističnimi napadi 11. septembra 2001, in sicer v okviru projekta "Pioneer Groundbreaker", ki je začel nastajati junija 2000 in s katerim je NSA zaradi razpada informacijskega sistema 24. januarja 2000 (Bamford, 2002: 451–454) začela modernizacijo in izboljšanje svoje tehnološke infrastrukture (Harris, 2006). Glede na to, da ima NSA že tradicijo tovrstnega sodelovanja s telekomunikacijskimi podjetji, ni nemogoče, da podobno množično nadzorovanje poteka tudi danes. V letih od 1945 do 1975 je namreč NSA oziroma njen predhodnik Black Chamber v ustnem dogovoru z nekaterimi telekomunikacijskimi podjetji prestrezal vsa teleprinterska sporočila. Šlo je za projekt Shamrock[237], zaradi katerega je potekala senatna preiskava in je njen predsednik, senator Frank Church, izjavil, da je bil Shamrock "*verjetno največji vladni prisluškovalni program, usmerjen na Američane*", posledica preiskave pa je bil tudi sprejem *Foreign Intelligence Surveillance Act*[238], ki naj bi omejil poseganje NSA v zasebnost Američanov (Schneier, 2006b). Razlika je morda le v obsegu nadzorovanja, saj tokrat NSA verjetno nadzoruje praktično vsa poglavitna telekomunikacijska vozlišča v ZDA.

Izogibanje kriptografski zaščiti

Kadar je kriptografija vgrajena v storitev ponudnika telekomunikacijskih storitev, zakonodaja od njega zahteva, da preiskovalnim organom omogoči dostop do nešifriranih komunikacij. Naprave, ki bi uporabljale od ponudnika storitev neodvisno šifriranje (t. i. '*end-to-end šifriranje*'), niso preveč razširjene (to velja predvsem za klasične komunikacijske naprave, npr. telefone itd.), saj so razmeroma drage ali pa jih celo sploh ni mogoče kupiti v prosti prodaji (to velja npr. za mobilne telefone, ki uporabljajo močno kriptografijo). Praktično edina izjema je računalniški program PGPfone, razvit v okviru projekta PGP, ki s pomočjo šifrirane povezave med dvema računalnikoma, opremljenima z modemom (ali povezana v internet) ter zvočno kartico in slušalkami, omogoča šifriranje telefonskih pogovorov. Res pa je, da je uporaba te rešitve za vsakdanje namene precej neprimerna. To se morda utegne spremeniti s šifrirnimi orodji za komunikacije VoIP.[239] Praktično edino področje, na katerem je raba kriptografije razmeroma razširjena, oziroma so za to vsaj potencialne možnosti, pa je internet. Na internetu je mogoče najti precej brezplačnih računalniških programov, ki omogočajo močno šifriranje (večinoma elektronske pošte), programi pa so dovolj prijazni do uporabnikov in enostavni za uporabo, da bi jih lahko uporabljal

---

[237] Vzporedno s projektom *Shamrock* je potekal tudi projekt *Minaret*, v okviru katerega so nadzorovali komunikacije nekaterih ameriških političnih aktivistov.

[238] Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. (1978).

[239] V začetku leta 2006 je Phill Zimmermann, avtor šifrirnega programa PGP, začel razvijati program za šifriranje katerekoli telefonske povezave VoIP z imenom Zfone.

praktično kdorkoli. Kljub temu da njihova raba ni množična, pa tajne službe in preiskovalni organi skušajo najti različne načine, da bi si zagotovili dostop do nešifriranih vsebin.

Nekatere države so poizkušale sprejeti določila, ki bi od posameznikov zahtevala, naj na podlagi sodne odredbe preiskovalcem izročijo svoje ključe ali pa dovolijo dostop do nešifriranih podatkov. Šesto načelo kriptografskih smernic OECD[240] govori o zakonitem dostopu do šifrirnih ključev, vendar take rešitve ne zahteva: "*Nacionalne kriptografske politike lahko dovolijo zakonit dostop do nešifriranega besedila ali šifrirnih ključev*".[241] Vendar pa so na zasedanju G8 istega leta zapisali priporočilo, da naj vsaka vlada zagotovi zakonit dostop do nešifriranih informacij za potrebe preprečevanja terorizma (Madsen in Banisar, 2000: 23). Precej kritik je bila deležna tudi 4. točka 19. člena *Konvencije o kibernetski kriminaliteti*, v kateri je zapisano, da "*pogodbenica sprejme potrebne zakonodajne in druge ukrepe, s katerimi pristojne organe pooblasti, da odredijo vsakomur, ki je seznanjen z načinom delovanja računalniškega sistema ali ukrepi za zavarovanje računalniških podatkov v njem, kadar je primerno, da zagotovi potrebne informacije, ki omogočijo izvajanje ukrepov iz prvega in drugega odstavka.*" (4. točka 19. člena Konvencije o kibernetski kriminaliteti[242]). Kritiki so opozarjali, da so takšne določbe v nasprotju z načelom, ki prepoveduje samoobtožbo (ang. *self-incrimination*), ki je med drugim uveljavljeno v 5. amandmaju ameriške ustave,[243] 6. členu Evropske konvencije o človekovih pravicah[244] (ki govori o pravici do poštenega sojenja) ter 14. (3) (g) členu Mednarodnega pakta o državljanskih in političnih pravicah.[245]

Po navedbah EPIC sta zakonodajo, ki od posameznika zahteva razkritje šifrirnih gesel, sprejela samo Singapur in Malezija, nekoliko drugačno rešitev pa je sprejela Irska. Junija 1998 je irsko ministrstvo za javno podjetništvo (*Department of Public Enterprise*) pripravilo dokument *Framework for Irelands Policy on Encryption and Electronic Signatures*,[246] v katerem so zapisali, da bo "*za omogočanje zakonitega dostopa do šifriranih podatkov sprejeta zakonodaja, ki bo od uporabnikov kriptografskih proizvodov zahtevala, naj na podlagi zakonitega pooblastila [preiskovalnim organom] izročijo ali nešifrirano sporočilo, ki je preverljivo povezano s šifriranimi podatki, ali pa ključe ali algoritme, ki omogočajo pridobitev nešifriranega sporočila.*" (Madsen in Banisar, 2000: 67 ter Grossman, 1998), kar je v bistvu implementacija 6. načela iz *Smernic o kriptografski politiki OECD*.[247]

---

[240] OECD. 1997. Smernice o kriptografski politiki (Guidelines on Cryptography Policy), sprejete 27. marca 1997.

[241] OECD. 1997. Smernice o kriptografski politiki (Guidelines on Cryptography Policy), sprejete 27. marca 1997.

[242] Svet Evrope. 2001. Konvencija o kibernetski kriminaliteti (Convention on Cybercrime), sprejel jo je Svet Evrope, 23. novembra 2001. Uradni list RS, Mednarodne pogodbe, št. 17/2004. Konvencijo je državni zbor Republike Slovenije ratificiral dne 20. 5. 2004. Veljati je začela dne 1. 1. 2005.

[243] 5. amandma, Listina svoboščin (Bill of Rights), 1791.

[244] Svet Evrope. 1950. Evropska konvencija o varstvu človekovih pravic in mednarodnih svoboščin, spremenjena s protokoli št. 3, 5 in 8 ter dopolnjena s protokolom št. 2, ter njeni protokoli št. 1, 4, 6, 7, 9, 10 in 11 (*Convention on Human Rights and Fundamental Freedoms as amended by Protocols Nos. 3, 5 and 8 and amended by Protocol No. 2 and its Protocols Nos. 1, 4, 6, 7, 9, 10 and 11*), sprejel jo je Svet Evrope leta 1950. Uradni list RS, št. 33/1994, "Mednarodne pogodbe", št. 7/1994, 13. 6. 1994. Konvencijo je državni zbor Republike Slovenije ratificiral 13. 6. 1994. Veljati je začela 28. 6. 1994.

[245] OZN. 1966. Mednarodni pakt o državljanskih in političnih pravicah (International Covenant on Civil and Political Rights), sprejeta v OZN 1966. Uradni list SFRJ, št. 7/1971. Pakt je ratificiral Zvezni zbor skupščine SFRJ 30. 1. 1971. Veljati je začel 12. 2. 1971.

[246] Dokument je bil do združitve z ministrstvom za promet dostopen na naslovu: <http://www.irlgov.ie/tec/html/signat.htm>, del dokumenta je objavljen v Madsen in Banisar, 2000: 67.

[247] OECD. 1997. Smernice o kriptografski politiki (Guidelines on Cryptography Policy), sprejete 27. marca 1997.

V leta 2000 sprejetem zakonu *Electronic Commerce Act*[248] so v 28. členu zapisali: "*Nič v tem zakonu se ne sme tolmačiti kot zahteva za razkritje ali omogočanje zasega edinstvenih podatkov, kot npr. kod, gesel, algoritmov, zasebnih šifrirnih ključev ali drugih podatkov, ki bi bili nujni za povrnitev informacije ali za jasnost komunikacije*", vendar pa 27. (c) člen preiskovalcem omogoča, da "*se v primeru, da zasežena stvar vsebuje informacije ali komunikacije v nerazumljivi obliki (torej so zašifrirane, m. op.), lahko zahteva razkritje informacije ali elektronske komunikacije v razumljivi obliki*" (27. in 28. člen *Electronic Commerce Act*[249]). Po navedbah EPIC so o podobnih rešitvah razmišljali tudi v Kanadi, Veliki Britaniji in Indiji. Vsekakor so taka načela v nasprotju s pravico do prepovedi samoobtožbe. Kritiki pa opozarjajo tudi na to, da bi bili zaradi takih določil lahko kaznovani nedolžni posamezniki, ki bi gesla izgubili ali pa bi jih nekdo drug naredil v njihovem imenu. Na problem je humorno pokazal tudi britanski projekt 'Dear Jack', ko je skupina aktivistov v protestu ob podobnemu zakonu, ki se je pripravljal v Veliki Britaniji, Jacku Strawu, notranjemu ministru, poslala pismo, v katerem je bilo s šifrirnim ključem, narejenim v njegovem imenu, zašifrirano priznanje izmišljenega zločina, ključ pa so uničili. Aktivisti so mu v javnem pismu napisali, da upajo, da "*so pokazali, da zaradi tega zakona*[250] *ne bodo kaznovani le tisti, ki so zagrešili zločin, pač pa tudi nedolžni posamezniki* " (STAND, Operation Dear Jack).

Dokončen odgovor na vprašanje, ali so take določbe v skladu z mednarodnimi pravnimi akti, bodo verjetno dale razsodbe ustavnih sodišč oziroma sodba Evropskega sodišča za človekove pravice, ki je pravico do molka v kazenskem postopku na podlagi 6. člena Evropske konvencije o človekovih pravicah[251] v nekaj razsodbah že podprlo. Zato se bo verjetno bolj uveljavila rešitev, ki so jo uveljavili v ZDA (kjer 5. amandma[252] prepoveduje samoobtožbe), ki predvideva prisilna dejanja za razkritje ključev ali vsebine komunikacije samo za tretje osebe, torej priče, in ne za obtožence.

Zakonodajalec lahko k razkritju šifrirnih ključev prisili posameznike, ki te ključe hranijo za druge osebe, ne more pa prisiliti osumljencev, da izdajo svoje lastne ključe (*Mednarodni pakt o državljanskih in političnih pravicah*[253] so podpisale tudi Irska, Velika Britanija in Kanada). Delna izjema je primer *People proti Price*, ki se je zgodil na višjem kalifornijskem sodišču v ZDA, ko je tožilstvo uspešno izsililo šifrirno geslo od obtoženca. Vendar v tem primeru gesla niso uporabili za pridobitev dokazov, temveč za ugotavljanje, ali naj policija obtoženemu vrne zaplenjeni računalnik. V računalniku je bilo namreč več šifriranih datotek, za katere je policija domnevala,

---

248 Electronic Commerce Act, 2000, Irska.

249 Electronic Commerce Act, 2000, Irska.

250 *Regulation of Investigatory Powers Act*, 2000, Velika Britanija. Razkritje ključev je opredeljeno v členih 49–51.

251 Svet Evrope. 1950. Evropska konvencija o varstvu človekovih pravic in mednarodnih svoboščin, spremenjena s protokoli št. 3, 5 in 8 ter dopolnjena s protokolom št. 2, ter njeni protokoli št. 1, 4, 6, 7, 9, 10 in 11 (Convention on Human Rights and Fundamental Freedoms as amended by Protocols Nos. 3, 5 and 8 and amended by Protocol No. 2 and its Protocols Nos. 1, 4, 6, 7, 9, 10 and 11), sprejel jo je Svet Evrope leta 1950. Uradni list RS, št. 33/1994, "Mednarodne pogodbe", št. 7/1994, 13. 6. 1994. Konvencijo je državni zbor Republike Slovenije ratificiral 13. 6. 1994. Veljati je začela 28. 6. 1994.

252 5. amandma, Listina svoboščin (Bill of Rights), 1791.

253 OZN. 1966. Mednarodni pakt o državljanskih in političnih pravicah (International Covenant on Civil and Political Rights), sprejet v OZN 1966. Uradni list SFRJ, št. 7/1971. Pakt je ratificiral Zvezni zbor skupščine SFRJ 30. 1. 1971. Veljati je začel 12. 2. 1971.

da je v njih otroška pornografija (obtoženec je že bil kaznovan zaradi nadlegovanja otrok), to domnevo pa sta potrjevali datoteki "Boys.gif" ter "Boys.pgp", ki so ju našli v računalniku.[254] Obtoženec je želel dokazati, da v njegovem računalniku ni otroške pornografije (in s tem pridobiti računalnik nazaj), zato so preiskovalci zagnali šifrirni program PGP do točke, ko je treba vpisati geslo, obtoženec pa je geslo povedal zapriseženemu sodnemu uradniku in ta je geslo vpisal brez navzočnosti preiskovalcev. Preiskovalci so nato dokončali postopek dešifriranja datotek (Denning in Baugh, 2000: 116).[255]

Ta postopek pa je bil učinkovit zgolj zato, ker so preiskovalci že pred tem našli nešifrirano datoteko in so torej dokaze pridobili brez dostopa do šifrirnega gesla; v primerih, ko nešifriranih datotek ni v računalniku, pa v demokratični družbi obdolženca ni mogoče prisiliti, da priča proti sebi. Preiskovalni organi in tajne službe so zato ubrali drugačne pristope k pridobivanju nešifriranih podatkov, vendar sodijo že v polje protiobveščevalne dejavnosti. Kriptografijo so namreč skušali zaobiti, pri tem pa so vsaj v enem primeru posegli po podobih metodah, ki se jih poslužujejo računalniški kriminalci, priljubljeno imenovani tudi hekerji.

Primer Scarfo

Leta 1999 je FBI vodil preiskavo proti domnevnemu Nicodemu S. Scarfu iz New Jerseyja, ki je bil osumljen nelegalnih igralniških poslov in oderuškega posojanja denarja. Agenti FBI so sumili, da ima v računalniku v svojem uradu shranjene podatke o svojih nezakonitih poslih, zato so mu podatke januarja 1999 zasegli, vendar so odkrili, da so datoteke s podatki zašifrirane s programom PGP. Agentje FBI so poizkušali razbiti kriptogram, a neuspešno.
Zato so 7. maja 1999 agenti FBI zaprosili za sodni nalog za tajni vstop v njegov urad in namestitev posebne programske opreme, s katero bi prestregli Scarfovo geslo.[256] Sodni nalog so dobili in 10. maja 1999 tajno vstopili v Scarfov urad v New Jerseyju, v njegov računalnik namestili dotlej neznano programsko opremo in tako prestregli njegovo geslo za šifriranje elektronskih sporočil (McCullagh, 2000 in Schneier, 2001a).

Izkazalo se je, da je FBI razvil posebno orodje za prestrezanje gesel z imenom *Magic Lantern*, ki deluje kot program za prestrezanje tipkanja (ang. *keyboard-sniffing device*). Podobne programe so pred tem že razvili hekerji.[257] Podrobnosti o programu niso bile znane, FBI pa jih ni želel

---

[254] Obtožnec je uporabljal šifrirni program PGP, ki šifrirani datoteki samodejno nastavi končnico '.pgp'. Na podlagi tega je policija sklepala, da je datoteka "Boys.pgp" šifrirana datoteka "Boys.zip"

[255] Postopek se je končal tako, da so v računalniku našli otroško pornografijo, sodišče pa je nato ukazalo računalnik uničiti, kljub temu da je obtoženec trdil, da gre za raziskovalno gradivo.

[256] Kopija prošnje za izdajo sodnega naloga, naslovljena na okrožno sodišče v New Jerseyju, 8. maj 1999. Kopijo je pridobil EPIC na podlagi zahtevka FOIA (Freedom of Information Act of 2002, 5 U.S.C. (2002)) in je dostopna na spletnih straneh EPIC.

[257] Poznamo pa tudi posebne strojne prestreznike (posebne naprave), ki jih je mogoče namestiti na kabel med tipkovnico in računalnikom, kjer zaznavajo tipkanje uporabnika. Neko podjetje je že pred časom v ZDA prodajalo miniaturno prestrezno napravo *KeyGhost*, ki se jo namesti na kabel računalniške tipkovnice in zaznava tipke, pritisnjene na tipkovnici. Naprava stane 89 dolarjev in več (Vir: <http://www.keyghost.com>).

razkriti niti Scarfovi obrambi, in sicer na podlagi zakona *Classified Information Procedures Act*,[258] sodišče pa je FBI-jevim argumentom pritrdilo (United States proti Scarfo, Criminal No. 00-404 (2001)).

Kmalu so se razširila ugibanja, da gre za nekakšnega trojanskega konja (trojanski konj je ena izmed oblik računalniških virusov), po možnosti takega, ki izkorišča razpoke v varnosti in pomanjkljivosti v računalniških sistemih in ga je v nekaterih primerih mogoče namestiti v računalnik celo na daljavo oziroma prek interneta. Podobna orodja, dotlej je bilo znano hekersko orodje *Dirt* (*Data Interception by Remote Transmission*; orodje je pozneje začelo tržiti podjetje Codex Data Systems, Inc.), so pred tem namreč že uporabljali hekerji za vdore v računalniške sisteme. Kmalu po tistem, ko je FBI odkril in potrdil obstoj tega orodja, se je razvnela razprava o tem, ali naj podjetja, ki prodajajo protivirusno programsko opremo, svoje programe priredijo tako, da protivirusni program uporabnika ne bi obvestil, če bi na njegovem računalniku zaznal *Magic Lantern*. Razpravo je podžgal članek Associated Press, ki je trdil, da FBI sodeluje s protivirusnim podjetjem McAffe, a so to v podjetju zanikali. Novinar AP Ted Bridis je pozneje izjavil, da za svojim člankom kljub temu stoji (McCullagh, 2001e). Protivirusna podjetja so potem javno zatrdila, da z FBI ne bodo sodelovala in se bodo trudila še naprej odkrivati vse viruse, ne glede na njihov izvor (Reuters, 2001). Kljub temu so dogodki okrog Scarfa še vedno vir številnih govoric in sumničenj.[259]

Kleptografija in primer Crypto AG

Leta 1883 je flamski lingvist in kriptolog Auguste Kerckhoffs objavil članek *La Cryptographie Militaire*, v katerem je izpostavil šest načel, ki jih morajo upoštevati dobri šifrirni sistemi. Eno izmed teh se imenuje Kerchoffsov zakon in pravi, da je dober šifrirni sistem varen, tudi če je o njem znano vse, razen šifrirnega ključa (Wikipedia, geslo: "Kerchoffs' law").[260] Kerchoffsov zakon tako zavrača načelo, da je mogoče varnost zagotoviti s skrivanjem (t. i. '*security through obscurity*'). Kerchoffsov zakon sicer ne govori neposredno o tem, da *mora* biti kriptografska naprava oziroma algoritem javen, temveč le opozarja na to, da skrivnost ne zagotavlja varnosti, marveč jo v resnici lahko celo ogroža (če npr. pade sovražniku v roke šifrirna naprava, seveda pa je mogoče delovanje šifrirne naprave ugotoviti tudi z matematično analizo). Po nastanku javno dostopne kriptografije se je v kriptografski skupnosti izoblikovalo načelo objave algoritmov.

---

[258] Classified Information Procedures Act of 1980, 18 U.S.C. (1980).

[259] Nekateri varnostni strokovnjaki ugotavljajo, da bi bilo treba v tradicionalni varnostni model vključiti tudi preverjanje zaupanja v (končno) napravo, iz katere se uporabnik overi (avtenticira, ang. *to authenticate*). Na tej napravi je lahko podtaknjena zlonamerna koda ali zlonamerna strojna oprema za prestrezanje. Overjanje bi bilo dopustno šele po tem, ko bi bilo zagotovljeno zaupanje v napravo, iz katere poteka overjanje. Za ta korak predlagajo izraz *admissibility*, kar bi lahko prevedli kot "upoštevanja vrednost" (Schneier, 2006g). Nadgradnja varnostnega modela je posledica zavedanja, da postajajo čedalje večja šibka točka varnosti omrežnih sistemov prav končni računalniki uporabnikov, ki so lahko okuženi z zlonamerno kodo ali strojnimi prestreznimi sistemi in so lahko podvrženi tudi krajam podatkov z diskov (na klasični način ali celo s forenzično rekonstrukcijo izbrisanih podatkov) itd.

[260] Podobno pravi Shannonova maksima, ki predpostavlja, da sovražnik pozna šifrirni sistem. Do te ugotovitve je verjetno neodvisno prišel Claude E. Shannon.

Schneier pravi, da je korist od javne objave predvsem v tem, da lahko drugi kriptologi algoritem ali zamisel ocenijo in kritično ovrednotijo. To pripomore k izboljšavi kakovosti in k hitrejšemu razvoju (Schneier, 2002). Pri sistemih, ki niso bili odprti, je veliko večja verjetnost, da je v njih kakšna napaka, ki bi jo javni pregled verjetno odkril, avtorji pa bi s tem dobili možnost, da jo odpravijo. Schneier pravi: "*Ne spominjam se nobenega kriptografskega sistema, razvitega na skrivaj, v katerem ne bi, potem ko je bil razkrit javnosti, kriptografska skupnost našla napake.*" (Schneier, 2002).

Vendar pa načelo odprtosti in transparentnosti v kritografiji ni vedno upoštevano. Tajne službe so že po svoji naravi nenaklonjene odprtosti, čeprav imajo za neodprtost včasih tudi dobre razloge. NSA ima na primer dolgo prakso neobjavljanja kriptoloških odkritij, in sicer zato, da sovražnika ne bi opozorila na napake v njegovem šifrirnem sistemu ali da ne bi sovražnik dobil podatkov o slabostih njihovih šifrirnih sistemov. Poleg tega transparentnost pogosto tudi ni v interesu izdelovalca ali izumitelja. Zaradi transparentnosti namreč podjetje tvega, da si bo kdo njihovo rešitev prilastil ali pa morda celo razkril, da izdelek v resnici ni zanesljiv. Pogost argument je tudi ta, da bi transparentnost omogočila razkritje morebitnih varnostnih pomanjkljivosti in njihovo nepooblaščeno izkoriščanje.

Podobno velja tudi za izvorno kodo (ang. *source code*) računalniških programov. V računalništvu se je oblikovalo močno gibanje za odprto kodo (ang. *open source*)[261] oziroma odprto programje (predvsem okrog operacijskega sistema Linux), katerega privrženci pa opozarjajo na še eno pomembno pomanjkljivost zaprtih sistemov (včasih imenovanih tudi sistemi '*black-box*'): transparentnost je nujni predpogoj za zagotovilo, da v algoritmu ali programu niso vgrajena kakšna stranska vrata.

Leta 1919 je švedski kriptolog Arvid Gerhard Damm zaprosil za patent za mehanični šifrirni stroj. Skupaj s kriptologom Borisom Caesarjem Wilhelmom Hagelinom sta nato razvila v tistem času edino uspešno kriptografsko podjetje. Ker je grozila nevarnost, da bo švedska vlada njune izume zaplenila in si jih prilastila, se je podjetje leta 1952 preselilo v Švico (Dupuis, 1999). Imenovalo se je Crypto AG in je v šestdesetih letih veljalo za največje kriptografsko podjetje na svetu. S spletne strani podjetja je razvidno, da so njihove stranke tako diplomacija, vojske, notranja ministrstva kot tudi zasebna podjetja. Po nekaterih podatkih naj bi njihove izdelke kupovale osamosvojene afriške kolonije, ki so želele zaščititi svoje komunikacije pred nekdanjimi kolonizatorji (Bamford, 1983: 407–408), v preteklosti pa naj bi svoje izdelke prodajali tudi Iraku, Iranu, Libiji in Jugoslaviji (McCullagh, 2001e). Podjetje na svojih spletnih straneh poudarja, da je neodvisno in ker je locirano v nevtralni Švici, ni izpostavljeno nikakršnim izvoznim omejitvam, to pa je "*edinstven položaj*" (Crypto AG, 2005a).

[261] Odprta programska oprema (ang. *open source*) ne pomeni nujno brezplačne programske opreme, čeprav je med odprtim programjem najbolj znan Linux. Odprto programje omogoča vpogled v izvirno kodo programa, pri čemer ni nujno, da je sam program brezplačen.

Vendar so se okrog podjetja spletle številne govorice, češ da je v preteklosti sodelovalo z NSA. V prvi izdaji knjige *The Puzzle Palace* leta 1982 je Bamford prvič omenil domnevno povezavo med NSA in Crypto AG. Bamford trdi, da je do sredine 50. let 20. stoletja ZDA znala razbiti kriptograme evropskih držav, po letu 1957 pa so se zbali, da bodo to prednost izgubili, saj so v Evropi začeli izdelovati nove in boljše kriptografske naprave. Dokler je NSA lahko nadzorovala izvoz kriptografskih naprav iz ZDA, je lahko obdržala prednost, ko pa so zunaj ZDA nastala neodvisna podjetja z dobrimi kriptografskimi proizvodi, pa se je NSA znašla v težavah. Bamford nato trdi, da se je NSA začela dogovarjati s podjetjem Crypto AG o sodelovanju. Na sestanku, ki ga naj bi imel predstavnik NSA William F. Friedman z direktorjem Crypto AG Wilhelmom Hagelinom, naj bi bil sklenjen dogovor in Hagelin naj bi NSA posredoval podrobnosti o svojih šifrirnih strojih. To naj bi NSA omogočilo, da v precej krajšem času razbijejo kriptograme, narejene s temi napravami (Bamford, 1983: 408). Nadalje Bamford navaja dve izjavi neimenovanih uslužbencev GCHQ in NSA,[262] ki sta trdila, da je bila večina kriptogramov, ki so jih uporabljale države tretjega sveta, takih, da jih je bilo moč enostavno razbiti, saj so na začetku te države uporabljale ročno šifriranje, pozneje pa mehansko, pri čemer so večinoma uporabljale Hagelinove šifrirne stroje. Izjava uslužbenca NSA je bila, da je "*Hagelin enostaven*" (Bamford, 1983: 499).

Crypto AG na svoji spletni strani trdi, da je žrtev številnih govoric, ki izvirajo večinoma iz leta 1992 (Bamfordove knjige pa ne omenjajo), ko so njihovega nekdanjega uslužbenca aretirali v Iranu, mediji pa so potem špekulirali, da je razlog za aretacijo sodelovanje podjetja s tajnimi službami (Crypto AG, 2005b). Časopis Baltimore Sun je decembra 1995 v članku "*Rigging the Game*" (Jya.com, 1997)[263] zapisal, da naj bi šlo za Hansa Bühlerja (nekateri navajajo tudi priimek Buehler), ki naj bi bil v Iranu obtožen vohunstva za ZDA in Nemčijo, podjetje Crypto AG pa naj bi devet mesecev po njegovi aretaciji za njegovo izpustitev plačalo milijon mark, vendar naj bi pozneje od njega zahtevalo vračilo denarja. Büehler naj bi zato začel ugotavljati, ali je podjetje res povezano s tajnimi službami, in svoje ugotovitve posredoval medijem (nekateri trdijo, da je celo nameraval napisati knjigo), zato naj bi Crypto AG proti njemu leta 1995 vložilo tožbo. Vendar naj bi v zadnjem hipu prišlo do poravnave, zato javnega sojenja nikoli ni bilo. Baltimore Sun naj bi do zgodbe prišel na podlagi intervjujev z nekdanjimi uslužbenci in internimi dokumenti podjetja. Podobno zgodbo je leta 1996 objavil tudi Der Spiegel. Hkrati pa Bamford v knjigi *Body Of Secrets* tudi navaja, da je bil eden izmed motivov NSA za nakup zmogljive računalniške opreme tudi "*Hagelinov problem*" (Bamford, 2002: 585–586); to kaže, da je NSA za Hagelinove šifrirne stroje vendarle potrebovala tudi računsko moč za kriptoanalizo.

Seveda je razumljivo, da je preverljive podatke o morebitnih dogovorih med neodvisnimi kriptografskimi podjetji in tajnimi službami težko dobiti, oziroma so dostopni samo iz sekundarne literature. Kljub vsemu bi bili taki poizkusi s strani tajnih služb povsem razumljivi in pričakovani.

---

[262] Njegova knjiga je nastala na podlagi dokumentov, ki jih je pridobil s pomočjo *Freedom of Information Act* (Freedom of Information Act of 2002, 5 U.S.C. (2002)) in intervjujev z uslužbenci tajnih služb.

[263] Kopija članka (The Baltimore Sun, 4. december, 1995, str. 9–11) je dostopna na naslovu <http://jya.com/nsa-sun.htm>.

Kakorkoli že, na konferenci Crypto leta 1996 in Eurocrypt leta 1997 sta raziskovalca Adam Young in Moti Yung prvič predstavila zamisel o *kleptografiji*.[264] V članku "*Mitigating Insider Threats to RSA Key Generation*", objavljenem v reviji *Cryptobytes,* je Young opisal metodo SETUP (*secretly embedded trapdoor with universal protection* – tajno vključena stranska vrata z univerzalno zaščito), ki s pomočjo prirejenega algoritma zgenerira tak par šifrirnih ključev (pri asimetrični kriptografiji), da je na videz (matematično) povsem enak kakor navaden par ključev, poleg tega pa je tudi enako varen, razen pred napadalcem, saj tajno vključena stranska vrata predstavljajo napadalčev javni ključ. Young pravi, da napad SETUP oziroma kleptografija napadalcu daje ekskluzivno prednost, saj je zaradi lastnosti prirejenih ključev le-te nemogoče ločiti od neprirejenih. To pomeni, da je nemogoče ugotoviti, ali je bil napad SETUP izveden ali ne (Young, 2004: 5). Young in Yung sta pokazala, da je napad mogoče implementirati v RSA, DSA (*Digital Signature Algorithm*) ter Diffie-Hellmanovo izmenjavo ključev. Bistvo njunih ugotovitev pa je v tem, da so takšna stranska vrata mogoča pri t. i. kriptografskih napravah *black-box*, torej pri napravah, katerih delovanje ni transparentno.

V zvezi s podjetjem Crypto AG verjetno nikoli ne bo mogoče odkiti vse resnice, dejstvo pa je, da so se kmalu po odkritju kleptografije začele širiti govorice, da je morda NSA v njihove naprave implementirala kak podoben napad. Takšna ugibanja temeljijo tudi na dogajanju okrog algoritma DES oziroma vpletenosti NSA v njegov razvoj. Poleg tega je bilo odkritih že več primerov skrivnega vgrajevanja stranskih vrat oziroma drugih nadzornih tehnologij v programsko opremo iz takih ali drugačnih razlogov (podjetja včasih kakšno tako tehnologijo vgradijo tudi zaradi boja proti piratstvu); o tem več v prihodnjih poglavjih. V vsaj enem primeru pa je šlo za tehnologijo, s pomočjo katere je FBI ujel pisca nekega virusa.[265]

Glede na neuspehe pri omejevanju širjenja kriptografije je povsem verjetno, da se NSA poslužuje predvsem metod kraje šifrirnih ključev ali zasega podatkov pred šifriranjem oziroma po dešifriranju. Bamford v knjigi *Body Of Secrets* navaja, da je NSA skupaj s tajno službo CIA (Central Intelligence Agency) leta 1978 ustanovila poseben oddelek *Special Collection Service* (SCS), ki se ukvarja z nameščanjem prisluškovalne opreme, krajo šifrirnih ključev, podkupovanjem sistemskih upraviteljev in podobnimi dejavnostmi, s katerimi se lahko "izognejo" kriptografski zaščiti, ki jo uporablja cilj njihovega nadzora (Bamford, 2002: 477–479). Prav tako je povsem verjetno, da so tajne službe že v preteklosti vzdrževale ali vsaj nadzorovale anonimizacijske sisteme na internetu in na njih prisluškovale prometu. S tem so skušale nadzorovati prav komunikacije tistih, ki so se želeli izogniti nadzoru.[266]

---

[264] Adam Young je pozneje na to temo leta 2002 doktoriral na *Columbia University*, naslov teze pa je bil '*Kleptography: Using Cryptography Against Cryptography*'.

[265] S pomočjo na skrivaj vgrajene sledilne tehnologije v Microsoft Office 97 je FBI leta 1999 ujel avtorja virusa Melissa.

[266] Sredi leta 2005 so na spletni strani ruske Tor izhodne točke na strežniku unixgu.ru pričeli objavljati sezname prestreženih uporabniških imen in gesel uporabnikov, ki so preko Tor omrežja uporabljali nešifrirane protokole za dostop do storitev interneta (v obliki, ki ne omogoča neposredne zlorabe). Ob tem so zapisali, da sezname objavljajo v opomin, da je potrebno pri uporabi anonimizacijskih sistemov uporabljati tudi druge varnostne mehanizme (Schmieder, 2005). Eden izmed operaterjev Tor omrežja je v reakciji na ta dogodek napisal program z imenom *Snakes On A Tor*, ki je namenjen ugotavljanju, ali nekdo na Tor izhodni točki ne spreminja prometa s pomočjo tehnike vrivanja (ang. *injection*) oz. ne spreminja SSL certifikatov (tim. napad s posrednikom (*man-in-the-middle* napad)). Po nekaj dneh poiskusnega delovanja je program dejansko odkril zlonamerno izhodno točko, ki je izvajala napad s posrednikom ter vse SSL certifikate zamenjevala s svojimi. To napadalcu omogoča, da si kljub uporabi SSL šifriranja pridobi podatke v nekriptirani obliki. Kasnejše analize so pokazale, da se je ta izhodna točka nahajala na Kitajskem in da je zelo verjetno sama žrtev napada (Perry, 2006).

Strah pred kriptoanarhijo

Vsekakor je kriptografija eno izmed orodij za zaščito zasebnosti (t. i. PET - *privacy enhacing technologies*)[267], vendar jo je mogoče tudi zlorabiti. Svobodni uporabi kriptografije so najbolj nasprotovali ameriški preiskovalni organi in tajne službe. Razumljivo pa je, da so ji nasprotovale tudi nekatere totalitarne države, čeprav se v večini držav s problemom kriptografije sploh niso ukvarjali, verjetno tudi zaradi nerazširjenosti informacijske tehnologije, ki omogoča njeno uporabo.
Z nastankom kriptografije se je namreč porodil strah, da država ne bi mogla več nadzorovati kriminala oziroma sovražnih dejavnosti proti njej sami. Uporaba šifriranja namreč onemogoči prestrezanje komunikacij tako nezakonitemu kakor tudi zakonitemu prisluškovalcu. Zastavlja se torej vprašanje, ali naj imajo preiskovalni organi zgolj *možnost,* da posameznike nadzorujejo, ali pa naj imajo *absolutno pravico* do nadzorovanja, oziroma ali naj imajo tudi pravico, da je uspeh njihovega prisluškovanja zagotovljen (da torej uspešno prestrežejo vsebino komunikacije).

Problem je zelo pereč predvsem v primerih, ko je kriptografija uporabljena v kriminalne namene. Do prvih primerov uporabe kriptografije v take namene pa je prišlo že konec 20. let prejšnjega stoletja v ZDA v obdobju prohibicije (Dupuis, 1999). Ameriški FBI je zato v tistem času ustanovil poseben oddelek *Cryptanalytical and Translation Section*, ki se je ukvarjal z dešifriranjem sporočil, ki so jih uporabljali tihotapci alkohola (Shireen, 1998 ter Bamford, 1983: 471), v posebej zapletenih primerih pa je za pomoč zaprosil NSA, čeprav je bilo sodelovanje med agencijama v tistem času neformalno in je včasih NSA sodelovanje tudi zavrnila.[268] Bamford celo navaja, da FBI v nekem primeru množičnega izsiljevanja ni uspelo razbiti kriptogramov, zato se je na pomoč obrnil na NSA. NSA je uspelo in ko se je FBI lotil aretacij, je med gangsterji izbruhnila vojna, saj so bili drug za drugega prepričani, da so izdajalci (Bamford, 1983: 472).

Denningova in Baugh sta zbrala kar nekaj primerov uporabe kriptografije v kriminalne namene, čeprav je treba priznati, da je pri praktično vseh preiskovalcem uspelo razbiti šifre, oziroma je do obsodbe prišlo na podlagi drugih dokazov. Primeri segajo od *terorizma* (šifriranje naj bi uporabljala japonska sekta Aum Shinri Kyo, ki je na tokijski podzemni železnici leta 1995 izvedla napad s sarinom; Ramsey Yousef, ki je bil odgovoren na bombni napad na WTC leta 1993; bolivijski teroristi, odgovorni za smrt štirih ameriških marincev; Hamas, ki naj bi prek interneta in z uporabo kriptografije razpošiljal zemljevide, slike in druge podrobnosti,

---

[267] Nekateri trdijo, da je kriptografija samo oblika govora in s tem zaščitena s pravico do svobode govora. Eden vodilnih Cypherpunkerjev, Timothy C. May, je zapisal, da je "*osnovna pravica svobode govora pravica govoriti v jeziku, ki je sosedom in vladi nerazumljiv: šifriranem jeziku*" (May, 1995). Razlog za tako argumentacijo je verjetno tudi to, da je v ZDA nesporno, da je svoboda govora ustavno zaščitena (saj je nedvoumno zapisana v prvem amandmaju ameriške ustave (1. amandma, Listina svoboščin (Bill of Rights), 1791)), o ustavnosti pravice do zasebnosti pa kroži precej nasprotujočih si stališč. Zagovorniki takega razumevanja kriptografije pravijo, da je prenašanje šifriranih sporočil enako kot pogovor v tujem jeziku. Temu videnju nekateri nasprotniki kriptografije oporekajo in trdijo, da je kriptografija prvenstveno tehnologija za zaščito zasebnosti, čeprav priznavajo, da bi se jo morda vendarle dalo razumeti v kontekstu svobode govora (Denning, 1995).

[268] Od predsednika Reagana naprej je naloga NSA, da v primerih, ko so ogrožena človeška življenja, katerikoli vladni ustanovi ponudi pomoč v obliki kriptoanalize (Bamford, 1983: 473).

potrebne za načrtovanje terorističnih napadov; domnevno tudi baskovska ETA ter še nekaj domačih ameriških teroristov), *organiziranega kriminala* (trgovina z mamili, ilegalno igralništvo, finančne prevare, kraje številk kreditnih kartic in ponarejanje; prav tako pa Denningova in Baugh navajata, da naj bi opazili povečano rabo kriptografije pri italijanski mafiji; v nekem primeru na Nizozemskem pa naj bi skupina mafijcev najela nekaj hekerjev, da so jih oskrbeli s prenosnimi računalniki, ki so vsebovali šifrirane podatke) do *otroške pornografije* (pedofili naj bi si izmenjevali podatke in slike v šifrirani obliki; senator Charles Grassley je leta 1997 navedel tudi primer, ko je neki 11-leten deček, potem ko je bil spolno zlorabljen, naredil samomor, preiskovalci pa niso mogli do njegovega dnevnika, v katerem naj bi bili podatki o tem, kdo ga je zlorabil) ter *vohunstva* (najbolj znan je primer Aldricha Hazena Amesa, uslužbenca CIE, ki je bil obsojen zaradi vohunstva; poznamo tudi nekaj primerov industrijske špijonaže in primer hekerja Kevina Poulsena, ki je spreminjal nagradne igre tako, da je lahko pobiral glavne nagrade ter vdiral v telefonska omrežja in spreminjal policijske prisluhe). Kljub vsemu teh primerov ni zelo veliko, saj je leta 1998 oddelek računalniških strokovnjakov ameriške FBI obravnaval 299 primerov, ko so bili računalniki uporabljeni v kriminalne namene, uporabo kriptografije pa so zaznali le v štirih odstotkih primerov (Denning in Baugh, 2000: 112 ter Denning in Baugh, 1997).

V vseh teh primerih so kriminalci kriptografijo uporabljali za zakrivanje dokazov (podatke, ki so jih imeli v svojih računalnikih, so šifrirali). A večinoma je preiskovalcem uspelo razbiti kriptograme,[269] čeprav je to nekajkrat časovno zavleklo preiskavo in je kriptoanaliza stala precej denarja. Te primere nasprotniki javno dostopne kriptografije pogosto uporabljajo kot argument proti kriptografiji. Pri tem včasih pride do pretiravanja, oziroma se skuša celo neresnične primere zlorabe kriptografije uporabiti kot izgovor za omejevanje kriptografije. Po terorističnih napadih 11. septembra 2001 so se sprva porajali številni sumi, da je bila pri načrtovanju terorističnih napadov uporabljena kriptografija, in že so se oglasili pozivi o prepovedi kriptografije, vendar pozneje ti sumi niso bili dokazani (Harrison, 2001). Po drugi strani pa je res, da če lahko kriptogram razbije preiskovalni organ, ga prav lahko tudi kdorkoli drug. Denningova in Baugh navajata primer britanskega izsiljevalca, ki je prestregel bančne transakcije, jih dešifriral, nato pa banko in njene stranke izsiljeval, da jih bo prijavil davčnemu uradu (Denning in Baugh, 1997).

Čeprav primerov uporabe šifriranja s strani kriminala ni veliko, pa njihovo število narašča. Poleg tega Denningova in Baugh ugotavljata, da se povečuje uporaba takih vrst šifriranja, ki jih ni moč razbiti, torej popolnoma onemogočajo prisluškovanje. Avtorja navajata, da ameriški zvezni policiji leta 1995 ni uspelo razbiti pet, leta 1996 pa že dvanajst šifriranih informacij (Denning in Baugh, 2000: 106). Čeprav po njunih opažanjih visoka cena in nezdružljivost posameznih vrst naprav za šifriranje telefonskih pogovorov upočasnjujeta razširitev uporabe kriptografije v telefoniji, pa opozarjata na internetno telefonijo, ki je zelo poceni in omogoča šifriranje zvočnih komunikacij z minimalnimi stroški. Po njunem mnenju največji problem ni uporaba interneta, temveč uporaba kriptografije.

---

[269] V primeru Aldricha Amesa naj bi po nekaterih podatkih preiskovalci do dokazov o njegovem vohunstvu prišli s prestrezanjem elektromagnetnih signalov, ki jih je oddajal njegov računalnik, tj. tehnike, znane tudi pod imenom napad tempest (infiNity, 1997), in ne na podlagi kriptoanalize.

Odgovori na kritike in gibanje cypherpunk

V zvezi s širjenjem javno dostopne kriptografije in njene zlorabe v kriminalne namene se je med kritiki in zagovorniki uporabe kriptografije izoblikoval izraz *kriptoanarhija*. Vendar pa ima za prve in druge izraz povsem različen pomen.

Ena najglasnejših kritičark javne dostopnosti kriptografije je zapisala: "*Zaradi te tehnologije država ne bo mogla več nadzorovati informacij, sestavljati dosjejev, prisluškovati, uravnavati ekonomije in celo pobirati davkov."* (Denning, 1997: 175). Povedano drugače: s tem, ko se državi onemogoči nadzor nad računalniki in telekomunikacijskimi sistemi, le-ti postanejo "*nebesa za kriminalce*" (Denning, 1997: 177), to pa naj bi vodilo v družbeni nered. V razpravi okrog uvedbe čipa Clipper je Denningova zapisala: "*Ustava nam ne daje absolutne zasebnosti pred sodno odrejenimi preiskavami in zasegi, in to z dobrim razlogom. Prevladalo bi brezzakonje. Šifrirne tehnologije, ki ponujajo zasebnost, so v koliziji z največjim orodjem za boj proti kriminalu: prisluškovanjem.*" (Denning, 1994).

Kriptografija naj bi bila torej naperjena predvsem proti državi (Denning, 1997: 187 in Zimmermann, 1999), s tem pa posredno tudi proti državljanom. A ne samo to. Kriptografija ne bi prinesla brezzakonja le zato, ker preiskovalci ne mogli zbrati ustreznih dokazov (Denning, 1993), temveč tudi zato, ker bi po njenem lahko pomanjkanje dokazov privedlo do tega, da bi represivni organi posameznike zapirali že ob sumu kaznivega dejanja, oziroma bi lahko prišlo do tega, da bi se teža dokazov, potrebnih za obsodbo, zmanjšala (Denning, 1993). Utemeljenost njenega razmišljanja morda kaže tudi nastanek t. i. klateškega prisluškovanja (ang. *roving wiretap*) v ZDA, ki je posledica tega, da sodobna tehnologija omogoča bolj razpršeno komuniciranje. Tradicionalne metode prisluškovanja, ki predvidevajo izdajo sodne odredbe za vsak telekomunikacijski priključek posebej, ob hitri menjavi in uporabi več različnih vrst telekomunikacijskih priključkov niso več učinkovite. To je verjetno tudi razlog, da je nova zakonodaja v ZDA dovolila take metode prisluškovanja, ki so bolj invazivne v smislu varstva človekovih pravic.

Ronald Rivest je na tovrstne kritike odgovoril z javnim pismom: "*Lahko si zgradim kakršnokoli hišo (na primer iz železa), si namestim kakršnokoli vrsto ključavnice, vlomne detektorje itd. A vlada, oborožena s preiskovalnim nalogom, nima jamstva, da bo lahko vstopila v moj dom. Analogni sklep je, da lahko posamezniki uporabljajo kakršnokoli vrsto šifriranja želijo, vladi pa je dovoljeno (kadar ima ustrezno pooblastilo), da skuša njihov kriptogram razbiti*" (Rivest, 1994). Tako je odgovoril tudi na dilemo, ali naj bo uspeh prestrezanja zagotovljen ali ne. Poleg tega je Rivest opozoril še na en problem prepovedi šifriranja zaradi zagotavljanja učinkovitosti organov pregona. Denningovo je opozoril, da ni nujno, da je vse, kar pripomore k preganjanju kriminala, tudi dobro in za demokratično družbo sprejemljivo, pa čeprav ne pride do zlorabe: "*Na primer sistem, ki bi lahko vsak telefon, tudi kadar je odložen, spremenil v pooblaščeno prisluškovalno napravo, bi verjetno pomagal preiskovalcem, vendar bi bil nesprejemljiv za večino Američanov... Ali pa zahteva, da vsi državljani nosijo zapestnice, ki jih je mogoče locirati (elektronsko in samo na podlagi sodnega pooblastila).*" (Rivest, 1994).

Drugi nasprotniki omejevanja kriptografije so izpostavili še nekatere druge argumente. Izpostavili so to, da je kriptografija kriminalcem že tako ali tako dostopna (oziroma jim bo dostopna tudi ob morebitni prepovedi), vprašanje je torej, zakaj ne bi bila dostopna tudi drugim državljanom. Prav tako so opozorili na to, da je prisluškovanje samo ena izmed metod boja proti kriminalu (in še to ne največ rabljena – v ZDA). Zato ni verjetno, da bi uporaba kriptografije povzročila "*družbeno opustošenje*", kot je trdila Denningova. Po njihovem mnenju je zgodovina zlorabe prisluškovanja močan argument za svobodno uporabo kriptografije (Thomas, 1994).

Etzioni, ki sicer meni, da zloraba zasebnosti s strani demokratične vlade ni velik problem in da je večji problem zloraba zasebnosti s strani zasebnega sektorja, pravi, da so zagovorniki uporabe kriptografije skrajni individualisti in libertarci. Za zgled takih skrajnežev navaja *cypherpunkerje* (izraz izvira iz izraza *cyberpunk* – kiberpank in vključuje izraz *cipher*, šifra).

Cypherpunkerji izvirajo iz hekerske subkulture, gibanje pa je bilo ustanovljeno leta 1992 na Berkleyski univerzi, čeprav segajo njegovi začetki že v konec 80. let 20. stoletja. Cypherpunkerji zagovarjajo individualne svoboščine posameznika nasproti državi v virtualnem svetu. Sami vidijo izraz *anarhija* povsem drugače kakor kritiki javne rabe kriptografije. Anarhija je po njihovem mnenju odsotnost zunanje prisile in predstavlja svobodo izbire. Leta 1988 je Timothy C. May v *Crypto Anarcist Manifesto* zapisal: "*Vstanite, ničesar ne morete izgubiti, razen bodeče žice, ki vas obdaja!*" (May, 1988). Vendar sami poudarjajo, da anarhija ne pomeni absolutne svobode: "*...'anarhija' ne pomeni anarhije v poljudnem pojmovanju: brezzakonja, nereda, kaosa ... Morda bi bil bolj razumljiv izraz 'kibersvoboda' (ang. cyber liberty)... Anarhija v tem smislu ne pomeni, da ni lokalne hierarhije, niti ne pomeni, da ni vladarjev...*" (May, 1995). Pri tem je ključna uporaba tehnologije: "*Šele pred kratkim so računalniki in omrežja postali dovolj hitri, da so te ideje postale praktično uresničljive. V naslednjih desetih letih pa bodo postali dovolj hitri, da bodo te ideje tudi ekonomsko izvedljive in praktično izvedljive.*" ter "*Ta razvoj [gre za razvoj tehnologije, m. op.] bo popolnoma spremenil naravo državne regulacije, njeno zmožnost pobiranja davkov in nadzora ekonomskih interakcij, sposobnost ohranjanja skritih informacij...*" (May, 1988).

Eric Hughes v *Cypherpunks manifesto* izpostavlja temeljne vrednote gibanja: svobodo izražanja, ki pomeni tako uporabo šifriranega govora kot svoboden pretok vseh informacij[270], ter zasebnost in iz nje izhajajočo anonimnost, ki posameznikom omogoča, da svojo identiteto razkrijejo samo, kadar to sami želijo in v to niso prisiljeni. "*Anonimni sistemi omogočajo posameznikom, da razkrijejo svojo identiteto, kadar to želijo in samo takrat; to je bistvo zasebnosti*" (Hughes, 1993).

Ključni tehnologiji, ki povezujeta te tri vrednote, pa sta po njihovem mnenju kriptografija in internet. "*Internet je anarhija... ni osrednjega nadzora, ni vladarja, ni vodje, ni 'zakonov'. Nobena nacija ga ne nadzoruje, noben upravni organ ne določa regulacijske politike*" (May, 1995). To naj bi bilo po njihovem mnenju polje za popolno svobodo posameznikov.

---

[270] Timothy C. May je v *Crypto Anarchist Manifesto* zapisal: "*Kriptoanarhija bo omogočila svobodno trgovanje z državnimi skrivnostmi in trgovanje s prepovedanimi in ukradenimi gradivi... Navidezno majhno odkritje s skrivnostne veje matematike bo kot žične škarje, ki bodo odstranile bodečo žico okrog intelektualne lastnine*" (May, 1988).

Delovanje cypherpunkerjev pa ni ostalo samo na načelni ravni, temveč je bilo gibanje ustanovljeno z namenom neposredne akcije: "*Svojo lastno zasebnost moramo braniti, če pričakujemo, da jo bomo sploh imeli,*" je leta 1993 zapisal Hughes v svojem manifestu. Cypherpunksi so bili ustanovljeni z namenom razvijanja programov za anonimizacijo na internetu (anonimne strežnike za pošiljanje elektronske pošte (ang. *remailer*), ki izbrišejo podatke o izvoru elektronskega sporočila, ter anonimne zastopniške programe (ang. *anonymous proxy*)[271] za uporabo drugih internetnih storitev), šifriranje podatkov in sporočil, elektronsko podpisovanje in anonimni digitalni denar.

Hughes pravi, da so v preteklosti ljudje branili svojo zasebnost na različne načine, vendar jim tehnologija ni omogočala močne zasebnosti. Elektronska tehnologija je to spremenila. To je po njegovem mnenju treba izkoristiti: "*Tehnologija je spustila duha iz steklenice ... Nacionalne meje bolj kot kdaj prej postajajo bolj transparentne za podatke ... Ustavljanje podatkov na mejah je manj kot brezupno.*" (May, 1995).

Številne člane gibanja je pozneje mogoče zaslediti v različnih nevladnih organizacijah (na primer *Global Internet Liberty Campaign*, *Electronic Frontier Foundation*, *Electronic Privacy Information Center* itd.), člani gibanja pa so verjetno tudi najbolj zaslužni za razvoj brezplačne in proste šifrirne programske opreme in njeno razširjanje po vsem svetu.

Vendar pa kaže, da so cypherpunkerji problem zasebnosti razumeli preveč enostransko, saj so ga gledali predvsem skozi odnos med posameznikom in državo, povsem pa spregledali družbeno sfero in vlogo nadzora v sodobni družbi. Timothy C. May pravi, da je kriptoanarhija pravzaprav nekakšen anarhokapitalizem, ki zagovarja popolno svobodo ekonomskih transakcij. Pri tem pa seveda nastopi kolizija med svobodo izmenjevanja informacij in zasebnostjo, kar je očitno predvsem pri informacijski zasebnosti. Poleg tega dosledno nasprotovanje kakršnikoli državni regulaciji zaščiti zasebnosti celo škoduje, saj lahko prevelika deregulacija, kot je bilo prikazano v prejšnjih poglavjih, da preveč proste roke družbenemu poseganju v zasebnost.

To se je izkazalo tudi na primeru anonimizacijskih strežnikov, predvsem v povezavi z bojem proti smetju. Pritiski na anonimizacijske sisteme namreč niso prihajali samo od države,[272] temveč tudi od nevladnih organizacij za boj proti smetju in otroški pornografiji, tem pritiskom pa se je bilo veliko teže upreti. Da so v praksi pritiski družbene sfere lahko veliko bolj problematični

---

[271] Zastopniški programi se v internetu predstavljajo s svojim internetnim naslovom, zato lahko skrijejo identiteto pravega uporabnika interneta. Anonimni zastopniški programi identifikacijskih podatkov o svojih uporabnikih ne posredujejo nikamor in jih ne shranjujejo, s tem pa svojim uporabnikom zagotavljajo anonimno brskanje po internetu. V grobem ločimo navadne anonimne zastopniške programe (ang. *standalone anonymous proxy*) in njihove spletne različice (ang. *web-based anonymous proxy*). Danes se namesto anonimnih zastopniških programov uporabljajo predvsem anonimizacijska omrežja.

[272] Najbolj znan je primer psevdoanonimnega strežnika za pošiljanje elektronske pošte *Penet* iz Finske. Strežnik namreč ni bil povsem anonimizacijski, saj je lokalno shranjeval identifikacijske podatke uporabnikov. Leta 1995 je *scientološka cerkev* s sodno odredbo zahtevala razkritje identitete uporabnika, ki je v USENET anonimno objavil neki njihov dokument. Upravitelj strežnika je bil zato prisiljen razkriti identiteto uporabnika. Naslednje leto je britanski časopis *The Observer* Penet obtožil, da je omogočil objavo otroške pornografije na USENET. Penetu je obtožbe uspelo ovreči, vendar je konec leta upravitelj zaradi pritiskov zaprl strežnik in uničil podatke o njegovih uporabnikih (Wikipedia, geslo: "Penet remailer"). Podobno se utegne zgoditi tudi sodobnim anonimizacijskim sistemom, npr. omrežju Tor ali sistemu Freenet. Freenet že zdaj velja za "leglo otroške pornografije", znani pa so tudi primeri zlorab omrežja Tor za razširjanje vsebin z otroško pornografijo (Barbut, 2006).

kot pritiski države, dokazuje primer Edwarda Feltena, profesorja s princetonske univerze v ZDA. Felten namreč piše spletni dnevnik (ang. *blog*), v katerem objavlja svoja razmišljanja o kriptografiji in informacijski varnosti. Leta 2002 je nekdo poslal na neki poštni seznam povezavo do njegove spletne strani. Neki drug član istega poštnega seznama je organizaciji *SpamCop* sporočilo pomotoma prijavil kot smetje. *SpamCop* vzdržuje črne sezname smetilnih strežnikov (ang. *blacklist*) in Feltenovo spletno stran so takoj uvrstili na črni seznam (ker naj bi bila v domnevnem nezaželenem sporočilu oglaševana). Od Feltenovega ponudnika dostopa do interneta so zahtevali, naj Feltena izključi iz omrežja. Feltenu, ki sploh ni poslal sporne elektronske pošte, niso dali možnosti, da se brani, niti mu niso želeli povedati, kdo ga je prijavil, niti tega, kakšna je bila vsebina spornega sporočila, ki ga v resnici sploh ni poslal. Feltenu je nato samemu uspelo ugotoviti, kdo je podal prijavo, in vsi vpleteni (Felten, avtor spornega sporočila, prijavitelj in Feltenov ponudnik dostopa do interneta) so *SpamCop*u skušali pojasniti, da je prišlo do pomote. Vendar so jih v *SpamCop*u ignorirali, ponudniku dostopa do interneta pa celo zagrozili, da bodo na svoj črni seznam dali vse njegove uporabnike, če Feltena ne izključi iz omrežja (Felten, 2002).

Podobne izkušnje imajo tudi vzdrževalci omrežja Tor oziroma lastniki izhodnih anonimizacijskih strežnikov Tor. Eden izmed upraviteljev teh strežnikov je na poštnem seznamu uporabnikov omrežja Tor takole opisal svoje izkušnje:

> "*Drugo obvestilo je bilo od 'The National Communications System (NCS), agencije ameriškega ministrstva za domovinsko varnost'. Obveščalo je mojega ponudnika dostopa do interneta, da imam virus ali trojanskega konja. ... Vsekakor je obvestilo ministrstva za domovinsko varnost, da širiš viruse, lahko zelo resna stvar.*
>
> ...
>
> *Žal nisem dovolj bogat, da bi si kupil svojo omrežno infrastrukturo. Odkar me je prva 'smetilna' obtožba za več kot 12 ur izključila iz interneta ..., sem moral sprejeti zame bolečo odločitev, da svojo 'izhodno politiko' nastavim na 'reject *:*'* [to pomeni, da upravitelj strežnika Tor v svojem strežniku ne omogoča izhoda iz anonimizacijskega omrežja Tor v internet; smisel omrežja Tor pa je, da ima čim več odprtih izhodov, m. op.]
>
> ...
>
> *Anonimni dostop do omrežja je bistveno orodje svobode, zato tiste, ki lahko te vrste zlorab otežite (z zlorabo mislim biti kaznovan zaradi domnevne kršitve pravil sprejemljive uporabe omrežja*[273]*), prosim, da ste malo bolj aktivni.* " (Heschong, 2005; besedilo je slovnično urejeno).

[273] Posledica kršitve pravil sprejemljive uporabe omrežja (ang. *Acceptable Use Policy*) je izključitev uporabnika iz omrežja.

Večina anonimizacijskih strežnikov, ki so jih razvijali cypherpunkerji danes ni več javno dostopna, razlog za to pa niso prepovedi držav, temveč zlorabe s strani smetilcev in kiberkriminalcev ter pritiski zasebnih organizacij za boj proti nezaželeni pošti ali smetju. Zato popolna odsotnost državne regulacije interneta ne pomeni nujno razvoja interneta proti večji svobodi, kot so bili prepričani cypherpunkerji; pravzaprav je prišlo celo do nasprotnega učinka. Kljub temu zamisel o anonimizaciji ni povsem zamrla. Konec leta 2004 jo je oživila ameriška nevladna organizacija *Electronic Frontier Foundation*, in sicer v obliki razvoja anonimizacijskega omrežja Tor.[274] Gre za porazdeljeno omrežje anonimizacijskih strežnikov, med katerimi se preusmerja šifriran promet posameznega uporabnika, dokler ga v eni izmed izhodnih točk omrežja ne zapusti.

Razlogi za tak odnos cypherpunkerjev do zasebnosti pa verjetno niso samo ideološki. Cypherpunkerji so očitno spregledali to, da pritiski niso samo politični, temveč tudi ekonomski in družbeni, čeprav so nastopili tudi proti intelektualni lastnini. Ljudje se danes svoji zasebnosti večinoma odpovedujejo zaradi ekonomskih koristi in ne samo zaradi neposrednega pritiska države. Hughes je sicer v svojem manifestu dal velik poudarek anonimnosti ("*Ko v trgovini kupim časopis in plačam z denarjem, ni treba vedeti, kdo sem.*" (Hughes, 1993)), vendar kaže, da so cypherpunkerji anonimnost in zasebnost razumeli predvsem kot anonimnost in zasebnost nasproti *oblasti*, zato Boyle upravičeno ugotavlja, da je "*digitalni libertanizem neustrezen zaradi svoje slepote do učinkov zasebne moči*" (Boyle, 1997).

Še en pomemben argument je, ki ga zagovorniki kriptografije v ZDA praviloma ne izpostavljajo, poleg tega tudi ni povezan s človekovimi pravicami. Maja 2004 je spletni časopis Computerworld objavil zgodbo o tem, da namerava EU financirati vzpostavitev sistema kvantne kriptografije (Willan, 2004). Gre za poseben sistem, ki popolnoma onemogoča prestrezanje, saj je vsak poskus prestrezanja moč zaznati, če je sistem pravilno zasnovan. Namen projekta je onemogočiti prestrezanje s strani sistema ECHELON, o katerem je odbor EU *Temporary Committee on the ECHELON Interception System* v svojem poročilu Evropskemu parlamentu z dne 4. maja 2001 zapisal, da "*sistem za prestrezanje komunikacij obstaja ... pomembno pa je, da je njegov namen prestrezanje civilnih in poslovnih komunikacij,*[275] *in ne vojaških komunikacij*" (Temporary Committee on the ECHELON Interception System 2001, 88).[276] Argument

---

[274] Začetki razvoja tega anonimizacijskega omrežja, t. i. *Onion routers*, segajo v raziskovalni laboratorij ameriške mornarice leta 2002 (EFF, 2005c).

[275] Bamford pravi, da so se tajne službe na poslovne komunikacije usmerile že kmalu po drugi svetovni vojni, saj so postala pomembna vprašanja kot "*kje in s kom se posluje ali katera nova orožja se načrtuje v naslednjih petih letih*" itd. (Bamford, 1983: 488).

[276] Gre za sistem globalnega nadzora komunikacij s strani obveščevalnih služb, nastal pa naj bi po tajnem sporazumu med ZDA in Veliko Britanijo iz leta 1947, znanem pod imenom UKUSA (*United Kingdom - United States of America Agreement*. Pozneje so se jima pridružile še nekatere druge države) (Bamford, 1983: 410, 511). Obstoj sporazuma je potrdila tudi komisija Evropskega parlamenta (Temporary Committee on the ECHELON Interception System, 2001). Sporazum predvideva sodelovanje in izmenjavo informacij ter delitev pristojnosti za prisluškovanje med tajnimi službami ZDA, Velike Britanije, Kanade, Avstralije in Nove Zelandije (Bamford, 1983: 488-489). Ker imajo tajne službe načeloma omejitve pri prisluškovanju doma, ne pa tudi v tujini, nekateri domnevajo, da tajne službe uporabljajo ECHELON, da zaobidejo omejitve pri prisluškovanju. Obstoj sistema je postal javnosti bolj poznan konec 90-tih let, 21. oktobra 2001 pa so na internetu celo organizirali Jam Echelon Day, kjer so organizatorji uporabnike interneta pozivali, naj pošljejo čim več elektronskih sporočil z besedami, ki naj bi sistem Echelon aktivirale, s čimer naj bi dosegli njegovo preobremenitev. Da bi to kakšne večje preobremenitve zares prišlo je sicer malo verjetno, kljub temu pa takšne akcije pomagajo povečati zavedanje uporabnikov interneta o tem problemu (Oakes, 1999).

izpostavlja problem industrijskega vohunjenja v korist ameriških podjetij. Zagovorniki razvoja kriptografije pa pravijo, da kriptografija lahko pomembno pripomore k preprečevanju industrijske špijonaže, s čimer se zagotavlja poštena konkurenčnost.

Kriptografija na tehtnici

Vprašanje kriptografije je pravzaprav vprašanje zasebnosti v digitalnem svetu, pri čemer se je razprava o problemu zasebnosti v virtualnem svetu vrtela predvsem okrog razmerja med državo in posameznikom: "*Kriptoanarhija osvobaja posameznike pred ... vlado. Za libertarce močna kriptografija zagotavlja sredstva za izogibanje vladi [mišljeno je izogibanje vladnemu nadzoru, m. op.].*" (May, 1995).

Trenja med nasprotniki in zagovorniki neomejene uporabe kriptografije delno izvirajo iz njihovega različnega razumevanja vloge države, delno pa gre tudi za različne interese. Medtem ko nasprotniki neomejene uporabe kriptografije vidijo državo kot dobrega čuvaja, ki skrbi za varnost in blaginjo svojih državljanov, jo zagovorniki vidijo kot institucijo, ki omejuje njihove pravice in svoboščine: *"To, česar se, kot kaže, vlada resnično boji pri Zimmermanovem programu, ni precej dobra zasebnost (Pretty Good Privacy – ime Zimmermanovega programa, op. p.), temveč zasebnost kot taka.*" (The Ethical Spectacle, 1995).

Kriptoanarhisti pa so šli v konfrontaciji z državo še dlje: "*...Virtualne skupnosti zunaj dosega vladnega nadzora bodo lahko povzročile probleme pri zagotavljanju zakonitosti (ang. law enforcement) in pobiranju davkov. (Nekaterim od nas je ta vidik všeč.)*" in "*... moč nacionalnih držav bo zmanjšana... Je to dobro? Večinoma da.*" (May, 1995). Še več, države ne vidijo le kot institucije, ki omejuje pravice posameznikov, temveč celo kot institucijo, ki posameznike pobija: "*Toda ne pozabimo, da so nacionalne države pod pretvezo, da nas ščitijo pred drugimi, samo v tem stoletju pobile več kot 100 milijonov ljudi.*" (May, 1995).

Zagovorniki javno dostopne kriptografije in cypherpunkerji priznavajo, da je kriptografijo mogoče zlorabiti. Vendar pa pravijo, da koristi pretehtajo nad stroški. Poleg tega so opozarjali tudi na to, da se večina zločinov zgodi zunaj kiberprostora, nekateri nasilni zločini pa se v kiberprostoru sploh ne morejo zgoditi (Thomas, 1994); to ponazarja stavek "*You can't eat cyberspace*" ("*V kibersvetu ni mogoče jesti.*") in "*Sticks and stones can break my bones but bytes can never hurt me.*" ("*Palice in kamni mi lahko polomijo kosti, biti pa me ne morejo poškodovati.*" (Boyle, 1997)). V razpravi okrog čipa Clipper so nekateri zagovarjali stališče, da prepoved učinkovite kriptografije ne bi vplivala na širjenje kriminala, saj je uporaba kriptografije s strani kriminalcev zanemarljiva (Rivest, 1994).

Ne glede na argumente za ali proti uporabi kriptografije pa so zagovorniki uporabe kriptografije vedno računali na to, da je duh spuščen iz steklenice, da je torej razvoj nepovraten in neustavljiv: "*Informacije ne samo, da želijo biti svobodne, informacije hrepenijo po svobodi ... Vemo, da programska oprema ne more biti uničena in da široko razpršenega sistema ni mogoče ugasniti.*" (Hughes, 1993). Timothy May je zato zapisal: "*Mi bomo kolonizatorji kiberprostora.*" (May, 1995).

Kot rečeno, sodobna informacijsko-komunikacijska tehnologija omogoča številne posege v zasebnost, saj je pogosto že zasnovana za nadzor. Vendar pa tehnologija posameznikom tudi omogoča, da se izognejo nadzorovanju. A podobno kot pri primerjavi Benthamove zamisli o Panoptikonu in načela publicitete v delovanju politične skupščine lahko tudi pri tehnologiji ugotovimo, da je večinoma uporabljena za nadzor posameznikov in ne toliko za njihovo zaščito pred nadzorom. Uporabo tehnologij, ki onemogočajo nadzor, skušajo države in njihovi represivni organi sistematično omejevati, zato je ta tehnologija dostopna le manjšemu številu posameznikov, ki si jim uporabo teh tehnologij uspe izboriti. Ena takih tipičnih tehnologij je kriptografija, katere rabo so skušale države pravno in dejansko omejevati, njeni zagovorniki pa so bili deležni številnih očitkov oziroma družbenih pritiskov, češ da kriptografija pomaga pri skrivanju kriminalcev in teroristov. Primer kriptografije in gibanja za elektronsko zasebnost tako lepo kaže, da je uporaba tehnologij, ki posamezniku omogočajo, da se izogne nadzoru, v praksi zelo omejena in celo velja za družbeno nezaželeno; vendar to ne velja za tehnologije, namenjene nadzoru. Uporaba le-teh je zelo razširjena in navadno velja za družbeno povsem sprejemljivo.

Cypherpunkerjem je šifrirne programe, npr. PGP, uspelo razširiti po vsem kiberprostoru. Prepričani so bili, da bo kriptografija temeljno spremenila naravo korporacij in vlade (May, 1988). Kljub temu je danes kriptografija razširjena predvsem na področju elektronskega poslovanja in ne pri običajnem medsebojnem komuniciranju; to kaže na to, da je osvobodilna funkcija kriptografije v praksi zapostavljena. Poleg tega se kriptografija uporablja predvsem za šifriranje podatkov med prenosom po nezaščitenih komunikacijskih omrežjih (s čimer je omejen nepooblaščen dostop do njih), zakonodaja pa pooblaščenim preiskovalcem (državi) omogoča, da imajo do podatkov še vedno lahko dostop tako, da od upravljavcev podatkov zahtevajo dostop. To je še posebej problematično zato, ker je čedalje več osebnih podatkov posameznikov pa tudi komunikacij (elektronska in glasovna pošta) vse pogosteje shranjenih na pomnilniških nosilcih v lasti različnih podjetij. Podatke, ki so bili včasih pod neposrednim nadzorom posameznikov, tako zdaj nadzorujejo in upravljajo ponudniki storitev; ti podatki se do uporabnika sicer res prenašajo po šifriranih povezavah, pri ponudniku storitev pa so preiskovalcem kljub uporabi šifriranja povsem dostopni. Prav tako so sodobni informacijski sistemi zasnovani tako, da tudi ob uporabi kriptografije čim bolj zmanjšajo anonimnost posameznika (saj to zagotavlja varnost transakcij, hkrati pa omogoča izvajanje sodobnih tržnih prijemov). To pomeni, da ima kriptografija namesto vloge varovanja človekove pravice do zasebnosti predvsem vlogo pospeševanja elektronskega poslovanja, torej varovanja ekonomskih interesov korporacij.

Če so se cypherpunkerji v 90. letih razglasili za kolonizatorje kiberprostora, se danes zastavlja vprašanje, kdo je pravi kolonizator tega prostora. Danes namreč v kiberprostoru po eni strani čedalje bolj prevladujejo virusi, črvi, nezaželena pošta in hekerski napadi, po drugi strani pa se veča uporaba neposrednega trženja in tehnologij za zaščito avtorskih pravic, katerih stranski učinek je poseganje v zasebnost posameznikov. Prav tako tudi države čedalje dejavneje posegajo v internet in vzpostavljajo nadzorne mehanizme. Je panoptičnost že vgrajena v internet?

PROBLEM ZASEBNOSTI NA INTERNETU

Tehnologija osvobaja…?

Cypherpunkerji so bili prepričani, da tehnologija oziroma internet omogoča osvoboditev posameznika pred državo in da ju je zaradi njune narave[277] nemogoče nadzorovati, čeprav si države to želijo: "*To [da internet razume cenzuro kot škodo in jo skuša zaobiti*[278]*] velja tudi za poskuse zakonodajne regulacije obnašanja na internetu ... [Države] še vedno govorijo o 'nadzoru' interneta, v resnici pa imajo zakoni ene nacije pogosto zelo malo vpliva v drugih državah.*" (May, 1995). Pri tem naj ne bi šlo za napako, temveč za lastnost interneta ("*it is not a bug, but a feature*"). Na prve poizkuse regulacije interneta v ZDA, šlo je za *Communications Decency Act*,[279] se je internetna skupnost burno odzvala z geslom "*Keep your laws off our Net! / Držite svoje zakone stran od našega interneta!*" (Boyle, 1997). Slogan ponazarja libertaren odnos cypherpunkerjev – *vaši* zakoni, *naš* internet. Internet je torej nekaj, česar država ne samo, da ne razume, temveč v njem tudi nima kaj iskati. Govorili so celo o "*tehnološki neizogibnosti*" (ang. *Technological Inevitability*), ki bi jo bilo mogoče zaustaviti samo z drakonskimi ukrepi, denimo prepovedjo uporabe tehnologije. Internet naj bi bil torej neki nov prostor, ki ga države ne morejo nadzorovati in ki posameznikom omogoča popolno svobodo. Razvoj proti popolni svobodi naj bi bil neizogiben – tehnološko neizogiben. Dejansko je internet teže nadzorovati kakor druge informacijske tehnologije in Boyle je zapisal, da je "*dostop kot prisluškovanje, ki ima samo dvoje nastavitev: izključeno ali pa popolno*".[280] (Boyle, 1997). Boyle je govoril predvsem o dostopu do tehnologije (interneta) in ne zgolj o nadzoru. A kot se je izkazalo že pri nastanku javno dostopne kriptografije in poizkusih ameriške vlade, da bi jo skušala prepovedati ali vsaj omejiti, se država nikoli ni mogla sprijazniti s tem, da bi bil nadzor 'izključen'.

…ali pa je panoptičnost že vgrajena v internet?

Leta 1996 je bil v ZDA sprejet *Communications Decency Act*,[281] ki je prepovedoval objavljanje nespodobnih ali žaljivih vsebin na internetu. Zakon je povzročil val nasprotovanja, saj so ga nasprotniki dojemali kot poizkus cenzure interneta. Proti zakonu je bila takoj vložena ustavna pritožba in leta 1997 je Vrhovno sodišče ZDA v primeru *Reno proti ACLU*[282] presodilo, da zakon krši svobodo govora, ki je zagotovljena v prvem amandmaju ameriške ustave.[283] Odločitev je

---

277 Boyle te lastnosti (tehnologija medija, geografska razpršenost in narava njegove vsebine) imenuje internetna sveta trojica (Boyle, 1997).

278 "*The Net interprets cenzorship as damage and routes around it.*" – gre za znano izjavo Johna Gillmora.

279 Communications Decency Act of 1996, 47 U.S.C. (1996).

280 Na podoben problem je pokazal tudi primer Carnivora. Zaradi lastnosti paketnih omrežij je prestrezanje v internetu mogoče izvesti samo tako, da se prestreza *ves* internetni promet, vsebino, ki se jo želi prestreči, pa se nato izloči s filtriranjem.

281 Communications Decency Act of 1996, 47 U.S.C. (1996).

282 Reno v. American Civil Liberties Union, 521 U.S. 844 (1997).

283 1. amandma, Listina svoboščin (Bill of Rights), 1791.

sprožila val odobravanja in zdelo se je, da je vsak poizkus regulacije interneta že vnaprej obsojen na neuspeh.

Vendar pa Boyle ugotavlja, da nastanek "*'tehnologij svobode' pravzaprav zahteva poostritev mehanizmov nadzora, tako javnih kot zasebnih*" (Boyle, 1997). Da do takih teženj prihaja tudi na internetu, ni presenetljivo, sploh ne v luči razvoja digitalne telefonije, za katero je na začetku prav tako kazalo, da posameznikom obljublja možnost, da se izognejo nadzoru. Po sprejemu CALEA Act[284] leta 1994 pa se je izkazalo, da digitalna telefonija prisluškovanje pravzaprav celo olajšuje. Internet je bil za državo nekaj novega in neobvladljivega samo na začetku. Ko pa se je njegova uporaba dovolj razširila, so državni organi in kapitalistične korporacije začeli odkrivati privlačnost nadzorovanja po internetu.

Še več. Kot je bilo delno že prikazano pri prikazu razvoja in problemov informacijske zasebnosti v ZDA, se zdi, da neobstoj s strani države postavljenih regulacijskih pravil ne pomeni nujno priložnosti za razvoj svobode, kot so bili prepričani kiberanarhisti, temveč prav nasprotno. Tehnologija je namreč nekakšen 'množitelj moči' (ang. *force multiplier*) za tiste, ki jo uporabljajo – njihovo moč lahko povečuje za dobro ali slabo (Geer et. al., 2003: 8). Popolna ali prevelika neregulacija uporabe nadzorovalnih mehanizmov je tako privedla do množice *Malih bratov*, prišlo pa je tudi do privatizacije nadzorovalnih sistemov. Prav slednje je lahko precej problematično, saj je nad zasebnimi podjetji oziroma nedržavnimi akterji, ki izvajajo nadzor, načeloma veliko manjši javni nadzor kakor nad državo, dodaten problem pa predstavlja tudi računalniška kriminaliteta. Če so bili prvi zakonski posegi v internet razumljeni kot omejevanje svobode in so zato sprožili nasprotovanje javnosti, pa je prevelika odsotnost neregulacije privedla do tega, da uporabniki sami čedalje bolj zahtevajo zakonodajno regulacijo interneta zaradi zaščite svojih pravic; to je razvidno predvsem pri problemu nezaželene elektronske pošte (t. i. smetje ali spam) ter pri informacijski zasebnosti. Prišli smo do točke, ko poglavitni problem ni več država, temveč družba, in ko bi morala država posameznike zaščititi pred družbenimi akterji.

Zaradi odsotnosti državne regulacije so se nekateri uporabniki hitro zavedeli pomena samozaščitnega ravnanja in razvoja ustrezne varnostne kulture. Računalniška industrija pa je v trženju varnostnih tehnologij našla novo tržno nišo. Vendar *International Working Group on Data Protection in Telecommunications* ugotavlja, da samozaščitno ravnanje uporabnikov interneta samo po sebi ne more zagotoviti ustrezne stopnje varstva zasebnosti na internetu; za to je potreben celovit pravni okvir (International Working Group on Data Protection in Telecommunications, 1998). Problem varnosti in zasebnosti na internetu namreč ni samo tehnični, temveč predvsem družbeni problem.

Organizacija Privacy Rights Clearinghouse je že kmalu po množični razširitvi uporabe interneta ugotovila, da "*pravzaprav ni internetne (on-line) dejavnosti, ki bi omogočila popolno zasebnost*" (Privacy Rights Clearinghouse, 1998). Problem interneta je tako predvsem v tem,

[284] Communications Assistance for Law Enforcement Act (Digital Telephony Act) of 1994, 47 U.S.C. (1994).

da tehnologija že sama po sebi, zaradi svojih lastnosti, omogoča nekatere zlorabe zasebnosti bolj, kot bi bile te mogoče v fizičnem prostoru. Povečana možnost ubikvitete, vsenavzočnost, in prepustnost teritorialnih meja je privedla do tega, da prostor odpravljamo kot oviro, vendar pa s tem tudi izgubljamo zaščitno vlogo prostora (Mlinar, 1994: 11). Pri tem ne gre zgolj za to, da bi bila tehnologija že vnaprej zasnovana z namenom nadzorovanja posameznikov, do česar sicer tudi prihaja, temveč tudi za uporabo uveljavljenih tehnologij na način, ki omogoča nadzorovanje. Glede panoptične moči interneta je treba opozoriti na dve pomembni lastnosti računalniške tehnologije: računalniška omrežja omogočajo decentraliziran nadzor, saj lahko omogočijo povezovanje formalno ločenih nadzornih sistemov prek telekomunikacijskih sredstev; pomembna lastnost računalnikov pa je tudi njihova zmožnost shranjevanja oziroma arhiviranja podatkov, kar omogoča gradnjo arhivov oziroma dosjejev (Kovačič, 2003b: 39–40). Gre torej za podobne oblike zlorab zasebnosti kot v fizičnem svetu, le s to razliko, da se te zlorabe v internetu kažejo drugače in da so zaradi tehnologije številčnejše, saj je (informacijska) tehnologija nadzorovanje poglobila in okrepila.

Ena izmed posledic teh stranskih učinkov internetne tehnologije je tako predvsem ogroženost informacijske zasebnosti. Delovni organ EU *Data Protection Working Party* je v svojem poročilu leta 2000 ugotovil, da se danes na internetu zbira veliko število osebnih podatkov, in to brez privolitve oziroma celo brez vednosti posameznikov (Data Protection Working Party 2000, 19).

Hekerji: specifični akterji nadzora na internetu

Tako kot v fizičnem svetu tudi na internetu poteka disciplinski in regulacijski nadzor, pogosto v obliki nadzora državljana in nadzora potrošnika. Zaradi narave kiberprostora pa je zelo razširjen tudi t. i. nezakoniti nadzor, ki sicer sodi na polje računalniške kriminalitete, izvajajo pa ga ljudje, ki jih popularno označujemo z izrazom hekerji.

Izraz "heker" (ang. *hacker*) je izumil Joseph Weizenbaum leta 1976 (Voiskounsky, Babveva in Smyslova, 2000: 57), popularno pa danes z njim opisujemo posameznika, ki ima veliko računalniško-tehničnega znanja, to znanje pa izkorišča za napad na računalniške sisteme; to hekerje uvršča na polje računalniške kriminalitete. Izraz hekanje se večinoma uporablja za "*zapleteno mešanico zakonitih in nezakonitih dejavnosti, od legitimnega ustvarjalnega programiranja, do prepovedanega vdiranja in manipulacije svetovnih telefonskih ali računalniških sistemov*" (Taylor, 2000: 36); najpogosteje pa se ga dojema kot prefinjeno ilegalno dejavnost. Nekateri nadvse prefinjeni informacijski napadi dajejo slutiti, da je hekanje postalo tudi del informacijskega vojskovanja. Na to nakazuje primer Mirrim Colledgea v Severni Koreji in operacija Titan Rain. Davies v besedilu *Information warfare and the future of the spy* ugotavlja, da je bila nekdanja Sovjetska zveza ob koncu hladne vojne največji izvor računalniških virusov (33,4 % virusov z znanim izvorom naj bi prihajalo iz SZ in držav vzhodne Evrope) in ta podatek je glede na razširjenost računalnikov v teh državah vsekakor vreden razmisleka (Davies, 2000:

262). Nekatere hekerske skupine pa so tudi že javno priznale sodelovanje s policijo in tajnimi službami.[285]

Douglas Thomas in Brian D. Loader sicer menita, da kiberkriminal ni zgolj uporaba informacijsko-komunikacijske tehnologije v kriminalne namene, temveč je bistveno to, da ta kriminal ne bi bil mogoč brez uporabe tehnologije, vsaj ne v takem obsegu (Thomas in Loader, 2000: 6). Poleg tega se kiberkriminal po Reitingerju razlikuje od navadnega kriminala še po treh pomembnih značilnostih: lahko je izveden na daljavo; identiteto tistega, ki kaznivo dejanje izvede, je mogoče razmeroma enostavno zakriti ali ponarediti (to je tudi razlog za številne internetne prevare, t. i. *phishing*); poleg tega sledenje izvornemu komunikacijskemu sredstvu, prek katerega se je nekdo povezal v kiberprostor, ni vedno mogoče, saj izurjeni napadalci pogosto uporabljajo tehniko povezovanja prek različnih sistemov (ang. *looping* ali *weaving*, gre za tehniko, ko se napadalec na ciljni sistem ne poveže neposredno, temveč prek številnih drugih sistemov, po možnosti lociranih v različnih državah, kar onemogoči ali vsaj oteži sledenje) (Reitinger, 2000: 137). Thomas pravi: "*[Hekerji] razumejo, da če 'kriminal' ne more biti povezan s telesom, le-to ne more biti kaznovano*" (Thomas, 2000: 24). To je tudi razlog, zakaj ljudje kiberkriminalce pogosto dojemajo kot napol čudežna bitja in zakaj se o hekerjih in njihovih sposobnostih pogosto spletajo napol mi(s)tične predstave.

Danes izraz heker poljudno označuje kateregakoli kiberkriminalca, vendar Thomas in Loader kiberkriminalce delita v tri kategorije: na hekerje in phreakerje (ang. *phreaker*; gre za "telefonske hekerje", ki se ukvarjajo z zlorabo telefonskih sistemov; phreakerji so bili predhodniki hekerjev, razvijati pa so se začeli v ZDA konec 70. let; dandanes jih skorajda ni več), ki vdirajo v sisteme večinoma iz radovednosti in ne povzročajo škode; na trgovce z informacijami, katerih poglavitni motiv je profit; ter na teroriste, ekstremiste in deviantneže, ki informacijske sisteme uporabljajo za nezakonite politične ali družbene dejavnosti (npr. razširjanje sovražnega govora, otroške pornografije, napade na strežnike sovražnih držav itd.) (Thomas, 2000: 6–8).

Poznamo pa še drugo delitev. Levy pravi, da so štiri generacije hekerjev, s katerimi se je pojem hekerja spreminjal skozi čas. Prva generacija, ki izvira z MIT, naj bi v 50. in 60. letih prejšnjega stoletja razvila prve programske tehnike. Drugo generacijo predstavljajo tisti posamezniki, ki so razvili prve osebne računalnike in s tem omogočili dostop računalniške tehnologije širšim množicam. Tretjo generacijo označujejo vodilni razvijalci računalniških iger. Četrto pa tisti, ki na nedovoljene načine vstopajo v tuje računalnike (Taylor, 2000: 36). Po samodefiniciji

[285] Člani ameriške hekerske skupine *Cult Of The Dead Cow* (*CDC*) so 26. novembra 2001 FBI javno ponudili vsakršno pomoč v "vojni proti terorizmu" (Ruffin, 2001) in to je med različnimi hekerskimi skupinami povzročilo velik razkol. Znano je tudi, da so člani druge ameriške hekerske skupine *L0pht* 18. maja 1998 pričali pred ameriškim senatom (pričanje je bilo sicer tajno, informacija o tem in povzetek pričanja pa je v Thompson, 2000); menda naj bi izjavili, da so za *National Security Agency* pripravili več seminarjev. Oktobra 1999 pa je New York Times z njimi objavil intervju v njihovih prostorih; iz opisa je razvidno, da so posedovali nadvse sofisticirano in drago opremo, med drugim tudi več kot 200 računalnikov različnih vrst (tudi drage Sunove delovne postaje), osciloskope, radijske ter satelitske sprejemnike itd. Samo po sebi se zastavlja vprašanje, od kod jim denar za vso to opremo glede na to, da gre za osem mladeničev, starih med 20 in 30 let (Gottlieb, 1999). Skupini *L0pht* in *CDC* sta sicer tesno povezani, povezani pa sta tudi s politično aktivistično hekersko skupino *Hacktivismo*.

pa se hekerji v hekerskem slovarju (*Jargonfile*) opisujejo kot "*ljudje, ki uživajo v raziskovanju računalniških sistemov in iskanju novih načinov njihove rabe; ljudje, ki navdušeno (celo obsedeno) programirajo ... ljudje, ki uživajo v intelektualnih izzivih v aktivnem premagovanju in zaobhajanju omejitev*" (MIT, 2003).

Eden njihovih osrednjih idealov je svoboda: svoboda govora, svoboda raziskovanja (kar zajema tudi obratno inženirstvo), svoboda deljenja informacij ("*informacije želijo biti svobodne*") ter svoboda od oblasti. Zato so bili hekerji eni prvih razvijalcev prosto dostopnih šifrirnih programov, prostega programja, odprte kode in nasprotniki kakršnekoli oblike cenzure in državne regulacije interneta. Znano besedilo iz filma *Hackers*, s katerim se sodobni hekerji pogosto identificirajo in ga citirajo, to dobro opisuje: "*Da, sem kriminalec. Moj zločin je radovednost. Moj zločin je, da sodim ljudi po tem, kar rečejo in mislijo, ne po tem, kako so videti. Moj zločin je, da sem bolj bistroumen kot vi, česar mi ne boste nikoli oprostili. / Yes, I am a criminal. My crime is that of curiosity. My crime is that of judging people by what they say and think, not what they look like. My crime is that of outsmarting you, something that you will never forgive me for.*".

Hekerji sami vzpostavljajo razliko v primerjavi s krekerji (ang. *cracker*), to so tisti, ki hekersko znanje zlorabljajo za slabe namene, predvsem nezakonito vdiranje v računalnike s pridobitnimi nameni ter povzročanje škode. Izraz kreker se sicer uporablja tudi za posameznike, ki se ukvarjajo z omenjenim obratnim inženirstvom programske opreme, predvsem z namenom razbijanja zaščite programov prek kopiranjem. Za hekerje s slabimi nameni se včasih uporablja tudi izraz "črni hekerji" (ang. *black hat*). Za razliko od njih t. i. "beli hekerji" (ang. *white hat*) poudarjajo, da spoštujejo določena etična načela, predvsem se izogibajo namernemu povzročanju škode. Poleg njih pa se t. i. beli hekerji ograjujejo tudi od skriptarjev (ang. *script kiddie*), to je tistih, ki nimajo pretiranega računalniškega znanja in za vdore uporabljajo javno dostopna vdiralska orodja, ki so jih razvili drugi. Če so krekerji praviloma visoko motivirani in vdirajo v točno določene sisteme, pa skriptarji navadno ne iščejo točno določenih žrtev, temveč po internetu povsem naključno iščejo slabo zaščitene računalnike, v katere potem poizkušajo vdreti, njihovi motivi pa so večinoma samodokazovanje, zabava ali vandalizem.

Prav pri skriptarjih je vdor v zasebnost oziroma povzročanje varnostnih problemov pogosto le stranski učinek drugih dejavnosti, predvsem bojevanja v kibervojnah, katerih značilnost je, da potekajo na plečih nedolžnih uporabnikov. Tipičen zgled so vzpostavljanje prikritih omrežij, iz katerih potekajo napadi na internetne strežnike[286], ter vojne za kanale v omrežju IRC.[287]

---

[286] Na primer napadi na islamistične spletne strani (npr. <http://www.jihadonline.org/>), v Sloveniji pa napad na Siol in 24ur.com leta 2004.

[287] Bojevanje na plečih nedolžnih uporabnikov je sicer opaziti tudi pri krekerjih. Eden takih primerov so vojne med pisci virusov, v katerih se skušajo pisci virusov dokazovati pred nasprotno skupino (eden bolj znanih primerov je vojna med skupinama, ki sta napisali virusa *Bagle* in *Netsky.* V kodi virusa *Netsky* je bilo med drugim najdeno sporočilo, ki pravi: "*Bagle je usrane, odpre vam stranska vrata in služi veliko denarja"* (Schneier, 2004a), ali pa skušajo uničevati druge viruse (npr. *Code Green* iz septembra 2001, ki je odstranjeval *Code Red* iz julija 2001, *Welchia/Nachi,* ki se je avgusta 2003 pojavil le teden dni po virusu *Blaster* in ga je odstranjeval, virus *Anti-Santy*, ki se je decembra 2004 pojavil le deset dni po virusu *Santy* itd.).

S stališča zasebnosti sta gotovo najbolj problematični slednji dve skupini, ki svoje znanje in orodja namenoma ali nenamenoma uporabljata za vdore v zasebnost, hkrati pa celo pomagata reproducirati veljavni sistem, saj krepita disciplinske odzive države.

Po drugi strani pa so ravno hekerji v pozitivnem pomenu besede (oziroma hekerji po lastni samodefiniciji) zaslužni za razvoj številnih orodij za zaščito zasebnosti, orodij za povečevanje informacijske varnosti, pa tudi širjenje zavedanja o pomenu človekovih pravic v kiberprostoru. Prav tako ni naključje, da so pravi hekerji pogosto tudi politično angažirani, a ne v smislu dnevne politike, temveč v smislu aktivnega državljanstva in zavzemanja za državljanske pravice in svoboščine (predvsem v kiberprostoru). Zato se hekerji pogosto povezujejo tudi s klasičnimi političnimi aktivisti in jim brezplačno ponujajo tehnično podporo pri vzdrževanju informacijskih servisov ter političnem delovanju v spletu, za kar se uporablja izraz haktivizem (ang. *hacktivism*). Tako številni (beli) hekerji tvorijo jedro civilne družbe na internetu, ki je precej zaslužna za varovanje digitalnih človekovih pravic in je včasih bila tudi eden izmed pomembnih branikov zasebnosti v kiberprostoru.

Informacijska zasebnost na internetu

Kljub temu da je v 80. letih problem informacijske zasebnosti postal izrazito mednaroden in so ga začeli reševati z mednarodnimi konvencijami in poenotenjem zakonodaje, pa na internetu večinoma prevladuje pristop 'laissez faire', ki je posledica tega, da v ZDA za zasebni sektor ne veljajo praktično nikakršne omejitve pri zbiranju in obdelavi osebnih podatkov. Pravzaprav do poskusov regulacije zbiranja in uporabe osebnih podatkov prihaja šele v zadnjem času, prvi tak resnejši poskus pa je v EU leta 2002 sprejeta direktiva *Direktiva o zasebnosti in elektronskih komunikacijah* 2002/58/EC,[288] ki izhaja iz ugotovitve, da "*javno dostopne elektronske komunikacijske storitve prek interneta posameznikom odpirajo nove priložnosti, predstavljajo pa tudi nove nevarnosti za njihove osebne podatke in zasebnost.*" (6. točka).

Elektronske sledi

Leta 1983 je David Burnham v svoji knjigi *The Rise Of The Computer State* opozoril na tako imenovano *elektronsko sled*, ki jo posamezniki puščajo za sabo. Gre za transakcijske oziroma prometne podatke, ki jih nadzorni sistemi samodejno zbirajo in shranjujejo, pri čemer pa Rule ugotavlja, da spremljata razvoj nadzorovalnih sistemov dve nevarni težnji, zaradi katerih se posamezniki ne zavedajo obsega nadzorovanja toliko, kot bi se ga lahko. Posamezniki namreč s svojimi dejanji samodejno sprožajo te sisteme, hkrati pa ti sistemi podatke in informacije tudi iščejo in preverjajo iz sekundarnih virov in ne neposredno od posameznika (Lyon, 1994: 52). Ta

[288] Direktiva 2002/58/EC o obdelovanju osebnih podatkov in varstvu zasebnosti na področju elektronskih komunikacij (Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector), sprejeta 12. julija 2002. Official Journal L 201, 31/07/2002 p. 0037 - 0047.

ugotovitev velja praktično za vse elektronske informacijske in komunikacijske sisteme, predvsem pa za internet. Na internetu se namreč elektronske sledi njegovih uporabnikov zapisujejo samodejno, predvsem pa nezaznavno.

Samarajiva pravi, da je konec 80. let 20. stoletja začelo prihajati do sprememb v zaračunavanju storitev. Podjetja so namreč začela zaračunavati glede na (upo)rabo storitve in ne več zgolj za dostop do storitve (t. i. "*pay-per*" nasproti "*flat-rate*"). Posledica te plačilne sheme pa je potreba po podatkih, na podlagi katerih je mogoče izračunati porabo. Samarajiva opozarja, da se v tem primeru zbiranje podatkov ne zdi več invazivno, temveč postane samoumevno (Samarajiva, 2001: 281). Te težnje so še posebej močno vidne pri poizkusih industrije, da bi preprečila kršenje avtorskih pravic digitalnih vsebin in programske opreme. Z nastankom digitalizacije, ki avtorjem otežuje nadzor nad uporabo njihovih avtorsko zaščitenih del ter omrežij P2P (*peer-to-peer*) za izmenjavo datotek prek interneta, se je izkazalo, da pravna zaščita avtorskih pravic ni več učinkovita, temveč so veliko bolj učinkoviti tehnični ukrepi za omejevanje dostopa do uporabe avtorsko zaščitenih vsebin in nadzor nad njihovo uporabo (Bogataj, 2003: 62). Založniška industrija je zato začela razvijati številne tehnologije, s katerimi želijo preprečiti nezakonito rabo avtorsko zaščitenih digitalnih vsebin. Gre za t. i. upravljanje digitalnih pravic (ang. *Digital Rights Management* – DRM), pri čemer pa teh tehnologij ni mogoče uporabljati samo za zaščito pred nezakonitim kopiranjem, temveč tudi za uveljavitev poslovnega modela obračunavanja stroškov glede na dostop do digitalnih vsebin (ogled filma, poslušanje glasbe itd.). V tem primeru je seveda potrebna identifikacija uporabnika, posledica tega pa je, da je mogoče podatke o potrošnji posameznih medijskih vsebin povezati z identiteto posameznega potrošnika; s tem ti podatki postanejo osebni podatki. EPIC ugotavlja, da tehnologije DRM lahko preprečijo anonimno potrošnjo digitalnih vsebin, se uporabljajo za profiliranje, privedejo pa lahko tudi do cenovnega diskriminiranja uporabnikov (EPIC, 2004d).

EPIC pravzaprav opozarja na to, da je mogoče osebne podatke, ko so enkrat zbrani, analizirati in uporabiti za povsem poljubne namene, v nekaterih državah, npr. ZDA, pa jih je brez večjih zakonskih omejitev mogoče tudi prodati komurkoli. Dodatni problem potrošniškega nadzorovanja pa je tudi ta, da si posamezniki izstopa iz takega sistema nadzorovanja včasih niti ne želijo, ker jim na videz prinaša dodatne ugodnosti oziroma popuste ali pa je za izstop treba celo plačati. Večinoma pa sploh ni mogoč, saj podjetja povezujejo uporabo svojih storitev s potrošniškim nadzorovanjem; potrošniki, ki želijo ohraniti svojo zasebnost, tako sploh ne morejo stopiti v razmerje ali uporabljati storitev takega podjetja. Potrošniki in državljani tako živimo v svetu, v katerem se moramo nujno odpovedati delu svoje zasebnosti na rovaš večje funkcionalnosti in obvladovanja kompleksnosti življenja v sodobni družbi. Kot bomo videli v nadaljevanju, informacijska tehnologija oziroma internet zbiranje elektronskih sledi poenostavlja, predvsem pa tehnologija omogoča razpršeni (decentralizirani) nadzor, ki je cenejši od centraliziranega, a nič manj učinkovit, saj je ob pomoči tehnologije mogoče zbrane podatke povezovati. Poleg tega tehnologija omogoča trajno hranjenje zbranih podatkov, kar pomeni kvalitativen preskok glede na nadzor, ki se je včasih odvijal v majhnih skupnostih in med sosedi: "*Biti opazovan od sosedov, nima enakega pomena, kot biti opazovan s strani ... podatkovne mreže, ki zgreši malo in ne pozabi nič.*" (Sykes, 1999: 16).

Datoteke aktivnosti

Datoteke aktivnosti (ang. *log file*) so v informacijskih sistemih namenjene zapisovanju aktivnosti uporabnikov oziroma prometnih podatkov. Datoteke aktivnosti so uporabne za odkrivanje zlorab, pa tudi za ugotavljanje in odpravljanje napak, zato so pravzaprav nepogrešljiv del vsakega informacijskega sistema.

Med gibanjem po internetu puščajo uporabniki veliko elektronskih sledi, največ pa jih seveda lahko pustijo pri svojem ponudniku dostopa do interneta. Ta namreč lahko zapisuje *vse* dejavnosti posameznega uporabnika interneta (kdaj in katere storitve interneta je uporabljal), hkrati pa se v te datoteke aktivnosti lahko zapisujejo tudi identifikacijski podatki: npr. uporabniško ime, ki ga je mogoče povezati z uporabnikovo fizično identiteto, številka IP, ki jo je uporabnik uporabljal, in telefonska številka oziroma druga vstopna točka, prek katere se je povezal v internet. Glede na to, da gre za osebne podatke, se seveda zastavlja vprašanje, kako je z njihovim varstvom, časom hranjenja in nadaljnjo rabo. Neformalno je znano, da se podatki iz datotek aktivnosti pri nekaterih slovenskih ponudnikih dostopa do interneta hranijo zelo dolgo časa. Eden izmed zaposlenih pri slovenskem ponudniku dostopa do interneta je v klepetalnici ministrstva za informacijsko družbo 17. februarja 2004 javno priznal, da hranijo podatke od začetka njihovega obstoja, v času pogovora je bilo to že več kot 8 let[289]). Znano je tudi, da je do bilo včasih do teh podatkov mogoče priti nezakonito, in sicer zaradi hitre odzivnosti pri odpravi napak in motenj v omrežju ter preganjanja kiberkriminala in pošiljateljev nezaželenih elektronskih sporočil s strani ponudnikov dostopa do interneta. Te anomalije verjetno izvirajo iz dejstva, da so se administratorji internetnih strežnikov na začetku med seboj osebno poznali, pozneje pa se je med njimi razvila tudi cehovska pripadnost. Poleg tega gre za ljudi, ki se načeloma ne spoznajo na zakonodajo in se verjetno niti niso zavedali svojih pravnih obveznosti do drugih uporabnikov interneta. Seveda pa to niso edine datoteke aktivnosti na internetu.

Ponudniki dostopa do interneta imajo navadno v lasti tudi strežnike DNS,[290] katerih upravitelj lahko zapisuje, do katerih strežnikov je neki uporabnik želel dostop. Če ima ponudnik dostopa

---

[289] Prepis MID-ove klepetalnice '*Internet - iluzija varnosti in zasebnosti?*' z dne 17. 2. 2004 (Ministrstvo za informacijsko družbo, 2004a; besedilo je urejeno):

> [20:07] <MatejK> DarkoB: mislim, da so v GB pred par leti že nekaj takega predlagali... namreč, naj ISPji na lastne stroške hranijo loge za par let nazaj
> ...
> [20:08] <DarkoB> MatejK, no problem... Pri nas jih hranimo odkar obstajamo.. (8 let)
> ...
> [20:08] <Rumbo> DarkoB: Ali so uporabniki seznanjeni s tem, da hranite podatke v nedogled?
> ...
> [20:10] <idioterna> Pri obeh ISP-jih kjer sem zaposlen se hrani ogromno podatkov.
> [20:10] <DarkoB> Rumbo, loge hranimo izključno zaradi morebitnih reklamacij.

[290] DNS (ang. *Domain Name System*) so leta 1983 zasnovali na University of Wisconsin, gre pa za sistem, ki skrbi za pretvorbo internetnih domen v ustrezne naslove IP teh domen. Računalniki v internetu so namreč predstavljeni s številkami IP, ker pa si človeški uporabniki laže zapomnimo besede (imena domen) kot številke IP, se je uporaba DNS na internetu hitro prijela. Gre torej za nekakšen "telefonski imenik" domen in ko uporabnik interneta v npr. svoj brskalnik vpiše spletno mesto, ki ga želi obiskati, njegov računalnik najprej v strežniku DNS preveri številko IP strežnika, kateremu potem pošlje zahtevek za spletno storitev.

do interneta v lasti tudi DNS (in praviloma je tako), lahko zelo enostavno fizično identiteto uporabnikov poveže z njihovimi brskalnimi navadami in izdela – sicer razmeroma grobe, a vendarle – profile uporabnikov. Na voljo je še ena možnost zbiranja podatkov o uporabniških okusih. Ponudniki dostopa do interneta imajo lahko v lasti tudi dveri,[291] prek katerih zapisujejo, do katerih vsebin ima dostop posamezni uporabnik. *Nizozemski inšpektorat za varstvo osebnih podatkov* (ang. *Dutch Data Protection Authority*) je v poročilu iz leta 2000 ugotovil, da ponudnik dostopa do interneta, ki ima v lasti spletne dveri, lahko ugotovi, koliko reklam je njegov uporabnik videl, kako pogosto obišče elektronsko trgovino, katere izdelke je kupil, in celo, koliko je zanje plačal (Data Protection Working Party, 2000: 43). Seveda to velja samo za tiste uporabnike, ki dveri uporabljajo, dejstvo pa je, da skušajo dveri ponuditi čim več vsebine in storitev na enem mestu in so zaradi tega med uporabniki čedalje bolj priljubljene. Poleg tega ponudniki dostopa prek programov za pomoč pri nastavitvah interneta uporabnikom lahko vnaprej nastavijo svoje dveri kot domačo stran (spletno stran, ki se uporabniku začne nalagati ob zagonu brskalnika) in s tem uporabo svojih dveri še bolj razširijo. Spletne dveri slovenskega ponudnika dostopa do interneta SiOL na primer uporabnikom ponujajo vremensko napoved, dnevne novice, dostop do specializiranih dveri, ki so tudi v lasti SiOL-a (film, igre, avtomobilistika itd.), ter različne storitve: pregled mesečne porabe, branje in pisanje elektronske pošte, dostop do forumov in klepetalnic, oddajo in iskanje med malimi oglasi, dostop do spletne trgovine itd. Skratka, vse na enem mestu. S stališča tehnologije pa bi bilo precej trivialno vzpostaviti sistem, ki bi za vse uporabnike storitev spletnih dveri zapisoval njihove aktivnosti in s pomočjo teh podatkov izvajal profiliranje. Tak nadzor pa bi bil tudi povsem nezaznaven, saj uporabnik ne more ugotoviti, ali je tak sistem vključen ali ne. Še podrobnejše podatke o vedenju uporabnikov pa je mogoče odkriti ob pomoči datotek aktivnosti ponudnikov internetnih storitev in vsebin in v kombinaciji z nekaterimi drugimi tehnikami nadzora.

Elektronske sledi pri ponudniku internetnih storitev in vsebin

Praktično vsi strežniki za različne internetne storitve omogočajo zapisovanje datotek aktivnosti. Tipičen primer so spletni strežniki, ki so zaradi konvergence storitev sposobni poskrbeti za večino interakcij z uporabnikom. Datoteke aktivnosti ponudnikov spletnih storitev zapisujejo čas in vrsto storitve, ki so jo opravili (npr. katero vsebino si je uporabnik ogledal), in določene identifikacijske podatke (npr. naslov IP uporabnika). Vendar s pomočjo teh identifikacijskih podatkov načeloma ni mogoče ugotoviti prave identitete uporabnika, v nekaterih primerih pa niti ni mogoče razlikovati med različnimi računalniki, kaj šele med različnimi uporabniki.

Ker pa so podatki o obiskovalcih marketinško nadvse zanimivi, je bila kmalu razvita tehnologija, ki je te začetne ovire premagala, poleg tega so kmalu odkrili načine, kako zaobiti tehnološke omejitve.

---

[291] Dveri ali t. i. razširjene vstopne točke so spletne strani, na katerih je zbrano večje število povezav in koristnih informacij (vremenska napoved, agencijske novice ...) in so uporabnikovo izhodišče za deskanje po internetu.

Spletni strežniki lahko zapisujejo nekatere spremenljivke o uporabnikovem virtualnem okolju[292] (ang. *environment variables*), ki jih strežniku pošilja uporabnikov spletni brskalnik. Sicer je res, da uporabniki nekaterih spletnih brskalnikov nekatere od teh podatkov lahko spremenijo ali preprečijo, da se pošiljajo v strežnik, vendar pri najbolj razširjenem spletnem brskalniku *Microsoft Internet Explorer* to ni mogoče na enostaven način. Poleg tega večina uporabnikov s temi postopki ni seznanjena niti se ne zaveda, da se ti podatki sploh posredujejo v spletni strežnik. Nekateri spletni brskalniki so celo v osnovi zasnovani tako, da strežnikom pošiljajo veliko podatkov, v zvezi s tem se celo uporablja izraz klepetavost brskalnikov (ang. *browser's chattering)*. Tipičen primer klepetavega brskalnika je že omenjeni najbolj razširjeni *Microsoft Internet Explorer*. V poročilu z naslovom *Privacy on the Internet – An integrated EU Approach to On-line Data Protection* je bilo s primerjalno analizo različnih spletnih brskalnikov ugotovljeno, da *Internet Explorer* razkrije celo, ali ima uporabnik v svojem računalniku nameščene programske pakete Word, Excel in PowerPoint (Data Protection Working Party, 2000: 14–15).

Dodatne možnosti odpira uporaba skriptnih ukazov oziroma spletnih aplikacij, ki so vključene v spletno stran. Tipični primeri so kontrolniki ActiveX[293], Java[294] in JavaScript.[295] Na spletno stran je mogoče vključiti poseben program, ki sicer deluje le takrat, kadar uporabnik v spletnem brskalniku nima onemogočenega izvajanja programskih ukazov v skriptnem jeziku. Ker pa je privzeta nastavitev navadno taka, da je izvajanje skriptnih jezikov vključeno (omejitve v zvezi s kontrolniki ActiveX pa je Microsoft uvedel šele po številnih zlorabah s strani virusov), poleg tega je izklop povezan z manjšo funkcionalnostjo spleta za uporabnika, imajo uporabniki to tehnologijo večinoma vključeno. Zato upravitelj spletne strani z nekaj preprostimi programskimi ukazi lahko ugotovi še nekaj dodatnih podatkov o uporabnikovem okolju. S pomočjo JavaScripta je tako mogoče ugotoviti npr. ločljivost zaslona, katere priključne module (ang. *plug-in*) za prikaz večpredstavnih vsebin ima uporabnik nameščene, oceno hitrosti dostopa do interneta itd. Te podatke ponudniki vsebin večinoma uporabljajo za spremljanje obiskanosti spletnih strani in večpredstavnih vsebin, z njihovo pomočjo pa strežnik lahko ugotovi stopnjo večpredstavne opremljenosti uporabnikovega računalnika in glede na te podatke pošlje uporabniku spletno vsebino v ustreznem formatu (npr. ali lahko pošlje animacijo *flash* ali pa raje film v formatu AVI itd.).

Zaradi konvergence tehnologij čedalje več storitev opravljamo s pomočjo informacijskih sistemov oziroma za dostop do storitev uporabljamo internet, pri tem pa se čedalje manj zavedamo, da pravzaprav uporabljamo internetne storitve, saj se v internet povezujejo tudi druge 'neračunalniške' naprave. Značilen zgled teh teženj sta internetna televizija in internetna

---

[292] Upravitelji spletnih strani lahko zaznajo npr. tip uporabnikovega spletnega brskalnika, operacijski sistem, ki teče v njegovem računalniku, vrsto vključenih jezikovnih podpor, s katere spletne strani je uporabnik prišel do njihove spletne strani itd.

[293] *ActiveX kontrolniki* so programski gradniki, ki jih je mogoče integrirati v spletno stran. Tehnologijo je razvilo podjetje Microsoft sredi 90. let 20. stoletja in je vključena v njihov spletni brskalnik Internet Explorer.

[294] *Java* je predmetni programski jezik, ki ga je razvilo podjetje Sun Microsystems, zaradi svoje razširjenosti pa je primeren za izvajanje spletnih aplikacij.

[295] *JavaScript* je skriptni programski jezik, ki ga je razvilo podjetje Netscape, namenjen pa je uporabi na spletnih straneh.

telefonija (VoIP), za uporabo katerih že ne potrebujemo več računalnika. Poleg tega prek interneta uporabljamo čedalje več storitev in vsebin (npr. branje časopisov, poslušanje internetnega radia itd.) in ponudniki teh storitev imajo možnost natančnega zapisovanja uporabe le-teh.[296]

Piškotki

Podatki iz datotek aktivnosti se najpogosteje uporabljajo za ugotavljanje števila *obiskov* na posamezni spletni strani. Ti podatki so posebej pomembni za spletne strani, ki oglašujejo, saj je cena oglasov in zaslužek od oglaševanja navadno povezan s številom obiskovalcev. Podatki o obiskih spletnih strani pa so pomembni tudi za spletne trgovine in ponudnike spletnih storitev, še posebej, kadar je mogoča identifikacija posameznega obiskovalca. S temi podatki namreč ni mogoče zgolj izvedeti, katere proizvode ali storitve je neki posamezni uporabnik kupil, temveč tudi to, katere si je ogledal, iz tega pa je mogoče ugotoviti njegove potrošniške preference. Spletna trgovina Amazon je bila eno prvih podjetij, ki so začela uporabljati oglaševanje proizvodov glede na profil uporabnika, ki ga izdelajo na podlagi njegovih potrošniških preferenc.

Problem (s stališča marketinga) pa je, ker je mogoče s tehnologijo datotek aktivnosti ugotoviti le število dostopov do posamezne spletne strani, ne pa tudi vedno števila *različnih* obiskovalcev. To je za marketing posebej pereče pri uporabnikih, ki prihajajo prek klicnega dostopa (oziroma preko dinamičnih naslovov IP), prehoda (ang. *gateway*) ali anonimnega zastopniškega programa (ang. *anonymous proxy*) oziroma prek anonimizacijskih omrežij, saj posamezni obiskovalec lahko pride večkrat prek različnih naslovov IP ali pa prek enega naslova IP pride več različnih uporabnikov. Poleg tega je načeloma mogoče identificirati samo računalnike, ne pa tudi uporabnikov, ki si morda delijo uporabo istega računalnika. Industrija se je problema zavedla že kmalu po razvoju prvega grafičnega spletnega brskalnika *Mosaic for X* leta 1993. Leta 1994 je namreč Lou Montulli za podjetje *Netscape* že razvil tehnologijo piškotkov (ang. *cookies*).

Piškotki so majhni paketi podatkov, ki jih spletni strežnik pošlje spletnemu brskalniku, ta pa jih shrani v uporabnikov računalnik in jih vrne strežniku, ko ta to zahteva od njega. Strežnik lahko nastavi čas veljavnosti piškotka in določi, kateri del spletnega strežnika ima lahko dostop do njega. Po času trajanja ločimo t. i. sejne piškotke (ang. *session cookies*) in trajne piškotke (ang. *persistent cookies*). Prvi potečejo ob koncu brskalne seje, torej ko uporabnik zapre spletni brskalnik, drugi pa imajo čas trajanja daljši, lahko tudi več let. Piškotek je strežniku dostopen ves čas trajanja, če ga seveda uporabnik prej ne izbriše. Poleg tega ločimo piškotke obiskane spletne strani (ang. *first-party cookies*) in piškotke, ki jih pošiljajo tretje spletne strani, ki so vključene v obiskano spletno stran (ang. *third-party cookies*). Razlikovati so jih začeli šele pred nekaj leti, pomembno pa je, da piškotke tretjih spletnih strani večinoma uporabljajo oglaševalska omrežja, namenjeni pa so sledenju uporabnikov (Data Protection Working Party 2000, 52).

---

[296] Tipična razlika med navadno, kabelsko televizijo in internetno televizijo je v tem, da pri kabelski televiziji operater ne more natanko vedeti, kateri program gledamo v danem trenutku (ve le to, katere dodatne programe smo naročili), pri internetni televiziji pa ponudnik storitve natančno ve, na katero številko IP se v danem trenutku pošilja televizijska slika, poleg tega pa seveda lahko ve tudi za identiteto lastnika te številke IP.

Piškotek ima navadno interno identifikacijsko številko uporabnika in ko se uporabnik giblje po spletnem mestu, lahko spletni strežnik te identifikacijske številke zapisuje. Piškotki so bili prvotno razviti z namenom, da bi omogočili spletne nakupne košarice, danes pa jih množično uporabljajo na vseh vrstah spletnih strani. Tako lahko spletni strežnik pri drugem obisku uporabnika ugotovi, ali je uporabnik že bil na spletni strani in kaj je na njej počel. Seveda pa je mogoče to identifikacijsko številko povezati tudi z drugimi podatki, na primer z identifikacijskimi podatki posameznika. Na piškotke zato lahko gledamo kot na razpršeno zbirko podatkov, saj so podatki o obiskovalcih razpršeni po računalnikih obiskovalcev spletne strani.

Vendar pa so bili piškotki v osnovi zasnovani tako, da lahko potujejo samo znotraj ene domene, med domenami pa si jih ni mogoče izmenjevati. To pomeni, da je mogoče sledenje uporabnikom samo znotraj posamezne domene oziroma spletne strani, ni pa mogoče slediti njihovemu gibanju med spletnimi stranmi na različnih domenah. A ta 'problem' je bil zaradi potreb oglaševalcev kmalu rešen. Že leta 1996 je nastala rešitev za opazovanje in profiliranje uporabnikov interneta *SelectCast*, sistem pa je bil razvit s strani podjetja *HNC Software*, pri čemer je vidno pronicanje vojaške in obveščevalne tehnologije v zasebni sektor (marketing). Gre namreč za podjetje, ki je za ameriško vojsko in tajne službe razvijalo sisteme AI (Sykes, 1999: 68–69). *SelectCast* konec 90. let 20. stoletja ni pritegnil večje pozornosti javnosti, razlogi za to pa so verjetno premajhna razširjenost interneta ter nerazvitost oglaševanja na internetu. Poleg tega so ravno v tistem času potekale razprave o omejevanju kriptografije in uvedbi čipa Clipper, zato je bila pozornost javnosti preusmerjena k drugim problemom zasebnosti. A ne za dolgo. V začetku leta 2000 se je izkazalo, da oglaševalsko podjetje *DoubleClick* piškotke uporablja na način, s katerim je obšlo prej opisane omejitve.

Ker je neposredno trženje oglasnega prostora na internetu nepraktično, so se kmalu našla podjetja, ki so od množice lastnikov manjših spletnih strani kupovala oglasni prostor in ga nato prodajala naprej oglaševalcem. Eno takih podjetij je tudi *DoubleClick*. V njem so ugotovili, da je s trenutno tehnologijo za vsak prikazani oglas mogoče določiti, na kateri spletni strani je bil prikazan, ta podatek pa je mogoče povezati z identifikacijsko številko piškotka, ki ga po celotnem oglaševalskem omrežju pošilja njihov strežnik.[297] Namesto oglasa je lahko uporabljena tudi majhna slika, navadno velikosti ene pike (1x1 piksel), torej je praktično nevidna. Za ta postopek se uporablja tudi izraz sledenje s *tehnologijo slikovnih pik* (*pixel* je slikovna pika na zaslonu), take slike pa se imenujejo tudi *spletni hrošči* (ang. *web bugs*). Ta postopek upravljavcu oglasnega omrežja omogoča, da ugotovi, po katerih spletnih straneh v celotnem oglaševalskem omrežju se giblje posamezni uporabnik. Enaka tehnika se uporablja tudi za merjenje obiskanosti spletnih strani, kar upravljavcu omrežja omogoča izdelavo profilov uporabnikov. S tem so v *DoubleClicku* zaobšli prvotno zamišljeno omejitev dostopnosti do piškotka zgolj za spletne strani znotraj domene. In če je omrežje dovolj veliko, je mogoče na podlagi zbranih podatkov dokaj natančno ugotoviti brskalne navade posameznega uporabnika.

[297] Na spletnih straneh podjetja DoubleClick je bilo 25. oktobra 2002 objavljeno sporočilo za javnost, v katerem je objavljen podatek, da so maja 2001 prikazali 55 milijard oglasov (Doubleclick, 2002).

Vendar pa je s takimi podatki mogoče razlikovati le med različnimi uporabniki (pravzaprav računalniki oziroma uporabniškimi imeni znotraj njih), dejanskih fizičnih uporabnikov pa ni mogoče identificirati. Zato so nekatera podjetja začela razvijati tehnologijo, s katero je te podatke mogoče povezati z elektronskim naslovom posameznika in celo s t. i. *odklopno (off-line)* identiteto.

Povezovanje brskalnih navad z elektronskim naslovom posameznika poteka tako, da podjetje razpošlje množico elektronskih sporočil s poosebljenimi povezavami, prejemniki elektronskih sporočil pa so vabljeni, naj kliknejo povezavo. Poosebljena povezava pomeni, da je na vsak elektronski naslov poslana drugačna povezava, taka, ki za vsakega prejemnika vsebuje enolično identifikacijsko oznako. Pošiljatelj torej natančno ve, na katere elektronske naslove je poslal katero povezavo. Ko uporabnik klikne poosebljeno povezavo, prejemnik ta klik zazna in s tem ugotovi, da je elektronski naslov aktiven (da ga nekdo bere), ob pomoči piškotka, ki ga pošlje prek spletne strani, pa elektronski naslov poveže z identifikacijsko številko piškotka, prek nje pa še z uporabnikovimi brskalnimi navadami.

Mogoče pa je razposlati tudi tako prirejena elektronska sporočila, ki ne zahtevajo klika na povezavo, temveč je dovolj, da jih uporabnik samo prebere. V tem primeru morajo biti sporočila oblikovana v formatu HTML, vsebujejo pa spletnega hrošča (ang. *web bug*), prek katerega uporabnik ob ogledu sporočila prejme tudi piškotek. Seveda tako deluje le, če so izpolnjeni določeni pogoji: v trenutku branja sporočila mora biti uporabnik povezan v internet, oziroma mora imeti stalno povezavo v internet, program za branje elektronske pošte mora podpirati prikaz HTML oblikovanih sporočil, uporabnik mora imeti omogočeno sprejemanje piškotkov in ne sme blokirati zahtevkov HTTP iz poštnega odjemalca. Vendar je v povezavi z drugimi načini nadzora lahko nadvse učinkovit. Poleg tega je včasih veljalo (večinoma pa to velja tudi sedaj), da so pri večini uporabnikov interneta ti pogoji navadno vedno izpolnjeni, saj je dovolj, da je uporabnik uporabljal privzete nastavitve poštnega odjemalca. Tehnologije za onemogočanje takšnega nadzora se namreč vgrajujejo v poštne odjemalce šele v zanjem času.

Fizično, *odklopno (off-line)* identiteto uporabnika pa je mogoče ugotoviti tako, da uporabnik svoje identifikacijske podatke posreduje katerikoli spletni strani v omrežju, ti podatki pa se potem povežejo z identifikacijsko številko piškotka. Uporabniki svoje osebne podatke navadno vpisujejo v kakšnih spletnih trgovinah, lahko tudi pri naročanju različnega brezplačnega gradiva ali pri sodelovanju v nagradnih igrah, ki potekajo prek spletnih strani. Dokument *Privacy on the Internet An integrated Approach to On-line Data Protection* tako navaja, da spletne strani pogosto uporabljajo t. i. programe zvestobe, npr. igre, anketne vprašalnike in spletne biltene, s katerimi pridobivajo osebne podatke o svojih obiskovalcih (Data Protection Working Party, 2000: 18). Tako profiliranje je do posameznika na videz prijazno, saj potrošnika potiska, kamor si sam želi, oziroma ga zalaga z dobrinami in vsebinami, ki ustrezajo njegovemu okusu in potrebam. (Značilen zgled so reklame, prilagojene zaznanemu okusu in predvidenim potrebam potrošnika.)

Ko je ustrezna tehnologija enkrat razvita, je tako zbiranje podatkov mogoče z minimalnimi stroški in povsem neopazno. Da pa se to dogaja v velikem obsegu, se je pokazalo v začetku

leta 2000, ko je časnik USA Today razkril, da je podjetje *DoubleClick* po tej poti spremljalo brskalne navade obiskovalcev interneta (na podlagi tega so izdelovali uporabniške profile in prikazovali poosebljene oglase), piškotke pa so skušali povezati tudi z imeni uporabnikov in z njihovo identiteto v resničnem življenju (Schneier, 2000).[298] *Data Protection Working Party* je v svojem poročilu iz leta 2000 zapisala, da se je *DoubleClick* povezal s podjetjem Abacus Alliance, ki je v ZDA vodilno podjetje za zbiranje podatkov o potrošnikih; novembra 1999 sta podjetji začeli združevati podatke o potrošnikih iz obeh svojih zbirk (Data Protection Working Party, 2000: 45).

Naivno bi bilo pričakovati, da velika internetna podjetja teh podatkov ne bodo zbirala in uporabljala pri svojem poslovanju. V začetku avgusta 2006 je tako ameriški ponudnik dostopa do interneta AOL na posebni spletni strani objavil iskalne nize (iskalne pojme, ki jih uporabniki vpisujejo v iskalnike) več kot 650.000 svojih uporabnikov interneta, ki so jih ti vpisovali v spletne iskalnike od marca do maja 2006.[299] Šlo je za več kot 20 milijonov vpisov (ali 1 % AOL-ovih podatkov za to obdobje), ki so bili sicer anonimizirani, a očitno ne dovolj, da spletni raziskovalci ne bi kmalu začeli odkrivati prave identitete posameznih uporabnikov (Schneier, 2006d). Med drugim so odkrili tudi uporabnika, katerega iskalni nizi so kazali na to, da načrtuje umor svoje žene (Frind, 2006). AOL je zbirko podatkov zaradi številnih protestov pozneje sicer umaknil (Kawamoto in Mills, 2006), a je dogodek pokazal na to, kakšen je dejanski obseg zbiranja osebnih podatkov in kako hitro so ti podatki lahko zlorabljeni.

Zaradi strahu pred zbiranjem osebnih podatkov nekateri uporabniki interneta onemogočajo uporabo piškotkov[300] in JavaScripta, kljub temu da to lahko povzroči zmanjšano funkcionalnost spleta.[301] Uporabniki, ki želijo blokirati t. i. zlonamerne skripte lahko uporabijo tudi program Privoxy, ki skuša med brskanjem po spletu zaznati in odstraniti vse skrite identifikatorje, piškotke, oglase itd. A tudi če uporabnik privoli v zmanjšano funkcionalnost spleta, to še ne pomeni, da bo v zameno zares dobil večjo zasebnost. Marca leta 2005 ameriško podjetje *United Virtualities* začelo tržiti tehnologijo, imenovano PIE (ang. *persistent identification element*, trajni identifikator). Gre za tehnologijo, ki omogoča identificiranje uporabnikov interneta na podoben način, kot ga omogočajo piškotki, vendar ta t. i. trajni identifikator deluje tudi, kadar uporabnik

---

[298] Kljub vsemu kaže, da se pri zbiranju teh podatkov oblikujejo neki standardi zaščite zasebnosti. DoubleClick je konec avgusta 2002 napovedal, da bo uporabnikom omogočil vpogled v nekatere podatke, zbrane s piškotki. Uporabniki naj bi s t. i. pregledovalnikom piškotkov (ang. *cookie viewer*) lahko pogledali, v katero kategorijo jih je uvrstil DoubleClick (Glasner, 2002).

[299] Šlo je za spletno stran <http://research.aol.com>. Spletna stran ni več dostopna, podatke z nje pa je še vedno moč najti v omrežjih P2P.

[300] Sledenje uporabnikom je mogoče tudi v kombinaciji s spletnimi piškotki in/ali s pomočjo brskalnikovega medpomnilnika. Če ima namreč uporabnik omogočeno izvajanje JavaScripta, je mogoče v medpomnilnik spletnega brskalnika vriniti posebno JavaScript kodo, ki vsebuje identifikacijo. V primeru, da uporabnik medpomnilnika po zaključeni brskalni seji ne izbriše, ga spletna stran ob naslednjem obisku kljub izbrisanim spletnim piškotkom uspešno identificira (Sivaraman, 2006).

[301] Nekoliko več možnosti ponuja selektivno onemogočanje piškotkov. Program *Bugnosis* (njegov razvoj je opuščen) je namenjen odkrivanju in prikazu spletnih hroščev, ki pošiljajo piškotke, nekateri spletni brskalniki, na primer *Mozilla* ali *Firefox*, pa omogočajo selektivno blokiranje in uničevanje piškotkov.

onemogoča piškotke. Tehnologija temelji na gradnikih (ang. *local shared objects*) predvajalnika Flash, ki je nameščen v večini računalnikov z dostopom do interneta, njenih nadzorovalnih zmožnosti pa zaenkrat ni mogoče onemogočiti na enostaven način (Gonsalves, 2005). Pa tudi uporabniki, ki predvajalnika Flash nimajo nameščenega, se temu nadzoru ne morejo popolnoma izogniti. Felten in Schneider s princetonske univerze sta na konferenci o računalniški in komunikacijski varnosti združenja *Association for Computing Machinery* novembra 2000 v Atenah opisala tehniko za ugotavljanje brskalnih navad uporabnikov z izrabo nekaterih lastnosti spletnega medpomnilnika (ang. *browser's cache*, *web caching*). Poimenovala sta jo časovni napad (ang. *timing attack*). Z njo pa je mogoče odkriti nekaj uporabnikovih brskalnih navad tudi, kadar ima uporabnik blokirano uporabo piškotkov, izključeno izvajanje Jave in JavaScripta in celo če uporablja sisteme za anonimizacijo (Felten in Schneider, 2000 ter Science Daily, 2000). Z njuno tehniko sicer ni mogoče odkriti fizične identitete uporabnikov, kljub vsemu pa njuno odkritje kaže na to, da je na internetu mogoče zbirati nekatere podatke o uporabnikih celo, če uporabniki uporabljajo drastične zaščitne ukrepe.

Primer 'Google Toolbar'

Google Toolbar je programski dodatek k spletnemu brskalniku, ki ga je razvilo podjetje Google, ki trenutno upravlja največji spletni iskalnik na svetu. Uporabniku omogoči uporabo Googlovih storitev neposredno iz brskalnika, ne da bi mu bilo treba iti na Googlovo spletno stran. Vendar pa *Google Toolbar* omogoča tudi spremljanje uporabnikovih spletnih dejavnosti, ki se posredujejo v nadaljnjo analizo Googlu. Iskalniki lahko na podlagi teh podatkov in podatkov o uporabljenih iskanih pojmih izvajajo profiliranje uporabnikov (Data Protection Working Party, 2000: 44) in s tem izboljšujejo svoje storitve, zato so seveda zelo zainteresirani za njihovo zbiranje. Ob namestitvi Googlove orodne vrstice je uporabnik sicer jasno seznanjen s tem, kateri podatki se zbirajo in za kakšen namen, in da so anonimizirani. Prenašanje teh podatkov lahko tudi izključi, vendar je privzeta nastavitev taka, da je zbiranje in prenašanje teh podatkov vključeno. Na poštnem seznamu PGP-USERS je bilo 28. aprila 2004 objavljeno elektronsko pismo, v katerem je neki uporabnik opozoril na eno izmed možnih nevarnosti takega zbiranja podatkov. Opisal je izkušnjo svojega znanca, ki si je namestil Googlovo orodno vrstico in dovolil zbiranje in posredovanje podatkov, med drugim tudi zato, ker Google zagotavlja, da se podatki pred posredovanjem anonimizirajo. Potem pa mu je nekdo želel po elektronski pošti poslati datoteko. Ker je uporabnik zaradi tehničnih težav ni mogel sprejeti, mu je pošiljatelj ponudil, naj datoteko postavi na 'zasebno' spletno stran, torej na spletno mesto, ki ni vpisano v noben iskalnik in na katero ne kaže nobena povezava. Povezavo do datoteke mu je poslal po elektronski pošti in prejemnik je datoteko prenesel k sebi prek spletnega brskalnika. Datoteka, v kateri so bile zelo občutljive osebne informacije pošiljatelja, pa se je v kratkem znašla na Googlu, saj je Googlova orodna vrstica, nameščena *pri prejemniku*, ugotovila, da je uporabnik obiskal spletno mesto, ki ga Google še nima na svojem seznamu, in povezavo do njega posredovala Googlovemu iskalniku. Kljub temu da je pošiljatelj datoteko pozneje odstranil, je še vedno ostala v Googlovem medpomnilniku (ang. *cache*) in je bila še nekaj časa dostopna (Teranson, 2004).

Dogodek kaže na enega bistvenih problemov zasebnosti, ko je v proces izmenjave osebnih podatkov ali informacij vključenih več oseb, pri čemer ena oseba prostovoljno in zavestno dovoli izvajanje nadzora nad njo, ostale pa s tem niso seznanjene, so pa nadzoru ravno tako posredno izpostavljene. Gre skratka za vprašanje pravic tretjih oseb, ki se sicer pojavlja tudi pri nadzoru komunikacij med dvema ali več osebami (npr. pri nadzoru službene elektronske pošte).

Preprodaja osebnih podatkov, oddaja zunanjim izvajalcem in primer Toysmart

Na številnih spletnih straneh je izjava o zasebnosti (ang. *privacy statement*), v kateri lastnik spletne strani pove, kakšni osebni podatki se zbirajo, kakšen je namen zbiranja in za kaj bodo uporabljeni zbrani osebni podatki. (Izjavo o zasebnosti so začeli najprej uvajati na ameriških spletnih straneh, saj ameriški model varstva informacijske zasebnosti predvideva t. i. samoregulacijo, pozneje pa se je njena raba razširila še drugod po svetu.) Vendar izjava sama po sebi ne zagotavlja, da bo informacijska zasebnost obiskovalca spletne strani res varovana. Gre zgolj za obvestilo o tem, kaj se zbira in za kakšne namene. To pomeni, da je v njih lahko preprosto zapisano, da bodo zbrani podatki uporabljeni za katerekoli potrebe in namene. Kljub temu večje ameriške spletne strani že spreminjajo svojo politiko zasebnosti in sprejemajo evropske standarde informacijske zasebnosti, saj jih k temu sili sporazum med ZDA in EU *Safe Harbor Agreement* oziroma želja po poslovanju z Evropo. Verjetno jim bodo sledile tudi manjše spletne strani oziroma vsaj tiste, ki želijo doseči mednarodno publiko.

Kljub temu je še vedno precej držav, v katerih nimajo urejene tovrstne zakonodaje ali pa se zakonodaja ne izvaja, povprečni uporabnik interneta pa navadno ne more ugotoviti, v kateri državi je spletna stran ali deli spletne strani, ki jo pregleduje. Značilen zgled take države je Rusija, v kateri po podatkih iz poročila Privacy & Human Rights 2003 cveti črni trg z osebnimi podatki. Poročilo navaja, da je za ceno do 1500 ameriških dolarjev mogoče kupiti celo podatke o davčnih zavezancih, kaznivih dejanjih itd. V začetku leta 2003 je nekdo vdrl v zbirko podjetja Mobile Telesystems in ukradel zbirko podatkov o več milijonih njihovih strank (Laurant, 2003: 418). Ob takem stanju informacijske zasebnosti se zdi trgovanje z zakonito pridobljenimi podatki na internetu skoraj zanemarljiv problem.

Črni trg z osebnimi podatki namreč sproža predvsem vprašanje zavarovanja dostopa do osebnih podatkov in nadzora nad njim. Poleg številnih možnosti vdorov v računalniške sisteme, o čemer več v nadaljevanju, je pomembno tudi, kdo ima dostop do osebnih podatkov, zbranih prek interneta. Problem je t. i. oddaja del zunanjim izvajalcem *(outsourcing)*. Navadno gre za specializirana podjetja ali analitike, ki za zunanje naročnike izvajajo analize spletne obiskanosti (Data Protection Working Party, 2000: 43). Pri tem je v nevarnosti prenos podatkov po internetu (če podatki med prenosom niso ustrezno zavarovani), postavlja pa se tudi vprašanje zaupanja zunanjim izvajalcem, da podatkov ne bodo zlorabili ali da jim ti ne bodo ukradeni. Sporazum *Safe Harbor* sicer predvideva izvajanje nadzora nad zunanjimi izvajalci, a kot je bilo že omenjeno, gre pri sporazumu za t. i. samocertificiranje s strani podjetij, "*status safe harbor*" pa ni nadzorovan s strani zunanje entitete.

Grozi pa še drugačna nevarnost, da se zbrani podatki ne uporabijo za tisto, za kar so bili zbrani, temveč za druge namene. Podjetje Toysmart.com je bilo ena večjih spletnih prodajaln otroških igrač, na svoji spletni strani pa je zbiralo številne osebne podatke o obiskovalcih (poleg nakupovalnih navad in osebnih podatkov, potrebnih za dostavo in izvedbo plačila, celo rojstne dneve in imena otrok). V svoji izjavi o zasebnosti iz septembra 1999 je zapisalo, da zbranih osebnih podatkov ne bo nikoli posredovalo nikomur. Toda podjetje je zašlo v finančne težave in se maja 2000 znašlo v stečaju. Odločili so se, da svoje premoženje prodajo, v stečajno maso pa so vključili tudi zbrane osebne podatke. 10 julija 2000 je zato ameriška *Federal Trade Comission* sodno zahtevala prepoved prodaje te zbirke (Federal Trade Comission, 2000a), 21. julija pa je sprožila tudi postopek zaradi kršitve[302] *Children's Online Privacy Protection Act of 1998*.[303] Ta od upraviteljev spletnih strani, ki zbirajo osebne podatke od otrok, mlajših od 13 let, zahteva, da za tako zbiranje pridobijo soglasje staršev (Federal Trade Comission, 2000b). Napaka podjetja Toysmart je bila, da je želelo zbirko osebnih podatkov prodati ločeno od preostalega premoženja, FTC pa je menilo, da je prodaja te zbirke osebnih podatkov mogoča samo skupaj s prodajo celotnega podjetja, pa še to ne najboljšemu ponudniku, temveč ponudniku, ki bo najbolj 'kvalificiran'; to pomeni, da mora zagotoviti, da bo nadaljeval dejavnost propadlega podjetja. Poleg tega je FTC opozorila še na en pomemben vidik: če bi se novi lastnik odločil spremeniti izjavo o zasebnosti, nova, spremenjena izjava za stare uporabnike ne velja, razen če se izrecno ne strinjajo z njo (Federal Trade Comission, 2000b).

Javno dostopni podatki in imeniki elektronske pošte

Številni podatki se na internetu zapisujejo samodejno, mnoge pa posamezniki iz takih ali drugačnih razlogov sami posredujejo v zbirke ali objavijo na javno dostopnih spletnih straneh. Ti podatki so razpršeni, vendar računalniška omrežja omogočajo decentraliziran nadzor, saj lahko omogočijo povezovanje formalno ločenih nadzornih sistemov in informacij prek telekomunikacijskih sredstev. Prav tako pomembna lastnost računalnikov je tudi njihova zmožnost shranjevanja oziroma arhiviranja podatkov. To omogoča gradnjo arhivov oziroma dosjejev, po katerih je s sodobno informacijsko tehnologijo prav tako mogoče iskati.

Zbirke podatkov je mogoče povezovati ob pomoči tehnik računalniškega ujemanja in povezovanja zapisov (ang. *computer matching and record linkage*). Lahko pa so zbirke podatkov že v izhodišču zasnovane kot relacijske, kar omogoča povezovanje med njimi. Te tehnike so prvi uporabili vladni oddelki v ZDA konec 70. let, njihova uporaba pa se je razširila v 90. letih (Lyon, 1994: 9).

Danes so zbirke podatkov eno poglavitnih orodij množičnega nadzora, saj so lahko zelo kompaktne in jih je po začetnem vložku tudi poceni vzdrževati, zato so še posebno privlačne. Clarke zato govori o podatkovnem nadzoru (ang. *dataveillance*), ki je veliko cenejši in učinkovitejši od centraliziranega nadzora (Clarke, 1988). Omrežnost (ang. *networking*) in razpršenost sta namreč veliko bolj gospodarni, seveda pa je pogoj za uspešen podatkovni nadzor povezanost različnih podatkovnih sistemov prek

[302] Šlo je za prvi sodni postopek zaradi kršitve tega zakona.
[303] Children's Online Privacy Protection Act of 1998, 15 U.S.C. (1998).

univerzalne identifikacijske sheme, po možnosti s pomočjo telekomunikacijskih omrežij (Lyon, 1994: 48). Internet je za tak nadzor prav idealno okolje. Značilen zgled podatkovnega nadzora pa je povezovanje elektronskih sledi, ki jih uporabniki puščajo na spletnih straneh v oglaševalskem omrežju.

Posebno privlačno je zbiranje javno dostopnih in prostovoljno posredovanih osebnih podatkov. Posamezniki sodelujejo na dopisnih seznamih, katerih arhivi so lahko javno dostopni, na spletnih forumih, novičarskih skupinah, vzdržujejo svojo spletno stran ali spletni dnevnik (t. i. *blog*), izpolnjujejo vprašalnike, male oglase ali zasebne stike, uporabljajo spletne koledarje, voščilnice ali adresarje ali pa preizkušajo preizkusne zbirke podatkov. Vir osebnih podatkov je lahko tudi kak dokument, ki se znajde v javno dostopnem arhivu.[304] Pri tem se posamezniki pogosto ne zavedajo, da so podatki javno dostopni, poleg tega lahko podatki postanejo javno dostopni tudi po pomoti. Znan je recimo primer, ko je zaradi napačne konfiguracije programa za vzdrževanje poštnega seznama celoten poštni arhiv enega izmed poštnih seznamov ameriške National Security Agency leta 2004 postal javno dostopen. To so izkoristili aktivisti avstrijske organizacije za varstvo zasebnosti *quintessenz* in si vsa sporočila v njem arhivirali (quintessenz, 2005). Zaradi podobnih napak lahko postanejo javno dostopne tudi različne datoteke aktivnosti, povezave do nazornih kamer, tiskalnikov in drugih delov virtualnega prostora, ki jih lastniki načeloma ne želijo javno dostopnih.[305]

Zbiranje in klasifikacija na spletnih straneh objavljenih osebnih podatkov že dolgo časa ne pomeni večjega tehničnega problema. Poleg tega je tako zbiranje podatkov tudi sorazmerno poceni. Te programe za zbiranje javno dostopnih podatkov uporabljajo iskalniki, zanje pa se uporabljajo izrazi robot, pajek, črv ali tudi žanjec (ang. *spider, worm, [ro]bot*, *harvester*). Programi iščejo po vseh javno dostopnih spletnih mestih. Upravitelji, ki želijo tako zbiranje preprečiti, sicer lahko določijo področje spletnega strežnika, na katerem je vstop robotom prepovedan,[306] vendar ni nujno, da se roboti teh navodil držijo.[307] Včasih imajo poskusi takih omejitev ravno nasproten učinek in za robote 'prepovedani' deli spletnih strežnikov pritegnejo še večjo pozornost.[308]

---

[304] Nevarnost zlorabe lahko predstavlja tudi praksa nekaterih organizacij, da na internetu objavljajo različna poročila ali evalvacijske študije z osebnimi podatki. Takih primerov je veliko. Kot primer lahko navedem Center nevladnih organizacij Slovenije, ki je na internetu (<http://www.cnvos.si/grafi/Zemljevid/Forum%202.doc>) objavil poročilo ter seznam udeležencev 2. foruma nevladnih organizacij iz leta 2003. V dokumentu je navedenih 64 predstavnikov nevladnih organizacij, ob njih pa njihovi osebni elektronski naslovi in številke zasebnih mobilnih telefonov. Objavljeni so bili podatki nekaterih precej izpostavljenih javnih osebnosti.

[305] To je problematično predvsem zato, ker sodobni iskalniki take datoteke hitro najdejo. Nekateri se načrtno ukvarjajo z uporabo iskalnikov za iskanje takih datotek. Več primerov si je mogoče ogledati na spletni strani <http://johnny.ihackstuff.com/index.php> oziroma v knjigi *Google Hacking for Penetration Testers* Johnnyja Longa.

[306] Gre za t. i. *robot exclusion protocol*, seznam za robote prepovedanih spletnih strani. Shrani se ga v datoteko robots.txt v spletnem strežniku.

[307] Robot se obnaša kot povsem navaden spletni brskalnik, mogoče pa ga je prepoznati po vrednosti posebne okoljske spremenljivke, ki vsebuje podpis spletnega brskalnika (USER_AGENT). Vendar pa ni nobenih tehničnih ovir, da se robot ne bi izdajal za povsem navaden spletni brskalnik.

[308] Konec leta 2003 je začela po internetu krožiti informacija, da datoteka robots.txt spletnega strežnika ameriške Bele hiše vsebuje nenavadno veliko spletnih mest, ki imajo v naslovu besedo 'Iraq'. Analiza z začetka novembra 2003 je pokazala, da je bilo na seznamu prepovedanih spletnih mest večina (46,5 %) takih, ki so imela v naslovu besedo 'Iraq'. Od teh spletnih mest je bilo dejansko odstranjenih 99,9 , drugih s seznama pa 36,4 %. Poleg tega na seznamu niso bila vsa spletna mesta z besedo 'Iraq', temveč je bila med njimi opravljena predhodna selekcija.

Pogosto pa so roboti namenjeni iskanju in zbiranju elektronskih naslovov. Ti naslovi lahko rabijo za sestavljanje imenika elektronskih naslovov, lahko pa jih podjetja prodajo oglaševalcem.[309] Zato se pri objavi elektronskih naslovov pogosto uporabljajo različne zvijače, ki robote zmedejo tako zelo, da podatka niso več sposobni prepoznati kot elektronski naslov.[310]

Prvi primer javnega imenika elektronske pošte v Sloveniji je bil Telekomov *Imenik elektronske pošte Slovenije* (<http://afna.telekom.si>), ki je začel delovati 6. oktobra 1997. Pozneje je bil na voljo imenik e-pošte iskalnika Najdi.si. Zaradi številnih pritožb, da taki imeniki omogočajo t. i. smetilcem (posameznikom ali organizacijam, ki se ukvarjajo s pošiljanjem oglasne elektronske pošte) enostavno krajo elektronskih naslovov, je Najdi.si pozneje prikaz elektronskih naslovov spremenil tako, da se e-naslovi ne prikazujejo več kot besedilo, temveč kot slika; to robotom onemogoča krajo elektronskih naslovov, posamezniki pa še vedno dobijo želeno informacijo.

Nekaterim načinom kraje elektronskega naslova in drugih osebnih podatkov se posamezniki s previdnostjo lahko izognejo. Med te štejemo tudi različne bolj ali manj prozorne poizkuse prevar, ki pa nevednega uporabnika interneta lahko hitro zavedejo.[311] Nekaterim načinom kraje osebnih podatkov pa se žal ni mogoče izogniti. Primer slednjega je zbirka Whois.

Zbirka Whois

Zbirka Whois (v bistvu gre za več zbirk, ki pa so enotno dostopne) je zbirka registrantov internetnih domen, ki jo za mednarodne domene upravlja ICANN (*Internet Corporation for Assigned Names and Numbers*). Ob registraciji domene je poleg tehničnih podatkov in imena domene treba vpisati kontaktne podatke ljudi, ki vzdržujejo domeno. Vpisati je treba upraviteljski stik, tehnični stik in plačilni stik. Po pravilih ICANN morata biti upraviteljski in tehnični stik vsake domene javno dostopna, saj so ti podatki v osnovi namenjeni sodelovanju med upravitelji internetnih strežnikov v primerih odkrivanja in odpravljanja napak v omrežjih; podatki pa morajo biti tudi točni, saj v nasprotnem primeru lastnik domene le-to izgubi. Zbirka zato obsega imena, naslove, telefonske in faksirne številke ter elektronske naslove posameznikov. Predvsem zaradi slednjega je postala zbirka Whois tarča trgovcev z elektronskimi naslovi in smetilcev. Leta 2001

---

309 Leta 2003 je Gospodarski vestnik izdal CD z elektronskimi naslovi slovenskih uporabnikov interneta.

310 Na voljo pa so tudi skripti, ki generirajo naključne elektronske naslove, ki jih v resnici seveda ni. Njihov namen je robota oskrbeti z lažnimi podatki, zbirka elektronskih naslovov, ki jo ustvari tak robot, pa je zato neuporabna.

311 Znan način kraje osebnih podatkov, ki sicer spada v kategorijo prevar (t. i. socialno inženirstvo, *social engineering*), je t. i. ribarjenje (ang. *phishing*). Napadalec v tem primeru pošlje lažno obvestilo, ki je oblikovano tako, kot bi bilo poslano s strani npr. banke, sporočilo pa vsebuje povezavo na spletni strežnik, v katerega naj prejemnik vpiše svoje osebne podatke. Povezava na spletni strežnik je prirejena tako, da na videz kaže na spletno stran banke, v resnici pa kaže na lažno spletno stran. Zloraba je možna tudi s pomočjo zlorabe XSS. Gre za zlorabo možnosti izvajanja skript ene spletne strani preko URL naslova druge spletne strani (tim. *cross-site scripting*), kar omogoča prikaz vsebine prve spletne strani v drugi. Na ta način je mogoče znotraj ranljive spletne strani prikazati npr. vnosni obrazec za osebne podatke ali poljubno besedilo in s tem zavesti uporabnika. Ribarjenje se najpogosteje uporablja za krajo bančnih in drugih finančnih podatkov, ki jih kriminalci pozneje uporabijo za pranje denarja prek tujih računov (Božič, 2004). So pa tudi drugi, npr. spletne strani, ki omogočajo pošiljanje spletnih voščilnic (pošiljatelj vpiše svoj in prejemnikov elektronski naslov).

pa se je celo izkazalo, da je podjetje VeriSign, najstarejši in največji registrar, ki je od ICANN dobil koncesijo za trženje domen, prodajalo podatke iz zbirke Whois. To je sicer sprožalo proteste, vendar je bilo v skladu z objavljeno politiko VeriSigna (McGuire, 2001), zato ICANN proti VeriSignu ni ukrepal.[312] Ker pa je zbirka javno dostopna, so trgovci z osebnimi podatki z roboti kopirali podatke iz nje. Zato so zbirko zaščitili tako, da so podatki dostopni samo fizičnim osebam, ne pa tudi robotom,[313] oziroma so podatki prikazani tako, da jih lahko preberejo samo fizične osebe, in ne roboti. S tem je bil problem množične kraje podatkov iz zbirke Whois sicer rešen, vendar strokovnjaki opozarjajo na dva dodatna problema.

Prvi je ta, da je za javno dostopno zbirko Whois nemogoče zagotoviti, da se bodo podatki iz nje uporabljali samo za namen, za katerega so bili zbrani. Podatki se dejansko uporabljajo za iskanje lastnikov domen s privlačnimi imeni, ki jim potem trgovci z domenami ponujajo odkup domene, za krajo identitete itd. Zaradi tega je politika ICANN v nasprotju z mednarodno zakonodajo o varstvu informacijske zasebnosti, saj se podatki uporabljajo za drugačne namene, kot so bili zbrani (Laurant, 2003: 100). Drugi problem pa je ta, da imajo dostop do teh podatkov tudi totalitarne vlade ter preiskovalci in odvetniki brez sodne odredbe, to pa ima lahko posledice za svobodo govora (Laurant, 2003: 100).

Nekateri registrarji sicer registrantu ob prodaji domene dodelijo tudi poseben elektronski naslov, ki je javno objavljen v zbirki in prek katerega registrant prejema obvestila, oziroma v zbirko Whois posredujejo svoje podatke.[314] ICANN namreč občasno preverja pravilnost vpisanih podatkov, vendar večinoma preverijo samo odzivnost na sporočilo, poslano na elektronski naslov, ki je vpisan v zbirko Whois, drugih podatkov pa ne. Registranti disidentskih ali aktivističnih domen zato pogosto vpisujejo lažne podatke, s katerimi skušajo skriti svojo identiteto, pa tudi drugi registranti pri tem niso izjema, saj se upravičeno bojijo, da bodo na elektronski ali navaden naslov začeli dobivati nezaželena oglasna sporočila. Tako ravnanje ni sicer nič nenavadnega, saj se podobno podajanje lažnih elektronskih naslovov dogaja tudi pri objavah sporočil v konferenčnem sistemu USENET. Raziskava *Trust and privacy online: Why Americans want to rewrite the rules*, ki jo je leta 2000 izvedel The Pew Internet & American Life Project, je pokazala, da med t. i. gverilskimi samozaščitnimi taktikami, s katerimi želijo uporabniki zaščititi svojo zasebnost, prevladuje vpisovanje lažnega imena in osebnih podatkov. To, da vpisujejo lažne podatke, je v raziskavi izjavilo 24 % ameriških uporabnikov interneta, da uporabljajo alternativni elektronski naslov 20 %, le 9 % uporablja šifriranje elektronske pošte in le 5 % tehnike za skrivanje identitete (t. i. *proxy*) v spletu (The Pew Internet & American Life Project, 2000: 10).

---

[312] Je pa nasprotno ICANN VeriSignu zagrozil z odvzemom koncesije v primeru, ko VeriSign ni upošteval njegovih zahtev za zagotavljanje pravilnosti in točnosti podatkov iz zbirke Whois (McGuire, 2002).

[313] Zbirka je dostopna samo ob vpisu posebnega gesla, ki se vsakič na novo generira. Geslo je na spletni strani prikazano kot slika z nekaterimi dodatnimi grafičnimi elementi (barvni prelivi, črte, itd.), kar robotom onemogoča samodejno prepoznavanje vsebine gesla, posameznik pa ga brez težav prepozna in vpiše.

[314] Ena prvih sta bili podjetji GKG, ki uporabniku dodeli naslov v obliki *številka*@whois.gkg.net, ter GoDaddy.com, ki v zbirko Whois posreduje svoje podatke.

Iz teh razlogov je Data Protection Working Party iz EU junija 2003 izdala *Mnenje 2/2003 o uporabi načel zaščite osebnih podatkov na imenikih Whois* (*Opinion 2/2003 on the application of the data protection principles to the Whois directories*). V njem so poudarili, da vprašanje zaščite osebnih podatkov v zbirki Whois postaja čedalje pomembnejše, ker internetnih domen ne registrirajo samo organizacije, temveč vse več posamezniki. V svojem mnenju so opozorili na načelo, naj se zbira samo tiste podatke, ki so nujno potrebni za dosego namena, zaradi katerega se podatki zbirajo. Poudarili pa so, da morajo imeti posamezniki možnost registrirati domeno na tak način, da njihovi osebni podatki ne bodo javno dostopni (Data Protection Working Party, 2003). Oktobra 2003, nekaj dni pred sestankom ICANN, je EPIC sprožil podpisovanje peticije, s katero so ICANN pozvali k zaščiti zbirke Whois. V peticiji so izrazili željo, da se od lastnikov domen ne bi zbiralo podatkov, na podlagi katerih bi lastnik domene lahko postal žrtev goljufije, viktimizacije ali političnega preganjanja (EPIC, 2003a). Peticija je sprožila javno razpravo o tem vprašanju, na ICANN pa so začeli pritiskati tudi predstavniki organov za varstvo osebnih podatkov ter Evropske komisije (EPIC, 2004e). Kljub temu da je ICANN problematiko zasebnosti zbirke Whois začel resno obravnavati in je nezaščita osebnih podatkov iz nje resen problem, pa se lahko uresniči prav nasprotno od pričakovanj borcev za elektronsko zasebnost. V ZDA so namreč leta 2004 sprejeli *Fraudulent Online Identity Sanctions Act*,[315] ki predvideva celo dodatnih sedem let zaporne kazni za tiste, ki bi ob registraciji internetne domene namerno vpisali napačne podatke in prek te domene storili kaznivo dejanje. Zakon je bil sicer vložen z namenom preprečevanja internetnih prevar (izrecno so omenjene kršitve avtorskih pravic), vendar so kritiki mnenja, da bodo s kaznovanjem prizadeti predvsem posamezniki, ki se skušajo zaščititi pred nezaželeno oglasno elektronsko pošto – smetjem, in tisti, ki zaradi svobode govora želijo ostati anonimni (Singel, 2004).

Smetje (spam)

Izraz *smetje* ali ang. *spam*[316] (uporablja se tudi izraz *unsolicited commercial e-mail* (UCE), *unsolicited bulk e-mail* (UBE) ali *junk mail*) označuje nezaželena oziroma nenaročena elektronska sporočila, pri čemer gre večinoma za oglasna elektronska sporočila.[317] Smetje je eden izmed resnih problemov interneta, saj so raziskave pokazale, da se količina takih sporočil veča in je leta 2003 obsegala že več kot 50 % vseh sporočil. To bi celo utegnilo uničiti uporabnost elektronske pošte. Smetje je zaradi možnosti velikih zaslužkov tudi eden izmed pomembnih

---

[315] Zakon *Fraudulent Online Identity Sanctions Act* (Fraudulent Online Identity Sanctions Act of 2004, 15 U.S.C. (2004)), je del zakona *Intellectual Property Protection and Courts Amendments Act of 2004* (Intellectual Property Protection and Courts Amendments Act of 2004, 15 U.S.C. (2004)) (EPIC, 2004b).

[316] Izraz smetje (ang. *spam*) naj bi izhajal iz imena mesnega izdelka podjetja Hormel Foods. Izraz je v nekem skeču uporabila skupina Monty Python's Flying Circus, v katerem prepevanje spam, spam, spam preglasi vse drugo. Iz tega razloga se je izraz leta 1994 uveljavil tudi za množično poslana nezaželena elektronska sporočila.

[317] Kljub temu je znan vsaj en primer, ko je bilo t. i. smetje uporabljeno tudi kot metoda vojskovanja. Nekdanji svetovalec ameriške vlade za boj proti terorizmu Richard Clarke je namreč v nekem intervjuju navedel, da naj bi ameriška vojska višjim iraškim vojaškim uradnikom poslala poosebljena elektronska sporočila, v katerih so jih pozvali, naj ob začetku vojne odidejo domov in se izognejo spopadu, in to naj bi večina prejemnikov sporočila tudi res storila (Ilett, 2004).

dejavnikov za razmah kiberkriminala. A omejeno ni samo na elektronsko pošto, temveč so ga pošiljali tudi na USENET oziroma prek interaktivnih sistemov za klepet po internetu (MSN, ICQ, itd. t. i. SPIM[318]). V zadnjem času pa je priljubljena posebna oblika smetja, ko pošiljatelj dopisuje reklamne komentarje v t. i. spletne dnevnike (ang. *blog*). Čeprav smetje ne pomeni neposrednega vdora v zasebnost v smislu nadzorovanja, pa ga lahko štejemo za poseg v pravico biti puščen pri miru, skratka v tisti del zasebnosti, ki posamezniku omogoča, da se umakne iz družbe.

Že tri leta po izumu elektronske pošte leta 1972[319] je Jon Postel v dokumentu *RFC 706 - On the junk mail problem* opisal nevarnost izvedbe napada na računalnik z množico elektronskih sporočil. V dokumentu je zapisal, da nezmožnost selektivnega sprejemanja sporočil lahko povzroči onemogočanje dostopa do storitev računalnika za njegove uporabnike in omrežne težave (Postel, 1975). V času nastanka dokumenta še ni bilo interneta, bil pa je njegov vojaški predhodnik ARPAnet, zato si Postel ni mogel predstavljati, kakšne posledice bo imela neodprava te varnostne pomanjkljivosti za zasebnost.

Prvi primer reklamnega sporočila sega v leto 1978, ko je podjetje DEC na vse elektronske naslove na ameriški zahodni obali poslalo reklamo za nov računalnik DEC-20. DEC je bil kaznovan zaradi kršitve pravil uporabe ARPANET, drugi pa so bili opozorjeni, naj tega nihče več ne počenja. Leta 1979 so študent Steve Bellovin in programerja Tom Truscott ter Jim Ellis razvili USENET (novičarske skupine, ki so razdeljene na tematske konference) in kmalu se je izkazalo, da je mogoče v USENET objavljati sporočila, ki jih vidi veliko število ljudi. Zaradi številnih verižnih pisem, ki so v 80. letih krožila po USENET, so leta 1993 uvedli moderirane konference.[320]

Prvi primer množičnega pošiljanja sporočil se je zgodil januarja 1994, ko je upravitelj z Andrews University na vse konference USENET poslal sporočilo z naslovom '*Global Alert for All: Jesus is Coming Soon*'. Kmalu je sledilo komercialno sporočilo. Aprila leta 1994 sta odvetnika iz Phoenixa, Laurence A. Canter in Martha S. Siegel, v USENET poslala oglas, v katerem sta oglaševala pravno pomoč pri prošnji za delovno zeleno karto. Čeprav je bila delovna zelena karta brezplačna, sta v oglasu računala 100 dolarjev za pomoč pri njeni pridobitvi in to je skupaj z načinom oglaševanja sprožilo številne proteste; ti so povsem onesposobili njunega ponudnika dostopa do interneta, zato ju je izključil iz omrežja.

Vendar pa uvedba moderiranih konferenc problema smetja ni rešila. Ker smetilci niso več mogli pošiljati sporočil v USENET, so začeli po spletu in USENET zbirati elektronske naslove posameznikov,[321] obenem pa iskati načine, kako zaobiti omejitve. Leta 1995 je Jeff Slaton, ki si je nadel vzdevek 'Spam King', pod vtisom knjige,[322] ki sta jo napisala Canter in Siegelova, začel

---

318 SPIM – izraz izvira iz besede spam in IM - Instant Messenger (IM so sistemi za trenutno sporočanje).

319 Prvi program za pošiljanje elektronske pošte je napisal Ray Tomlison 5. oktobra 1972.

320 Od tod verjetno tudi izvira prepoved pošiljanja verižnih pisem, zapisana v RFC 1855 - Netiquette Guidelines (Hambridge, 1995), ki so jo povzeli številni ponudniki dostopa do interneta, med drugim tudi Arnes.

321 Moderatorstvo je preprečevalo samo neomejeno objavljanje, ne pa tudi branje USENET konferenc.

322 Naslov knjige je bil *How To Make A Fortune On The Information Superhighway*.

razmišljati o smetilnem marketingu. Julija 1995 je poslal prvo sporočilo, v katerem je prodajal načrte za atomsko bombo (Garfinkel, 1996). Za razliko od prejšnjih smetilcev se ni dosti oziral na sovražne odzive, temveč je začel svoje usluge ponujati tudi drugim podjetjem in celo ustanovil podjetje Unix/Eunuchs Etc., ki je prodajalo programsko opremo za pošiljanje smetja. Ker so ga zaradi pritožb redno izklapljali iz omrežja, je uporabljal številne zvijače za pošiljanje smetja in pridobivanje podatkov, med drugim tudi lažne možnosti odjave in pošiljanje elektronske pošte z lažnih naslovov (Garfinkel, 1996).

Čeprav je na smetje mogoče gledati kot na poseg v zasebnost (kršenje pravice biti puščen pri miru), oziroma da do posegov v informacijsko zasebnost pogosto prihaja zaradi smetja, pa je bil odziv t. i. 'internetne skupnosti' na smetje precej kontroverzen. Po eni strani so si namreč prizadevali za neomejeno svobodo govora, zasebnost in anonimnost, po drugi strani pa so želeli smetje prepovedati (cenzurirati) in javno objavljali tudi osebne podatke smetilcev ter jih nadlegovali po elektronski pošti in v resničnem življenju. Seveda je tak odziv povsem razumljiv in morda celo upravičen, vendar je nekoliko dvoličen. T. i. internetna skupnost, sestavljena iz računalnikarjev in kiberpunkerjev, je pogosto netransparentno (za razliko od demokratične države, ki pozna sistem volitev, delitev oblasti in vladavino prava) postavljala svoja lastna pravila in ni želela, da bi se v njihov svet vmešavala država; poleg tega je pogosto postavljala dvojna merila za izkušene uporabnike interneta nasproti novincem (za katere se je uveljavil zaničevalen izraz *newbie*).

Netiquette Guidelines na primer o nezaprošeni (ang. *unsolicited*) elektronski pošti pravi takole: "*Na splošno večina ljudi, ki uporablja internet, nima časa odgovarjati na splošna vprašanja o internetu in njegovem delovanju. Ne pošiljajte nezaprošene elektronske pošte z vprašanji ljudem, katerih imena ste morda našli na RFC-jih ali poštnih seznamih*". O nenaročeni pošti pa pravi: "*Ne pošiljajte* velikih količin *nenaročenih informacij ljudem.*" (Hambridge, 1995).

Seveda se smetilci s temi smernicami niso strinjali in so jih celo namerno kršili. Canter in Sieglova sta na primer v svoji knjigi zapisala, da internetne skupnosti ni in da posledično ni niti pravil te skupnosti, da veljajo edino pravila države, v kateri posameznik živi, in etika, ki jo posameznik sam spoštuje.[323] Slaton je v intervjuju za Wired izrazil ponos nad svojim početjem in na vprašanje o morebitnem fizičnem nadlegovanju s strani prejemnikov njegovih sporočil odvrnil, da sta "*njegova prijatelja Smith & Wesson zelo pripravljena govoriti*", pri čemer je seveda mislil na orožje[324] (Garfinkel, 1996).

V končni fazi je šlo torej zgolj za to, kdo bo pametnejši in kdo bo znal neobstoj s strani zunanje avtoritete postavljenih pravil obrniti v svojo korist. Čeprav je bilo proti smetilcem dobljenih nekaj odmevnih tožb (AOL je npr. leta 1998 proti Sanfordu Wallacu in njegovemu podjetju Cyber Promotion dosegel sodno prepoved pošiljanja sporočil v svoje omrežje[325]), pa to smetja ni zaustavilo. Smetilci so začeli izkoriščati orodja za anonimizacijo, ki so jih

[323] Knjiga ni več dostopna, citat pa je dostopen na EFF, 2005a.
[324] *Smith & Wesson* – gre za znano blagovno znamko strelnega orožja.
[325] Kopija razsodbe je na <http://legal.web.aol.com/decisions/dljunk/bigfooto.html>.

razvili cypherpunkerji (to je bil med drugim tudi eden izmed vzrokov za izginotje številnih javno dostopnih in brezplačnih anonimnih proxyev), pozneje pa so se začeli posluževati tudi kiberkriminala.

Smetje in kiberkriminal

Sprva so smetilci sami kradli osebne podatke posameznikov. Na začetku so bili to predvsem elektronski naslovi, ki so jih pogosto naključno generirali. Ker pa se elektronska sporočila, poslana na neobstoječe naslove, vrnejo pošiljatelju (oziroma v domeno, iz katere so bila poslana), pošiljatelj precej obremeni omrežje, učinek takega oglaševanja pa je majhen.
Seveda lahko pošiljatelj pošilja tudi prirejena elektronska sporočila, za katera kaže, da prihajajo iz neke neobstoječe ali celo obstoječe, a s pošiljateljem povsem nepovezane domene[326]. Znan je primer, ko je zlonamerni pošiljatelj skoraj uničil neko podjetje, ko je v njegovem imenu in iz njegove "ponarejene" domene poslal večjo količino nezaželenih elektronskih sporočil. Sporočila, poslana ne neobstoječe naslove, so se vrnila k lastniku zlorabljene domene in zapolnila njegov elektronski predal ter mu začasno onemogočila poslovanje, poleg tega so nezadovoljni prejemniki podjetje zasuli z jezno elektronsko pošto, trpel pa je tudi ugled podjetja (Delio, 2003).

Zaradi majhnega učinka pri pošiljanju sporočil na naključno generirane naslove so smetilci kmalu začeli še pred pošiljanjem preverjati, ali elektronski naslovi obstajajo ali ne. Pri tem so si pomagali z zbirko Whois, nabiranjem elektronskih naslovov, objavljenih na javnih spletnih straneh, ter z izkoriščanjem nekaterih ukazov, ki so bili uveljavljeni kot internetni standardi za poštne strežnike za odhodno pošto (tj. *strežnike SMTP*). Internetni standardi RFC so bili namreč na začetku napisani tako, da so zagotavljali čim bolj odprto delovanje interneta, pozneje pa so jih zaradi zlorab začeli zapirati. Značilen zgled je tehnični standard, ki opredeljuje delovanje strežnikov za odhodno pošto.

Dokument RFC 821 iz avgusta 1982 je predvideval, da strežnik za odhodno pošto odgovori na ukaza VRFY (*verify*) in EXPN (*expand*). Na zahtevo je tako poštni strežnik vrnil elektronski naslov in ime uporabnika poštnega strežnika oziroma poštnega seznama in njegovih članov (vhodni parameter je bilo uporabniško ime, ki so ga naključno generirali, a je bilo bolj učinkovito, saj je dolžina uporabniškega imena pogosto omejena in je zato znano število vseh možnih različnih uporabniških imen). Tako so smetilci lahko hitro pridobili seznam vseh elektronskih naslovov v nekem sistemu. Zato so v standard RFC 2505 iz leta 1999 zapisali priporočilo, naj se omenjeno funkcionalnost izključi, kot razlog pa so izrecno navedli, da je omenjena funkcionalnost pogosta tarča zlorab smetilcev (Lindberg, 1999).

Hkrati so ponudniki dostopa do interneta začeli kot zaščitni ukrep omejevati dostop do strežnikov za odhodno pošto. Elektronsko pošto je načeloma možno pošiljati po kateremkoli

[326] To stori tako, da priredi elektronski naslov pošiljatelja. Namesto svojega naslova vpiše lažni naslov. Pravega pošiljatelja je sicer še vedno mogoče izslediti prek naslova IP, a je tako sledenje težje.

strežniku za odhodno pošto, podobno kot je v fizičnem svetu mogoče oddati pisemsko pošiljko v katerikoli poštni nabiralnik. Ker pa navadno pošiljatelji pošiljajo elektronsko pošto po strežniku za odhodno pošto svojega ponudnika dostopa do interneta, lahko ta v primeru prijave ugotovi njihovo identiteto in jih v ob zlorabi odklopi iz svojega omrežja. Prejemnik namreč lahko ugotovi, kje je bilo sporočilo oddano in po kateri poti je potovalo do njega. Smetilci so zato začeli pošiljati elektronsko pošto po sprejemnih strežnikih drugih uporabnikov interneta, pa tudi po anonimizacijskih poštnih strežnikih; to je tudi razlog za propad teh strežnikov. Prvi zaščitni ukrep, ki so ga sprejeli ponudniki dostopa do interneta, je bila zato omejitev dostopa do njihovega strežnika za odhodno pošto samo na uporabnike njihovega omrežja. Ker pa se večina strežnikov za odhodno pošto teh priporočil ni držala, so upravitelji strežnikov za dohodno pošto začeli zavračati sporočila, ki so bila poslana iz t. i. odprtih strežnikov za odhodno pošto (ang. strežniki *open relay*). V ta namen so se oblikovali posebni seznami odprtih strežnikov (t. i. zbirke RBL – ang. *Realtime Blackhole List*, najbolj znan je primer zbirke ORDB – *Open Relay Database*).

Zaradi teh seznamov so bili pogosto prizadeti povsem nedolžni uporabniki sistemskih upraviteljev strežnikov, ki niso bili ustrezno zaprti (bodisi namerno, najpogosteje pa zaradi neznanja), saj niso mogli pošiljati elektronske pošte v strežnike, ki so upoštevali črno listo RBL.[327] Vendar pa so seznami RBL na začetku obsegali zgolj črno listo odprtih strežnikov. Problem je nastal, ko so smetilci začeli odpirati nove strežnike, ki še niso bili na črni listi. Zaradi tega so nekateri strežniki za dohodno pošto začeli uporabljati seznam preverjeno zaprtih strežnikov (t. i. beli seznam, ang. *Whitelist*). Vendar je tak način zelo neučinkovit, saj je zaprtih strežnikov lahko zelo veliko in je posledično seznam zelo dolg. To podaljša čas preverjanja, poleg tega so smetilci začeli vdirati v zaprte strežnike oziroma pošiljati nezaželena elektronska sporočila prek navadnih uporabnikov. Pri tem početju pa so stopili na področje klasične kiberkriminalitete.

"Spackers"

Izraz "spacker" je nastal konec leta 2003 v Wired magazinu, gre pa za skovanko angleških besed "spammer" in "cracker" (McWilliams, 2003b). Beseda *cracker* označuje posameznika, ki zlonamerno vdira v tuje računalnike (za razliko od t. i. hekerja, ki naj bi upošteval določena etična načela). "Spackerji" naj bi bili tako posamezniki, ki vdirajo v računalniške sisteme z namenom pošiljanja nezaželene elektronske pošte. Izraz pa se uporablja tudi za tiste, ki postavljajo lažne spletne strani, po katerih prodajajo različne dvomljive ali celo nezakonite izdelke ali storitve, te spletne strani pa pogosto oglašujejo z nezaželeno elektronsko pošto.

V začetku leta 2003 se je razširil prvi računalniški virus, katerega namen ni bil samo širjenje in povzročanje škode, temveč pošiljanje nezaželene elektronske pošte. Virus W32.SoBig.E se

[327] V Sloveniji je bil dolgo časa tako odprt strežnik ponudnika dostopa do interneta Siol. Znani so primeri, ko Siolovi uporabniki niso mogli komunicirati s poslovnimi partnerji, ker so poštni strežniki samodejno zavračali elektronsko pošto iz Siola. Navadni uporabniki pogosto niso vedeli, v čem je problem, zato ta informacija dolgo časa ni prišla do upraviteljev in težava kar nekaj časa ni bila odpravljena.

je širil po računalnikih z nameščenim operacijskim sistemom Windows in jih spreminjal v t. i. zombije. (V angleščini se za take računalnike včasih uporablja tudi izraz *drone machine.*) Pred tem so se sicer že širili virusi, ki so se po uspešni namestitvi razposlali na vse elektronske naslove, ki so jih našli v adresarju v okuženem računalniku, vendar je bil Sobig.E prvi, ki je razpošiljal smetje.[328] To pa ni bil edini napad, ki kaže na to, da so se smetilci začeli povezovati s kiberkriminalom. Maja 2003 se je razširil virus Fizzer, ki je v okuženi računalnik namestil spletni strežnik, prek katerega so spletni goljufi prodajali pornografijo in ponarejena zdravila, omrežje pa so uporabljali tudi za goljufije s kreditnimi karticami ter napade na omrežja organizacij, ki se borijo proti smetju[329] (Spamhaus, 2005).

Kiberkriminalci so kmalu začeli svoje storitve prodajati na črnem trgu in Wired news je konec leta 2003 objavil članek o poljski skupini *krekerjev*, ki so začeli oglaševati "*nevidno in neprebojno gostovanje*" strežnikov (ang. *invisible bulletproof hosting*). Za 1500 dolarjev so namreč ponujali postavitev spletnega strežnika, katerega internetno, kaj šele fizično lokacijo je z navadnimi orodji za analizo računalniških omrežij nemogoče oziroma zelo težko izslediti. Prek IRC so predstavniki Wireda stopili v stik s predstavnikom krekerske skupine in ta jim je povedal, da njegova skupina nadzoruje 450.000 ugrabljenih računalnikov, v katere je nameščena programska oprema, ki skrbi za preusmerjanje prometa; to onemogoča sledenje. Delovanje sistema jim je tudi demonstriral (McWilliams, 2003b). Morda je številka pretirana, vendar podobna poročila prihajajo tudi od drugod.[330] Po podatkih organizacije Spamhaus naj bi organizirane kriminalne skupine iz Rusije ameriške smetilce oskrbovale s podatki o ugrabljenih računalnikih, prek katerih je mogoče pošiljati smetje (Wearden, 2004).

Vdor v zasebnost kot 'stranski učinek' kiberkriminala

Če so se pred tem virusi širili neodvisno in bolj ali manj naključno, pa so na tej točki vdiralci začeli ugrabljene računalnike povezovati med seboj in načrtno graditi prikrita omrežja ugrabljenih računalnikov[331]. Richard Clarke, nekdanji svetovalec ameriške vlade za področje boja proti terorizmu, je v intervjuju za ZDNet 16. novembra 2004 povedal, da se je "*v zadnjih letih število prikritih omrežij (ang. botnet) povečalo z 2000 na okrog 30.000. Ne vem sicer, koliko računalnikov je povprečno v prikritem omrežju, lahko pa si mislite, da jih je na tisoče.*" (Ilett,

---

[328] Po nekaterih ocenah naj bi bili ugrabljeni računalniki (večinoma z nameščenim operacijskim sistemom Windows) v začetku leta 2004 vir 80 % vsega smetja. (Leyden, 2004).

[329] Zaradi številnih in ponavljajočih se napadov DDOS so bile nekatere organizacije, ki se borijo proti smetju, prisiljene zapreti svoje strežnike.

[330] Nekdo (verjetno iz Slovenije) je pred časom napisal program za vdiranje v računalnike in upravljanje ugrabljenih računalnikov na daljavo. Poimenoval ga je *sdbot*, njegovo izvirno kodo pa objavil na internetu. Kmalu so začele krožiti izboljšane različice programa in trenutno se je okrog programa in njegovih izvedenk razvila prava internetna skupnost. V pogovoru na IRC z nekom, ki razvoj *sdbota* spremlja že dlje časa, je ta povedal, da program išče nove žrtve povsem samodejno, je pa tako enostaven za upravljanje, da ga uporabljajo tudi 13-letniki. Na vprašanje, koliko računalnikov je mogoče s programom ugrabiti v krajšem času, sem dobil odgovor, da tudi do 5000 v eni noči.

[331] V angleščini se za omrežja, ki rabijo za napade DDOS, navadno uporablja izraz '*botnet*' (izraz izvira iz besed '*(ro)bot*' ter '*net(work)*'), za druga prikrita omrežja, o katerih bo govor v nadaljevanju, pa '*stealth networks*'.

2004).[332] Do tega je prihajalo še pred zlorabo kiberkriminala v pridobitne namene, ko so se ti ugrabljeni računalniki uporabljali večinoma zgolj za izvajanje DOS napadov[333], v času t. i. IRC-vojn. (Gre za bojevanje dveh ali več skupin, ki hočejo na IRCu druga drugi prevzeti kak kanal IRC, po izjavi Gorazda Božiča, vodje varnostnega centra SI-CERT, se taki napadi v Sloveniji dogajajo v povprečju dvakrat na teden, po podatkih SI-CERTa pa so leta 2003 obsegali 19 % vseh varnostnih incidentov, ki so jih obravnavali na Arnesu (Kovačič, 2004a)). Vendar v novejšem času prihaja do zlorabe teh prikritih omrežij v pridobitne kriminalne namene.[334] Te zlorabe obsegajo tako že omenjena primera razpošiljanja smetja in uporabe teh prikritih omrežij za skrivanje spletnih strežnikov, prišlo pa je tudi do uničevanja konkurence z DOS napadi[335] in do množične kraje podatkov za elektronsko bančništvo.[336]

Zaradi množičnosti pojava je prišlo do premika v razumevanju ogroženosti. Zasebnost uporabnika interneta ni ogrožena zgolj zato, ker napadalec meri ravno nanj ali ker ga želi napadalec neposredno oškodovati, temveč je žrtev anonimna, le del prikritega omrežja, ki napadalcu omogoča skrivanje pred organi pregona ali izvajanje kriminalnih dejavnosti. Gre torej za podoben premik, kot ga je opazil Foucault pri prehodu iz disciplinskih v regulacijske družbe – posameznik ni pomemben, pomembna je kategorija, populacija. To po eni strani pomeni, da napadalca praviloma (še) ne zanimajo podatki v napadenem računalniku, temveč bolj sistemska sredstva žrtve, ki jih lahko izkoristi za svoje namene (pasovna širina povezave v internet, procesorska moč...), po drugi strani pa se žrtev izpostavlja nevarnosti, da bo njen računalnik vpleten v izvajanje kaznivih dejanj. Znan je primer, ko je britanska policija pri nekom v domačem računalniku odkrila 172 pedofilskih fotografij, vendar je obtoženemu uspelo dokazati, da je slike v njegov računalnik prenesel t. i. trojanski konj (gre za posebno obliko računalniškega virusa)

---

[332] Po nekaterih ocenah je bilo v začetku leta 2005 takih računalnikov več kot milijon (BBC News, 2005), oktobra 2005 pa je Nizozemska policija aretirala tri ljudi, ki so posedovali prikrito omrežje z več kot 1,5 milijona računalnikov (Schneier, 2006c).

[333] Napad DOS – ang. napad *Denial Of Service*, gre za napad na razpoložljivost sistema oziroma oviranje njegovega delovanja. Navadno napadalec to stori tako, da napadenemu sistemu pošlje veliko količino strežniških zahtevkov. Ker ima napadeni sistem omejena sistemska sredstva, mu vseh zahtevkov ne uspe obdelati in njegovo delovanje se upočasni ali pa celo popolnoma preneha. Proti napadu DOS se je mogoče boriti z blokiranjem prometa iz zlonamernega strežnika, zato se za oviranje delovanja računalniških sistemov pogosteje uporablja napad DDOS (ang. *Distributed Denial Of Service*). Tu gre za podoben napad, ki pa simultano poteka iz večjega števila računalnikov, zato se ga je teže ubraniti. Napadi DOS in DDOS so od 6. 5. 2004 kaznivi tudi po slovenski zakonodaji (2. odstavek 225. člen KZ-B: "*Kdor podatke v informacijskem sistemu neupravičeno uporabi, spremeni, preslika, prenaša, uniči ali v informacijski sistem neupravičeno vnese kak podatek, <u>ovira prenos podatkov ali delovanje informacijskega sistema</u>, se kaznuje z zaporom do dveh let.*" (Novela Kazenskega zakonika (KZ-B), Uradni list RS, št. 40/04).

[334] Richard Clarke je v intervjuju za ZDNet potrdil izjavo Alana Palerja z inštituta SANS, ki je izjavil, da veliko igričarskih spletnih strani verjetno plačuje izsiljevalcem, da jih ne napadajo (Ilett, 2004).

[335] Leta 2003 je v ZDA stekla *Operacija Cyberslam,* v okviru katere so razpisali tiralico za Saadom Echouafnijem, direktorjem podjetja, ki je najel skupino hekerjev, da so izvedli napad DDOS na konkurenčno podjetje. Le-to je bilo zaradi napada onesposobljeno za skoraj dva tedna, ocenjena škoda pa se giblje od 200.000 dolarjev do več kot milijon dolarjev (FBI, 2004).

[336] 24. junija 2004 je SANS *Internet Storm Report Center* prejel obvestilo o odkritju novega virusa, ki v okuženi sistem namesti poseben dodatek za spletni brskalnik Internet Explorer (t. i. *Browser Helper Object*). Ta čaka, da se uporabnik poveže v katero izmed spletnih bank. Ko se to zgodi, virus prestreže uporabnikove podatke, še preden se po šifrirani povezavi pošljejo do banke, in jih posreduje v strežnik napadalcev. Prva različica virusa je prestrezala povezave do 49 najbolj znanih svetovnih bank (Liston in Bambenek, 2004).

in se s tem izognil do desetletni zaporni kazni (Leyden, 2003). Nekdo je bil na podlagi enake obrambe oproščen napada na informacijski sistem ladijskega pristanišča v Houstonu (BBC News, 2003), ugrabljeni računalniki so lahko spremenjeni v skladišča hekerskih orodij, pa tudi v Sloveniji je policija obravnavala primer, ko je nekdo prek računalnika, v katerega je vdrl, razpečeval datoteke z otroško pornografijo (Šavnik, 2005). Čeprav so bili nekateri obdolženci na koncu spoznani za žrtve kaznivih dejanj in oproščeni, pa primeri jasno kažejo na to, kako se kiberkriminalci z vdorom v računalniške sisteme naključnih žrtev lahko izogibajo kazenskemu pregonu in kakšnim nevarnostim so izpostavljene njihove žrtve.

'Spyware' in (zakonita) prikrita omrežja

Izraz 'spyware' ali vohunski program je bil prvič uporabljen na USENET 16. oktobra 1995, ko se je nekdo norčeval iz Microsoftove programske opreme, ki naj bi prikrito po internetu zbirala informacije o uporabnikih njihove programske opreme. Izraz se je dokončno uveljavil leta 1999, ko ga je uporabilo programersko podjetje *Zone Labs,* in v začetku leta 2000, ko je nastal prvi program za odstranjevanje teh vohunskih programov *OptOut* (Wienbar, 2004).

Izraz je sicer zavajajoč, saj niso vsi 'vohunski programi' namenjeni zgolj (prikritemu) zbiranju podatkov, temveč pogosto tudi prikazujejo oglase in podatkov ne posredujejo v internet, čeprav jih uporabljajo za odločanje o vsebini prikazanih oglasov. Poleg tega ne delujejo povsem prikrito, saj uporabnika, sicer pogosto v drobnem tisku, obvestijo o tem, kaj bodo počeli. Izraz 'spyware' se zato delno prekriva tudi s pojmoma 'adware' (programska oprema, namenjena prikazovanju oglasov) ter 'malware' (zlonamerna programska oprema, namenjena zgolj nezakonitim dejavnostim[337]). Nekateri izdelovalci protivohunskih programov pa mednje štejejo tudi spletne piškotke. Po mnenju Sharon Wienbar so se vohunski programi razvili zaradi neuspeha prodaje nizkocenovne programske opreme na drobno, nastanka omrežij P2P[338] ter cenovnega modela oglaševanja na klik[339] (Wienbar, 2004). Ti trije dejavniki so po eni strani povzročili nastanek poslovnega okolja, v katerem so morala podjetja uporabljati agresivnejše tržne prijeme, če so želela biti uspešna, oziroma so morala stroške razvoja programske opreme kriti z oglaševanjem; hkrati so ustvarili ugodno okolje za široko distribucijo tovrstnega programja. Ob dejstvu, da je stopnja zaščite informacijske zasebnosti v ZDA bistveno nižja kot v Evropi in da je pravno povsem dopustno, da se uporabnik dobesedno s klikom miške odpove svojim pravicam iz naslova informacijske zasebnosti, je uspeh takega tržnega pristopa povsem pričakovan.

---

[337] Tipičen primer zlonamernih programov so npr. t. i. klicalniki (ang. *dialer*), programi za povezovanje v internet prek telefonskega modema. Programi nadomestijo telefonsko številko ponudnika dostopa do interneta v uporabnikovih nastavitvah omrežja na klic z neko plačljivo telefonsko številko, po možnosti v tujini. Zlonamerni programi pa so pogosto namenjeni tudi prikritemu zbiranju ali celo kraji podatkov ali pa prikritemu obiskovanju oglasnih spletnih strežnikov, s čimer umetno povečujejo njihov obisk in s tem večajo zaslužek lastnika strežnika.

[338] P2P - ang. *Peer-to-peer* - gre za omrežja uporabnikov, ki omogočajo deljenje datotek. Omrežja P2P se v zadnjem času uporabljajo večinoma za nelegalno distribucijo avtorsko zaščitenih datotek prek interneta.

[339] T. i. '*cost-per-click*', '*pay-per-click*' – gre za tržni model oglaševanja, pri katerem se ne plačujejo prikazi oglasov, temveč samo tisti prikazi, ki so jih uporabniki dejansko kliknili.

Značilen zgled, ki je poskrbel za veliko razširjenost vohunskih programov, je primer omrežja P2P KaZaA. Program KaZaA podjetja Sharman Networks je namenjen vzpostavljanju omrežij P2P oziroma razdeljevanju datotek. Program je mogoče dobiti brezplačno, vendar je uporabnik ob namestitvi poleg KaZaA dobil tudi nekaj dodatnih programov, ki so pravzaprav klasični vohunski programi. Eden izmed njih je *b3d Projector* podjetja *Brilliant Digital Entertainment*, namenjen pa je prikazovanju oglasov. Ob namestitvi KaZaA in priključenih programov namestitveni program uporabnika vpraša, ali se strinja s pogoji namestitve. Žal izkušnje kažejo, da se uporabniki skoraj praviloma vedno "strinjajo", ne da bi si sploh prebrali pogoje, ki jih sprejemajo. Pogodba o uporabi b3d Projectorja tako navaja, da "*BDE dajete pravico do dostopa in uporabe prostega pomnilnika in računalniške moči v vašem računalniku, dostop do interneta ali pasovne širine za agregacijo vsebine in porazdeljeno uporabo računalnikov. Uporabnik to sprejema in omogoča brez pravice do kakršnegakoli povračila.*" (CIAC, 2002). Poleg tega se uporabnik strinja tudi s tem, da podjetje BDE uporablja računalnik uporabnika tudi po morebitni prekinitvi pogodbe. Podjetje BDE je 1. aprila 2002 v poročilu ameriški Komisiji za vrednostne papirje in denarni trg (ang. *Securities and Exchange Commission*) zapisalo, da je namen njihovega hčerinskega podjetja Brilliant P2P, pozneje preimenovanega v Altnet Inc., "*narediti zasebna, varna omrežja enakovrednih računalnikov, ki bodo uporabljala uveljavljeno, dokazano tehnologijo, ki bo izkoristila procesorsko, shranjevalno in porazdeljevalno moč omrežja enakovrednih računalnikov z več milijoni uporabnikov ... Altnetove storitve P2P bomo tržili na treh poglavitnih področjih: omrežne storitve, porazdeljeno shranjevanje podatkov in porazdeljena obdelava podatkov.*" (CIAC, 2002). Hkrati so zapisali, da mora biti v vsak računalnik, ki je del omrežja Altnet, nameščena ustrezna programska oprema, ki so jo distribuirali tako, "*da smo [ta program, m. op.] ga pripeli paketu, imenovanem ALTNET SECUREINSTALL, skupaj s programom Digital Projector. Po dogovoru s Sharman Networks je SecureInstall, skupaj z Digital Projectorjem [gre za b3d Projector, m. op.], prenesen kot del Sharman Networksovega KaZaA Media Desktop...*" (CIAC, 2002).

Zaradi teh razlogov se je na internetu pojavil program Kazaa Lite, ki je bil enako funkcionalen kot KaZaA, vendar ni vseboval vohunskih programov. Sharman Networks, Ltd. lastnik KaZaA je zato na podlagi ameriškega *Digital Millennium Copyright Act*[340] 22. septembra 2003 poslal iskalniku Google zahtevo,[341] naj pri prikazovanju rezultatov iskanja izpusti povezave na 15 strežnikov, ki vsebujejo kopije sicer brezplačne Kazaa Lite. To jasno kaže na to, da brezplačna KaZaA v resnici ni povsem brezplačna in da imajo njeni avtorji od vključenih vohunskih programov velike finančne koristi.

---

[340] Digital Millennium Copyright Act of 1998, 17 U.S.C. (1998).

[341] Pri iskanju "k-lite" Googlov iskalnik na dnu strani izpiše naslednje obvestilo: "*In response to a complaint we received under the Digital Millennium Copyright Act, we have removed 2 result(s) from this page. If you wish, you may read the DMCA complaint for these removed results.*" (*V odgovor na pritožbo, ki smo jo prejeli po Digital Millennium Copyright Act, smo umaknili prikaz dveh rezultatov iskanja. Če želite, si lahko preberete pritožbo DMCA za te umaknjene zadetke.*) Obvestilo kaže na vsebino zahtevka DMCA, iz katere je mogoče ugotoviti, katere povezave so bile umaknjene (Google, 2005). Zahteva po umiku najdenih zadetkov po zakonu DMCA (Digital Millennium Copyright Act of 1998, 17 U.S.C. (1998)) je dostopna na naslovu <http://www.chillingeffects.org/dmca512/notice.cgi?action= image_410>.

Po ameriški zakonodaji strinjanje s pogoji take pogodbe povsem zadostuje, da sme podjetje zakonito zbirati praktično kakršnekoli osebne podatke in računalnik v prikritem omrežju uporabljati za praktično karšnekoli zakonite namene. Pravzaprav so taka prikrita omrežja le komercialna različica nezakonitih prikritih omrežij, ki se uporabljajo za razpošiljanje smetja in napade DDOS. Da je gradnja teh omrežij, ki so ravno zaradi svoje zakonitosti (v smislu dejstva, da upravitelj omrežja na sicer sporen način pridobi soglasje uporabnikov, vključenih v omrežje) potencialno velika nevarnost za zlorabo zasebnosti, pa kaže tudi primer podjetja Claria, ki je razvilo enega prvih množičnih vohunskih programov *Gator*. Podjetje je leta 2003 porabilo 19,3 milijona dolarjev za razširjanje svojih vohunskih programov. To je po ocenah približno 43 centov na uporabnika, ki si skupaj z brezplačnim programom namesti tudi njihov vohunski program (Wienbar, 2004). O razširjenosti vohunskih programov pa pričajo tudi podatki, zbrani s strani ameriškega ponudnika dostopa do interneta Earthlink, ki je v okviru svojega programa za odstranjevanje vohunskih programov "*Earthlink Spy Audit*" do aprila 2005 v povprečju odkril 25 potencialnih vohunskih programov v posameznem pregledanem računalniku[342] (Earthlink, 2005).

* * *

Pravzaprav se vohunski programi za gradnjo prikritih omrežij uporabljajo šele v zadnjem času. Primarni namen teh programov pa je zbiranje podatkov, na podlagi katerih se potem prikazujejo t. i. kontekstualni oglasi. Ge pravzaprav za tipično neposredno trženje, torej prikazovanje oglasov, katerih vsebina je izbrana glede na trenutne internetne dejavnosti uporabnika, to pa seveda zahteva nadzorovanje le-teh. Pogosto se ti zbrani podatki tudi posredujejo upravljavcu vohunskega programa. Zato so za te programe včasih uporabljali tudi izraz aplikacije E. T.; potem, ko zberejo podatke, namreč "pokličejo domov" (izraz se je razvil na podlagi zgodbe iz filma E. T.).[343]

Vendar pa zmogljivosti prikritega zbiranja in posredovanja osebnih podatkov niso samo v domeni vohunskih programov, temveč so te zmogljivosti včasih vgrajene tudi v najbolj razširjene računalniške aplikacije. Na začetku leta 1999 se je namreč razširil makrovirus Melissa, FBI pa je avtorja uspelo izslediti v presenetljivo kratkem času. Glede na to, da je bil za pisanje virusa uporabljen skriptni jezik, ki je del okolja MS Office, je seveda takoj nastalo vprašanje, kako je FBI uspelo med milijoni uporabnikov programskega paketa MS Office odkriti pravega avtorja. Izkazalo se je, da je Microsoft v Office 97 skrivaj vgradil t. i. GUID, globalni univerzalni identifikator (ang. *Global Unique Identifier*), ki se zapiše v vsak dokument MS Office.[344] Če ima

---

[342] Ker se med vohunske programe štejejo tudi nekateri spletni piškotki, je dejansko število vohunskih programov verjetno precej nižje; kljub temu statistike kažejo, da je pojav močno razširjen.

[343] Med vohunske programe naj bi spadale tudi nekatere različice programov *RealPlayer* (Macavinta, 1999) in *Windows Media Player* (Labriola, 2002). Podjetji RealNetworks in Microsoft sta zbirali podatke o tem, kakšne glasbene in video vsebine si ogledujejo potrošniki, nekateri pa so sumili, da se ti podatki povezujejo z elektronskimi naslovi. Microsoft je to sicer zanikal, ni pa dvoma, da so tehnične možnosti za kaj takega bile na voljo.

[344] Pozneje so v Microsoftu zaradi kritik izdali program, ki je zapisovanje GUID onemogočil in omogočil odstranjevanje le-tega. V programskem paketu Office 2000 se GUID ne zapisuje več v dokument, razen v primerih, ko dokument vsebuje makre.

uporabnik v svoj računalnik vgrajeno omrežno kartico, serijska številka te kartice postane del GUID, na podlagi tega pa je mogoče natančno ugotoviti, v katerem računalniku je dokument nastal (Lemos, 1999). Zaradi tega so se zastavila resna vprašanja, ali ni mogoče take tehnologije zlorabiti tudi v drugačne namene, ne samo za odkrivanje piscev virusov, temveč tudi političnih oporečnikov (Joel 1999). Zaradi teh razlogov direktiva EU 2002/58/EC[345] opozarja, da vohunski programi in skriti identifikatorji resno ogrožajo pravico do zasebnosti, in zato določa, da smejo biti uporabljeni le v zakonite namene in z vednostjo uporabnikov (24. točka predgovora k direktivi 2002/58/EC).

Upravljanje dostopa do digitalnih vsebin (DRM - Digital Rights Management)

Vsekakor je pričakovati, da se bo uporaba teh tehnik zbiranja osebnih podatkov še razmahnila, zelo verjetno v povezavi z željo glasbene, filmske in industrije programske opreme po učinkoviti zaščiti avtorskih pravic. Zaradi novih tehnoloških zmožnosti, ki jih povzroča hranjenje vsebin v digitalni obliki (predvsem enostavnost kopiranja), so se lastniki avtorskih pravic odločili uvesti tudi tehnično zaščito sicer pravno že avtorsko zaščitenih vsebin. Predvsem naj bi tehnologija omogočila nadzor nad uporabo avtorsko zaščitenih vsebih, stranski učinek takega nadzora pa je seveda zbiranje podatkov o potrošnji teh vsebin. To je mogoče uporabiti tudi za poznejše profiliranje uporabnikov in izvajanje naprednih tržnih prijemov.

DRM ali upravljanje dostopa do digitalnih vsebin je skupek tehnologij, ki naj bi omejile dostop in uporabo računalniških datotek oziroma digitaliziranih vsebin. To naj bi dosegli tako, da bi onemogočili anonimni dostop do digitalnih vsebin, poleg tega bi se vsak dostop do vsebine tudi zapisal.[346] Poglavna kritika DRM se zato nanaša na dejstvo, da njihovi razvijalci ne upoštevajo zaščite zasebnosti, čeprav so na voljo tehnične alternative, ki omogočajo zaščito pred nelegalnim kopiranjem in hkrati ščitijo zasebnost uporabnikov digitalnih vsebin (EPIC, 2004d).

Ni naključje, da so se tehnologije DRM najprej pojavile v programih za pregledovanje video in zvočnih digitalnih zapisov (npr. *Microsoft Windows Media Player*, ki uporablja GUID za sledenje uporabnikom in centralnemu strežniku sporoča, katere vsebine si ogleduje ali posluša uporabnik) ter elektronskih knjig (npr. *Microsoft eBook Reader* spremlja branje elektronskih knjig in omejuje njihovo kopiranje), v zadnjem času pa se uporabljajo tudi pri zaščiti programske opreme. Pomemben korak na tem področju je naredilo podjetje Microsoft, ki je za svoj operacijski sistem Windows Xp za domače uporabnike uvedlo obvezno aktivacijo izdelka.

---

[345] Direktiva 2002/58/EC o obdelovanju osebnih podatkov in varstvu zasebnosti na področju elektronskih komunikacij (Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector), sprejeta 12. julija 2002. Official Journal L 201, 31/07/2002 p. 0037 - 0047.

[346] Dostop je v tem primeru mišljen v širšem smislu – gre tako za ogled, tiskanje, kopiranje, spreminjanje ali druge oblike posegov do digitalnih vsebin ali vanje.

To poteka tako, da se ob namestitvi operacijskega sistema v del registracijskega ključa vgradi tudi informacija o strojni opremi (serijska številka procesorja, omrežne kartice, diska itd.). Če uporabnik operacijski sistem prekopira v drug računalnik ali če v svojem računalniku zamenja večji del strojne opreme, ob naslednji uporabi operacijski sistem ne bo več hotel delovati in bo zahteval vnovično aktivacijo.

Problem pa je, ker aktivacija podjetju omogoča, da osebne podatke posameznega kupca poveže z natančno določeno kopijo svojega izdelka in tudi z natančno določeno strojno opremo, ki jo ta uporablja, v končni fazi pa tudi z vsebinami (pravzaprav tudi z natančno določeno digitalno kopijo večpredstavne vsebine), ki jih konzumira. Pravzaprav so v Microsoftu skušali te podatke povezati tudi s svojima storitvama *Microsoft Passport* in *Microsoft E-Wallet*, ki vsebujeta podrobne osebne in finančne podatke o posameznikih,[347] vendar se njihovi načrti vsaj za zdaj niso uresničili.

Če bi (ali bo) načrt uspel, bi Microsoft v kratkem času verjetno lahko zbral najobsežnejšo zbirko osebnih podatkov na svetu, posebej še zato, ker ima možnost, da svoje storitve intenzivno oglašuje prek drugih svojih izdelov; to se je izkazalo že v primeru *Passporta*. Na to kažejo tudi izjave nekaterih uslužbencev podjetja v protimonopolnem postopku iz aprila 2002 (npr. izjave podpredsednika družbe Davida Colea), da je cilj podjetja ustvariti profile vseh uporabnikov interneta in na podlagi tega izvajati usmerjeno oglaševanje ter ponujati poosebljene storitve in poosebljen dostop do vsebin za uporabnike storitve Passport (EPIC, 2004f). Povezovanje teh podatkov s podatki o potrošnji večredstavnih in avtorsko zaščitenih vsebin pa bi seveda moč take zbirke še povečalo.

Zaupanja vredno računalništvo ('Trusted Computing')

Poenoteni in standardizirani postopki identifikacije in plačevanja prek interneta bi zagotovo pripomogli k hitrejšemu razmahu elektronskih storitev in razvoju elektronskega poslovanja, predvsem pa bi pripomogli k uveljavljanju naprednejših tržnih pristopov, ki temeljijo na zbiranju in analizi velikih količin osebnih podatkov. Vendar je v zadnjem času opaziti težnjo po povezovanju teh nadzornih tehnologij s področjem zaščite avtorskih pravic, pri čemer se zbiranje osebnih podatkov pogosto predstavlja kot nujnost zaradi zaščite avtorskih pravic, na "stranske učinke" profiliranja pa se pogosto 'pozablja'. V EPIC so zato zapisali, da "*te tehnologije označujejo pomemben razvojni mejnik v uporabi avtorskega prava... Avtorske pravice*

[347] Microsoft je nekaj časa razvijal skupino storitev, imenovano *Hailstorm*, vendar je nadaljnji razvoj trenutno negotov, saj so storitve naletele na številne negativne odzive tako v javnosti kot tudi pri ponudnikih storitev, poleg tega se je pojavilo vprašanje zakonitosti uvedbe teh storitev v EU. Šlo naj bi za ponujanje storitev, ki bi posamezniku na internetu omogočile identifikacijo, digitalno reprezentacijo in opravljanje storitev (predvsem nakupov). Microsoft jih je poimenoval *MyAddress*, *MyProfile*, *MyContacts*, *MyNotifications*, *MyInbox*, *MyCalendar*, *MyDocuments*, *MyApplicationSettings*, *MyWallet*, *MyUsage* in *MyLocation*, vse storitve pa seveda temeljijo na obsežnem zbiranju osebnih podatkov, ki bi se hranili v Microsoftovih strežnikih, prek katerih bi se potem posameznik identificiral ponudnikom različnih storitev. Del načrta za uvedbo teh storitev je tudi Microsoftova platforma, imenovana .NET, ki jo je Microsoft sicer že uvedel v novejše različice svojega operacijskega sistema (EPIC, 2002c).

se uporabljajo kot opravičilo tako za zaščito vsebine kot tudi za profiliranje potrošnikov vsebine" (EPIC, 2004d). Primer, ki ponazarja to težnjo, je t. i. zaupanja vredno računalništvo – (ang. *Trusted Computing*).

Zaupanja vredno računalništvo je ime za naslednjo generacijo računalniških okolij, v katera naj bi bilo vgrajeno upravljanje dostopa do digitalnih vsebin. S tem naj bi po eni strani učinkovito preprečili piratstvo, saj naj bi uvedli večji nadzor nad distribucijo digitalnih vsebin, stranski učinek sistema pa bo zbiranje velikih količin osebnih podatkov z namenom profiliranja in trženja. Ker naj bi to novo računalniško okolje zmoglo zaznavati piratske ali kako drugače nelegalne vsebine in tudi njihovo uničevanje (t. i. *tratitor tracing*), kritiki opozarjajo, da bo sistem mogoče zlorabiti tudi za cenzuro (Anderson, 2003). Poleg tega bo za uporabnika sistema težje narediti prehod s t. i. 'programske opreme TC' na konkurenčno programsko opremo, ponudniki digitalnih vsebin pa bodo lahko uporabljali različne poslovne modele za prodajanje svojih izdelkov in storitev (npr. prodaja vsebin, ki si jih bo mogoče ogledati samo nekajkrat ali samo ob določenih datumih itd.).

V praksi naj bi bilo zaupanja vredno računalništvo videti tako, da se bo v vsak računalnik vgradil poseben čip, imenovan čip Fritz.[348] Poleg strojne podpore bo tehnologija potrebovala še programsko podporo (posebej prirejen operacijski sistem – Microsoft za ta sistem uporablja delovno ime *Palladium* – in posamezne programske aplikacije, ki bodo digitalne vsebine zaščitile na podlagi informacij s čipa Fritz). Tako bo mogoče ugotoviti nekakšen digitalni podpis računalniškega okolja, v katerem se predvaja digitalna vsebina, na podlagi tega pa bo potem vsebina dostopna (ali pa tudi ne). Dodaten motiv za uvedbo te tehnologije, vsaj v podjetjih, pa bo zelo verjetno tudi možnost večjega nadzora nad dokumenti in elektronsko pošto, saj bo s tehnologijo TC mogoče za vsak dokument natančno omejiti, kdo ima do njega dostop in kdo ne in koliko časa je ta dostop omogočen. (Nekakšno zgodnjo različico te tehnologije vsebuje *Windows Server 2003*, imenuje pa se *Enterprise Rights Management*.)[349] Če ob tem upoštevamo še težnjo po povečevanju dela na domu, pa bo zelo verjetno možnost nadzora nad dostopom do dokumentov pomemben motiv za uvedbo tehnologije TC ne samo v poslovnih okoljih, temveč tudi doma.

---

[348] Čip so poimenovali po ameriškemu senatorju Fritzu Hollingsu, ki si je močno prizadeval za sprejetje zakona, ki bi zahteval obvezno vgradnjo takega čipa v vse elektronske naprave. Tehnologija pa se že uporablja. Prva različica takega čipa je bil poizkus izdelovalca procesorjev Intel, da funkcionalnost čipa Fritz vgradi v sam procesor. To so izvedli z zapisom serijske številke v procesorje Pentium III konec 90. let, še razširjena tehnologija DRM pa je vgrajena v procesorje Cell. Od maja 2002 so čipi Fritz vgrajeni v prenosnike IBM ThinkPad, nekatere značilnosti tehnologije TC pa so že vgrajene v operacijski sistem Windows Xp in igralno konzolo X-Box. Nekateri deli te tehnologije se uporabljajo tudi na drugih področjih, npr. od leta 1996 je podjetje Xerox začelo v svoje tiskalnike vgrajevati avtentikacijske čipe, s katerimi onemogočijo uporabo neoriginalnega tiskalniškega barvila v prahu. Nekateri izdelovalci mobilnih telefonov pa podobno onemogočajo uporabo neoriginalnih baterij (Anderson, 2003). Tehnologija TC danes še ni popolnoma uvedena, razen na nekaterih področjih oziroma pri nekaterih izdelkih. Po nekaterih ocenah je trenutno v fazi testiranja, v naslednjih letih pa lahko pričakujemo njeno postopno uvedbo na vsa področja elektronike.

[349] Bill Gates, lastnik podjetja Microsoft, je ob neki priložnosti izjavil, da so o tehnologiji TC začeli razmišljati zaradi problema glasbenega piratstva, nato pa so ugotovili, da je področje elektronske pošte in elektronskih dokumentov veliko bolj zanimivo (Anderson, 2003).

Tudi če se identifikacijski podatki strojne opreme ne bodo povezovali s točno določenim fizičnim lastnikom, pa bo zelo verjetno tako povezovanje možno prek nakupa digitalnih vsebin in programske opreme. Zaščita avtorskih pravic in nadzor nad dostopom do dokumentov pa bosta imela za posledico obsežno zbiranje osebnih podatkov o konzumentih digitalnih vsebin in uporabnikih dokumentov. V EPIC so zato zapisali, da "*'zaupanja vredno računalništvo' pomeni nadzorovano računalništvo*"[350] (EPIC, 2002b).

* * *

Zaradi marketinške zanimivosti osebnih podatkov se obseg zbiranja le-teh vse bolj povečuje. Poleg tega Allard in Kass ugotavljata, da so zbirke osebnih podatkov in *spletne (on-line)* dejavnosti čedalje bolj javno dostopne (Allard in Kass, 1997: 572). Resnici na ljubo je treba priznati, da bi popolno onemogočanje takega zbiranja podatkov precej zmanjšalo funkcionalnost spleta, verjetno pa tudi zaustavilo razvoj internetne ekonomije. Zato direktiva EU 2002/58/EC[351] tako zbiranje podatkov dovoljuje, vendar pod pogojem, da je uporabnik o tem zbiranju in uporabi zbranih podatkov ustrezno obveščen, poleg tega mora imeti možnost takšno obdelovanje odkloniti (Možina, 2002: 3). Pravzaprav se zdi, da je edina smiselna zaščita pred takim posegom v zasebnost strog nadzor nad zbiranjem in uporabo, to pa pravzaprav na neki način pomeni zgolj legitimizacijo uveljavljene prakse.

Informacijska zasebnost na internetu in država

Čeprav se obseg zbiranja osebnih podatkov s strani zasebnega sektorja povečuje, pa ne smemo pozabiti, da so države še vedno velik porabnik osebnih podatkov posameznikov. Na splošno so državne zbirke osebnih podatkov veliko bolj regulirane kot zbirke podjetij, vendar se je treba zavedati, da ima država vedno dostop tudi do zasebnih zbirk podatkov. Da bi bil ta dostop v praksi tudi zagotovljen, pa so države za nekatere vrste osebnih podatkov začele določati obvezen čas hranjenja teh podatkov (gre za t. i. retencijo, ang. *retention*). Evropska unija, ki je v 15. členu direktive EU 2002/58/EC najprej le omogočila hrambo prometnih podatkov v primeru varovanja nacionalne varnosti, preprečevanja, preiskovanja, odkrivanja in preganjanja kriminala ali neavtorizirane uporabe komunikacijskih sistemov, je leta 2005 kljub številnim protestom in zapletom sprejela *Direktivo o obvezni hrambi prometnih podatkov.*[352] Direktiva za razliko od

[350] V izvirniku: *"'Trusted' Computing Means Controlled Computing".*

[351] Direktiva 2002/58/EC o obdelovanju osebnih podatkov in varstvu zasebnosti na področju elektronskih komunikacij (Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector), sprejeta 12. julija 2002. Official Journal L 201, 31/07/2002 p. 0037 - 0047.

[352] Direktiva 2006/24/ES Evropskega parlamenta in Sveta z dne 15. marca 2006 o hrambi podatkov, pridobljenih ali obdelanih v zvezi z zagotavljanjem javno dostopnih elektronskih komunikacijskih storitev ali javnih komunikacijskih omrežij, in spremembi Direktive 2002/58/ES (Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC), sprejeta 14. 12. 2005. Official Journal L 105, 13/04/2006, p. 0054 - 0063.

prejšnje, ki je shranjevanje prometnih podatkov dovoljevala le kot izjemo, zahteva obvezno hrambo prometnih podatkov telefonskih in internetnih komunikacij (z naslovi elektronske pošte vred) ter podatkov o nahajališču mobilnih telefonov. Čas hrambe je od 6 do 24 mesecev, v nekaterih primerih pa tudi več, poleg tega direktiva ne omejuje, za katera kazniva dejanja je mogoče shranjene podatke uporabiti.

Čeprav ni dvoma, da so prometni podatki zelo pomembno orodje pri preiskovanju kaznivih dejanj, pa je problematika hranjenja prometnih podatkov v tem, da se tako vse uporabnike neke storitve obravnava kot morebitne kriminalce. Sicer je res, da so tako zbrani prometni podatki dostopni samo pooblaščenim na podlagi določenih pravil (npr. sodne odredbe), vendar so nasprotniki nadzorovanja že večkrat opozorili na problematičnost obstoja osebnih podatkov. Tako je npr. predstavnik ACLU spraševal, kako bi bilo, če bi država zahtevala, da so v vse hiše vgrajene nadzorne kamere, ki bi jih preiskovalci lahko uporabili, seveda le, če bi pridobili ustrezno sodno odredbo (ACLU, 1994).

Dejstvo je, da se nekaj podobnega že dogaja v primeru prometnih podatkov na internetu (v Sloveniji nekateri ponudniki dostopa do interneta določene prometne podatke hranijo praktično ves čas svojega obstoja) ter prometnih podatkov ponudnikov telekomunikacijskih storitev. Znan je primer britanskega telekomunikacijskega podjetja Virgin Mobile, ki je dve leti hranilo podatke o lokacijah uporabnikov (Wearden, 2001), obstaja pa sum, da se je že pred uveljavitvijo obvezne hrambe prometnih podatkov podobno dogajalo tudi v Sloveniji.[353] Pri tem pa se je treba zavedati, da nad ponudniki dostopa do interneta zaenkrat poteka bistveno manjši nadzor kot nad operaterji telefonskih komunikacij, zato je teže ugotoviti, v kolikšnem obsegu pri njih prihaja do zlorab prometnih podatkov. *Zakon o varstvu osebnih podatkov*[354] od upravljavcev zbirk

---

[353] Vrhovno sodišče RS je bilo v odločbi I Ips 292/2004 ter I Ips 264/2005 mnenja, da nekaterih prometnih podatkov, katerih zbiranje zakon dovoljuje (konkretno podatkov iz 2. odstavka 131. člena Zakona o telekomunikacijah (Uradni list RS, št. 30/01, 52/02-ZJA, 110/02-ZGO-1 in 43/04-ZEKom, ne velja od : 01. 05. 2004): številko ali identifikacijo kličočega in klicanega, naslov naročnika in tip terminala, skupno število obračunskih enot v obračunani periodi ter vrsto datum, čas in trajanje klica oziroma količine prenesenih podatkov) "*praktično ni mogoče evidentirati, ne da bi bilo razvidno, katera bazna postaja je klic zabeležila*" (Odločba Vrhovnega sodišča RS, št. I Ips 264/2005 ter št. I Ips 292/2004). Iz tega je mogoče sklepati, da bazna postaja samodejno sporoča nabor prometnih podatkov, katerega del operater potrebuje za potrebe obračunavanja. V tem paketu so očitno tudi lokacijski podatki. Dogodek, ki kaže na to, da slovenski operaterji morda hranijo prometne podatke, čeprav Zakon o elektronskih komunikacijah (Uradni list RS, št. 43/04 in 86/04 – ZVOP-1) v 104. členu zahteva, da je prometne podatke, ki se nanašajo na uporabnike, treba takoj, ko niso več potrebni za prenos sporočil, izbrisati ali spremeniti v brezosebno obliko (razen v primeru pisnega soglasja naročnika, zakonitega prestrezanja komunikacij in do poplačila storitve oziroma preteka zastaralnega roka), pa se je zgodil 2. oktobra 2004. Operater Simobil je takrat poslal večje število politično-reklamnih SMS sporočil, ki jih je 70.000 uporabnikov podjetja Mobitel dobilo po polnoči v času predvolilnega molka. Mobitel je zato svojim 70.000 uporabnikom, ki so sporočila prejeli po polnoči, poslal opravičilo. Vprašanje je, kako so v Mobitelu vedeli, kdo so bili prejemniki sporočila po polnoči? Kot kaže, je to tehnično mogoče le s shranjevanjem vsebine sporočil ali pa prometnih podatkov. Pri Mobitelu so zanikali, da zapisujejo vsebino SMS sporočil, posredno pa so potrdili, da zapisujejo prometne podatke: "*V družbi Mobitel smo v skrbi za naše uporabnike in z namenom zagotavljanja učinkovite pomoči našim uporabnikom morali reagirati in poslati obvestilo s pojasnilom uporabnikom, ki so prejeli SMS iz Simobilovega strežnika (iz številke 94420390) po polnoči s petka na soboto, ko je začelo veljati pravilo volilnega molka.*" (Mobitel, 2004). Konec koncev pa na to, da mobilni operaterji morda shranjujejo prometne podatke o vseh uporabnikih, kaže tudi primer Ranc, ko je policija dobila izpis klicanih in kličočih telefonskih številk novinarja (Laurant, 2003: 448).

[354] Zakon o varstvu osebnih podatkov (ZVOP-1), Uradni list RS, št. 86/04.

osebnih podatkov v Sloveniji zahteva, da za vsako zbirko osebnih podatkov zagotovijo katalog podatkov, podatke iz kataloga pa je treba posredovati ministrstvu za pravosodje, ki vodi katalog zbirk osebnih podatkov.[355] Pregled kataloga zbirk osebnih podatkov na spletni strani ministrstva za pravosodje konec julija 2002 je pokazal, da je od ponudnikov dostopa do interneta podatke o svoji zbirki osebnih podatkov ministrstvu posredoval samo en ponudnik dostopa do interneta, pozneje pa se mu je pridružil še eden. Še v začetku leta 2005 največji slovenski ponudnik dostopa do interneta Siol v katalog še vedno ni posredoval zahtevanih podatkov. Glede na to lahko upravičeno dvomimo, da ponudniki dostopa do interneta *Zakon o varstvu osebnih podatkov*[356] sploh poznajo, kaj šele da bi ga pri svojem delu upoštevali.

Kot rečeno, pa je poleg shranjevanja podatkov problematičen še dostop do tako shranjenih podatkov, saj je razumljivo, da bo do podatkov, ki so zbrani tako ali drugače, vedno mogoč dostop. Precej zgovoren primer, ki to dokazuje, se je zgodil leta 1997, ko je mornariški častnik Timothy McVeigh (ne gre za moža z istim imenom, ki je izvedel bombni napad v Oklahomi) ženi svojega sodelavca poslal povsem nedolžno elektronsko sporočilo. A ker je bila v njegovem elektronskem naslovu besedica 'boysrch', je prejemnica sporočila posumila, da je to okrajšava za "*boy search*" (slo. *iskanje fantov*). Zato je pogledala v njegov uporabniški profil pri njegovem ponudniku dostopa do interneta AOL in ugotovila, da je pod svoja zanimanja vpisal: "*vožnja, opazovanje fantov, iskanje slik o drugih mladih žrebcih*", v rubriko o stanu pa je vpisal, da je gej (Sykes, 1999: 76). O tem je obvestila mornarico in ta je takoj začela preiskavo, v okviru katere je preiskovalec poklical (pri tem se ni predstavil kot preiskovalec) AOL in zahteval identifikacijske podatke o uporabniku z uporabniškim imenom 'boysrch'. McVeigh je bil nemudoma odpuščen zaradi kršitve politike "*don't ask, don't tell*", saj je vojska trdila, da je z vpisom svojih interesov in stanu v svoj uporabniški profil sam javno priznal, da je gej. Nasprotno pa je McVeigh trdil, da je vpis teh podatkov v zbirko povsem zasebna zadeva in da je mornarica kršila *Electronic Communications Privacy Act*.[357] Kljub temu da so gejevski aktivisti skušali problem predstaviti kot vprašanje pravic gejev, pa je McVeigh vztrajal, da gre izključno za vprašanje zasebnosti. Posebej še zato, ker so poleg tega, da je njegovo zasebnost ščitil zakon ECPA,[358] ki določa, da ponudnik elektronske storitve lahko posreduje informacijo vladnemu uslužbencu samo na podlagi sodne odredbe ali pred sodiščem, tudi interna pravila AOL jasno določala, da AOL ne bo posredoval nikakršnih osebnih podatkov komurkoli, razen kadar to zahteva zakon. Barry Steinhard iz EFF je v zvezi s tem primerom izjavil, da "*izpostavlja to, kako enostavno informacija postane javna in kako enostavno je zlorabljena*" (Sykes, 1999: 77). McVeighu je na koncu sicer uspelo s pritožbo (primer *McVeigh proti Cohen*[359] iz leta 1998 (Turtington in Allen, 2002: 339)) in se je izognil nečastnemu odpustu iz vojske, kljub temu pa je njegov primer pokazal, da kljub zakonodajni

---

[355] Katalog zbirk osebnih podatkov je bil včasih javno dostopen na spletnih straneh ministrstva za pravosodje (<http://www.sigov.si/mp/>), danes pa je dostopen na spletni strani Informacijskega pooblaščenca <http://www.ip-rs.si/>.[356] Zakon o varstvu osebnih podatkov (ZVOP-1), Uradni list RS, št. 86/04.

[357] Electronic Communication Privacy Act of 1986, 18 U.S.C. (1986).

[358] Electronic Communication Privacy Act of 1986, 18 U.S.C. (1986).

[359] McVeigh v. Cohen, 983 F.Supp. 215 (1998).

zaščiti že sam obstoj zbirke podatkov pomeni morebitno grožnjo zasebnosti. Še bolj pa je to morda vidno na primeru Kitajske, kjer sicer ne gre za poseg v informacijsko zasebnost, temveč že za poseg v komunikacijsko zasebnost.

Julija 2004 je namreč več spletnih medijev poročalo, da se je Kitajska odločila cenzurirati sporočila SMS v realnem času. Domnevno so se za ukrep odločili, ker jim ob izbruhu bolezni SARS leta 2003 ni uspelo nadzorovati informacij o širjenju bolezni, čeprav so, kot navajajo poročila, zaradi širjenja 'neresničnih govoric' o SARS v sporočilih SMS leta 2003 priprli okrog ducat ljudi (Richardson, 2004). Kot uradni razlog za ta ukrep navajajo preprečevanje pošiljanja goljufivih in obscenih sporočil SMS. Tu ni problematična samo cenzura, temveč tudi način izvedbe cenzure. Kitajska je namreč razvila tehnologijo, ki vsa prestrežena sporočila SMS pregleda s posebnimi algoritmi, ki iščejo ključne besede ali kombinacije ključnih besed; poročila pa navajajo, da je v primeru pošiljanja določenih besed o lokaciji pošiljateljevega mobilnega telefona takoj obveščena najbližja policijska postaja (Lim, 2004).

Kitajski primer kaže na tehnične zmožnosti izvajanja množičnega nadzora v realnem času, velja pa poudariti, da so podobne projekte za zbiranje in analizo velikanskih količin (prometnih) podatkov financirali tudi v ZDA. Gre za projekte TIA (*Terrorist (Total) Information Awareness*), *LifeLog*, CAPPS II (*Computer Assisted Passenger Pre-screening System*) ter MATRIX (*Multistate Anti-TeRrorism Information eXchange*), ki so bili zaradi pritiskov javnosti opuščeni, čeprav obstaja sum, da se skrivaj še vedno razvijajo naprej. Ti sumi so se okrepili predvsem po razkritju, da je NSA, verjetno že sedem mesecev pred terorističnimi napadi 11. septembra 2001 (Harris, 2006), zbirala prometne podatke o telefonskih klicih več deset milijonov Američanov znotraj ZDA ter nad zbranimi podatki izvajala statistične analize (Page, 2006). Inteligentna analiza prometnih podatkov je bila tudi že predmet akademskih analiz. V študijskem letu 2004/2005 so na *Massachusetts Institute of Technology* v ZDA v okviru *Reality Mining Project* s posebnim programom, ki so ga namestili na mobilni telefon, z operacijskim sistemom Symbian devet mesecev zajemali podatke o uporabi mobilnih telefonov sto prostovoljcev. V okviru projekta so zbirali podatke o nahajališču mobilnega telefona, komunikaciji (kdo in kako pogosto komunicira s kom) ter bližini drugih (ob pomoči skeniranja prek *bluetooth* povezave). Podatki so razkrili vzorce vsakdanjega vedenja uporabnikov, analiza podatkov pa je raziskovalcem omogočila, da s 85-odstotno natančnostjo predvidijo, kaj bodo uporabniki storili v naslednjem trenutku (MIT, 2005 ter Singel, 2005). Seveda ni trajalo dolgo, ko je nastal tudi tak komercialni izdelek. Aprila 2006 so namreč ponudili prvi vohunski program za mobilne telefone z operacijskim sistemom Symbian, Flexispy.A. Vohunski program shranjuje prometne podatke o klicih in sporočilih SMS ter vsebino sporočil SMS, podatke pa shranjuje v strežnik podjetja Flexispy. Programa ni mogoče odstraniti brez posebnega gesla (Niemelä in Heikkilä, 2006). Podjetje svoj izdelek oglašuje kot pripomoček za zakonske partnerje, ki sumijo, da jih partner vara, ter kot pripomoček za starše, ki želijo svoje otroke zaščititi pred škodljivimi sporočili SMS. Naročniki Flexispyevih storitev lahko vsebino prestreženih podatkov pregledujejo prek spletnega vmesnika (Flexispy, 2006).

To vse že kaže na nevarne težnje v razvoju nadzorovalnih tehnologij, ki so – pa ne v prihodnosti, temveč očitno že danes – zmožne izvajati množični nadzor v realnem času.

Komunikacijska zasebnost na internetu

Kot je bilo prikazano že v prejšnjih poglavjih, je varstvo komunikacijske zasebnosti bistveno bolje pravno varovano kot varstvo informacijske zasebnosti. Razlog je v tem, da ima uporaba prisluškovanja pri preiskovanju kaznivih dejanj že dolgo tradicijo, poleg tega pri prisluškovanju posamezniki veliko jasneje razumejo posledice vdora v zasebnost kot pri drugih oblikah nadzorovanja. Ne nazadnje pa je v praktično vseh demokratičnih državah izrecno prepovedano tudi prisluškovanje s strani zasebnikov. Izjema je le nadzor komunikacij na delovnem mestu, kjer v ZDA veljajo 'milejša' pravila (milejša za delodajalca) kot v Evropi, saj je načeloma dovoljen nadzor službenih komunikacij; poleg tega se v Evropi uveljavlja načelo, ki prepoveduje nesorazmerne prepovedi komuniciranja z zunanjim svetom (Klemenčič, 2002: 395).

Kljub temu internetne komunikacije predstavljajo nekakšno specifiko, to pa zato, ker je prestrezanje elektronskih, še posebej tekstovnih komunikacij mogoče povsem avtomatizirati, poleg tega je tako prestrezanje tudi povsem nezaznavno. Tudi tu tehnologija nastopa v vlogi pospeševalca nadzora. Dodaten problem pa je tudi dejstvo, da je za razliko od klasičnega prisluškovanja, ki je navadnim posameznikom praktično onemogočeno (poleg prisluškovalne opreme, ki je ni mogoče kupiti na prostem trgu,[360] posameznik potrebuje še ustrezno tehnično znanje in dostop do komunikacijskih vodov), prestrezanje internetnih komunikacij bistveno enostavnejše in v osnovi omogočeno praktično vsakomur, saj so orodja za prestrezanje internetnega prometa prosto dostopna.

Začetki državnega nadzora elektronske pošte

Eden prvih odmevnih primerov, ki je opozoril na problematiko prestrezanja elektronske pošte, je bil primer *Steve Jackson Games, Inc. proti United States Secret Service*.[361] 1. marca 1990 je namreč ameriška tajna služba (*Secret Service*) v okviru operacije Sundevil[362] zaplenila BBS *Illuminati* (BBS je kratica za *Bulletin Board System*, omrežje računalnikov, ki so omogočali izmenjavo elektronske pošte in datotek, so pa delovali večinoma mimo interneta) podjetja *Steve Jackson Games*. Razlog za zaplembo strežnika, v katerem je bilo tudi 162 neprebranih e-poštnih sporočil, je bil ta, da je uslužbenec podjetja Loyd Blankenship, znan tudi pod hekerskim imenom *The Mentor,* pomagal pri distribuciji Phrack magazina, ki je objavil zaupni dokument; ta je opisoval ameriški sistem za ugotavljanje nahajališča klicatelja v primeru klicev v sili. Ker je s sistemom Illuminati upravljal Blankenship in ker naj bi bila kopija zaupnega dokumenta

---

[360] Opremo za prestrezanje telefonom GSM med drugim prodaja tudi neko podjetje iz Južnoafriške republike. Na povpraševanje po ceniku pa sem dobil odgovor, da ponudbe pošiljajo samo preiskovalnim organom in državnim agencijam, torej teh naprav posameznik ne more kupiti (SPY, 2004).

[361] Steve Jackson Games, Inc. v. United States Secret Service, 36 F.3d 457 (1994).

[362] Operacijo Sundevil so izvedli leta 1990 in velja za eno najobsežnejših protihekerskih operacij v ZDA, potekala je v 13 zveznih državah. V okviru operacije so ameriški preiskovalci preiskovali številne goljufije s kreditnimi karticami, telefonske zlorabe ter krajo dokumenta, ki je opisoval sistem za ugotavljanje lokacije klicatelja v primeru klicev v sili E911. Dokument je v 24. številki objavila hekerska revija Phrack.

dostopna na BBS sistemu podjetja Steve Jackson Games (dokumenta pozneje v preiskavi niso našli), je tajna služba zaplenila računalnik in več disket podjetja, ki s krajo dokumenta ni bilo povezano. Pozneje se je izkazalo, da so pregledali in izbrisali tudi elektronsko pošto vseh drugih uporabnikov (Turkington in Allen, 2002: 329–333), ki niso bili osumljeni ničesar.

Lastnik zaplenjenega strežnika se je pritožil in sodišče je v primeru *Steve Jackson Games, Inc. proti United States Secret Service*[363] ugotovilo, da pri zaplembi strežnika ni šlo za prestrezanje elektronske pošte, temveč za zaseg. V tem so nekateri videli nižanje standardov za zakoniti dostop do elektronske pošte (Kennedy, 1993), saj za prestrezanje komunikacij v ZDA veljajo višji standardi kot za zaseg. Vendar pa je sodišče ugotovilo, da je zaplemba in uničenje elektronske pošte uporabnikov, ki niso ničesar osumljeni, uporabljajo pa isti strežnik kot osumljenec, kršitev in zato nedopustna. Eden izmed odvetnikov, ki je zastopal tožnika, je zapisal, da je tajna služba "*ignorirala zakonite pravice posameznikov, ki niso bili osumljeni zločina, temveč so si samo delili skupni elektronski prostor [z osumljencem]... Bližina ljudi, ki bivajo v kiberprostoru, pomeni, da mora vlada najti nove načine za vodenje preiskav, da ne bi pri tem kršila pravice drugih nedolžnih članov spletne skupnosti*" (Kennedy, 1993).

Primer Enron

Podobno vprašanje – vprašanje pravic posameznikov, ki so si delili isti virtualni prostor, pa se zastavlja tudi v primeru preiskave proti ameriškemu podjetju Enron. (Šlo je za enega večjih finančnih škandalov v ameriški zgodovini.) V okviru preiskave proti podjetju je namreč ameriška *Zvezna komisija za regulacijo energetike* (ang. *Federal Energy Regulatory Commission*) na svoji spletni strani objavila elektronsko pošto vseh uslužbencev Enrona. Elektronska pošta – šlo je tako za poslovna kot tudi za zasebna sporočila – je bila povsem javno dostopna vsakomur. Pozneje so jo kupili raziskovalci na MIT z namenom opravljanja statističnih analiz, predvsem analize socialnih omrežij. Eden izmed raziskovalcev, William W. Cohen, je na spletni strani projekta *Cognitive Assistant that Learns and Organizes*, ki se ukvarja z analizo teh podatkov, zapisal: "*Ti podatki so dragoceni; po mojem vedenju gre za edino obsežno zbirko 'pravih' elektronskih sporočil, ki je javna. Druge niso javne zaradi zadržkov glede zasebnosti*" (Cohen, 2004). Podatki, ki jih je mogoče prenesti z iste spletne strani, so prečiščeni. To pomeni, da so odstranjene datotečne priloge, nekaj sporočil pa je bilo odstranjenih zaradi zahtev nekdanjih uslužbencev Enrona. Kljub temu okrog 400 Mb velika zbirka obsega kar 517.431 elektronskih sporočil 151 uslužbencev podjetja (Shetty in Adibi, 2004).

Ne glede na to, da imajo podatki veliko vrednost za raziskovalce in preiskovalce, pa je njihova javna objava nevaren precedens, saj so preiskovalci očitno presodili, da pomeni zagotavljanje transparentnosti poslovanja podjetij prevlado nad pravico vseh v njih zaposlenih posameznikov do zasebnosti.

[363] Steve Jackson Games, Inc. v. United States Secret Service, 36 F.3d 457 (1994).

Primer GMail ter Združene države proti Bradford C. Councilman[364]

Zaradi marketinške zanimivosti osebnih podatkov člani organizacije *Privacy Rights Clearinghouse* ugotavljajo, da se njihovo zbiranje, predvsem informacij o obisku spletnih strani, povečuje (Privacy Rights Clearinghouse, 1998). Seveda ni presenetljivo, da zato številne iskalnike financirajo marketinška podjetja (Data Protection Working Party, 2000: 18). Vendar pa so za tržnike zanimiva tarča tudi ponudniki brezplačnih elektronskih naslovov. Nekateri ponudniki v zameno za "brezplačno" storitev uporabnikom tu in tam pošiljajo reklamna elektronska sporočila, drugi jim prikazujejo reklamne oglase, vendar pa pomeni resnejšo nevarnost možnost razkritja oziroma prodaje elektronskega naslova posameznika (Data Protection Working Party, 2000: 36). Pri tem gre lahko tako za elektronski naslov uporabnika kot za elektronski naslov, na kateri se posreduje prejeta pošta (če ga uporabnik vpiše), lahko pa tudi za adresar, v katerem uporabnik hrani elektronske naslove tistih, s katerimi si dopisuje.

Vendar pa je leta 2004 podjetje Google šlo še korak dlje. Prvega aprila 2004 so namreč napovedali novo storitev, ki so jo poimenovali GMail. Primer je zanimiv zato, ker je z njim Google postavil nove standarde brezplačne elektronske pošte, poleg tega pa Gmail postaja največji ponudnik brezplačne elektronske pošte na svetu. V okviru svoje storitve je namreč Google ponudil brezplačne elektronske naslove, vsak uporabnik pa je na začetku imel v svojem poštnem predalu na voljo 1 Gb prostora, kasneje pa so kapaciteto še povečali. Že to je velika konkurenčna prednost v primerjavi z drugimi ponudniki brezplačne elektronske pošte, ki so dotlej ponujali od 10 do 20 Mb prostora. Poleg tega je Google napovedal uporabo dobrih protismetnih (*antispam*) filtrov ter možnost naprednega iskanja po arhivu sporočil. Sporočila je mogoče razvrščati v različne kategorije, posamezno sporočilo tudi v več kategorij. Iskalnik upošteva sosledje sporočil, ključne besede, povezanost med kategorijami itd. S tem naj bi tudi odpadla potreba po brisanju sporočil, saj zaradi velike količine prostora, ki je na voljo, uporabniki lahko shranjujejo praktično vsa sporočila, ki jih dobivajo; z vgrajenim iskalnikom pa se med njimi tudi povsem enostavno znajdejo. (GMailov reklamni slogan celo govori o tem, da sporočil ni več treba brisati, temveč naj jih uporabniki le arhivirajo.)

Vendar pa so se kmalu po napovedi nove storitve oglasile številke kritike. Kritiki so poudarjali možnost, da bo Google, ki je v ameriški lasti, nekoč v prihodnosti imel arhiv praktično vseh elektronskih sporočil na svetu (Privacy International, 2004: 2). To je ob dejstvu, da se obseg komuniciranja po elektronski pošti povečuje, lahko zaskrbljujoče. Poleg tega pa obstaja nevarnost, da bo podjetje Google zaradi želje po dobičku oz. možnosti nemotenega poslovanja bolj občutjivo na pritiske posameznih vlad. Tako se je Google leta 2006 že uklonil cenzorskim pritiskom Kitajske (BBC News, 2006b). Kritiki so tudi poudarjali, da ne gre samo za odnos med uporabnikom in ponudnikom brezplačne elektronske pošte, temveč je treba upoštevati tudi pravice tretjih oseb. To pa je lahko posebej problematično, ker Google tudi nad dohodno elektronsko pošto izvaja napredne statistične analize in izkopavanje podatkov (t. i. *data mining*),

[364] United States of America v. Bradford C. Councilman, No. 03-1383 (1st Cir., June 29, 2004).

pošiljatelji elektronske pošte v sistem Gmail pa s tem niso niti seznanjeni, kaj šele da bi k taki obdelavi dali soglasje.

GMail pošto preiskuje in analizira z namenom odstranjevanja smetja, virusov ter *prikazovanja usmerjenih oglasov*, pri čemer pa prikazovalnik oglasov upošteva tudi fizično lokacijo uporabnika[365] (Privacy International, 2004: 3). Res pa je, da je to preiskovanje avtomatično in ne vključuje človeške intervencije. Google je na kritike odgovoril, da ne kršijo pravic pošiljateljev, saj njihove pošte ne bere nihče drug razen prejemnika, oglase pa vidi samo prejemnik (Google, 2004a). Dejstvo pa je, da gre pri preiskovanju dohodne pošte za obdelavo podatkov, za to pa bi po mnenju borcev za zasebnost Google potreboval soglasje tako prejemnika kot tudi pošiljatelja. To je bil tudi eden poglavitnih očitkov GMailu, saj Googlovi splošni pogoji uporabe veljajo tudi za dohodno pošto, torej jim zapade tudi pošta tistih uporabnikov, ki uporabljajo druge poštne račune in svoja elektronska sporočila pošiljajo uporabnikom GMaila. Google sicer trdi, da se vsakdo lahko odloči, da v GMail ne bo pošiljal elektronske pošte, vendar je to v praksi skoraj povsem neizvedljivo. Prav tako so v svojem odgovoru na kritike zapisali, da preiskovanje za smetjem in računalniškimi virusi ter samodejno razvrščanje, označevanje in pretvorbo sporočil izvajajo vsi ponudniki elektronske pošte. To sicer drži, vendar pa je GMail stopil korak naprej in razvil tehnologijo za prikazovanje oglasov na podlagi analize vsebine elektronskih sporočil. Komisija *Data Protection Working Party* je v dokumentu *Privacy on the Internet – An integrated EU Approach to On-line Data Protection* novembra 2000 zapisala, da "*če je prestrezanje izvedeno na centralnem vozlu ali križišču na internetu, to omogoča prestrezanje in nadzor elektronske pošte ali prometnih podatkov v velikem obsegu*" (Data Protection Working Party, 2000: 34), zato je po mnenju Daviesa iz *Privacy International* lahko problematično že pregledovanje elektronske pošte za smetjem, kot je to določeno v 4. členu Googlovih splošnih pogojev rabe (Privacy International, 2004).

Poleg tega so v *Electronic Frontier Foundation* opozorili na možnost, da Google podatke iz storitve GMail poveže z iskalnimi navadami posameznika, saj je GMail na Googlovi in ne na svoji domeni (gmail.google.com).[366] Poleg tega pa je Google povezan tudi s sistemom za vzpostavljanje *spletne (on-line)* skupnosti Orkut.[367] Google bi to lahko storil prek piškotkov, s katerimi že zdaj spremlja iskalne navade svojih uporabnikov (EFF, 2004), pri čemer Googlovi piškotki potečejo šele leta 2038. Sicer so predstavniki Googla zatrdili, da GMaila ne bodo uporabljali za ugotavljanje iskalnih navad v Googlu, vendar tega v svoji izjavi o zasebnosti in splošnih pogojih uporabe niso jasno zapisali (EFF, 2004), kot izhaja iz njihovih splošnih

---

[365] Gre za prikazovanje t. i. geografsko usmerjenih oglasov (ang. *geographically targeted ads*). Prikazovalnik oglasov najprej na podlagi vsebine ugotovi, katere usmerjene oglase lahko prikaže, med njimi pa izbere tiste, ki ponujajo storitve, ki so prejemniku oglasa geografsko najbliže. Oglaševanje je torej mogoče usmeriti glede na vsebino, ki jo posameznik konzumira, na posamezno geografsko področje ali na kombinacijo obojega.

[366] Pa tudi, če bi bil na lastni domeni, bi bilo mogoče s spletnimi hrošči podatke o iskalnih navadah povezati z računom GMail.

[367] Sistem za izgradnjo *spletne (on-line)* skupnosti oziroma socialnega omrežja Orkut je dostopen na <http://www.orkut.com>. Namenjen je vzpostavitvi prijateljskih omrežij, člani omrežja pa se lahko virtualno srečujejo in družijo ter si izmenjujejo informacije. Orkut je delo inženirja, zaposlenega pri Googlu.

pogojev, pa se le-ti lahko kadarkoli spremenijo. Simon Davies iz *Privacy International* opozarja, da bi morala taka storitev imeti bolj dolgotrajno in stabilno zaščito. Poleg tega se Google v svoji pogodbi odvezuje vsakršne odgovornosti glede varnosti storitve, kar je v nasprotju z direktivo EU o zaščiti osebnih podatkov (95/46/EC[368]). Google tudi ni podpisal *sporazuma Safe Harbour* (Privacy International, 2004: 10), v 7. členu svojih splošnih pogojev rabe pa od posameznikov zahteva, da se strinjajo s prenosom svojih osebnih podatkov v ZDA ali katerokoli državo, v kateri ima Google podružnice.

Google sicer trdi, da ima vsakdo možnost, da njihovih storitev ne uporablja, če se ne strinja z njihovimi pogodbenimi določili. Vendar pa je, kot je ugotovil že Deleuze, v družbi nadzora to precej jalov argument. Posameznik ima namreč na voljo samo sprejetje pogojev, v katerih je nadzorovan, ali pa izključitev – gre torej za vsiljeno izbiro. Pri tem se zastavlja tudi vprašanje, ali za GMail velja samo ameriška zakonodaja in ali se posameznik lahko s pogodbo odpove nekaterim svojim pravicam. Odgovor na to vprašanje je morda podala komisija *Data Protection Working Party* v dokumentu *Working document on determining the international application of EU data protection law to personal data processing on the Internet by non-EU based web sites* z dne 30. maja 2002, ko je obravnavala prenos zakonodaje Evropske unije na internet. V dokumentu so izrazili stališče, da zakonodaja EU velja tudi za spletne strani zunaj EU, če jih uporabljajo državljani EU.[369] *Data Protection Working Party* je zato predlagala, da v konkretnih primerih organi držav članic EU najprej ugotovijo, ali zanje veljajo direktive EU, in če je tako, stopijo v stik s spletno stranjo in skušajo sporazumno rešiti problem. Ob morebitnem neuspehu pa predlagajo, da o zadevi odloči sodišče države članice, kjer stanuje posameznik, ki je sprožil postopek (Data Protection Working Party, 2002: 15). S tem stališčem pa je v nasprotju 13. člen Googlovih splošnih pogojev rabe, ki pravi, da se pogodbena partnerja strinjata, da se pogodba tolmači po zakonih ameriške zvezne države Kalifornija, posameznik pa se strinja, da vsi pravni postopki v zvezi s temi splošnimi pogoji zapadejo pod jurisdikcijo kalifornijskih sodišč.[370]

Google si tudi pridržuje pravico, da na zahtevo vlade ali če ugotovi, če posameznik krši pogodbo z njim (Google govori o preiskovanju *potencialnih* kršitev (ang. *investigation of potential violations*)), preišče posameznikovo uporabo storitve; to zajema pravico dostopa do kakršnekoli informacije in razkritja le-te (3., 4. in 7. člen Googlovih splošnih pogojev rabe (Google, 2004b)). Vsaj slednje

---

[368] Direktiva 95/46/EC o varstvu posameznikov pri obdelovanju osebnih podatkov in svobodnem pretoku teh podatkov (Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data), sprejeta 24. oktobra 1995. Official Journal L 281, 23/11/1995 p. 0031 - 0050.

[369] Ameriški *Children's Online Privacy Protection Act* (Children's Online Privacy Protection Act of 1998, 15 U.S.C. (1998)) tako ne velja samo za ameriška podjetja, temveč za vsa 'podjetja na internetu' (Data Protection Working Party, 2002: 4); poleg tega je bilo v preteklosti že nekaj primerov, ko so posamezne države (med drugim tudi Slovenija v primeru udba.net) omejile dostop do določenih spletnih strani v tujini.

[370] Zastavlja se tudi vprašanje, kaj bi se zgodilo, če bi ameriški preiskovalni organi zahtevali podatke iz kakšne neameriške Googlove podružnice. Oktobra 2004 je ameriško zvezno sodišče podjetju Rackspace (ameriški ponudnik dostopa do interneta, ki ima podružnico tudi v Veliki Britaniji) izdalo sodno odredbo, v kateri je zahtevalo, naj jim izroči enega izmed strežnikov neodvisnega internetnega medija Indymedia, ki se je nahajal v Veliki Britaniji. Podjetje je zahtevo izpolnilo (Indymedia, 2004).

je v nasprotju s 5. členom direktive EU o zasebnosti telekomunikacij 97/66/EC,[371] pa tudi druga določila po mnenju Daviesa puščajo odprte možnosti za zlorabe, saj ameriški preiskovalni organi na podlagi USA PATRIOT Act[372] lahko v nekaterih primeri pridejo do teh podatkov tudi brez sodne odredbe.

Google si v 11. členu splošnih pogojev rabe pridržuje pravico, da kadarkoli in iz kakršnegakoli razloga uporabniku odtegne ponujene storitve, v njihovem sistemu pa lahko ostanejo ostanki kopij informacij (ang. *residual copies of information*). To so si kritiki razlagali, kot da čas hrambe osebnih podatkov ni natančno definiran. Google je v odgovor zapisal, da podatki nekaj časa ostanejo v sistemu, ker GMail shranjuje varnostne kopije podatkov v različne strežnike, in da si bodo prizadevali ob prekinitve pogodbe podatke čim prej izbrisati iz svojega sistema (Google, 2004a). Vendar je sistem že zasnovan tako, da se lahko hrani vsa pošta uporabnika (in Google to oglašuje kot svojo prednost). Brisanje pošte pa je precej bolj zapleteno kot t. i. arhiviranje, saj je sporočilo treba premakniti v koš, nato pa ga izbrisati še iz koša, sicer določen čas ostane v košu in ga je mogoče obnoviti. Mimogrede se torej lahko zgodi, da bo imelo veliko število uporabnikov na neki osrednji točki shranjeno svojo celotno e-poštno zgodovino. Kritiki zato opozarjajo na leta 1986 sprejeti ECPA,[373] ki preiskovalcem v sekciji 2703 omogoča, da do elektronske pošte, shranjene v javnem sistemu več kot 180 dni, lahko pridejo na podlagi sodnega poziva (t. i. *subpoena*) ali na podlagi naloga brez obvestila (ang. *warrant without notice*) (Banisar, 1994). Dodatna vprašanja je - vsaj za krajši čas, dokler odločitev ni bila revidirana - odprla razsodba ameriškega prizivnega sodišča prvega okrožja v primeru *Združene države proti Bradford C. Councilman*[374] iz junija 2004.

Na začetku leta 1998 je podjetje *Interloc*, ki je svojim strankam ponujalo brezplačne elektronske naslove, začelo skrivaj spremljati vso elektronsko pošto, ki so jo njihove stranke dobivale od knjigarne Amazon. Podjetje *Interloc* se je namreč ukvarjalo tudi s prodajo knjig, Amazon pa jim je bil konkurenca. Zato je podjetje skušalo z analizo elektronske pošte, ki so jo dobivale njihove stranke od Amazona, pridobiti konkurenčno prednost. Podjetje je bilo obtoženo kršitve ECPA, vendar je prizivno sodišče prvega okrožja 29. junija 2004 presodilo, da ni šlo za kršitev, saj elektronska pošta ni bila prestrežena med prenosom, temveč so jo zasegli v svojih računalnikih (z diska ali iz pomnilnika), tega pa ECPA ne prepoveduje (Zetter, 2004c). S tem so tudi zavrnili argumente tožnika, da je za prestrezanje dovolj že to, da nekdo pridobi sporočilo, ki se prenaša, pa čeprav se prenaša tako, da se vmes tudi začasno shrani. Sodnik Lipez je v ločenem negativnem mnenju zapisal, da se elektronske komunikacije na internetu pogosto hkrati prenašajo in so shranjene (shranjene so vsaj v delovnem pomnilniku računalnika), shranjevanje

---

[371] Direktiva 97/66/EC o obdelavi osebnih podatkov in varstvu zasebnosti v telekomunikacijskem sektorju (Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector), sprejeta 15. decembra 1997. Official Journal L 024, 30/01/1998 p. 0001 - 0008.

[372] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001, 18 U.S.C. (2001).

[373] Electronic Communication Privacy Act of 1986, 18 U.S.C. (1986).

[374] United States of America v. Bradford C. Councilman, No. 03-1383 (1st Cir., June 29, 2004).

pa je bistveni del procesa prenašanja. Ker drugi sodniki njegovih argumentov niso sprejeli, je Lipez sklenil, da se bodo preiskovalci zaradi tako ozko razumevanega zakona v prihodnje verjetno posluževali pomoči ponudnikov e-poštnih storitev pri prestrezanju elektronske pošte in ne bodo več iskali sodne odredbe. To bo po njegovem mnenju privedlo do pomembnega zmanjšanja pravice do zasebnosti. Menil je, da bi preiskovalci lahko isto načelo uporabili tudi za prisluškovanje zvočnim komunikacijam, saj bi lahko zvočno komunikacijo zasegli, ko bi se začasno shranila na usmernikih telefonskih podjetij.[375] Primer je vsekakor postavil temelje nevarnemu precedensu, a je prizivno sodišče prvega okrožja na srečo zagovornikov zasebnosti zadevo pozneje obravnavalo še enkrat v polni sestavi (tim. *En Banc*) in avgusta 2005 zavzelo nasprotno stališče, da je prestrezanje začasno shranjenega elektronskega sporočila kršitev zakona. Kljub temu je sodnik Juan Torruella izrazil ločeno negativno mnenje, da ECPA v prvem poglavju ne velja takrat, kadar gre za shranjevanje, pa čeprav to shranjevanje traja le nekaj milisekund.[376]

Nastanek GMaila in tehnologije, ki stoji za njim, sta vsekakor odprla številna vprašanja glede zasebnosti. Zato je 20. aprila senatorka Liz Figueroa vložila predlog zakona, ki bi od ponudnikov elektronske pošte zateval, naj pridobijo soglasje tako od prejemnika kot od pošiljatelja, preden lahko preiskujejo njihovo elektronsko pošto in na podlagi analize prikazujejo oglase; vendar so poznejši amandmaji, vloženi nekaj dni po predstavitvi zakona, izločili soglasje. Predlagateljica zakona je v javnem pismu, objavljenem junija 2004, zapisala, da ni problem Google, temveč tehnologija: "*Ko bo Googlova zamisel splošno sprejeta, bodo druga manj ugledna podjetja razvila podobno tehnologijo in z njo počela stvari, ki jih Google ne bi počel. Podrobni osebni dosjeji, narejeni na podlagi vsebine elektronske pošte, bi bili lahko – na podlagi sedanje zakonodaje – narejeni in prodani komurkoli. To je brez primere.*" (Figueroa, 2004).
Na argument, da gre samo za računalniško pregledovanje in da nadzora ne izvajajo ljudje, pa je odgovorila, da "*če zmaga argument 'saj je samo stroj', ne bo noben del in prostor vašega življenja varen pred radovednimi očmi takih naprav*" (Figueroa, 2004).

Poleg tega je mogoče videti tudi nekaj vzporednic med Googlovo tehnologijo in tehnologijo določanja lokacije uporabnikov mobilnih telefonov. Etzioni namreč navaja, da je FBI v ZDA več časa skušal prepričati operaterje mobilnih komunikacij, da bi mu omogočili lociranje uporabnikov mobilnih telefonov. Podjetja so razvoj te tehnologije zavračala, sklicujoč se na argument zasebnosti (Etzioni, 1999: 130). Potem pa je to tehnologijo začel zahtevati trg. Operaterji so zaslutili, da bi bilo mogoče storitev določanja lokacije tržiti in so tehnologijo razvili sami. Sredi leta 2006 je drugi največji ponudnik mobilne telefonije v ZDA, podjetje Verizon, začelo tržiti storitev sledenja uporabnikom mobilnih telefonov. Sistem je zaenkrat namenjen staršem, ki želijo spremljati, kje se gibljejo njihovi otroci. Sistem omogoča, da se lokacija mobilnega telefona otroka izriše na zemljevidu (na računalniku ali na mobilni napravi), mogoče pa je nastaviti

[375] United States of America v. Bradford C. Councilman, No. 03-1383 (1st Cir., June 29, 2004), strani 44-45.
[376] United States of America v. Bradford C. Councilman, 385 F.3d 793 (1st Cir. 2004). Kopija odločitve je dostopna na naslovu <http://www.ca1.uscourts.gov/pdf.opinions/03-1383EB-01A.pdf>.

tudi prostorsko območje, po katerem se uporabnik lahko giblje. Če uporabnik območje zapusti, sistem o tem obvesti naročnika storitve s sporočilom SMS (Reuters, 2006). Podobno je bilo tudi na internetu zaznati velik odpor proti programom ameriške DARPE *TIA*, *MATRIX* in *LifeLog*. Kritiki so trdili, da so programi, ki omogočajo samodejno zbiranje in analizo velikanskih količin podatkov, tehnologija Velikega brata. A ko je nastal Googlov komercialni in z vlado nepovezan GMail, je bila ta tehnologija kljub kritikam razmeroma dobro sprejeta,[377] Googlovi oglasi pa celo veljajo za najmanj invazivne.

Prestrezanje podatkov po omrežju

Prestrezanje komunikacij je v internetu tehnično precej enostavnejše kot npr. v telefonskih omrežjih, poleg tega so prestrezna orodja prosto dostopna in na voljo praktično komurkoli. Prestrezanje podatkov v omrežju je v računalniških omrežjih podobno prisluškovanju v telefonskem omrežju, toda z veliko razliko, ki je zelo pomembna tudi pri državnem prestrezanju, o čemer smo delno že govorili pri obravnavi ameriškega sistema za nadzor interneta Carnivore.

Internetni protokol (IP), ki določa način prenašanja podatkov po internetu, namreč ne predvideva stalne povezave med dvema točkama (gre za t. i. *brezpovezavni (*ang. *connectionless) protokol.*) Komunikacija se razdeli na paketke, ki potem vsak posebej potujejo po omrežju do ciljnega naslova, paketki pa lahko do cilja potujejo po različnih poteh. Iz tega sledi, da je mogoče prestrezanje prometa npr. točno določenega osumljenca izvesti le tako, da se prestreže vsak paketek in ugotovi, ali je del osumljenčeve komunikacije ali ne. Tehnično je torej mogoče izvesti zakonito prestrezanje prometa posameznega osumljenca v internetu zgolj tako, da se prestrežejo vsi podatki, s filtriranjem pa se potem izloči paketke, ki sestavljajo promet osumljenca, druge pa zavrže. Po tem se bistveno razlikuje od prestrezanja glasovnih komunikacij, pri čemer je mogoče prestrezanje omejiti samo na telefonski priključek osumljenca, pri paketnih omrežjih pa je treba prestreči vsak podatkovni paketek in zanj ugotoviti, ali je del komunikacije, ki jo preiskovalci želijo prestrezati oziroma imajo sodno odredbo zanjo. V čem je nevarnost zlorabe, je očitno, saj je teoretično vedno možno, da bo prestrezna naprava shranjevala več, kot je zakonsko dovoljeno. Ta nevarnost je seveda večja pri t. i. zaprtih (ang. *black-box*) napravah, s katerimi upravljajo preiskovalci in tajni agentje sami, brez sodelovanja ponudnika dostopa do interneta in brez zunanjega neodvisnega nadzora (več o tem v Branch, 2003). Četudi je taka zloraba nezakonita, pa jo je težko zaznati in to v praksi seveda povečuje možnost, da pride do nje.

Tehniko prestrezanja paketkov (ang. *packet sniffing*) pa so še pred preiskovalci začeli uporabljati upravitelji računalniških sistemov za nadzor nad delovanjem omrežja, pa tudi računalniški hekerji. To je vsaj v slednjem primeru sicer nezakonito, a ker ne gre za aktivni vdor, temveč je prestrezanje paketkov pasivno (prisluškovalec samo spremlja promet), je to tehniko težko odkriti. Prestrezanje paketkov (t. i. *promisc sniffing*) je bilo včasih posebej priljubljeno v

[377] V začetnem obdobju se ni bilo mogoče prijaviti na GMail, uporabnika je moral nekdo povabiti. Zaradi tega je bil GMail račun nekakšen statusni simbol. Vabila na GMail so bila na začetku celo predmet dražb in trgovanja.

krajevnih ethernetnih omrežjih, ki so temeljila na tehnologiji razdelilnikov (ang. *hub*). Taka omrežja so omogočala, da vsi računalniki v posameznem delu omrežja spremljajo promet vseh računalnikov v istem delu omrežja. Če je posamezen računalnik vključil t. i. 'način promisc' (*promisc* je okrajšava za *promiskuitetno*), je lahko prisluškoval prometu drugih računalnikov v omrežju.[378] Vendar pa je mogoče paketke prestrezati tudi v omrežjih, ki namesto razdelilnikov uporabljajo stikala (ang. *switch*), in sicer s tehnikami napadov ARP (npr. s tehnikami zastrupljanja tabele ARP (ang. *ARP cache poisoning*), poplavljanja naslova MAC (*MAC address flooding*) ali podvajanja MAC (ang. *MAC duplication*)).[379] Hekerji to tehniko prestrezanja pogosto uporabljajo za krajo gesel (ang. *password sniffing*).

Orodja, ki omogočajo tako prestrezanje, so dostopna večinoma brezplačno. Večinoma so sicer napisana za okolje Linux, vse pogosteje pa so na voljo tudi različice za okolje Windows, zaradi česar so še bolj dostopna. Eno takih orodij sta *ethereal* in *ettercap*, ki sta na voljo tako za okolje Linux kot tudi za Windows.[380] Na spletni *ettercapa* avtorja program opisujeta kot orodje za t. i. napad s posrednikom (tim. *man-in-the-middle oz. MITM napad* - gre za napad, pri katerem se napadalec vrine med dve komunikacijski točki in tako spremlja promet med njima) v krajevnem omrežju, ki omogoča prestrezanje živih povezav, filtriranje vsebine ter analizo različnih komunikacijskih protokolov (in s tem krajo gesel), celo šifriranih. Novejše različice teh programov je mogoče zagnati v grafičnem načinu in z miško upravljati prek menujev, na voljo pa je tudi obsežna dokumentacija.

Prestrezanje elektronske pošte in tehnologija za analizo vsebine sporočil: SpamAssasin

Za razliko od navadne pošte ali telefonskih komunikacij je torej elektronska sporočila mogoče veliko bolj preprosto prestrezati in pozneje v njih iskati nekatere besede, saj se elektronska pošta po internetu načeloma prenaša nešifrirano, torej kot navadno besedilo. Protislovje elektronske pošte je torej v tem, da je tehnično videti bolj kot razglednica, v resnici in v percepciji uporabnikov pa je seveda zasebna pošta oziroma zaprta pisemska ovojnica.

Poleg tega imajo do elektronske pošte svojih uporabnikov načeloma povsem prost dostop upravitelji poštnih strežnikov in tudi upravitelji posredniških poštnih strežnikov (ang. *relay server*), po katerih se sporočilo posreduje od enega poštnega strežnika do drugega v internetu, čeprav v večini držav velja načelo pisemske tajnosti. Za vpogled v elektronsko sporočilo tudi ni nujno le-tega prestreči, 'zaseči' ga je mogoče tudi, ko se shranjuje na disku ali v pomnilniku enega izmed omenjenih sistemov. Pri prenosih elektronske pošte zato velja, da mora biti sporočilo iz posredniškega poštnega strežnika izbrisano takoj, ko je bilo posredovano naprej (Data Protection Working Party, 2000: 33). Enako velja tudi za končni poštni strežnik uporabnika, razen če se uporabnik sam odloči, da bo sporočilo po prenosu ohranil v svojem poštnem strežniku.

---

[378] To tehniko oz. vklop tim. *promisc načina* je mogoče zaznati.

[379] Prestrezanje podatkov je sicer možno izvesti s spremljanjem prometa na usmerjevalnikih (ang. *router*) oziroma podatkovnih povezavah, a načeloma lahko to stori samo upravitelj omrežja. V zadnjem času pa postaja priljubljeno tudi prestrezanje prometa v brezžičnih omrežjih.

[380] Dostopna sta na naslovu <http://ettercap.sourceforge.net/> ter <http://www.ethereal.com/>.

Pomembno je tudi ločevanje med prometnimi podatki, ki so nujni za prenos sporočila in morebitno zaračunavanje stroškov, in med osebnimi podatki ter vsebino sporočila. Poštni strežnik namreč o sporočilu samodejno zazna nekaj tehničnih podatkov, in sicer velikost sporočila, elektronski naslov pošiljatelja in sprejemnika, datum in čas pošiljanja sporočila ter še nekaj podatkov o poteku prenosa sporočila. S posebnimi nastavitvami programske opreme pa je seveda mogoče spremljati še veliko drugih prometnih podatkov, na primer število in velikost datotečnih prilog, uporabljeni nabor znakov, temo (ang. *subject*) in seveda tudi vsebino sporočila itd. Poročilo *Privacy on the Internet – An Integrated EU Approach to On-line Data Protection* opozarja na nevarnost, da upravitelji poštnih strežnikov nekatere od teh podatkov napačno obravnavajo kot prometne podatke, ki jih lahko shranjujejo npr. zaradi statistične analize (Data Protection Working Party, 2000: 33). Številni izmed teh prometnih podatkov zato ostajajo v obliki datotek aktivnosti, shranjenih v sistemu še dolgo potem, ko je prenos elektronske pošte že davno končan.

Ker je elektronska pošta ena najbolj temeljnih oblik medčloveške komunikacije po internetu, pomeni digitalizacija in tekstovna oblika sporočil posebno nevarnost za množične zlorabe. Phill Zimmermann je že leta 1993 opozoril na to, da je podatke v digitalni obliki (in še posebej v tekstovni) veliko laže in veliko bolj množično analizirati z naprednimi statističnimi metodami in matematičnimi algoritmi kakor glasovne komunikacije ali podatke na papirju oziroma podatke v nedigitalni obliki (Zimmermann, 1993).

V praksi bi bilo zelo nepraktično, če ne celo nemogoče, v realnem času spremljati in na klasični način (z branjem) analizirati vso elektronsko pošto vseh uporabnikov določenega omrežja, saj je količina podatkov preprosto prevelika. Ker pa je internetni promet že v digitalni obliki, je tehnično povsem mogoče v prestreženih podatkih iskati ključne besede in vzorce. Tehnike, ki se s tem ukvarjajo, imenujemo tehnike izkopavanja podatkov (ang. *data mining*). Ni naključje, da sta se razvoj in uporaba teh metod povečala konec devetdesetih in v začetku 21. stoletja.

Taka tehnologija se pravzaprav že množično uporablja, namenjena pa je iskanju računalniških virusov in odstranjevanju nezaželene elektronske pošte. Eden prvih programov, ki je uporabljal te tehnike, je *SpamAssasin*. Deluje tako, da analizira vso elektronsko pošto v nekem računalniškem sistemu in vsakemu sporočilu pripiše število točk, ki označujejo, kolikšna je verjetnost, da gre za nezaželeno sporočilo. Prednost matematičnih algoritmov, ki jih uporablja *SpamAssasin*, pa je, da so se možni učiti novih pravil, oziroma je možno prilagajati kriterije, na podlagi katerih se točkujejo elektronska sporočila. To seveda pomeni, da bi bilo razmeroma enostavno izdelati ali prirediti računalniški program, ki bi iz velikega števila elektronskih sporočil izločil manjše število takih, ki najbolj ustrezajo poljubno danim kriterijem. Za nekoga, ki bi v praksi želel nadzorovati veliko število elektronskih sporočil, to pomeni, da mu ni treba pregledati vseh prestreženih elektronskih sporočil (ki jih je lahko tudi nekaj milijonov na dan), temveč ob pomoči računalniške tehnologije izloči le nekaj najbolj relevatnih, ki jih potem preberejo in analizirajo ljudje. Data Protection Working Party zato priporoča, da programi za analizo elektronske pošte ne smejo posredovati okužene ali nezaželene pošte nobeni tretji osebi (Data Protection Working Party, 2000: 34); podobno je lahko sporno tudi filtriranje (brisanje) elektronske pošte. Če je filtriranje virusov načeloma še sprejemljivo (čeprav lahko pride tudi do lažne klasifikacije sporočila), pa je

brisanje nezaželene pošte po merilih, ki jih uporabnik morda ni odobril, že nekoliko sporno.

Prestrezanje je skupaj z naprednimi statističnimi analizami tipičen primer tehnologije, ki lahko zelo poveča učinkovitost in obseg nadzorovanja. Dejansko se je konec leta 2005 in sredi leta 2006 izkazalo, da je ameriška NSA verjetno že sedem mesecev pred terorističnimi napadi 11. septembra 2001 (Harris, 2006) zbirala prometne podatke o telefonskih klicih več deset milijonov Američanov znotraj ZDA ter nad zbranimi podatki izvajala statistične analize (Page, 2006) in da ima na (vsaj nekaterih) poglavitnih internetnih vozliščih usmerjanje lokalnega in mednarodnega internetnega in telefonskega prometa posebne prostore, iz katerih lahko nadzoruje celoten omrežni promet.

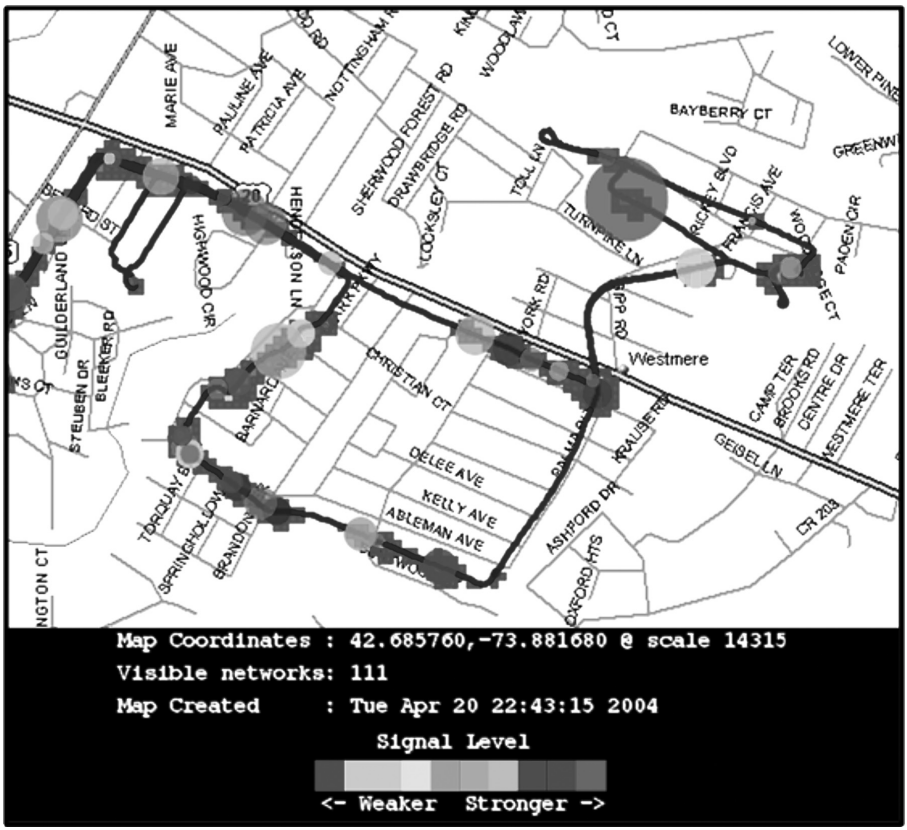
Ta tehnologija je bila do nedavna večinoma v domeni tajnih služb, v zadnjih letih pa se pospešeno razvija tudi področje izkopavanja podatkov (data mining) na področju marketinga. To pomeni, da se tehnologije, ki omogočajo obsežen nadzor nad podatki, pospešeno razvijajo tako za vladni kot za komercialni sektor.

Prestrezanje prometa v brezžičnih omrežjih

Z nastankom cenovno dostopnih brezžičnih krajevnih omrežij (WLAN, ang. *wireless LAN network*, včasih se uporablja tudi izraz Wi-Fi, gre za omrežja, ki temeljijo na protokolu 802.11) so se razvile nove možnosti zlorab, ki obsegajo tako krajo dostopa do interneta (z neavtoriziranim vstopom v omrežje ali krajo gesel za dostop do omrežja), prestrezanje omrežnega prometa pa tudi napade na omrežje oziroma na druge računalnike v brezžičnem omrežju (Internet Security Systems, 2002). Ker se je cena naprav za vzpostavitev brezžičnega omrežja (t. i. *WLAN Access Point*) v zadnjih letih močno znižala, naprave pa omogočajo hitro in enostavno deljenje internetne povezave (npr. ADSL ali kabelskega priključka), so se te naprave zelo razširile tudi med t. i. domačimi uporabniki.

Brezžična omrežja sicer omogočajo vzpostavitev šifrirane povezave, vendar je ta možnost privzeto izključena, nastavitev šifriranja pa zahteva branje navodil za uporabo in nastavitev ter vpis gesel, zato je veliko uporabnikov ne uporablja. Pri tem se zanašajo na to, da je območje dostopa do brezžičnega omrežja razmeroma majhno (v teoriji do 120 metrov, v praksi pa pogosto bistveno manj) in da je težko zaznati vključeno brezžično omrežje. Vendar ni tako, še posebej na urbanih območjih, saj že sprehod po npr. večjih slovenskih mestih z vključenim prenosnikom hitro odkrije množico povsem nezaščitenih brezžičnih omrežij.

V hekerski skupnosti se je že izoblikoval poseben sistem oznak, ki v fizičnem svetu označujejo točke, kjer je mogoč dostop do brezžičnih omrežij. Gre za t. i. *warchalking* (iskanje nezaščitenih brezžičnih omrežij pa *wardriving*), kjer hekerji s kredo (ali s sprejem) na javnih mestih označijo navzočnost in način vključitve v brezžično omrežje (Loney, 2002). Za take točke se je uveljavil tudi angleški izraz *hotspot.* So pa tudi projekti, v okviru katerih posamezniki razvijajo programsko opremo za odkrivanje brezžičnih omrežij, pri čemer je mogoče ob pomoči sprejemnika GPS (ang. *Global Positioning System* – sistem za določanje položaja) in brezžične kartice WLAN izrisati lokacijo brezžičnih omrežij na zemljevidu.



Slika 1: Slika lokacij in moči signalov brezžičnih omrežij, ki jo izriše program *KismetWireless* (Vir in avtorstvo: Kismet, 2005).

Ker je brezžično omrežje že v osnovi bolj občutljivo za prestrezanje kot žično omrežje, je bil v okviru komunikacijskega protokola 802.11 razvit tudi poseben šifrirni algoritem, ki omogoča šifriranje povezav. Gre za algoritem WEP (ang. *Wireless Equivalent Privacy*), ki je prazaprav sistem za šifriranje povezav in nadzor nad dostopom do omrežja (avtentikacijo).[381] Vendar

[381] Trenutno sta na voljo t. i. 64-bitni in t. i. 128-bitni WEP, vendar gre v resnici za 40-bitni in 104-bitni algoritem RC4. Drugih 24 bitov tvorijo sistemsko generirani podatki, t. i. "inicializacijski vektor", ki rabi za zagotavljanje nemotenega toka oziroma sinhronizacijo podatkovnih paketov. Raziskovalci so leta 2001 dokazali, da je mogoče z minimalnimi stroški (manj kot 100 dolarjev) v nekaj urah obnoviti 128-bitni ključ v brezžičnem omrežju (Stubblefield, Ioannidis in Rubin, 2001). Vendar pomanjkljivosti WEP ne izhajajo iz algoritma RC4 (ta se uporablja tudi v implementaciji SSL), temveč iz slabe zasnove samega sistema. Dodatna varnostna pomanjkljivost sistema je tudi to, da si vsi uporabniki omrežja delijo isti dostopni ključ (Schneier, 2001b). Nekatere teh pomanjkljivosti naj bi odpravil nov standard 802.11i. Strokovnjaki zato v brezžičnih omrežjih priporočajo uporabo zaščitnih protokolov IPsec (ang. *IP security protocol*) in VPN (ang. *Virtual Private Networking*).

je bilo pri zasnovi WEP storjenih precej napak. Schneier tako navaja, da je WEP, čeprav je bil tehnično gledano razvit javno, v resnici razvojno zaprt, saj so bila gradiva, ki so opisovala standard, dostopna samo proti plačilu (Schneier, 2001b).

Februarja 2001 so raziskovalci z berkeleyske univerze objavili, da jim je uspelo v realnem času razbiti šifrirni algoritem WEP;[382] ugotovili so celo, da je ta varnostni protokol tako slabo zasnovan, da omogoča neopazno ponarejanje paketkov, ki se prenašajo po brezžičnem omrežju (Sandberg, 2001). Kmalu so nastali programi, ki omogočajo prestrezanje šifriranih podatkov in kriptoanalizo. Programi (npr. KismetWireless, AirSnort, itd.) so na voljo brezplačno na internetu in jih je razmeroma enostavno uporabljati. Zaradi tega so pozneje razvili WPA (*Wi-Fi Protected Access*), v katerem pa je novembra 2004 Robert Moskowitz odkril nekaj varnostnih pomanjkljivosti, ki prav tako omogočajo zlorabo (Moskowitz, 2003). Skoraj natanko leto dni po tem odkritju je na internetu že na voljo računalniški program, ki omogoča razbijanje ključev WPA (Fleishman, 2004).

Čeprav je domet brezžičnega omrežja le 120 metrov, pa se je mogoče z uporabo usmerjenih anten na omrežje priključiti tudi z večje razdalje, celo z razdalje nekaj kilometrov.[383] To pa kar kliče po zlorabah, saj je morebitnega napadalca težko, navadno celo nemogoče locirati. Če namreč napadalec prek pomanjkljivo zavarovanega brezžičnega omrežja vstopi v internet in tam izvaja kaznive dejavnosti, grozi nevarnost, da ga nikoli ne bodo izsledili, oziroma da bo krivda padla na lastnika brezžičnega omrežja.

Koliko je zlorab brezžičnih omrežij, je težko ugotoviti. Dejstvo pa je, da je priložnosti za take zlorabe veliko, tveganje za napadalca pa minimalno, saj se mu ni treba fizično povezati v omrežje. Odkritih zlorab je bilo doslej razmeroma malo. Praviloma so dveh vrst. Pri prvi vrsti zlorab gre za uporabo brezžičnega omrežja za krajo dostopa do interneta. Eden bolj znanih primerov se je zgodil konec leta 2004, ko je policija v Los Angelesu aretirala 37-letnega moškega, ki je uporabljal odprta brezžična omrežja stanovalcev tega mesta za pošiljanje smetja.[384] Že pred tem pa je ameriška policija obravnavala nekaj primerov nezakonite uporabe brezžičnih omrežij za vdiranje v tuje računalnike, pošiljanje izsiljevalskih zahtev, kraje kreditnih kartic (Poulsen,

---

[382] Dostop do brezžičnega omrežja je mogoče zavarovati tudi z nadzorom nad dostopom na ravni serijskih številk omrežnih vmesnikov, t. i. strojnih naslovov MAC (ang. *Media Access Control address*). Upravitelj omrežja namreč lahko dovoli uporabo brezžičnega omrežja samo uporabnikom z določenimi naslovi MAC (ti naj bi se razlikovali za vsako omrežno kartico). Vendar je mogoče naslove MAC programsko ponarejati, kar omogoča tehnika prikrivanja MAC naslovov (ang. *MAC spoofing*). Nekatere brezžične omrežne kartice pa uporabnikom celo omogočajo, da sami vpišejo poljubno serijsko številko MAC.

[383] V praksi so brezžična omrežja tipa Wi-Fi bistveno bolj razširjena kot brezžična omrežja tipa *bluetooth*. Slednja imajo domet le nekaj metrov in se večinoma uporabljajo v mobilni telefoniji za povezavanje mobilnih telefonov ali mobilnega telefona in računalnika. Podobno kot pri tehnologiji Wi-Fi pa so tudi pri tehnologiji *bluetooth* odkrili zlorabe, ki omogočajo krajo dostopa do interneta (nezakonita uporaba povezave GPRS) in krajo vsebine telefonskega imenika – gre za tehniki, poimenovani *bluejacking* in *bluesnarfing*. Zanimivo pa je, da so tudi pri tej tehnologiji, ki ima domet le nekaj metrov, s posebnimi antenami uspešno izvedli preizkus prenosa podatkov na razdalji 1 km (več o tem na Wi-Fi Toys, 2004).

[384] Moški je bil obtožen na podlagi SPAM-CAN Act. Gre za zakon, ki kriminalizira nekatere sporne prakse pošiljanja nezaželene elektronske pošte v ZDA, veljati je začel 1. januarja 2004. V omenjenem primeru gre za prvo rabo tega zakona v ZDA.

2004a ter Poulsen, 2004b), kraje podatkov,[385] v enem primeru je šlo celo za politično špijonažo v ameriškem Kongresu.[386]

To pa žal ni edina nevarnost, ki jo prinašajo brezžična omrežja, saj je mogoča še drugačna vrsta zlorabe. Konec leta 2003 so namreč vlomili v poštno banko v Haifi v Izraelu. Ko je policija prišla na kraj dogodka, niso odkrili nič sumljivega, kljub temu pa je čez dober mesec na tej pošti z bančnih računov nenadoma izginilo okrog 13.000 dolarjev. Poznejša preiskava je pokazala, da so vlomilci ob prvem vlomu v omrežje pošte podtaknili brezžično dostopno točko, prek katere so lahko nezakonito vstopili v sicer močno zaščiteno bančno omrežje (Evron, 2004) in s tem enostavno zaobšli zaščito.

Prostorska zasebnost na internetu

Razvoj tehnologije spreminja tudi definicijo teritorija. Če na internet gledamo kot na virtualni prostor, lahko osebne računalnike uporabnikov interneta razumemo kot zasebni virtualni prostor. Seveda pa pri tem zaradi same tehnologije hitro naletimo na vprašanje, kdaj je neki del virtualnega prostora javen in kdaj že zaseben. Primer, ki to najbolje ponazarja, je prostor v javno dostopnih spletnih strežnikih, kjer uporabnik lahko del prostora v takem strežniku nameni javnosti (npr. za spletno stran), drugi del pa javnosti ni dostopen (npr. je zaščiten z geslom) in tako predstavlja zasebni prostor posameznika. S temi dejstvi se dejansko srečujejo uporabniki interneta, ki neki del kiberprostora dojemajo kot zasebnega, čeprav je v resnici morda javen ali v lastni nekoga drugega.[387] Tako napačno dojemanje kiberprostora pa je mogoče izkoriščati. Član znane hekerske skupine L0pht je v nekem intervjuju povedal, da zaposleni v podjetjih pogosto puščajo interne dokumente v javnih strežnikih, zato je napisal program, ki redno preiskuje javne strežnike podjetij in v njih išče zaupne dokumente. Ob tem je izjavil: "*S tem ne kršim nobenega zakona, jemljem samo javne stvari.*" (Gottlieb, 1999) Tako iskanje zaupnih informacij in dokumentov pa je v zadnjem času mogoče tudi z uporabo iskalnikov, recimo z uporabo iskalnika Google. (Gre za t. i. *Google hacking*, hekanje z Googlom. Predavanje na to temo je imel avgusta 2003 na Defconu, največji hekerski konferenci, Johnny Long,[388] pozneje je o tem napisal še knjigo *Google Hacking for Penetration Testers.*). Znan je celo primer, ko so se zaradi napačnih nastavitev programa P2P v omrežju P2P znašli celo zaupni dokumenti neke japonske jedrske elektrarne (Schneier, 2006e), dokumenti o vojaških operacijah v Iraku (CmdrTaco, 2004), pa tudi številni zasebni dokumenti in fotografije.

---

[385] Prvi primer pregona zaradi zlorabe brezžičnega omrežja se je zgodil konec leta 2003. Šlo je za krajo zaupnih medicinskih podatkov (Chanell3000.com, 2003).

[386] Člani republikanske stranke so imeli okrog leto dni dostop do računalnikov demokratske stranke, iz katerih so kradli zaupne dokumente in jih občasno pošiljali v javnost (Schneier, 2004b).

[387] To je na splošno problem tudi pri shranjevanju osebnih podatkov in informacij v strežnikih ponudnikov storitev (npr. v primeru mobilnih operaterjev), ki včasih prostora, ki ga oddajajo posameznikom, ne zaščitijo dovolj skrbno.

[388] Prosojnice s predavanja so na <http://www.defcon.org/images/defcon-12/dc-12-presentations/Long/dc-12-long.pdf>. Johnny Jong pa ima tudi spletno stran <http://johhny.ihackstuff.com>, na kateri objavlja svoja najnovejša odkritja, vzdržuje pa tudi zbirko možnih zlorab, tim. *Google Hacking Database* (GHDB).

Vdiranje v računalniške sisteme je klasična oblika kiberkriminala in tudi eden izmed najbolj neposrednih napadov na zasebnost. A do vdorov ne prihaja zgolj zaradi kraje podatkov, temveč tudi z namenom podtikanja spornih vsebin (npr. otroške pornografije) in poznejšega izsiljevanja.[389] Znan pa je tudi primer podtikanja spornih vsebin z namenom maščevanja. 22. novembra 2004 so neznani napadalci v računalnike italijanskega senata naložili slike s trdo homoseksualno pornografijo, domnevno zaradi maščevanja gejevskih aktivistov, ker je bil zaradi fotografij iz gejevskega nočnega kluba odpuščen pomočnik predsednika senata (Jacques, 2004).

Do vdorov sicer lahko pride zaradi napak pri postavitvi in vzdrževanju sistemov, npr. zaradi nepravilno nastavljenih pravil za dostop do datotek, slabo napisanih programov (značilen primer so npr. spletni programi, ki ne preverjajo ukazov za delo s podatkovnimi zbirkami) ali uporabe privzetih ali rezervnih privzetih gesel za dostop do sistema. Vendar gre pri takih vdorih bolj za malomarnost tistega, ki je sistem postavil, kot pa za aktivni vdor. Problematični pa so prav slednji, saj gre pri klasičnih vdorih navadno za bolj prefinjene načine iskanja varnostnih pomanjkljivosti (ang. *vulnerability*) in njihovo izkoriščanje. Praviloma slednje zahteva veliko računalniškega znanja. Vendar pa se je to v zadnjih letih začelo korenito spreminjati in za napade ni več treba velikega znanja, saj postajajo avtomatizirani.

Eno prvih orodij za avtomatizacijo iskanja razpok v sistemu varnosti je nastalo leta 1995, ko sta računalniška programerja Wietse Venema in Dan Farmer na internetu objavila program SATAN (*Security Administrator's Tool for Analyzing Networks*). Njegova naloga je bilo samodejno odkrivanje varnostnih pomanjkljivosti v računalniških sistemih (Dittrich, 1996). Program je bil sicer namenjen odkrivanju, ne pa tudi izkoriščanju razpok v varnosti, avtorja pa sta ob njegovi brezplačni objavi na internetu zatrdila, da je namenjen predvsem upraviteljem računalniških sistemov za izboljšanje varnosti njihovega lastnega sistema (Woodcock, 1995). Danes je takih orodij na internetu kar nekaj. Eno bolj znanih je Whoppix, poseben Linux CD (tim "živi CD"), s katerim zaženemo računalnik, na CDju pa je množica orodij za preverjanje varnosti sistema, vdore in odkrivanje razpok v varnosti.[390] ISO slika CDja je brezplačno na voljo na internetu (<http://www.whoppix.net/>).[391]

Kmalu so začela nastajati orodja, ki so namensko omogočala izkoriščanje razpok v varnosti. Leta 1998 je skupina računalniških hekerjev, zbranih v skupini *Cult of the Dead Cow*, na svoji

---

[389] Obsega takih groženj žal ni mogoče ugotoviti, saj jih žrtve nerade prijavljajo. Znan pa je primer iz oktobra 2004, ko so izsiljevalci skušali od založbe podjetja Blue Square izsiliti 7000 evrov z grožnjo, da bodo v nasprotnem v njihovem imenu začeli razpošiljati elektronsko pošto z otroško pornografijo (McCue in Ilett, 2004). Sicer pa so različna izsiljevanja prek interneta kar pogosta.

[390] Večinoma gre le za konceptualna orodja (t. i. *orodja proof-of-concept*), ki najdejo in izkoristijo razpoko v sistemu varnosti, ne povzročijo pa dejanske škode, samo demonstrirajo vdor. Od tod tudi ime Whoppix, gre za Whitehat Knoppix; '*whitehat*' za razliko od orodij '*blackhat*' ni namenjeno povzročanju škode, temveč prikazu varnostnih pomanjkljivosti, Knoppix pa je ime znane distribucije 'živega' (ang. *live CD*) Linuxa.

[391] Poznamo tudi podobne zbirke plošč CD z zbirkami vdiralskih orodij. Ena obsežnejših je na živem CD-ju BackTrack, ki je združil orodja dveh znanih sistemov za preverjanje varnosti računalniških sistemov Whax in Auditor. Orodje je na internetu na naslovu <http://www.remote-exploit.org/index.php/BackTrack>.

spletni strani objavila trojanskega konja[392] *Back Orifice.* Namenjen je nadzorovanju računalnikov, v katerih teče operacijski sistem Windows, na daljavo. Kmalu pa so nastali tudi "konkurenčni" programi, npr. *NetBus* in *Sub7*. Po namestitvi je program v računalniku odprl t. i. stranska vrata (ang. *back door*) in skoznje napadalcu omogočil popoln dostop do računalnika in upravljanje le-tega prek interneta, ne da bi lastnik sicer nadzorovanega računalnika to opazil.[393] Program je zelo preprosto uporabljati, poleg tega je tudi brezplačen. S tem so že nakazane smeri razvoja teh orodij, ki postajajo čedalje enostavnejša in vedno bolj avtomatizirana.

Razvoj vdiralskih orodij

Čeprav da je bilo BackOrifice enostaven uporabljati, pa je bil poglavitni problem napadalca, kako program podtakniti v računalnik žrtve. BackOrifice je omogočal pripenjanje samega sebe na neko drugo izvršilno datoteko (.EXE), napadalci pa so to datoteko s kakšno pretvezo poslali žrtvi in ta ga je morala sama pognati. Program je bilo mogoče tudi samodejno pognati v računalniku žrtve, vendar je bilo za to treba nekaj izkušenj in sreče. Napad je bilo torej mogoče izvesti z nekaj truda, ni pa potekal samodejno. Ker pa je bil prvi zlonamerni program, ki se je širil samodejno (gre za t. i. črv), napisan že novembra 1988 (t. i. *Morris Worm*[394]), je kmalu postalo jasno, da bo razvoj vdiralskih orodij krenil v smeri avtomatizacije vdorov.

Razvoj vdiralskih orodij verjetno najbolj ponazarja razvoj orodij za DOS napade. Prvotno, v začetku in sredi 90. let 20. stoletja, so hekerji za te napade uporabljali različna orodja, ki so bila razpršena po internetu in jih je bilo težko dobiti. Leta 1998 pa je nastala prva zbirka orodij, ki so bila med seboj povezana s skriptom, imenovanim "*rape*" (ang. *posilstvo*). Konec junija 1998 je nemški heker Mixter napisal program "*targa.c*", ki je združeval različna orodja v enoten program in ga je bilo zato tudi laže distribuirati. Vendar so ta orodja omogočala napad samo na en sistem hkrati, in še to le iz ene točke, zato je bil naslednji logični korak v razvoju teh orodij njihovo povezovanje v omrežja.

---

[392] Trojanski konj je zlonamerni program, ki se za razliko od virusov ne širi samodejno, niti ne more okuževati drugih datotek v računalniku. Trojanski konji se navadno pretvarjajo, da so povsem navadni programi (od tod tudi njihovo ime), njihove skrite funkcije pa so najpogosteje namenjene odpiranju t. i. stranskih vrat na žrtvinem računalniku, kraji gesel ali povzročanju druge škode.

[393] Program je bil sestavljen iz dveh delov, enega je bilo treba namestiti v računalnik žrtve, z drugim pa je upravljal napadalec. Vendar je imel program za upravljanje vgrajena tudi posebna stranska vrata, skozi katera so avtorji programa dobili dostop do računalnika napadalca.

[394] Morris Worm je 2. novembra 1988 aktiviral Robert Tappan Morris. Črv je okužil okrog 6000 računalnikov; to je bilo v tistem času dovolj za močno oviranje delovanja interneta. Zaradi nastanka tega črva so pozneje na internetu ustanovili organizacijo za spremljanje in obravnavanje varnostnih incidentov CERT. Morris pa je bil kot prvi obtožen na podlagi *Computer Abuse and Fraud Act*. Danes je Morris profesor na MIT (Wikipedia, geslo: "Morris worm").

Konec junija 1999 so zato hekerji že začeli preizkušati nov program, ki so ga poimenovali *trinoo* (oziroma včasih tudi *trin00*), prikrita omrežja pa so obsegala tudi do 2000 računalnikov (Dittrich, 1999a). Konec avgusta 1999 je že nastalo orodje *Tribe Flood Network*[395] ali *TFN*, ki je združevalo lastnosti prejšnjih orodij (več možnih napadov, gradnja omrežja). Konec septembra pa orodje *Stacheldraht* (nem. *bodeča žica*), ki pa je že vsebovalo take protokole za komunikacijo z napadalcem, ki jih je težko zaznati; poleg tega so avtorji vgradili tudi zaščito za napadalca, saj je orodje omogočalo šifrirano komunikacijo z napadalcem in avtentikacijo lastnika prikritega omrežja z geslom (Dittrich, 1999a, Dittrich, 1999b ter Dittrich, 1999c).

Orodje *stacheldraht* je bilo sicer že močno zmogljivo, vendar se ni bilo sposobno širiti samodejno. Nadaljnji razvoj je zato začel izkoriščati številne varnostne pomanjkljivosti operacijskih sistemov Windows in to je napadalskim orodjem omogočilo samodejno širjenje. Značilni predstavniki te generacije so številne različice napadalskih orodij *sdbot* in *rxbot*. Njihov namen je ugrabljanje velikega števila računalnikov in gradnja prikritih omrežij za poznejše napade, sam vdor v točno določen sistem pa je za napadalca postranskega pomena.
Napad z njimi je videti tako, da napadalec najprej vdre v neki strežnik in vanj namesti kopijo programa za nadaljnje širjenje. Nato aktivira virus, ki išče varnostne pomanjkljivosti v drugih računalnikih, in ko jih odkrije, vanje namesti kopijo vdiralskega orodja iz strežnika FTP.

Eno izmed značilnih takih orodij je bilo konec leta 2004 najdeno v računalniku na Fakulteti za družbene vede z nameščenim operacijskim sistemom Windows Xp, Service Pack 2 in vključenimi vgrajenimi varnostnimi mehanizmi operacijskega sistema Windows. Analiza je pokazala, da je vdiralsko orodje (verjetno gre za eno izmed različic *rxbot* ali *sdbot*) povezano na namenski strežnik IRC na Finskem (v katerega je bil verjetno prav tako vdrto). Po priklopu in prijavi na finski strežnik z odjemalcem IRC (podatki, potrebni za priklop, so bili pridobljeni s prestrezanjem povezave med vdiralskim orodjem in namenskim strežnikom IRC) je bilo mogoče v živo spremljati širjenje prikritega omrežja. Eden izmed ugrabljenih računalnikov z imenom "[tws]706151" je ob 10:48:47 poizkušal vdreti v računalnik na naslovu IP "203.232.133.153", ki je bil na neki korejski univerzi. Vdor in namestitev kopije vdiralskega orodja sta uspela v dveh sekundah. Čez približno minuto in pol je bil ugrabljeni računalnik že vključen v omrežje in je začel tudi sam iskati nove žrtve in se tako širiti. V približno dobri uri opazovanja (od 10:36:02 do 11:38:38) se je v prikrito omrežje vključilo že deset računalnikov.[396]

---

[395] Kmalu zatem (leta 2000 in pozneje) so se zvrstili številni napadi na velike spletne strani, npr. na Yahoo, eBAY, Amazon, CNN, Buy.com, pozneje tudi na strežnike P2P in celo na korenske strežnike DNS, kar je skoraj ohromilo delovanje interneta. Razvoj orodij je namreč potekal tudi s preizkušanjem v praksi in verjetno so se ravno ob uporabi napadalci največ naučili. Avtor programa Mixter je v nekem intervjuju povedal, da so bila pri teh napadih zagotovo uporabljena njegova orodja, čeprav je zanikal, da bi pri napadih sodeloval tudi sam (Shankland, 2000).

[396] Pravzaprav je šlo za omrežje, ki se je širilo razmeroma počasi. Gorazd Božič, vodja varnostnega centra SI-CERT, je na predavanju na varnostni konferenci Infosek 2004 predstavil primer prikritega omrežja, ki se je širilo s hitrostjo 10–15 novih računalnikov na minuto (Božič, 2004).

datum in čas sporočila	sporočilo	opombe
[01-12-2004 10:48:47]	[tws]706151 [lsass_445]: Exploiting IP: 203.232.133.153.	Eden izmed računalnikov v prikritem omrežju obvešča, da je začel iskati varnostne pomanjkljivosti na določenem naslovu IP.
[01-12-2004 10:48:49]	[tws]706151 [FTP]: File transfer complete to IP: 203.232.133.153 (C:\WINDOWS\System32\ mswins.exe).	Uspel jih je najti in izkoristiti v dveh sekundah.
[01-12-2004 10:50:22]	*[tws]866541 (~itxuyafw@203.232.133.rox-62925) has joined #bots	Računalnik, v katerega je bilo vdrto, se je že prijavil v prikrito omrežje in prejel ukaze za nove napade.

Prikaz samodejnega širjenja vdiralskega orodja. Ugrabljeni računalniki (t. i. boti) na kanalu IRC prejemajo navodila za napade, prav tako samodejno poročajo o svojih dejavnostih. V konkretnem primeru je bilo omrežje nadzorovano prek (verjetno ugrabljenega) računalnika na Finskem, v katerem je bil postavljen strežnik IRC. Roboti so se zbirali na kanalu #bots.

Po tehnični plati bo šel razvoj teh orodij verjetno v smer še bolj decentraliziranega širjenja, izogibanja varnostnim mehanizmom na napadenih sistemih in izkoriščanja novih varnostnih pomanjkljivosti. (13. julija 2004 je bil v hekerskem magazinu Phrack objavljen članek, ki opisuje, kako zaobiti programske požarne zidove v osebnih računalnikih (Butler, 2004), torej enega poglavitnih mehanizmov za zaščito osebnega računalnika.) Zanimivo pa je, da velik razvoj poteka tudi na strani enostavnosti rabe in prijaznosti do uporabnika - napadalca, oziroma kar na vzpostavitvi nekakšne virtualne skupnosti razvijalcev in uporabnikov teh programov.

Orodje *sdbot* je domnevno nastalo tako, da je nekdo prvo različico *sdbota* skupaj s preprostimi navodili za uporabo in izvorno kodo objavil na internetu. (Po govoricah v omrežju IRCNet naj bi bil eden izmed avtorjev programa iz Slovenije, na to nakazuje tudi stavek v priročniku za uporabo programa, ki kot zgled rabe nekega ukaza vsebuje oznako Slovenije ".si".) Okrog prvotnih avtorjev (ali avtorja) se je hitro oblikovala skupina posameznikov, ki so program dopolnjevali in razvijali, izvorno kodo pa vračali nazaj v svojo skupnost in s tem omogočili hiter razvoj programa.

Zanimivo, da so pri tem uporabili t. i. odprtokodni model razvoja, ki se je kot zelo uspešen izkazal že pri razvoju druge programske opreme, npr. Linuxa, Mozille, OpenOffice.org in drugih. Ker je koda programa javno dostopna pod licenco GNU GPL, ki določa, da lahko program kdorkoli spreminja ali dopolnjuje, edina zahteva je, da spremembe tudi sam javno objavi, se napake v odprtokodnih programih v primerjavi z zaprtokodnimi odpravljajo zelo hitro. Prav tako se hitro dodajajo nove funkcionalnosti.[397]

[397] Za primerjavo: medtem ko je od odkritja varnostne pomanjkljivosti in izdaje popravka zanjo za programe npr. podjetja Microsoft treba čakati tudi nekaj mesecev, so varnostni popravki za Linux izdani zelo hitro, navadno v nekaj dneh, včasih celo v nekaj urah.

Ob tem, da se program zelo hitro razvija s stališča tehnologije, pa se razvija tudi v smislu uporabniške prijaznosti. Poleg programa so namreč na voljo podrobna navodila za njegovo pripravo (program je na voljo v obliki izvorne kode, kar pomeni, da ga je treba prevesti v binarno obliko; brezplačni prevajalnik je na voljo na internetu in je velik le nekaj Mb, torej si ga je mogoče prenesti tudi na počasni klicni povezavi, pred prevajanjem pa je treba nastaviti nekaj parametrov, katerih pomen je podrobno razložen) in navodila za uporabo, skupaj z nazornimi primeri uporabe v praksi. Avtorji programa imajo spletno stran, na kateri so objavljeni njihovi kontaktni podatki in celo fotografije (skupaj z novicami, koga so zaradi računalniškega kriminala zaprli). Storitev pa ne bi bila popolna, če ne bi bilo na voljo tudi uporabniške podpore: na voljo je spletni forum za izmenjavo nasvetov in izkušenj ter celo kanal IRC, na katerem lahko uporabniki povprašajo za brezplačen nasvet bolj izkušene uporabnike.

```
// bot configuration
 const char botid[ ] = “user”; // bot id
 const char password[ ] = “passwd”; // bot password
 const char server[ ] = “irc.server.net”; // server
 const int port = 6667; // server port
 const char serverpass[ ] = “”; // server password
 const char channel[ ] = “#channel”; // channel that the bot should join
 const char chanpass[ ] = “”; // channel password
```

Slika 2: Del konfiguracijske datoteke za vdiralsko orodje *sdbot 0.5b*.
Uporabnik mora zgolj vnesti vrednosti programskih konstant in program prevesti (kako program prevesti, je obširno napisano v datoteki s pogostimi vprašanji) in že je “napisana” nova različica virusa. Pomen posameznih vrednosti je zelo jasno obrazložen, pogosto z zgledi.

Uporaba teh orodij je zato tako enostavna, da mora potencialni napadalec ugotoviti le, kje je spletna stran z vdiralskimi orodji (spletno stran namreč občasno selijo), in znati dovolj dobro angleško, da si prebere podrobna navodila za uporabo orodij oziroma uporabi ‘uporabniško podporo’.

Od vdora do kraje podatkov

Četudi so omenjena orodja namenjena vzpostavitvi obsežnih prikritih omrežij, iz katerih pozneje potekajo DOS napadi, ne pa napadom na točno določene računalnike, je verjetno le vprašanje časa, kdaj bodo napadalci začeli v ugrabljenih računalnikih preiskovati tudi dokumente in druge datoteke. To se verjetno že dogaja, čeprav so razlogi bržkone prej politični, ekonomski in vojaški kot pa izsiljevanje ali tešitev radovednosti. Že od leta 1994 namreč vojaški strokovnjaki opozarjajo na *Mirrim College* (znan tudi pod imenom *Automated Warfare Institute*) v Severni Koreji, kjer naj bi se načrtno šolali računalniški strokovnjaki in hekerji (McWilliams, 2003a). Oktobra 2004 pa je precej odmevalo poročilo obrambnega ministra Južne Koreje

parlamentarnemu odboru za obrambo, v katerem je navedel, da naj bi po njihovih obveščevalnih podatkih Severna Koreja izšolala okrog 600 hekerjev, ki so zadolženi za izvajanje obveščevalnih dejavnosti proti Južni Koreji, Japonski in ZDA (Soo-Jeong, 2004).

Da je tak scenarij verjeten, nakazuje to, da so v Južni Koreji sredi leta 2004 zaznali 211 uspešnih vdorov v računalnike desetih državnih ustanov, med drugim tudi južnokorejskega parlamenta, inštituta za obrambne študije, univerz in zasebnih podjetij. Do vdorov je prišlo iz kitajskih računalnikov (Agence France-Presse, 2004). Poleg tega so po mnenju Oxblooda Ruffina, ustanovitelja hekerske skupine *Hactivismo* in člana hekerske skupine *Cult of the Dead Cow*, južnokorejski hekerji "*najbolj nadarjeni in neizprosni tehnologisti, kar me navaja na misel, da v Severni Koreji deluje ali se poraja podobna skupina navdušencev, morda še bolj motiviranih*" (Soo-Jeong, 2004). Na uporabo hekerskih tehnik kot del informacijskega bojevanja daje slutiti tudi operacija Titan Rain. Gre za serijo napadov na ameriške vladne in poslovne strežnike, ki jih amerški varnostni strokovnjaki zaznavajo že vse od leta 2003, vrhunec pa so dosegli leta 2005. ZDA sumijo, da za napadi stoji kitajska vojska. Po besedah direktorja inštituta SANS Alana Pallerja se napadalci pri vdorih, opravljenih 1. novembra 2005, niso niti enkrat zatipkali, niso pustili odvečnih sledov in so v manj kot pol ure namestili stranska vrata. Meni, da taka sistematičnost in izurjenost kaže na vojaško organizacijo. Napadalci naj bi med drugim ukradli programsko opremo za načrtovanje vojaških poletov, uspešno pa so vdrli tudi v različne računalnike podjetij, ki pogodbeno sodelujejo z vojsko (Espiner, 2005).

Vsekakor so v ameriški NSA v okviru vojaške simulacije *Operation Eligible Receiver* že leta 1997 dokazali, da je tako bojevanje lahko uspešno. V okviru operacije je 35 računalniških strokovnjakov NSA poskušalo vdreti v številne vojaške in civilne računalnike, ki so nadzorovali ključne infrastrukturne sisteme. To jim je tudi uspelo in s tem so dokazali, da je mogoče s kiberbojevanjem narediti precej škode (Robinson, 2002).[398]

[398] Informacija o tej operaciji je dostopna tudi v poročilu, pripravljenem za *Cyber Security Research and Development Act*, ki ga je 4. februarja 2002 v *House of Representatives* podal Boehlert iz odbora za znanost, str. 3–4 (Boehlert, 2002).

Glede na zmožnost novih hekerskih orodij, da se samodejno širijo, in ob ugotovitvah nekaterih hekerjev (npr. članov skupine L0pht, Johnny Long itd.), da so na javnih spletnih straneh pogosto pomotoma objavljeni zaupni dokumenti,[399] je pričakovati, da bodo kmalu nastala tudi orodja, ki ne bodo preiskovala samo javnega kiberprostora, temveč tudi zasebnega, do katerega bodo prišla z vdorom. Na to nevarnost je maja 2000 opozoril nekdanji direktor CIE R. James Woolsey, ki govori o novi vrsti virusov – instruktivnih virusih (Poulsen, 2000). Ti naj bi se širili čim bolj neopazno in za svoje delovanje uporabili kar najmanj zmogljivosti sistema, njihov namen pa naj bi bila kraja podatkov, spreminjanje vsebine datotek ali elektronsko prisluškovanje. Verjetno je zgolj vprašanje časa, kdaj bodo taka orodja na voljo na internetu.[400]

To, da do večjega števila kraj podatkov ne prihaja zgolj zato, ker hekerji tuje računalnike potrebujejo za vzpostavitev prikritih omrežij, kaže tudi pogovor z anonimnim slovenskim hekerjem, opravljen prek IRC 17. julija 2003. Povedal je, da si je z vdorom pridobil podatke o 13.011 študentih za leto 2002 v Sloveniji.[401] Zbirka podatkov je poleg imena, naslova, številke EMŠO, končane srednje šole in fakultete, na katero se je posameznik vpisal, vsebovala še število točk, ki jih je študent dosegel na maturi (Kovačič, 2003a). Do nedavna je bila na internetu tudi spletna stran slovenske hekerske skupine *Phone Losers of Slovenia* (PLS),[402] na kateri so bili javno objavljeni podatki o vdorih članov skupine. Poleg tega pa je bilo na njej objavljenih tudi nekaj zaupnih poslovnih dokumentov.

---

399 Nevarnost pa predstavljajo tudi skriti podatki v javnih dokumentih, npr. podatki o tem kdo vse je nek dokument urejal, možnost sledenja spremembam, itd. Britanska vlada je konec januarja 2003 na svoji spletni strani objavila domnevno obveščevalno poročilo o iraški vojaški infrastrukturi, za katerega se je izkazalo, da je bilo ponarejeno. Poročilo je bilo namreč v večjem delu kopija besedila študenta Ibrahima al-Marashija. Kasneje je bilo s pomočjo skritih podatkov o spremembah dokumenta ugotovljeno, kdo je omenjeno poročilo urejal. Izkazalo se je, da so bili to visoki državni uslužbenci (Smith, 2003). Na podoben način so nasprotniki programskih patentov v EU uspeli ugotoviti, da je večji del enega izmed predlogov direktive EU o programskih patentih pripravil odvetnik BSA (Stallman, 2005). Novinarji Corriere Della Sera pa so npr. leta 2005 uspeli pridobiti zaupni del vsebine poročila o uboju agenta italijanske tajne službe Nicola Caliparija s strani ameriških vojakov v Iraku. Zaupni del besedila je bil "skrit" v javno objavljenem PDF dokumentu, novinarji pa so ga obnovili s preprostim kopiranjem in lepljenjem (CmdrTaco, 2005). Takšnih primerov je še več.

400 Pravzaprav so se že pojavila, vendar še niso razširjena. Eno takih je "*Echelon for Dummies*", ki ga je napisal Mixter (avtor orodja *Tribe Flood Network*). Gre za distribuiran prestrezni program (ang. *sniffer*), ki v različnih delih omrežja prestreza internetni promet in išče ključne besede, podatke pa posreduje nadzornemu programu. Avtor na svoji spletni strani pravi, da je orodje napisal z namenom prikaza delovanja sistema Echelon. Orodje "Echelon for Dummies" je dostopno na spletni strani <http://packetstormsecurity.nl/groups/mixter/>).

401 Na prošnjo, naj svojo trditev dokaže, je poslal izpis podatkov za nekoga, ki ga osebno poznam, in zaslonski posnetek pregledovanja zbirke, na katerem so bili vidni podatki nekoga drugega, ki ga prav tako osebno poznam. Preverjanje je potrdilo točnost podatkov.

402 Spletna stran ni več dostopna, tik pred prenehanjem delovanja je bilo objavljeno sporočilo o 'upokojitvi' enega najpomembnejših članov skupine. Eden izmed članov pa mi je 14. decembra 2004 v elektronskem sporočilu povedal, da je bila spletna stran zaprta zaradi pritiskov podjetja Mastercard. Hekerska skupina je namreč na svoji spletni strani objavila številke kreditnih kartic nekaj slovenskih uporabnikov Mastercarda (PLS, 2004). Pred prenehanjem delovanja spletne strani sem arhiviral zaslonske posnetke in del vsebine spletne strani.

<---->	Jaz imam podatke o vseh študentih v Sloveniji, od leta 1994 do 2002. Ime, priimek, faks, EMŠO, naslov, št. točk na maturi itd.
<Matej>	Kje si staknil te podatke?
<---->	Hehe, če ti povem, ne boš verjel. Čisto po naključju sem jih našel. Imel sem jih doma v računalniku že eno leto, pa sploh nisem vedel, da jih imam.
<Matej>	Kako? Od nekod si jih moral sneti, ne?
<---->	Ja, ampak nisem vedel, kaj sem snel. Šele lani sem videl, kaj imam.
<Matej>	Kako si jih pa snel?
<---->	Prek interneta. IIS exploit. Nekdo je imel te podatke in mislim, da jih tudi on ne bi smel imeti, oziroma ni bil upravičen do tega, da jih ima.
<Matej>	Aha, se pravi, da je nekdo to imel, ti pa si potem njemu vdrl...
<---->	Da, ampak ta, ki je to imel, ni posameznik, temveč zavod. Pa ni bil maturitetni zavod ali kaj podobnega.
<Matej>	Kateri pa?
<---->	Neki drug zavod. ... Ti bom že povedal.

Zapis pogovora z anonimnim slovenskim hekerjem z dne 17. julija 2003. Pogovor je potekal prek IRC in je lektoriran. Sogovornik je uporabljal psevdonim (svoje hekersko ime), vendar ni želel, da ga navedemo. Pred objavo je bilo besedilo prek elektronske pošte avtorizirano s strani sogovornika (Kovačič, 2003a).

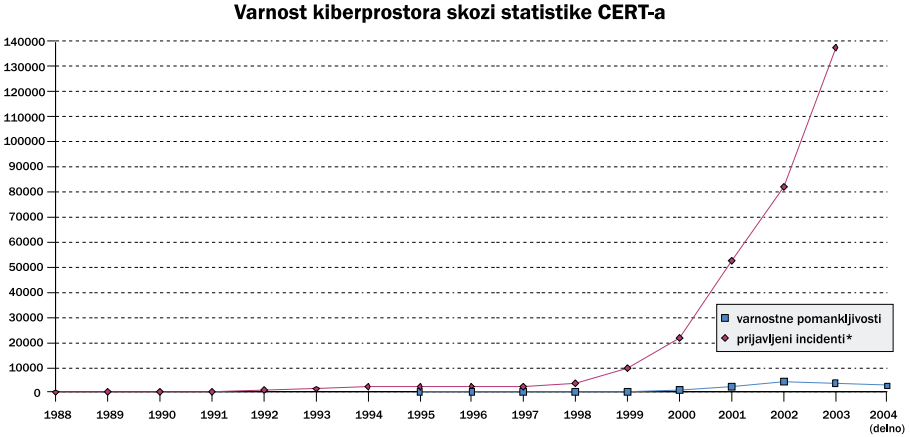
Vse to žal kaže na to, da je verjetno samo še vprašanje časa, kdaj bo v večjem obsegu začelo prihajati do vdorov in množične kraje osebnih datotek posameznikov, in ne samo podjetij, saj hekerji že zdaj nadzorujejo množico računalnikov. Zgolj vprašanje časa je, kdaj jih bodo začeli pregledovati, oziroma uporabljati programe za pregledovanje, indeksacijo in iskanje datotek v ugrabljenih računalnikih.[403] Zaradi pospešenega širjenja digitalne tehnologije posamezniki hranijo čedalje več dokumentov v elektronski obliki, hkrati pa stalna in hitra povezava v internet postaja cenovno zelo ugodna. V slabo zaščitenih in v internet vključenih osebnih računalnikih tako posamezniki hranijo vse več digitalnih fotografij, zasebne elektronske pošte, zasebnih dokumentov itd. To pomeni, da se dogaja, da je zasebni prostor posameznikov pa tudi podjetij lahko dostopen, napadalci pa imajo na voljo vse tehnologije in orodja za enostaven in hiter vdor. Nekateri primeri javne objave intimnih fotografij kažejo, da se to morda že dogaja tudi v Sloveniji.[404]

Zaradi povečanega števila varnostnih incidentov, delno pa tudi odkritih varnostnih pomanjkljivosti, se zastavlja vprašanje, ali lahko uporabniki v kiberprostoru v praksi sploh pričakujejo (prostorsko) zasebnost. In če jo lahko, koliko časa.

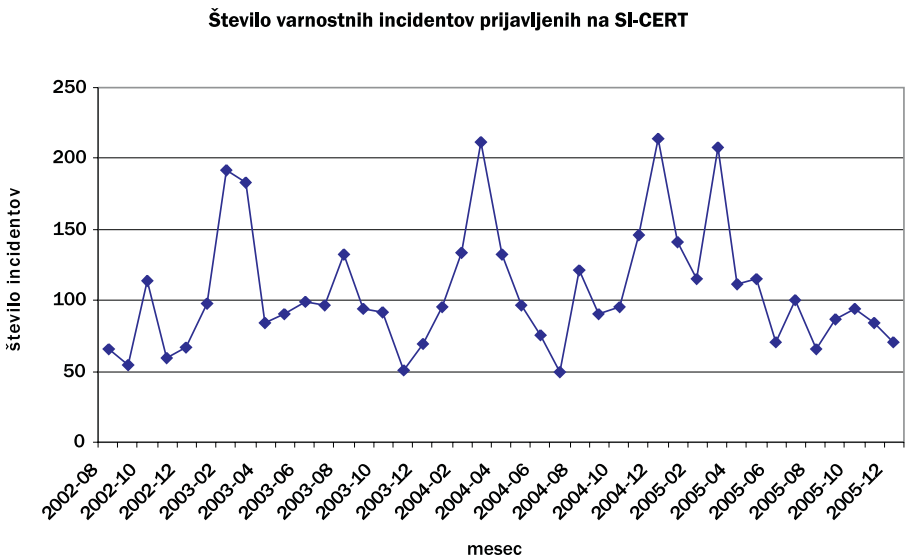
---

[403] Da je že začelo prihajati do tega, kaže primer industrijskega vohunjenja v Izraelu. Konec maja 2005 je izraelska policija zaradi suma industrijskega vohunjenja z računalniškimi trojanskimi konji aretirala nekaj oseb. Preiskava je pokazala, da so osumljenci vohunili v več uglednih izraelskih podjetjih. Za namestitev vohunskega trojanskega konja so zahtevali okrog 4000 dolarjev (Cohen, 2005).

[404] Leta 2004 in 2005 so po internetu krožile številne intimne slike različnih ljudi iz Slovenije. Kako so slike prišle v javnost, ni znano, pri nekaterih pa je bila izražena domneva, da jih je nekdo ukradel iz računalnika in posredoval v omrežja P2P.

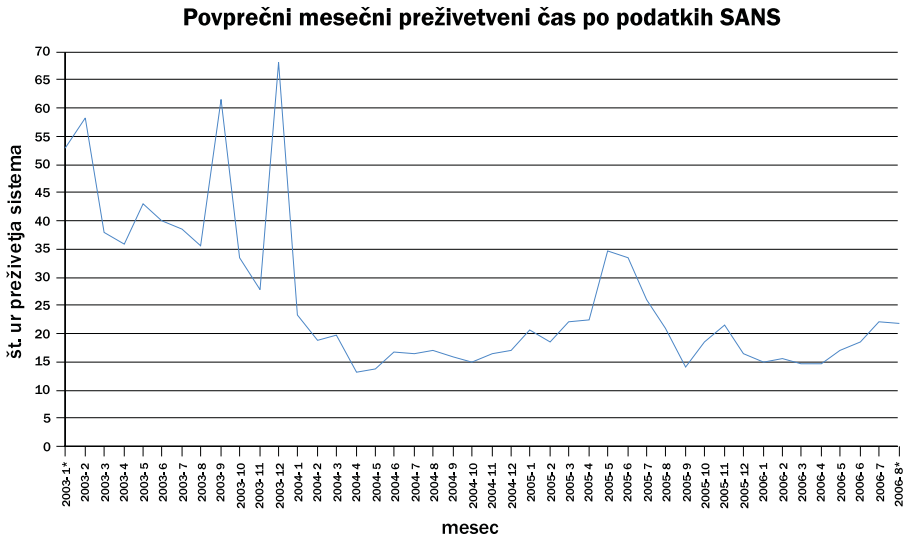


Graf 4: Varnostne pomanjkljivosti, ki so bile sporočene združenju CERT (Computer Emergency Response Team, združenje za ukrepanje ob varnostnih incidentih na internetu), ter število incidentov, ki so bili prijavljeni.
Statistika za varnostne pomanjkljivosti je na voljo od leta 1995. (*) Posamezen prijavljeni incident lahko obsega napad na večje število spletnih strani (lahko tudi več sto ali več tisoč), poleg tega gre pri posameznem incidentu lahko za zlonamerno dejavnost, ki je trajala več časa, oziroma se je večkrat ponovila. Podatki za leto 2004 so za prva tri četrtletja. Vir: CERT, 2004. Poudariti je treba, da gre samo za prijavljene incidente. CERT ocenjuje, da je prijavljenih le okrog 20 % vseh incidentov (Boehlert, 2002).



Graf 5: Število obravnavanih oz. prijavljenih incidentov s strani slovenskega SI-CERT v Sloveniji med avgustom 2002 in decembrom 2005; povprečje je 106 incidentov na mesec (Vir: Božič, 2006).

Na vprašanje, koliko časa preteče od vključitve v omrežje do uspešnega vdora, je skušala odgovoriti raziskava preživetvenega časa računalnika na internetu (ang. *time to live*, včasih tudi *survival time*). Preživetveni čas je definiran kot čas, ki poteče od vključitve računalnika brez vključenih posebnih varnostnih mehanizmov v internet do prvega poskusa oziroma vdora vanj; v primeru starejših sistemov npr. Windows 2000 ali Windows Xp brez SP pa je že prvi poizkus uspešen. Po raziskavi *Internet Storm Centra*, ki deluje v okviru inštituta SANS, se je povprečni preživetveni čas sveže naloženega sistema brez najnovejših varnostnih popravkov zmanjšal z dobrih 44 minut leta 2003 na dobrih 16 minut leta 2004 oziroma dobrih 21 minut leta 2005 (SANS, 2004 in SANS, 2006).



Graf 6: Povprečni mesečni preživetveni čas v minutah za obdobje od 15. januarja 2003 do 13. avgusta 2006 po podatkih SANS. Podatki za januar 2003 in avgust 2006 so delni. Povprečni preživetveni čas je izračunan po metodologiji SANS: povprečno število napadov na sistem na dan = število zabeleženih napadov/število napadenih sistemov; povprečni preživetveni čas v minutah = 24 * 60/povprečno število napadov na sistem na dan. (Vir: SANS, 2006).

Podobne rezultate je dal eksperiment Kevina Mitnicka in Marcusa V. Colombana, ki sta ga izvedla v času od 9. do 23. septembra 2004. V eksperimentu sta na internet priključila šest računalnikov z različnimi operacijskimi sistemi (Windows Xp SP1 z uporabo požarnega zidu in brez njega, Windows Xp SP2, Windows SBS, Mac OS X 10.3.5 ter Linspire (Linux)). V času napada so bili računalniki tarča 305.955 napadov, od tega je bilo deset napadov uspešnih, eden pa je celo uspel v manj kot štirih minutah po začetku eksperimenta.[405] Pri tem je ključnega pomena to, da so bili računalniki zgolj vključeni v omrežje in jih ni tedaj nihče uporabljal (Acohido in Swartz, 2004).

Uporaba novih tehnologij za povečanje nadzora nad posamezniki: nadzor interneta v Sloveniji

Zaradi povečanega obsega uporabe interneta in s tem posledično širjenja nezakonitih dejavnosti posameznikov na internet želijo države, razumljivo, nadzorovati internet in Slovenija ni pri tem nikakršna izjema. Problem pa je, ker se pri tem ne upošteva, da sodobna tehnologija možnosti nadzora povečuje že sama po sebi – tehtnico pomika v smer proti nadzoru in stran od zasebnosti. Zato bi bilo treba nameniti več pozornosti varstvu zasebnosti. Tako pa razmerje med zasebnostjo in nadzorom ostaja pod vplivom tehnologije praviloma neuravnoteženo, pravni sistem pa praviloma le legitimira trenutno stanje in s tem težišče dokončno premika stran od zasebnosti. To dokazujejo tudi začetki uvedbe nadzora nad internetom v Sloveniji. Slovenija je med podpisnicami *Konvencije o kibernetski kriminaliteti*,[406] ki v 20. členu daje podlago za prestrezanje prometnih podatkov v realnem času, v 21. členu pa podlago za prestrezanje vsebinskih podatkov (torej internetnega prometa). Na podlagi konvencije je bil sprejet *Zakon o elektronskih komunikacijah*,[407] v katerem v 107. členu piše, da mora operater "*na svoje stroške zagotoviti ustrezno opremo v svojem omrežju in primerne vmesnike, ki v njegovem omrežju omogočajo zakonito prestrezanje komunikacij.*" Operaterji so definirani kot "*fizične ali pravne osebe, ki zagotavljajo javna komunikacijska omrežja ali z njimi povezane zmogljivosti oziroma izvajajo javne komunikacijske storitve*" (3. člen), torej so operaterji tudi ponudniki dostopa do interneta.

107. člen ZeKOM[408] je sprožil številne odzive civilne družbe, predvsem ponudnikov dostopa do interneta, saj so cene prestreznih naprav, katerih stroške naj bi pokrili sami operaterji, razmeroma visoke (tudi nekaj sto tisoč dolarjev[409]). Taka rešitev zgodovinsko izvira iz dejstva, da

---

[405] Podoben eksperiment je bil izveden tudi na Fakulteti za družbene vede. V začetku decembra 2004 smo v fakultetno internetno omrežje vključili računalnik s sveže naloženim operacijskim sistemom Windows 2000 SP4. Računalnik je bil vključen v omrežje, vendar ni bil uporabljan. Uspešen vdor je bil zaznan v času od 17 do 20 ur po vključitvi v internet (Kovačič in Koren, 2004).

[406] Svet Evrope. 2001. Konvencija o kibernetski kriminaliteti (Convention on Cybercrime), sprejel jo je Svet Evrope, 23. novembra 2001. Uradni list RS, Mednarodne pogodbe, št. 17/2004. Konvencijo je državni zbor Republike Slovenije ratificiral 20. 5. 2004. Veljati je začela 1. 1. 2005.

[407] Zakon o elektronskih komunikacijah (ZeKOM), Uradni list RS, št. 43/04 in 86/04 – ZVOP-1.

[408] Zakon o elektronskih komunikacijah (ZeKOM), Uradni list RS, št. 43/04 in 86/04 – ZVOP-1.

[409] Darko Bulat, predsednik slovenskega združenja ponudnikov dostopa do interneta SISPA in direktor podjetja K2.net, je v intervjuju za Slo-Tech povedal: "*V najostrejši različici so stroški razreda velikosti 100.000 evrov do 700.000 evrov po posameznem ponudniku interneta.*" (Kovačič, 2004b).

so bila v preteklosti telekomunikacijska podjetja v državni lasti. Vprašanje pa je, ali je pokrivanje teh stroškov s strani operaterjev upravičeno v primeru zasebnih in od države neodvisnih gospodarskih družb, saj ostaja odprto, ali takšna določba ne vnaša nesorazmernosti med interes države in interes zasebnih operaterjev. Leta 2006 sprejeti *Pravilnik o opremi in vmesnikih za zakonito prestrezanje komunikacij*[410] v 5. členu omogoča operaterjem povezovanje prestrezne opreme in s tem nižanje stroškov. Tako lahko več operaterjev skupaj zagotovi potrebno opremo za prestrezanje, oziroma lahko posamezen operater svoje omrežje poveže s prestrezno opremo drugega operaterja. Podobno rešitev, kot velja v Sloveniji, sicer poznajo še v Rusiji in Ukrajini. A v Rusiji morajo ponudniki internetnih storitev pridobiti licenco za opravljanje svojih storitev, namestitev prestrezne naprave (gre za sistem SORM-2) pa je pogoj za pridobitev licence (Laurant, 2003: 420). V Ukrajini so tako rešitev podprli večji operaterji, saj pričakujejo, da bodo s tem onemogočili konkurenco manjših operaterjev (Laurant, 2003: 509). Povsem drugače pa je urejeno v Avstriji in ZDA. V ZDA je stroške namestitve in vzdrževanja Carnivora kril FBI, med drugim tudi zato, da so utišali nasprotovanja operaterjev. V Avstriji pa je na podlagi pritožbe avstrijskih ponudnikov telekomunikacijskih storitev avstrijsko zvezno ustavno sodišče 27. februarja 2003 razsodilo, da je prenašanje stroškov za nakup naprav za prestrezanje komunikacij na operaterje neustavno, razen v izjemnih primerih, ko lahko država dokaže, da je upravičeno, da stroške krije zasebni sektor (Schröder in Laurant, 2005).

Prestrezanje internetnega prometa pa je sporno še iz dveh razlogov, in sicer zaradi vprašljive učinkovitosti takega nadzora ter s stališča človekovih pravic. Obe dilemi sta se odprli tudi ob sprejemu ZeKOM[411] v Sloveniji. Glede učinkovitosti in uporabnosti nadzora se namreč postavlja vprašanje, v katerih primerih bi policija sploh lahko izvajala nadzor nad internetom in ali je kdaj naletela na tehnične omejitve pri tem nadzorovanju. *Zakon o kazenskem postopku*[412] namreč v 150. členu določa, da je mogoče odrediti nadzor elektronskih komunikacij s prisluškovanjem in snemanjem ter nadzor in zavarovanje dokazov o vseh oblikah komuniciranja, ki se prenašajo v elektronskem komunikacijskem omrežju, če obstajajo utemeljeni razlogi za sum, da je določena oseba izvedla, izvaja ali pripravlja oziroma organizira izvedbo katerega izmed kaznivih dejanj:

- kazniva dejanja zoper varnost Republike Slovenije in njeno ustavno ureditev in kazniva dejanja zoper človečnost in mednarodno pravo, za katera je v zakonu predpisana kazen zapora pet ali več let;
- kaznivo dejanje ugrabitve po 144. členu, prikazovanja, posesti, izdelave in posredovanja pornografskega gradiva po 187. členu, neopravičene proizvodnje in prometa z mamili po 196. členu, omogočanja uživanja mamil po 197. členu, izsiljevanja po 218. členu, zlorabe notranje informacije po 243. členu, nedovoljenega sprejemanja daril po 247. členu, neupravičenega dajanja daril po

[410] Pravilnik o opremi in vmesnikih za zakonito prestrezanje komunikacij, Uradni list RS, št. 29/2006.

[411] Zakon o elektronskih komunikacijah (ZeKOM), Uradni list RS, št. 43/04 in 86/04 – ZVOP-1.

[412] Zakon o kazenskem postopku (ZKP), Uradni list RS, št. 63/94, 70/94, 25/96-odl. US, 39/96-odl. US, 5/98-odl. US, 49/98, 66/98, 72/98, 6/99, 42/00-odl. US, 66/00, 111/01, 32/02 - odl. US, 110/02 - ZDT-B, 3/03 - odl. US, 21/03 - odl. US, 44/03 - odl. US, 56/03, 92/03-odl. US, 114/03-odl. US, 43/04, 68/04-odl. US in 83/04-odl. US.

248. členu, pranja denarja po 252. členu, tihotapstva po 255. členu, jemanja podkupnine po 267. členu, dajanja podkupnine po 268. členu, sprejemanja daril za nezakonito posredovanje po 269. členu, dajanja daril za nezakonito posredovanje po 269.a členu, hudodelskega združevanja po 297. členu, nedovoljene proizvodnje in prometa orožja ali razstrelilnih snovi po 310. členu ter povzročitve nevarnosti z jedrskimi snovmi po tretjem odstavku 319. člena kazenskega zakonika Republike Slovenije;

- druga kazniva dejanja, za katera je v zakonu predpisana kazen zapora osem ali več let;
- in če obstaja utemeljen sum, da se za komunikacijo v zvezi s tem kaznivim dejanjem uporablja določeno komunikacijsko sredstvo oziroma računalniški sistem, ali bo to sredstvo oziroma sistem uporabljen, pri tem pa je mogoče utemeljeno sklepati, da se z drugimi ukrepi ne bi dalo zbrati dokazov, oziroma bi njihovo zbiranje lahko ogrozilo življenje ali zdravje ljudi (150. člen ZKP).

V *Kazenskem zakoniku*[413] (KZ) so kot kazniva dejanja, ki bi jih lahko šteli med t. i. računalniška kazniva dejanja oziroma kazniva dejanja, ki jih je mogoče izvesti ob pomoči računalniška ali informacijske tehnologije, opredeljana naslednja ravnanja:

- neupravičeno prisluškovanje in zvočno snemanje (148.člen KZ, v osnovi ne gre za t. i. "računalniško kaznivo dejanje");
- neupravičeno slikovno snemanje (149.člen KZ, v osnovi ne gre za t. i. "računalniško kaznivo dejanje");
- kršitev tajnosti občil (2. točka 2. odstavka 150. člena KZ, v osnovi ne gre za t. i. "računalniško kaznivo dejanje");
- nedovoljena objava zasebnih pisanj (151. člen KZ, v osnovi ne gre za t. i. "računalniško kaznivo dejanje");
- zloraba osebnih podatkov (2. odstavek 154. člena KZ);
- kršitev avtorske pravice (2. odstavek 158. člena KZ);
- neupravičeno izkoriščanje avtorskega dela (159. člen KZ);
- kršitev avtorski sorodnih pravic (160. člen KZ, v osnovi ne gre za t. i. "računalniško kaznivo dejanje");
- neupravičen vstop v informacijski sistem (225. člen KZ);
- vdor v informacijski sistem (242. člen KZ);
- izdelovanje in pridobivanje orožja in pripomočkov, namenjenih za kaznivo dejanje (3. odstavek 309. člena KZ).

[413] Kazenski zakonik (KZ), Uradni list RS, št. 63/94, 70/94-popr., 23/99-KZ-A, 110/02-ZDT-B, 40/04-KZ-B in 95/04-KZ-UPB1.

Ker pa nobeno od teh kaznivih dejanj ni opredeljeno v 150. členu ZKP in za nobeno od teh kaznivih dejanj ni predpisana zaporna kazen, višja od 8 let, to pomeni, da za kazniva dejanja s področja računalniškega oziroma predvsem "klasičnega" internetnega kriminala trenutno sploh ni mogoče uporabiti ukrepa prestrezanja internetnega prometa.

Na vprašanje, kolikšen je siceršnji obseg nadzorovanja interneta oziroma ali je obseg nadzorovanja interneta tak, da upravičuje stroške iz 107. člena ZeKOM,[414] pa žal ni mogoče dobiti uradnega odgovora, saj policija statistično beleži le ukrepe po posameznih točkah prvega odstavka 150. člena, ne pa tudi po vrsti nadorovanega komunikacijskega sredstva (Policija, 2004). Je pa mogoče dobiti približne indikatorje iz nekaterih drugih policijskih evidenc.

leto	1998	1999	2000	2001	2002	2003	2004	2005
Policijski nadzor:*								
število nadzorovanih telekomunikacijskih sredstev	318	287	318	453	505	472	677	746
število oseb, ki jim je policija nadzorovala telekomunikacije	176	163	151	199	222	168	167	198
Kazniva dejanja:**								
neupravičeno izkoriščanje avtorskega dela	–	14	11	23	17	12	18	17
neupravičen vstop v zaščiteno računalniško bazo podatkov	–	9	12	2	6	2	–	–
vdor v računalniški sistem	–	13	15	6	1	–	0	5
neupravičen vstop v informacijski sistem	–	–	–	–	–	–	10	30
izdelava ali pridobitev pripomočkov za vdor v računalniški sistem	–	–	–	0	6	–	–	–

Tabela 1: Pregled nekaterih policijskih ukrepov nadzorovanja, števila zaseženih računalnikov ter kaznivih dejanj iz področja računalniške kriminalitete.

* Podatki so bili pridobljeni na podlagi zahteve za dostop do informacij javnega značaja. Policija je podatke posredovala v odgovoru z dne 17. 9. 2004 (Policija, 2004) in v odgovoru z dne 30. 8. 2006 (Policija, 2006). Gre za vsa telekomunikacijska sredstva skupaj, ne glede na obliko. V letih 2004 in 2005 policija ni prestrezala elektronske pošte ter izvedla prestrezanja internetnega prometa ali prestrezanja drugih oblik komunikacij (Policija, 2006).

** Podatki so bili pridobljeni iz letnih poročil o delu policije, ki so objavljena na spletni strani policije (<http://www.policija.si>).

[414] Zakon o elektronskih komunikacijah (ZeKOM), Uradni list RS, št. 43/04 in 86/04 – ZVOP-1.

Glede na pogovore s predstavniki ponudnikov dostopa do interneta je moč razbrati, da je obseg policijskega nadzora interneta v Sloveniji minimalen. Policijski nadzor komunikacij je torej verjetno usmerjen predvsem v nadzor telefonije. Večinoma pa gre pri nadzoru interneta za nadzor zaradi uporabe računalnika pri drugih kaznivih dejanjih (npr. v enem primeru pri nedovoljenem prometu z mamili (Kovačič, 2004a)) ali zaradi kršitve avtorskih pravic. Po neuradnih podatkih prejmejo slovenski ponudniki dostopa do interneta na leto le nekaj sodnih odredb, večinoma pa je v njih zahtevano, naj operater predloži podatke, ki omogočajo identifikacijo osumljenca na podlagi internetnih prometnih podatkov, ali pa gre za zahteve po zasegu elektronske pošte iz strežnika (Kovačič, 2004a ter pogovori z nekaterimi drugimi sistemskimi upravitelji, ki so želeli ostati anonimni).[415]

Podobno je v primeru *Slovenske obveščevalno varnostne agencije*, kjer *Zakon o Slovenski obveščevalno varnostni agenciji*[416] v 24. členu dovoljuje nadzorovanje in snemanje telekomunikacij v Republiki Sloveniji, če je podana velika verjetnost, da obstaja nevarnost za varnost države ter utemeljen sum, da se za komunikacijo uporablja določeno komunikacijsko sredstvo oziroma računalniški sistem in se z drugimi ukrepi ne bi dalo zbrati dokazov, oziroma bi njihovo zbiranje lahko ogrozilo življenje ali zdravje ljudi. Po noveli *Zakona o Slovenski obveščevalno varnostni agenciji*[417] pa je bila šestmesečna časovna omejitev osredotočenega in kontinuiranega tajnega nadzora komunikacij podaljšana na največ 24 mesecev. Razlika med policijskim nadzorom komunikacij in nadzorom SOVE je le v tem, da od SOVE ni mogoče dobiti niti splošnega podatka, koliko ukrepov nadzora komunikacij izvedejo na leto,[418] čeprav je od odločbe Up-412/03-21, ki jo je Ustavno sodišče RS izdalo decembra 2005, naprej znano, da je SOVA vsaj enkrat nezakonito prisluškovala. Leta 1996 je namreč nezakonito prisluškovala posamezniku, ki je bil osumljen in tudi obsojen za kaznivo dejanje neupravičene proizvodnje in prometa z mamili. Ustavno sodišče je ugotovilo, da je MNZ 9. 9. 1993 s SOVO sklenil tajni sporazum, na podlagi katerega je SOVA za potrebe MNZ izvajala vse postopke, vezane na ukrepe nadzora telekomunikacij. Sporazum se je uporabljal do 11. 4. 1997. Razlog za sporazum je bilo dejstvo,

---

[415] Zakon o kazenskem postopku v 3. odstavku 149.b člena določa: "*Če so podani razlogi za sum, da je bilo storjeno, oziroma da se pripravlja kaznivo dejanje, za katero se storilec preganja po uradni dolžnosti in je za odkritje tega kaznivega dejanja ali storilca potrebno pridobiti podatke o lastniku ali uporabniku določenega komunikacijskega sredstva za elektronski komunikacijski promet, ki niso objavljeni v naročniških imenikih in o času, v katerem je tako sredstvo bilo oziroma je v uporabi, lahko policija od operaterja elektronskega komunikacijskega omrežja zahteva, da ji na njeno pisno zahtevo, tudi brez privolitve posameznika, na katerega se ti podatki nanašajo, sporoči te podatke.*" (Zakon o kazenskem postopku (uradno prečiščeno besedilo) (ZKP-UPB3), Uradni list RS, št. 8/2006). Novela je bila uveljavljena aprila 2004 in sicer z Zakonom o spremembah in dopolnitvah Zakona o kazenskem postopku – ZKP-F (Uradni list RS, št. 43/04 z dne 26. 4. 2004).

[416] Zakon o Slovenski obveščevalno varnostni agenciji (ZSOVA), Uradni list RS, št. 23/99, 56/02-ZJU, 26/03-ZPNOVS, 126/03 in 54/04-ZDoh-1, 56/2004, 62/2004, 63/2004 - popr., 61/2006.

[417] Zakon o spremembah in dopolnitvah Zakona o Slovenski obveščevalno varnostni agenciji (ZSOVA-B), Uradni list RS, št. 61/2006.

[418] Odgovor SOVE z dne 23. 8. 2004 na zahtevo po dostopu do informacij javnega značaja, v katerem je SOVA delno zavrnila odgovor na vprašanje o letnem statističnem pregledu števila uporabljenih prikritih ukrepov (SOVA, 2004) ter odgovor Vrhovnega sodišča RS 20. 8. 2004 na zahtevo po dostopu do informacij javnega značaja, v katerem je le-to zavrnilo odgovor na vprašanje o letnem statističnem pregledu števila izdanih in zavrnjenih sodnih odredb predsednika Okrožnega sodišča v Ljubljani za SOVO (Vrhovno sodišče, 2004). Na obe odločbi je bila podana pritožba, vendar jo je pooblaščenka za dostop do informacij javnega 20. januarja 2005 zavrnila.

da v tistem času policija za prisluškovanje ni imela ustrezne tehnike. Ustavno sodišče je menilo, da "*težave represivnih organov s tehnično opremljenostjo ne morejo biti razlog za tak nedopusten poseg v pravico do zasebnosti in v varstvo tajnosti pisem in drugih pošiljk. Kršitve človekovih pravic in temeljnih svoboščin v kazenskem postopku namreč niso dopustne niti v 'skrajni sili'.*". Prav tako je menilo, da je tajni sporazum med MNZ in SOVO nezakonit.[419] Po nekaterih podatkih naj bi SOVA na leto pridobila okrog deset odredb za prisluškovanje (izjava Boštjana Šefica iz SOVE v oddaji 24ur, 26. avgusta 2004 (Plementaš in Sodja, 2004)). Zaenkrat pa je javno znan le en primer, ko naj bi SOVA od ponudnika dostopa do interneta zahtevala prestrezanje elektronske pošte (Žerdin, 2001).

Vsi ti podatki kažejo, da se zakoniti nadzor interneta v Sloveniji uporablja minimalno in da preiskovalci praviloma ne naletijo na primere, ko ponudnik dostopa do interneta sodne odredbe ni mogel izpolniti. (Izjema naj bi bil omenjeni primer SOVE, vendar uradnih podatkov o tem ni.) Zato so se kmalu po sprejemu ZeKOM[420] ponudniki dostopa do interneta začeli spraševati, ali so stroški, ki jim jih nalaga zakon, sploh upravičeni, med drugim tudi zato, ker zakonito prestrezanje na internetu poleg povečane možnosti zlorab že po definiciji ogroža omrežno varnost in omogoča nezakonite zlorabe s strani kiberkriminala. Ti sistemi so tudi zapleteni in jih je drago vzdrževati, zahtevajo pa tudi ustrezno kadrovsko usposabljanje, ki prav tako predstavlja strošek (Branch, 2003).

Vendar je nadzor interneta lahko vprašljiv tudi s stališča človekovih pravic, saj se ob njem zastavlja vprašanje, ali je tak ukrep sorazmeren ali pa morda nesorazmerno posega v pravice posameznika. Pri nadzoru interneta so namreč možnosti zlorab večje kot pri nadzoru drugih telekomunikacijskih sredstev. Da je tako vprašanje povsem na mestu, se je izkazalo tudi ob pripravi *Pravilnika o opremi in vmesnikih za zakonito prestrezanje komunikacij*.[421] Šesti odstavek 107. člena ZeKOM[422] namreč zahteva sprejem pravilnika, po katerem minister, pristojen za elektronske komunikacije, v soglasju z ministroma, pristojnima za notranje zadeve in za obrambo, ter direktorjem SOVE predpiše funkcionalnost opreme in določi primerne vmesnike za zakonito prestrezanje komunikacij prek interneta.

Ministrstvo za informacijsko družbo je zato 1. junija 2004 sklicalo sestanek na temo zakonitega prestrezanja internetnega prometa, na katerem naj bi našli predloge za pripravo omenjenega pravilnika. Na sestanek pa so bili povabljeni predstavniki policije ter nekateri predstavniki ponudnikov dostopa do interneta. Na sestanku so predstavniki policije (poleg operaterjev) opozorili na pogubne finančne posledice 107. člena ter predlagali tri možne rešitve:

---

[419] Julija 2005 so slovenski mediji poročali o tem, da so na SOVI odkrili dva primera uslužbencev, zaposlenih na podlagi ponarejenih spričeval. Eden izmed njiju je bil po poročanju POP TV "*šef t. i. oddelka prisluha etra in fizičnega priklopa, kar z drugimi besedami pomeni tehniko, ki s pomočjo računalniškega programa lahko razvozla zapletene signale mobilne telefonije*" (Vodušek, 2005). Če drži, da je bila na tako občutljivem mestu zaposlena oseba s ponarejenim spričevalom, je to vsekakor lahko zaskrbljujoče.

[420] Zakon o elektronskih komunikacijah (ZeKOM), Uradni list RS, št. 43/04 in 86/04 – ZVOP-1.

[421] Pravilnik o opremi in vmesnikih za zakonito prestrezanje komunikacij, Uradni list RS, št. 29/2006.

[422] Zakon o elektronskih komunikacijah (ZeKOM), Uradni list RS, št. 43/04 in 86/04 – ZVOP-1.

> "*1. Ponudniki internetnih storitev sami zagotovijo ustrezno opremo za prestrezanje in vmesnik po standardu ETSI. Ta možnost pomeni velik finančni vložek za ponudnike internetnih storitev in bi najverjetneje povzročila ugašanje dejavnosti ter tako oženje konkurence ponudnikov internetnih storitev.*
> *2. Veliki ponudniki internetnih storitev postavijo nadzorne centre za prestrezanje komunikacij, ki so v skladu s standardi ETSI. Manjšim operaterjem se priskrbi prestrezno mobilno opremo. Nadzor se prek zakupljenih vodov opravi v nadzornem centru policije.*
> *Ta način pomeni neenak položaj operaterjev, posebej problematična pa je logistika same izvedbe.*
> *3. Vzpostavitev nadzornega centra na ravni SISPe*[423] *z vmesnikom, ki bo v skladu s standardi ETSI. Vsi operaterji bi v svojih omrežjih zagotovili namestitev sond za prestrezanje.*"
> (Zapisnik sestanka "*Izvedba zakonitega prestrezanja telekomunikacijskega prometa, ki poteka prek interneta*" (Ministrstvo za informacijsko družbo, 2004b)).

Iz zapisnika sledi, da so predstavniki policije kljub nevarnostim, ki jih prinaša nadzor paketnih omrežij, kot eno izmed možnih in celo kot najbolj zaželeno rešitev predlagali prav centralizacijo nadzora interneta. Taki predlogi s strani represivnih organov so sicer razumljivi, a so kljub temu vsaj nevarni, saj povečujejo možnost zlorab, zato je bil predlog tarča številnih kritik.[424]

Pravilnik o zakonitem prestrezanju komunikacij, ki bo predpisal funkcionalnost opreme in primeren vmesnik tudi za zakonito prestrezanje komunikacij prek interneta, bi moral biti sprejet do novembra 2004, dejansko pa je bil v Uradnem listu objavljen šele konec maja 2006.[425] Zakoniti nadzor interneta se je tako uveljavil tudi v Sloveniji, še povečal pa se bo z uvedbo *Direktive o obvezni hrambi prometnih podatkov*[426] v slovenski pravni red. V praksi se bo tako razmerje med nadzorom in zasebnostjo pod vplivom tehnologije (in poznejše legitimacije trenutnega stanja) še enkrat premaknilo na škodo zasebnosti.

---

[423] SISPA – *Slovenian Internet Service Provider's Association* - združenje slovenskih ponudnikov dostopa do interneta. Vzpostavitev nadzornega centra na ravni SISPE pomeni vzpostavitev centralnega nadzornega centra za vse ponudnike dostopa do interneta v Sloveniji, razen za SiOL, ki ni član SISPE.

[424] 5. člen *Pravilnika o opremi in vmesnikih za zakonito prestrezanje komunikacij (Uradni list RS, št. 29/2006)* operaterjem omogoča povezovanje pri izvajanju nadzora komunikacij. Vzpostavitev enotnega nadzornega centra ni predvidena.

[425] Predlog Pravilnika o opremi in vmesnikih za zakonito prestrezanje komunikacij je ministrstvo za gospodarstvo pripravilo aprila 2005.

[426] Direktiva 2006/24/ES Evropskega parlamenta in Sveta z dne 15. marca 2006 o hrambi podatkov, pridobljenih ali obdelanih v zvezi z zagotavljanjem javno dostopnih elektronskih komunikacijskih storitev ali javnih komunikacijskih omrežij, in spremembi Direktive 2002/58/ES (Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC), sprejeta 14. 12. 2005. Official Journal L 105, 13/04/2006, p. 0054 - 0063.

Smeri nadzora in zasebnosti na internetu v prihodnosti

Dejstvo je, da imajo današnji računalniški sistemi, predvsem tisti v okolju Windows, številne varnostne pomanjkljivosti. Zanje se sicer prej ali slej najdejo ustrezni popravki, vendar si jih njihovi uporabniki pogosto ne namestijo dovolj hitro ali pa si jih sploh ne; včasih, ker popravki prinašajo nove varnostne[427] in siceršnje probleme, še pogosteje pa zato, ker zanje niti ne vedo. To sta pokazala tudi primera črvov *Blaster* in *Slammer*, za katera so bili pred izbruhom, ki je skoraj povsem ohromil internet, varnostni popravki že dalj časa na voljo, številni uporabniki pa si jih sploh niso naložili.[428] Razlog za tako ravnanje je v tem, da rast interneta poteka na obrobju, med uporabniki, ki nimajo računalniško-varnostnih znanj (Geer et. al., 2003: 9, 11); nevešči uporabniki na robu omrežja so zato čedalje pogostejša, predvsem pa lahka tarča napadalcev. S širjenjem tehnologije se ta problem le še poglablja. Po oceni avtorjev poročila *CyberInsecurity: The Cost of Monopoly* se moč tistih, ki zlorabljajo računalniške sisteme, vsakih 10 mesecev podvoji, in sicer zato, ker razvoj tehnologije omogoča, da si napadalci za isti denar kupijo čedalje boljšo tehnologijo, hkrati pa se veča tudi število nezaščitenih omreženih računalnikov (Geer et. al., 2003: 8). Zato se čedalje pogosteje dogaja, da imajo morebitni napadalci na voljo vsa orodja in informacije, potrebne za napad, uporabniki interneta pa ostajajo nezaščiteni. Slednji so čedalje pogosteje uporabniki na obrobju, torej uporabniki brez tehničnih znanj, zato lahko pričakujemo še več zlorab zasebnosti ravno nad njimi.

Vendar pa je odgovor na vprašanje, kaj je razlog za nevarnosti v sodobnem računalništvu (in kakšne bodo zaradi tega usmeritve v prihodnje), precej globji. Septembra 2003 je sedem uglednih strokovnjakov s področja računalniške varnosti pripravilo poročilo z naslovom *CyberInsecurity: The Cost of Monopoly*. V njem ugotavljajo, da se sodobni virusi silno hitro širijo iz enega sistema v drugega (po sistemu domin (ang. *cascade failure*)), ker imajo skoraj vsi sistemi enake varnostne pomanjkljivosti (Geer et. al., 2003: 10). Virusi in črvi tako skušajo pri vseh sistemih izkoristiti isto varnostno ranljivost, za napad pa ni potrebna podrobna analiza vsakega sistema.

Dejstvo je namreč, da ima Microsoft praktično monopolni tržni delež na trgu operacijskih sistemov (več kot 90 % leta 2002 (Geer et. al., 2003: 12)), zato navzočnost operacijskega sistema Windows v osebnih računalnikih in širjenje istega sistema še v strežniške računalnike po mnenju avtorjev poročila predstavlja monokulturo. Monokulturni sistemi pa so za napade veliko bolj občutljivi od multikulturnih.

---

[427] Po določeni stopnji kompleksnosti programske kode se začne dogajati, da krpanje razpok v sistemu varnosti začne povzročati nove razpoke (Geer et. al., 2003: 15). Ta problem se je dokaj očitno začel kazati pri izdaji popravkov za Windows Xp Service Pack 2, kjer so popravki poleg tega, da so povzročili številne probleme v delovanju računalnikov, prinesli še nekaj novih razpok v varnosti, ki jih je moral Microsoft pozneje odpraviti.

[428] Črv Slammer je leta 2003 celo za pet ur ohromil nadzorno varnostni sistem jedrske elektrarne v Ohiu. V času incidenta je bila jedrska elektrarna sicer v mirovanju, podvojeni del varnostnega sistema elektrarne pa ni bil ogrožen (Poulsen, 2003).

Nastanek monokulture pa ni naključje. To je dokazal tudi protimonopolni postopek proti Microsoftu v ZDA, ki se je začel leta 1998. Microsoft je namreč svojemu operacijskemu sistemu prilagal brezplačen brskalnik *Internet Explorer* in s tem začel s trga izrivati konkurenčni *Netscape Navigator* (Wired News, 2002). Podjetje Netscape je zahtevalo, da Microsoft operacijski sistem Windows začne prodajati brez priloženega spletnega brskalnika, zato je Microsoft začel *Internet Explorer* in druge dodatne programske module namerno integrirati globoko v operacijski sistem. Po mnenju avtorjev omenjenega poročila pa Microsoft te integracije ni opravil zato, ker je potrebna zaradi samih zahtev tehnologije, temveč zato, da bi onemogočal konkurenco in uporabnike priklenil nase (Geer et. al., 2003: 4, 13). S povečanjem kompleksnosti pa se je povečalo tudi število varnostnih pomanjkljivosti. Zato avtorji sklepajo, da je številčnost razpok v varnosti (ang. *security flaw*) posledica Microsoftove monopolne moči: "*Ko je monokultura podpirana in vsiljena s priklepanjem uporabnikov, kot se dogaja z operacijskim sistemom Windows, odgovornost za [varnostne] napake nosi tisti, ki to priklepanje uporabnikov izvaja – z drugimi besedami, odgovornost je na strani Microsofta.*" (Geer et. al., 2003: 18).

Avtorji celo menijo, da bodo neuspešni tudi poskusi podjetja Microsoft, da bi izboljšal varnost svojih sistemov, če bo stranski učinek tega še večje priklepanje uporabnikov nanje (Geer et. al., 2003: 5). V tem kontekstu razumevanja problema varnosti računalniških sistemov in s tem zasebnosti v kiberprostoru pa je t. i. zaupanja vredno računalništvo (*Trusted Computing*), povezano s poskusi zaščite intelektualne lastnine, problematično še z enega vidika. Ne zgolj zato, ker bo tehnologija TC omogočala zbiranje velikega števila osebnih podatkov, temveč tudi zato, ker bo uporabnike programskih izdelkov podjetja Microsoft še bolj priklenila nase (z onemogočanjem združljivosti in s tem prehoda med TC in neTC programi, storitvami in celo datotekami[429]). Tako bo ustvarila še obširnejšo monokulturo.

Danes je internet postal bojišče različnih interesov (marketinške industrije, kiberkriminala, državnih organov in tajnih služb) pa tudi avtomatov (virusov in črvov), ki postajajo pravi kolonizatorji kiberprostora. Nemoč držav, da bi sledile novemu in hitro razvijajočemu se mediju ter da bi regulirale (zlo)uporabo tehnologije v zasebnem sektorju (namesto tega so raje zgolj legalizirale trenutno stanje[430]) in zaščitile pravice posameznikov (namesto tega raje ščitijo pravice korporacij in lastnikov intelektualne lastnine), je privedla do tega, da so se znašli najbolj na udaru navadni uporabniki na obrobju. Ti se brez ustreznega znanja in izkušenj niso sposobni

---

[429] Ena izmed zelo razširjenih bojazni je, da uporabniki v aplikacijah, nezdružljivih s TC, ne bodo mogli uporabljati svojih dokumentov in elektronske pošte, ki bo ustvarjena v aplikacijah TC. Da je taka bojazen upravičena, kaže primer Mobitelove spletne glasbene trgovine *zabavaj.se*, ki omogoča nakup glasbe prek interneta, vendar mora kupec pri nakupu in predvajanju skladb uporabljati Microsoftov operacijski sistem *Microsoft Windows*, Microsoftov brskalnik *Internet Explorer* in Microsoftov predvajalnik glasbe *Windows Media Player*, kupljenih datotek pa ne more predvajati z drugačno programsko opremo, niti na drugih računalnikih z enako programsko opremo ne.

[430] Primer legalizacije obstoječega stanja je regulacija videonadzora v noveli zakona o vastvu osebnih podatkov (Zakonu o varstvu osebnih podatkov (ZVOP-1), Uradni list RS, št. 86/04) iz leta 2004. Če bi do uveljavitve te novele oziroma sprememb zakona o zasebnem varovanju (Zakon o zasebnem varovanju (ZZasV), Uradni list RS, št. 126/02) novembra 2004, dosledno izvajali stari zakon o varstvu osebnih podatkov, se videonadzora v Sloveniji zelo verjetno sploh ne bi moglo oziroma smelo izvajati. ZZasV pa je v 43. členu zgolj določil, kdo sme upravljati videonadzorni sistem, ZVOP-1 pa je v členih od 74 do 77 le nekoliko podrobneje določil, kako je treba posameznike obvestiti o videonadzoru in kako se sme videonadzor izvajati na nekaterih občutljivih lokacijah, kot so večstanovanjske zgradbe in delovno mesto.

ubraniti pred novimi nevarnostmi, ki jih prinaša tehnologija. Tembolj, ker jih ne ščitijo ne izdelovalci tehnoloških rešitev, ne država. Za stopnjo zasebnosti, ki je bila prej samoumevna, se morajo posamezniki zdaj boriti aktivneje in z veliko samodicipline. Hkrati zasebnost v sodobni družbi postaja strošek, nadzor pa sredstvo vključitve v družbo in možnost pridobiti si različne ugodnosti in koristi. Nadzor je postal neopazen, kdor pa si želi izboriti zasebnost, postane še bolj viden, saj izstopi iz povprečja.

Izdelovalci programske opreme nimajo interesa povečevati varnosti računalniškega delovanja, še manj jim je mar zasebnosti posameznikov; celo nasprotno, saj želijo učinkovito zaščititi intelektualno lastnino in uporabljati napredne marketinške prijeme. Države pa so protiteroristične ukrepe po 11. septembru izkoristile za povečevanje rabe nadzorovalnih tehnologij. Kam lahko vodijo taki ukrepi, kaže primer Kitajske. Aprila 2006 je Ethan Gutmann v pričanju pred ameriškim parlamentarnim komitejem za mednarodne odnose izjavil, da je podjetje Cisco kitajski vladi prodalo poseben požarni zid za cenzuriranje dostopa do interneta in vzpostavilo posebno omrežje (t. i. "Policenet") za državne varnostne organe. To, da Kitajska s cenzorskim sistemom, imenovanim tudi *Great Firewall of China*, razmeroma uspešno cenzurira internet kitajskim uporabnikom, je znano že dlje časa. Gutmann pa trdi, da s tehnologijo "Policeneta" kitajski policist lahko na ulici ustavi kateregakoli državljana, odčita njegovo osebno izkaznico in v realnem času odpre njegovo kartoteko, ki vsebuje: podatke o političnem vedenju, družinsko zgodovino, prstni odtis in druge slike, zgodovino njegove rabe interneta za zadnjih 60 dni (obiskane spletne strani itd.), ter prebere njegovo elektronsko pošto (Gutmann, 2006: 4). To pa so že zmožnosti nadzora, ki so bile še pred nekaj leti le oddaljena znanstvena fantastika.

Vse to za zasebnost posameznikov na internetu ne pomeni nič dobrega. Nove tehnologije so napravile transparentnega predvsem posameznika, njihova osvobodilna vloga pa praviloma ostaja neizkoriščena. Kaže, da se bo to na internetu le še poglabljalo.

SKLEP

Pomen nadzora posameznikov se v sodobni družbi kaže kot ambivalenten, in sicer v dveh smislih. Po eni strani je nadzor namenjen 'upravljanju' ljudi in gospodovanju nad njimi, po drugi strani pa ljudem sploh omogoča življenje v družbi. Poleg tega oblast ali družba lahko nadzor uporabljata proti posameznikom, hkrati pa lahko posameznik nadzor uporabi proti nosilcem moči.

Do prve ambivalentnosti je po Foucaultu začelo prihajati na prehodu iz disciplinskih v regulacijske družbe. Foucault ta prehod opisuje kot prehod iz družbe suverenosti, ki je usmrtila ali pustila živeti, v regulacijsko družbo, ki omogoča življenje ali pa pusti umreti (Foucault, 1997/2003: 157). Oblast postane pastoralna, deluje pa tako, da okrog naključnosti življenja namešča varnostne mehanizme (različna zavarovanja, regulacijske politike itd.), ki ne delujejo na ravni posameznika, temveč na ravni populacije. Če je bila zamisel o nadzoru tradicionalno povezana z Benthamovo zamislijo Panoptikona in Inšpektorja, ki bdi nad vedenjem zapornikov, zdaj Inšpektor postane Birokrat, namesto posameznikov pa nadzoruje družbo (Whitaker, 1999: 43).

Ni naključje, da se v tem prehodu razvije statistični nadzor, katerega namen je pridobivanje védenja zaradi upravljanja. Nekateri avtorji, npr. Whitaker, menijo, da je 20. stoletje stoletje obveščevalne dejavnosti. Obveščevalna dejavnost v smislu avtomatičnega pridobivanja, analize in interpretacije informacij ni več samo v domeni države, marveč jo čedalje bolj uporabljajo tudi zasebna podjetja. Primeri pronicanja obveščevalne tehnologije v zasebni sektor (npr. leta 1996 razviti sistem za opazovanje in profiliranje uporabnikov interneta *SelectCast*) zato niso naključni. Tarča obveščevalne dejavnosti nismo samo kot državljani, temveč čedalje bolj kot potrošniki.

Množični nadzor nad podatkovi postaja rutinski, ključna postane identifikacija tveganja in priložnosti ter ciljnih skupin, posledica pa je profiliranje posameznikov in njihovo razvrščanje v kategorije. V razvoju sodobnih nadzorovalnih sistemov postajajo čedalje pomembnejši katalogiziranje, predvidevanje in preventiva. Posledica tega je, da krivda ali nedolžnost posameznika nista pomembni, pomembno je tveganje (ali priložnost), ki ga skupina ljudi predstavlja za organizacijo.

Poleg tega se pri prehodu v regulacijske družbe, ki omogočajo življenje ali pustijo umreti, kot pravi Foucault, spremeni tudi način kaznovanja. Kazen ni samo neposredna, fizična, temveč se je spremenila v ekonomijo odvzetih pravic. Hkrati pa smo posamezniki že s samo participacijo v družbi izpostavljeni nadzoru; ta izpostavljenost je nujna, če želimo živeti v družbi. Slogan iz Orwellovega romana "*Veliki Brat te opazuje!*" se spreminja v "*Veliki Brat skrbi zate*" (Whitaker, 1999: 142), življenje v sodobni družbi pa nujno zahteva pristanek na določeno stopnjo nadzora. Posamezniku, ki ne želi biti nadzorovan, preostane samo eno – prostovoljen izstop iz družbe in s tem nekakšna (družbena) smrt. Če posameznik izstopi iz sistema nadzorovanja, ga družba kaznuje tako, da ga "pusti umreti", oziroma ga izključi iz možnosti, pridobiti si različne ugodnosti in koristi. Še več, če vstopi v sistem nadzorovanja, je nagrajen (npr. potrošniške

kartice zaupanja, ki so namenjene nadzorovanju potrošnikov, potrošniku pa prinašajo popuste). Zato so posamezniki postavljeni pred navidezno možnost izbire in se "prostovoljno" odločijo za podreditev nadzoru, ki je poleg tega še čedalje manj zaznaven in s tem domnevno manj invaziven. Whitaker ugotavlja, da za razliko od zgodnejših Panoptikonov današnji postaja "*bolj fin, bolj prožen, bolj participativen, bolj konsenzualen*" (Whitaker, 1999: 152). Nadzorovanje je zato danes dobilo na videz prijazen, v resnici pa dvoličen obraz. Zato Deleuze nadzor imenuje "pošast" (Deleuze, 2002: 174) in sklene, da gre za "*postopno razpršeno vzpostavitev novega režima gospostva*" (Deleuze, 2002: 177).

Vendar pa je nadzor dvosmeren. Če oblast ali družba nadzor uporabljata proti posameznikom, pa lahko posameznik nadzor uporabi tudi proti nosilcem moči. Bentham je v leta 1791 objavljenem delu *Of Publicity* razvil tezo, da netransparentnost in skrivanje oblasti kaže na njeno nemoralnost. O sovražnikih publicitete je zapisal, da jih lahko razvrstimo v tri kategorije: na hudodelce, ki skušajo ubežati roki pravice; na tirane, ki skušajo zadušiti javno mnenje; in na boječe ali lene posameznike, ki skušajo zakriti svojo nesposobnost (Bentham, 1791/1994: 582). Vendar pa sodobna tehnologija omogoča nadzorovanje predvsem v eno smer, torej bolj nadzorovanje posameznikov kot nadzorovanje oblasti. Poleg tega prihaja do sprevračanja Benthamove zamisli o transparentnosti, saj se argument nemoralnosti pogosto uporablja kot argument proti zasebnosti posameznikov: zakaj se izogibati nadzoru, če nimate česa skrivati?

Čeprav je nadzor tesno povezan s tehnologijo – informacijsko-komunikacijska tehnologija se namreč vzpostavlja kot centralna tehnologija nadzora, ki nadzorovanje poglablja in krepi – pa je vloga tehnologije prav tako ambivalentna. Tehnologija namreč omogoča tudi osvoboditev, saj jo je mogoče uporabiti tudi za varovanje zasebnosti. Prav ta "demokratični potencial" tehnologije je številne posameznike v 90. letih 20. stoletja navedel na misel o tehnološki neizogibnosti razvoja tehnologije proti polni svobodi. Člani gibanja cypherpunkerjev so bili prepričani, da tehnologija oziroma internet omogoča osvoboditev posameznika od države in da je internet zaradi svoje narave odporen proti državnemu nadzoru. Menili so, da je tehnologijo in njen demokratični potencial mogoče zaustaviti samo z drakonskimi ukrepi, npr. prepovedjo uporabe tehnologije. V tem prepričanju jih je utrdila še razveljavitev *Communications Decency Act*[431] s strani Vrhovnega sodišča ZDA,[432] ki so ga nasprotniki dojemali kot poskus cenzure interneta, saj je prepovedoval objavljanje nespodobnih ali žaljivih vsebin na internetu.

Takšno prepričanje, ki je na internetu še vedno močno razširjeno, se je utrdilo tudi po, formalno gledano, neuspešnih poskusih prepovedi kriptografije. Boyle sicer ugotavlja, da nastanek "tehnologij svobode" vedno povzroči poostritev mehanizmov nadzora (Boyle, 1997). Zato je razumljivo, da so se tehnologije varovanja zasebnosti, kot na primer kriptografija, znašle pred poskusi onemogočanja tako s strani tajnih služb kot tudi zakonodajnih organov. Vendar pa so bili ti neposredni poskusi zaradi odpora javnosti neučinkoviti in demokratičnim državam kriptografije ni uspelo prepovedati, pa tudi ne zaustaviti kriptografskih raziskav in razvoja. Kljub

[431] Communications Decency Act of 1996, 47 U.S.C. (1996).
[432] Reno v. American Civil Liberties Union, 521 U.S. 844 (1997).

temu tehnologije osvoboditve niso dosegle svojega namena, vsaj ne množično. Tehnologija sicer omogoča osvoboditev, vendar je ta osvoboditev le možnost, ki je večina posameznikov ne izkoristi.

Pri vprašanju, zakaj je tako, pridemo do bistva problema sodobnega nadzorovanja. Zasebnost posameznikov namreč ogrožata tako država kot družba. Zgodovinsko gledano, je največja grožnja zasebnosti sicer država, vendar lokomotiva tega procesa čedalje bolj postaja zasebni sektor, ki ima na voljo bistveno več sredstev za nakup in uporabo tehnologij nadzora kot država. Arendtova ugotavlja, da "*ogrožanje svobode v sodobni družbi ne prihaja od države, kot domneva liberalizem, temveč od družbe*" (Arendt, 1958/1995: 69). Iz tega tudi sledi, da državljanske svoboščine lahko zagotavlja edinole država nasproti družbi.

Cypherpunkerji in drugi aktivisti za zaščito zasebnosti na internetu so problem zasebnosti razumeli preveč enostransko, saj so ga gledali predvsem skozi optiko odnosa med posameznikom in državo, povsem pa so spregledali vpliv družbene sfere. Nekateri predstavniki gibanja, npr. Timothy C. May, so celo trdili, da je kriptoanarhija (ki naj bi bila posledica uvedbe javno dostopne kriptografije) pravzaprav nekakšen anarhokapitalizem, ki zagovarja popolno svobodo ekonomskih transakcij brez vmešavanja države. Tehnologija naj bi zmanjšala moč držav pri zagotavljanju zakonitosti in pobiranju davkov in to so razumeli kot nekaj pozitivnega (May, 1995). Ker so kot akterja, ki posega in omejuje svobodo posameznikov, dojemali predvsem državo, so spregledali, da nasprotovanje državni regulaciji celo škoduje zaščiti zasebnosti, saj na zasebnost posameznikov vplivajo tudi drugi posamezniki. Prevelika deregulacija namreč daje preveč proste roke družbenemu poseganju v zasebnost. Posamezniki se danes namreč svoji zasebnosti večinoma odpovedujejo zaradi ekonomskih koristi in zato, ker nimajo na voljo druge resne alternative.

V družbi nadzora osvoboditev od nadzora navadno pomeni tudi izključitev iz družbe. Pristajanje na nadzor je tako postalo nujnost za tiste, ki se želijo vključiti v internet; popolno nepristajanje nanj pa večinoma kot alternativo ponuja zgolj izključitev, v virtualnem smislu torej nekakšno kibersmrt. Osvoboditev nikakor ni samoumevna, predvsem pa ne tehnološko neizogibna, temveč si jo je treba izboriti. To je pogosto povezano z velikimi stroški, zato si večina potrošnikov (in državljanov) tega niti ne želi. Zasebnost ostaja zgolj možnost za tiste, ki si jo lahko privoščijo, cena zanjo pa postaja vse višja.

Danes se tehnologija za zaščito zasebnosti - kriptografija uporablja predvsem v sferi elektronskega poslovanja (za zaščito in s tem za spodbujanje finančnih transakcij po internetu) in za zaščito avtorskih pravic, bistveno manj pa za zaščito medčloveških komunikacij. Za zaščito komunikacij posameznikov se množično uporablja le šifriranje povezav znotraj zaprtega omrežja (ang. *link encryption*), na primer šifriranje podatkov med telefonom GSM in bazno postajo ali med spletno stranjo in internetno banko. To onemogoča le nepooblaščeno prestrezanje, ne pa prestrezanja nasploh, saj imajo državni organi oziroma operater dostop do podatkov na izhodu sistema. Uporaba močnega šifriranja pri elektronskem poslovanju prek spleta je povsem enostavna, standardizirana in globoko integrirana v informacijsko tehnologijo (npr. v spletni brskalnik). Šifriranje elektronske pošte in drugih medčloveških komunikacij pa je v primerjavi

s tem še vedno razmeroma zapleteno opravilo, saj zahteva nalaganje dodatnih programskih vmesnikov, poleg tega pa tudi ni standardizirano.

Tudi pri uveljavljanju mednarodnih načel varstva informacijske zasebnosti je opaziti privilegiranost ekonomske sfere glede na pravice posameznikov do zasebnosti. *Smernice OECD za zaščito zasebnosti in čezmejni pretok osebnih podatkov*[433] so bile sprejete zato, da bi odstranile ovire za čezmejni pretok osebnih podatkov; varstvo pravic posameznikov pa je na neki način le njihov stranski učinek. Enako velja za konvencijo *Sveta Evrope o varstvu posameznikov glede na avtomatsko obdelavo osebnih podatkov*[434] ter za direktivo EU o zaščiti osebnih podatkov 95/46/EC.[435] Poenotenje varstva informacijske zasebnosti tako v Evropi kot v ZDA nima namena varovati človekovih pravic, temveč zagotavljati neoviran pretok osebnih podatkov. To je pomembno predvsem zaradi pospeševanja ekonomskih transakcij.

Podobno velja tudi za kriptografijo, saj je navsezadnje IBM v 60. letih začel razvijati šifrirni algoritem Lucifer ravno zaradi nevarnosti računalniškega kriminala v bančništvu, in ne zaradi varstva medčloveških komunikacij na splošno. Tudi iz leta 1995 sprejetega *Priporočila Sveta Evrope št. R(95) 13*[436] glede problemov kazensko procesnega prava, povezanega z informacijskimi državami (14. člen), in leta 1997 sprejetih *Smernicah OECD o kriptografski politiki*[437] sledi, da države kriptografijo dopuščajo in spodbujajo predvsem zaradi razvoja elektronskega poslovanja. Ekonomski argumenti, in ne človekove pravice, so bili tudi poglavitni motivi za liberalizacijo kriptografske politike v Franciji in ZDA. Prevlado ekonomskih motivov kaže tudi Wassenaarski sporazum o prepovedi izvoza tehnologije dvojne rabe, ki močno kriptografijo sicer šteje za tehnologijo dvojne rabe, katere izvoz je omejen, vendar pa s seznama tehnologije dvojne rabe izloča tiste kriptografske proizvode, ki šifriranje uporabljajo za zaščito avtorskih pravic in intelektualne lastnine, ter nekatere proizvode, ki se uporabljajo v bančništvu.

Motivi za sprejem zakonodaje za zaščito informacijske zasebnosti, odprava omejevanja kriptografije v mednarodnih dokumentih in razvoj kriptografskih rešitev ter njihova množična uporaba na področju elektronskega poslovanja so torej predvsem ekonomski. Na neki način je protislovno, da je k razvoju in uveljavitvi zaščitne zakonodaje za varstvo zasebnosti ter ustrezne tehnologije toliko pripomogla ravno ekonomija, ki sicer (p)ostaja največji promotor in uporabnik tehnologij nadzora. Vendar pa ta paradoks hitro izgine, ko pogledamo, kakšna

---

433 OECD. 1980. Smernice za zaščito zasebnosti in čezmejni pretok osebnih podatkov (Guidelines on the Protection of Privacy and Transborder Flows of Personal Data), sprejete 23. septembra 1980.

434 Svet Evrope. 1981. Konvencija Sveta Evrope o varstvu posameznikov glede na avtomatsko obdelavo osebnih podatov (Convention for the Protection of Individuals with Automatic Processing of Personal Data), sprejel jo je Svet Evrope 28. 1. 1981. Uradni list RS, Mednarodne pogodbe, št. 3/1994. Konvencijo je državni zbor Republike Slovenije ratificiral 25. 1. 1994. Veljati je začela 1. 3. 1994.

435 Direktiva 95/46/EC o varstvu posameznikov pri obdelovanju osebnih podatkov in svobodnem pretoku teh podatkov (Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data), sprejeta 24. oktobra 1995. Official Journal L 281, 23/11/1995 p. 0031 - 0050.

436 Svet ministrov Sveta Evrope. 1995. Priporočilo Sveta Evrope št. R(95) 13 glede problemov kazensko procesnega prava, povezanega z informacijskimi državami (*Recommendation No. R(95) 13, Concerning Problems of Criminal Procedure Law Connected with Information states*), sprejeto 11. septembra 1995.

437 OECD. 1997. Smernice o kriptografski politiki (Guidelines on Cryptography Policy), sprejete 27. marca 1997.

je poglavitna naloga tehnologij varovanja zasebnosti v sodobni družbi. To namreč ni več absolutna zaščita medsebojne komunikacije, kot je bila prvotna zamisel, temveč je pospeševanje elektronskega poslovanja. Tehnologije varovanja zasebnosti ščitijo posameznike predvsem pred kriminalom, ne pa tudi pred državo in družbeno sfero. Njihova naloga je danes predvsem zaščita pred nepooblaščenim prestrezanjem, ne pa tudi pred prestrezanjem nasploh, čeprav so borci za svobodno rabo kriptografije v začetku 90. let 20. stoletja poudarjali predvsem slednji vidik, saj naj bi po napovedih kriptografija povsem onemogočila državno nadzorovanje. Kljub uporabi kriptografije pri prenosu podatkov prek nezaščitenih omrežij imajo država in zasebna podjetja možnost dostopa do elektronskih sledi posameznika, ki se shranjujejo pri ponudnikih storitev. To pomeni, da tehnologije varovanja zasebnosti ne onemogočajo tehnologij nadzora.

Tisto, kar so ameriške vladne agencije in tajne službe pri omejevanju kriptografije skušale doseči po pravni poti in s finančnimi pritiski na raziskovalce in podjetja, pa jim ni uspelo, so na nekoliko drugačen način dosegla zasebna podjetja, predvsem množični marketing. Posamezniki, ki ne želijo biti izključeni iz družbe, se morajo prilagoditi in sprejeti njena pravila.[438] V praksi to pomeni, da morajo pristati na nadzor, oziroma se odreči določeni stopnji zasebnosti. Uporaba tehnologij za varstvo zasebnosti je zato v praksi zelo omejena in celo velja za družbeno nezaželeno, saj zahteva uporabo in učenje dodatne (zaščitne) tehnologije tudi s strani drugih komunikacijskih partnerjev. Tehnologije nadzora pa so, nasprotno, zelo razširjene in navadno veljajo za družbeno povsem sprejemljive.

Tehnološki in družbeni razvoj sta tako prišla do točke, ko bi morala svoboščine posameznikov zagotavljati država nasproti družbi. Ob tem se zastavlja vprašanje, ali je država tega sploh sposobna. Problem je, da prihaja do sprevračanja kritičnega načela publicitete, saj danes publiciteta rabi za manipulacijo publike. Kritična publiciteta postaja manipulativna. Danes se rezoniranje (po Habermasu) šele oblikuje pod vplivom množičnih medijev, namesto da bi ga množični mediji le posredovali in krepili. Prek množičnih medijev namreč v javnost vdirajo zasebni interesi, ki se s tehnikami ustvarjanja javnega mnenja prikazujejo kot splošni. Zato se interesi korporacij po omogočanju potrošniškega nadzora in po omejevanju zasebnosti ter interesi preiskovalnih organov pri odstranjevanju domnevnih ovir za njihovo večjo uspešnost prek množičnih medijev in množične kulture prikazujejo kot splošni interesi. Povečanje nadzora se tako prikazuje kot splošni (javni) interes, zasebnost posameznikov pa kot ovira skupnemu dobremu.

Habermas v *Predgovoru k novi izdaji Strukturnih sprememb javnosti* nasproti manipulativnemu usmerjanju medijske moči za zagotavljanje množične lojalnosti povpraševanja in skladnosti s sistemskimi imperativi postavlja komunikativno proizvajanje legitimne moči (javni diskurz, ki vpliva na administrativno moč) (Habermas, 1990/1994). Podobno kot Arendtova poudarja politično delujočo javnost. Po njegovem mnenju se avtonomna javnost izoblikuje v civilni družbi.

---

[438] Ker šifriranje elektronske pošte poteka med dvema komunikacijskima partnerjema, morata seveda oba uporabljati šifrirno tehnologijo. Če eden izmed njiju te tehnologije ne zna ali noče uporabljati, lahko drugi z njim komunicira samo na navaden način, torej nešifrirano.

V Habermasovi teoriji bi lahko našli odgovor na vprašanje, kako doseči, da bo zaščita zasebnosti sledila tehnološkemu in družbenemu razvoju. Pogledi Habermasa in Arendtove dajejo zavzemanju za elektronsko zasebnost povsem nov pomen. Ne gre samo za skupine glasnih posameznikov, ki hočejo zaustaviti napredek in se vdajajo romantičnim mitom o družbi brez nadzora, temveč za otoke kritične in avtonomne javnosti, ki si sistematično prizadeva za konkuriranje medijski moči politike in korporacij ter zagovarja odpiranje javnega prostora za kritično in racionalno razpravo v zvezi z vprašanji zasebnosti.

Organizacije, kot so EPIC, EFF in Privacy International, ki sistematično analizirajo spremembe na področju zasebnosti, sledijo tehnologijam nadzora, lobirajo za sprejem ustrezne zakonodaje, razvijajo in promovirajo tehnologije varstva zasebnosti ter uveljavljajo načelo publicitete nasproti arkanski praksi preiskovalnih organov, tajnih služb in zasebnih korporacij. Tako danes predstavljajo model politično delujoče javnosti, ki sledi idealu proizvajanja komunikativne moči. Seveda je pri tem, kot ugotavlja Habermas, pomembna tudi interakcija med institucionalno organiziranim političnim oblikovanjem mnenja, ki je usmerjeno na odločanje, torej na državo, ter na civilno družbo, ki je usmerjena na odkrivanje in reševanje problemov. Vendar pa zaton gibanj za varstvo zasebnosti v začetku 90. let ter praktično popolna odsotnost vprašanj v zvezi z zasebnostjo kot pomembnim političnim problemom danes kaže, da je ključno ravno organiziranje tovrstnega dela civilne družbe in odpiranje javnega prostora za neobremenjeno javno razpravo v zvezi z vprašanji nadzora in zasebnosti.

Hannah Arendt je pod vtisom razvoja behavioristične znanosti zapisala: "*Čisto mogoče je, da se novi vek, ki se je začel z neverjetno obetavnim aktiviranjem človeških sposobnosti, konča z najbolj usodno, sterilno pasivnostjo, kar jih je kdaj poznala zgodovina.*" (Arendt, 1958/1995: 336) Če tehnološki in družbeni razvoj kažeta, da so njeni strahovi upravičeni, pa se zdi, da sta ravno organizacija civilne družbe ter odpiranje javnega prostora možna odgovora na zdajšnjo pasivnost.

VIRI IN LITERATURA

Viri in literatura

1. ACLU. 1994. ACLU Opposes FBI Wiretap Access Bill Legislation Would Create Dangerous Precedent. Sporočilo za javnost z dne 26. septembra 1994. <http://www.eff.org/Legislation/Bills_by_number/hr4922_94_aclu.analysis>. (Datum dostopa: 17. 5. 2004).
2. ACLU. 2003. Privacy in America: Electronic Monitoring. http://www.aclu.org/Privacy/Privacy.cfm?ID=14170&c=132 (Datum dostopa: 19. 4. 2005)
3. Acohido, Byron in Swartz, Jon. 2004. »Unprotected PCs can be hijacked in minutes«. USA Today, 29. 11. 2004. <http://www.usatoday.com/money/industries/technology/2004-11-29-honeypot_x.htm>. (Datum dostopa: 2. 12. 2004).
4. Agence France-Presse. 2004. »North Korea armed for cyber war«. Agence France-Presse, 6. oktober 2004. <http://www.dallascrimewatch.org/News_Database/News_Request.cfm?News_ID=105>. (Datum dostopa: 6. 10. 2004).
5. Agre, E. Philip. 2001. »Introduction«. V Agre E. Philip in Rotenberg Marc, (ur.). 2001. Technology and Privacy: The New Landscape, str. 1–28. Cambridge, Massachusetts, London, England: MIT Press.
6. Agre E. Philip in Rotenberg Marc, (ur.). 2001. Technology and Privacy: The New Landscape. Cambridge, Massachusetts, London, England: MIT Press.
7. Albrecht, Hans-Jörg, Dorsch Claudia in Krüpe Christiane. 2003. Rechtswirklichkeit und Effizienz der Überwachung der Telekomunikation nach den §§ 100a, 100b StPO und anderer verdeckter Ermitlungsmaßnahmen. Freiburg: Max Planck Institut für ausländishes und internationales Strafrecht. [Dostopno na: <http://www.iuscrim.mpg.de/verlag/online/Band_115.pdf>. (Datum dostopa: 5. 3. 2005).]
8. Allard, W. Nicholas in Kass, A. David. 1997. »Law And Order In Cyberspace: Washington Report«. V Hastings Communications and Entertainment Law Journal (Comm/Ent), 1997, Vol. 19, No. 3, str. 563–609. San Francisco: UC Hastings College of the Law.
9. Alvaro, Alexander Nuno. 2005. Draft report on the initiative by the French Republic, Ireland, the Kingdom of Sweden and the United Kingdom for a Draft Framework Decision on the retention of data processed and stored in connection with the provision of publicly available electronic communications services or data on public communications networks for the purpose of prevention, investigation, detection and prosecution of crime and criminal offences including terrorism (8958/2004 – C6-0198/2004 – 2004/0813(CNS)). Committee on Civil Liberties, Justice and Home Affairs, 18. 4. 2005. <http://www.statewatch.org/news/2005/may/ep-data-ret-alvaro-report.pdf>. (Datum dostopa: 24. oktober 2005).
10. Anderson, Ross. 2003. 'Trusted Computing' Frequently Asked Questions. <http://www.cl.cam.ac.uk/%7Erja14/tcpa-faq.html>. (Datum dostopa: 9. 11. 2004).

11. Arendt, Hannah. 1958/1995. Vita Activa. Ljubljana: Krtina.
12. Bamford, James. 1983. The Puzzle Palace. Baskerville: Penguin Books.
13. Bamford, James. 2002. Body Of Secrets. New York: Anchor Books.
14. Banisar, David. 1994. EPIC Analysis of New Justice Department Guidelines on Searching and Seizing Computers. Lectric Law Library, <http://www.lectlaw.com/files/cri05.htm>. (Datum dostopa: 21. 6. 2004).
15. Barbut, Olivier. 2006. »Some legal trouble with TOR in France«. Elektronsko sporočilo Olivierja Barbuta, poslano na poštni seznam uporabnikov orodja za anonimizacijo Tor <or-talk@seul.org>, dne 13. maja 2006. <http://archives.seul.org/or/talk/May-2006/msg00074.html>.
16. Batagelj, Zenel. 1997. Direktni marketing, oglaševanje in internet. <http://www.cati.si/papers/zbymm0003.html>. (Datum dostopa: 23. 5. 2000). [Objavljeno tudi v Marketing magazin, 1999, št. 9, str. 26.]
17. BBC News. 2003. »Questions cloud cyber crime cases«. BBC News, 17. 10. 2003. <http://news.bbc.co.uk/1/hi/technology/3202116.stm>. (Datum dostopa: 5. 11. 2004).
18. BBC News. 2005. »Have hackers recruited your PC?« BBC News, 17. marec 2005. <http://news.bbc.co.uk/2/hi/technology/4354109.stm>. (Datum dostopa: 5. 11. 2004).
19. BBC News. 2006a. »EU court annuls data deal with US.« BBC News, 30. maj 2006. <http://news.bbc.co.uk/2/hi/europe/5028918.stm>. (Datum dostopa: 14. 8. 2006).
20. BBC News. 2006b. »Google censors itself for China.« BBC News, 25. januar 2006. <http://news.bbc.co.uk/1/hi/technology/4645596.stm>. (Datum dostopa: 14. 8. 2006).
21. Bellotti, Victoria. 2001. »Design for Privacy in Multimedia Computing and Communications Environments«. V Agre E. Philip in Rotenberg Marc, (ur.). 2001. Technology and Privacy: The New Landscape, str. 63–98. Cambridge, Massachusetts, London, England: MIT Press.
22. Benhabib, Seyla. 1997. »Models of Public Space: Hannah Arendt, the Liberal Tradition, and Jürgen Habermas«. V Calhoun Craig (ur.). 1997. Habermas and the Public Sphere, str. 73–98. Cambridge, Massachusetts, London, England: MIT Press.
23. Beniger, R. James. 1986. The Control Revolution. Cambridge, Massachusetts, London, England: Harvard University Press.
24. Bennett, J. Colin. 2001. »Convergence Revisited: Toward a Global Policy for the Protection of Personal Data?«. V Agre E. Philip in Rotenberg Marc, (ur.). 2001. Technology and Privacy: The New Landscape, str. 99–123. Cambridge, Massachusetts, London, England: MIT Press.
25. Benson, L. Robert. 2005. The Venona Story. Center for Cryptologic History, National Security Agency, <http://www.nsa.gov/publications/publi00039.cfm>. (Datum dostopa: 21. 4. 2005).

26. Bentham, Jeremy. 1787/1995/2001. Panopticon or The Inspection-House. V Cartome. org, 16. junij 2001. <http://cartome.org/panopticon2.htm>. (Datum dostopa: 14. 12. 2004).
27. Bentham, Jeremy. 1791/1994. »Of Publicity«. V Public Culture, 1994, 6, str. 581–595. Durham: Duke University Press.
28. Berlin, Isaiah. 1969/1992. »Dva koncepta svobode«. V Rizman, Rudi (ur.). 1992. Sodobni liberalizem, str. 69–89. Ljubljana: Krt.
29. Bicknell, Craig. 2000. »Online Prices Not Created Equal«. Wired News. <http://www.wired.com/news/business/0,1367,38622,00.html>. (Datum dostopa: 17. avgust 2002).
30. Black, Edwin. 2002. IBM and the Holocaust. London: Time Warner.
31. Boehlert, Sherwood. 2002. Cyber Security Research And Development Act, Committed to the Committee of the Whole House on the State of the Union - Report of Mr. Boehlert, from the Committee on Science, 4. februar 2002. House of Representatives, 107th Congress, 2d Session. [Dostopno na: <http://thomas.loc.gov>].
32. Bogataj, Maja (ur.). 2003. Internet in pravo. Ljubljana: Pravna fakulteta.
33. Bogataj, Maja. 2003. »Pravno varstvo tehničnih ukrepov za zaščito avtorskih del«. V Bogataj, Maja (ur.). 2003. Internet in pravo, str. 61–71. Ljubljana: Pravna fakulteta.
34. Boyle, James. 1997. Foucault in Cyberspace- Surveillance, Sovereignity, and Hardwired Censors. University of Cincinnati Law Review 66 (1), str. 177–205. [Dostopno tudi na: <http://www.law.duke.edu/boylesite/foucault.htm>. (Datum dostopa: 30. 5. 2004)].
35. Božič, Gorazd. 2004. Pregled obravnave varnostnih incidentov. Predstavitev na konferenci Infosek 2004, 25. 11. 2004, Nova Gorica.
36. Božič, Gorazd. 2006. Pregled obravnave varnostnih incidentov. Elektronsko sporočilo Gorazda Božiča, poslano 18. januarja 2006 ob 10:26.
37. Branch, Phillip. 2003. »Lawful Interception of the Internet«. V Australian Journal of Emerging Technologies and Society, Issue 1: pomlad 2003. Australian Centre of Emerging Technologies and Society.
38. Burkert, Herbert. 2001. »Privacy-Enhancing Technologies: Typology, Critique, Vision«. V Agre E. Philip in Rotenberg Marc, (ur.). 2001. Technology and Privacy: The New Landscape, str. 125–142. Cambridge, Massachusetts, London, England: MIT Press.
39. Butler, Jamie. 2004. »Using Process Infection to Bypass Windows Software Firewalls«. Phrack Volume 0x0b, Issue 0x3e, Phile #0x0d of 0x10 (13. julij 2004). <http://www.phrack.org/show.php?p=62&a=13>. (Datum dostopa: 5. 12. 2004).
40. Calhoun, Craig (ur.). 1997. Habermas and the Public Sphere. Cambridge, Massachusetts, London, England: MIT Press.
41. Cate, H. Fred. 1997. Privacy in the Information Age. Washington: Brookings Institution Press.

42. CERT. 2004. CERT/ Statistics 1988-2004. <http://www.cert.org/stats/cert_stats.html>. (Datum dostopa: 6. 12. 2004).
43. Chanell3000.com. 2003. »Man Pleads Guilty To Hacking Into Patient Files«. Chanell3000.com, 5. november 2003. <http://www.channel3000.com/print/2613265/detail.html?use=print>. (Datum dostopa: 29. 11. 2004).
44. CIAC. 2002. CIACTech02-004: Parasite Programs; Adware, Spyware, and Stealth Networks. CIAC Technical Bulletin, 11. november 2002, <http://www.ciac.org/ciac/techbull/CIACTech02-004.shtml>. (Datum dostopa: 8. 11. 2004).
45. Clarke, A. Roger. 1988. »Information Technology and Dataveillance.« V Communications of the ACM, str. 498–512. Association for Computing Machinery. [Dostopno na: <http://www.anu.edu.au/people/Roger.Clarke/DV/CACM88.html>. (Datum dostopa: 19. 4. 2004)].
46. CmdrTaco. 2004. » P2P Leaks Surprises«. Slashdot, 28. julij 2004. <http://yro.slashdot.org/article.pl?sid=04/07/28/1813228&tid=158>. (Datum dostopa: 1. avgust 2006).
47. CmdrTaco. 2005. »Copy-and-Paste Reveals Classified U.S. Documents«. Slashdot, 1. maj 2005. <http://it.slashdot.org/article.pl?sid=05/05/01/1314216&tid=172&tid=103>. (Datum dostopa: 1. avgust 2006).
48. Cohen, Avi. 2005. »Scandal shocks business world.« Ynetnews.com, 29. maj 2005. <http://www.ynetnews.com/articles/0,7340,L-3091900,00.html>. (Datum dostopa: 6. 6. 2005).
49. Cohen, W. William. 2004. Enron Email Dataset. <http://www-2.cs.cmu.edu/~enron/>. (Datum dostopa: 7. 12. 2004).
50. Commission of the European Communities. 2002. Commission Staff Working Paper - The application of Commission Decision 520/2000/EC of 26 July 2000 pursuant to Directive 95/46 of the European Parliament and of the Council on the adequate protection of personal data provided by the Safe Harbour Privacy Principles and related Frequently Asked Questions issued by the US Department of Commerce, 13. 02. 2002. [Dostopno na: <http://europa.eu.int/comm/internal_market/privacy/docs/adequacy/sec-2002-196/sec-2002-196_en.pdf>. Datum dostopa: 3. 5. 2005).
51. Corn-Revere, Robert. 2000. Testimony of Robert Corn-Revere before the Subcommittee on the Constitution of the Committee on the Judiciary United States House of Representatives, The Fourth Amendment and the Internet, dne 6. aprila 2000. [Dostopno na: <http://judiciary.house.gov/legacy/corn0406.htm>. (Datum dostopa: 20. 4. 2005).]
52. Crypto AG. 2005a. 10 arguments that set security standard. <http://www.crypto.ch/pages/htm/crypto/10_arguments.htm>. (Datum dostopa: 22. 4. 2005).
53. Crypto AG. 2005b. Groundless rumours. <http://www.crypto.ch/pages/htm/crypto/facts.htm>. (Datum dostopa: 24. 5. 2004).

54. Čebulj, Janez. 1992. Varstvo informacijske zasebnosti v Evropi in Sloveniji. Ljubljana: Inštitut za javno upravo pri Pravni fakulteti v Ljubljani.
55. Čebulj, Janez. 2002. »38. člen (varstvo osebnih podatkov)«. V Šturm, Lovro (ur.). 2002. Komentar ustave republike Slovenije, str. 408–416. Ljubljana: Fakulteta za podiplomske državne in evropske študije.
56. Dam, W. Kenneth in Lin, S. Herbert (ur). 1996. Cryptography's Role in Securing the Information Society. Washington: National Academy Press.
57. Data Protection Working Party. 2000. Privacy on the Internet - An integrated EU Approach to On-line Data Protection (5063/00/EN/FINAL WP 37), sprejeto 21. novembra 2000. [Dokument je dostopen na: <http://www.europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2000/wp37en.pdf>. (Datum dostopa: 3. 5. 2005).]
58. Data Protection Working Party. 2002. Working document on determining the international application of EU data protection law to personal data processing on the Internet by non-EU based web sites (5035/01/EN/Final WP 56), sprejet dne 30. maja 2002. [Dokument je dostopen na: <http://www.europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2002/wp56_en.pdf>. (Datum dostopa: 3. 5. 2005).]
59. Data Protection Working Party. 2003. Opinion 2/2003 on the application of the data protection principles to the Whois directories (10972/03/EN FINAL WP 76), sprejeto dne 13. junija 2003. [Dokument je dostopen na: <http://www.europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2003/wp76_en.pdf>. (Datum dostopa: 3. 5. 2005).]
60. Data Protection Working Party. 2004. Opinion 2/2004 on the Adequate Protection of Personal Data Contained in the PNR of Air Passengers to Be Transferred to the United States' Bureau of Customs and Border Protection (US CBP) (10019/04/EN WP 87), sprejeto 29. januarja 2004. [Dokument je dostopen na: <http://www.europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2004/wp87_en.pdf>. (Datum dostopa: 3. 5. 2005).]
61. Davies, H. J. Philip. 2000. »Information warfare and the future of the spy«. V Thomas, Douglas in Loader D. Brian, (ur.). 2000. Cybercrime, str. 251–268. London, New York: Routledge.
62. Davies, G. Simon. 2001. »Re-ingeneering the Right to Privacy: How Privacy Has Been Transformed from a Right to a Comodity«. V Agre E. Philip in Rotenberg Marc, (ur.). 2001. Technology and Privacy: The New Landscape, str. 143–165. Cambridge, Massachusetts, London, England: MIT Press.
63. Delaney, Frank. 1995. History Of The Microcomputer Revolution, <http://www.virtualaltair.com/virtualaltair.com_/vac_history.asp>. (Datum dostopa: 27. 4. 2004).
64. Deleuze, Gilles. 2002. »Družba nadzora«. V Filozofski vestnik, št. 3, letnik XXIII, str, 167–177. Ljubljana: Filozofski inštitut ZRC SAZU.

65. Delio, Michelle. 2003. »Spam: This Time It's Personal«. Wired News, 29. september 2003. <http://www.wired.com/news/politics/0,1283,60635,00.html>. (Datum dostopa: 4. 11. 2004).
66. Denning, E. Dorothy in Baugh, E. William. 1997. Cases Involving Encryption In Crime And Terrorism. <http://www.cs.georgetown.edu/~denning/crypto/cases.html>. (Datum dostopa: 26. 5. 2004).
67. Denning, E. Dorothy in Baugh, E. William. 2000. »Hiding crimes in cyberspace«. V Thomas, Douglas in Loader D. Brian, (ur.). 2000. Cybercrime, str. 105–131. London, New York: Routledge.
68. Denning, E. Dorothy. 1993. »To Tap or Not to Tap«. V Communications of the ACM, Vol. 36, No. 3, marec 1993, str. 24–33. Association for Computing Machinery. [Dostopno tudi na: <http://www.cs.georgetown.edu/~denning/wiretap/ToTap.txt>. (Datum dostopa: 26. 5. 2004).]
69. Denning, E. Dorothy. 1994. »Elektronsko pismo Dorothy E. Denning, 'Clipper Chip Will Block Crime', 22. februar 1994«. Computer underground Digest, 27. februar 1994, Vol. 6, Issue 19. [Dostopno na: <http://www.totse.com/en/zines/cud_a/cud619.html>, (Datum dostopa: 26. 5. 2004).]
70. Denning, E. Dorothy. 1995. Is Encryption Speech? <http://www.cs.georgetown.edu/~denning/crypto/speech.txt>. (Datum dostopa: 26. 5. 2004).
71. Denning, E. Dorothy. 1997. »The Future of Cryptography«. V Loader, D. Brian (ur.). 1997. The Governance of Cyberspace, str. 175–190. London, New York: Routledge.
72. DG Information Society and DG Justice and Home Affairs. 2004. DG INFSO - DG JAI consultation document on traffic data retention. Delovni dokument, 30. julij 2004. [Dostopno na: <http://europa.eu.int/information_society/topics/ecomm/doc/useful_information/library/public_consult/data_retention/consultation_data_retention_30_7_04.pdf>, (Datum dostopa: 26. 5. 2004).]
73. Diffie, Whitfield in Landau, Susan. 1999. Privacy On the Line: The Politics of Wiretapping and Encryption. Cambridge, Massachusetts, London, England: MIT Press.
74. Digital Equipment Corporation. 1963. Programmed Data Processor-1 Handbook. Maynard, Massachusetts: Digital Equipment Corporation. <http://www.dbit.com/~greeng3/pdp1/pdp1.html>. (Datum dostopa: 18. 4. 2005).
75. Dittrich, David. 1996. SATAN. University of Washington, <http://staff.washington.edu/dittrich/misc/satan/>. (Datum dostopa: 11. 4. 2005).
76. Dittrich, David. 1999a. The DoS Project's "trinoo" distributed denial of service attack tool. University of Washington. <http://staff.washington.edu/dittrich/misc/trinoo.analysis>. (Datum dostopa: 5. 12. 2004).
77. Dittrich, David. 1999b. The "Tribe Flood Network" distributed denial of service attack tool. University of Washington. <http://staff.washington.edu/dittrich/misc/tfn.analysis.> (Datum dostopa: 3. 12. 2004).

78. Dittrich, David. 1999c. The “stacheldraht” distributed denial of service attack tool. University of Washington. <http://staff.washington.edu/dittrich/misc/stacheldraht.analysis.txt>. (Datum dostopa: 2. 12. 2004).
79. Dolar, Mladen. 1991. »Spremna beseda«. V Foucault, Michael. 1991. Vednost - oblast - subjekt, str. VII–XXXIV. Ljubljana: Krt.
80. DoubleClick. 2002. DoubleClick Ad Serving Data Shows Rich Media Click-Through Rates to Be Six Times Higher Than Standard Ads, sporočilo za javnost objavljeno 25. oktobra 2002. <http://ir.doubleclick.net/ireye/ir_site.zhtml?ticker=DCLK&script=410&layout=-6&item_id=305697>. (Datum dostopa: 19. 4. 2004).
81. Dupuis, Clement. 1999. CISSP Study Booklet on Cryptography. <http://comsec.theclerk.com/CISSP/Domain_5.html>. (Datum dostopa: 21. 4. 2005).
82. Earthlink. 2005. Earthlink Spy Audit, april 2005. <http://www.earthlink.net/spyaudit/press/>. (Datum dostopa: 23. 4. 2005).
83. EFF. 2001. EFF Quotes Collection 19.6. <http://www.eff.org/Misc/EFF/?f=quotes.eff.txt>. (Datum dostopa: 22. 4. 2005)
84. EFF. 2003. EFF Analysis Of The Provisions Of The USA PATRIOT Act That Relate To Online Activities. <http://www.eff.org/Privacy/Surveillance/Terrorism/20011031_eff_usa_patriot_analysis.php>. (Datum dostopa: 13. 3. 2004).
85. EFF. 2004. »Google’s Gmail: A Rough Guide to Protecting Your Privacy«. V EFFector, Vol 17. No. 13, 15. april 2004. <http://www.eff.org/effector/17/13.php#II>. (Datum dostopa: 19. 6. 2004).
86. EFF. 2005a. Citat iz knjige Laurenceja Canterja in Marthe Siegel How To Make a Fortune on the Information Superhighway, 1994. <http://www.eff.org/legal/cases/Canter_Siegel/c-n-s_book.quote>. (Datum dostopa: 11. 6. 2004).
87. EFF. 2005b. National Identification Systems. <http://www.eff.org/Privacy/Surveillance/?f=nationalidsystem-resources.html>. (Datum dostopa: 21. 1. 2005).
88. EFF. 2005c. Tor: An anonymous Internet communication system. <http://tor.eff.org/>. (Datum dostopa: 25. 4. 2005).
89. Eley, Geoff. 1997. »Nations, Publics, and Political Cultures: Placing Habermas in the Nineteenth Century«. V Calhoun Craig (ur.). 1997. Habermas and the Public Sphere, str. 289–339. Cambridge, Massachusetts, London, England: MIT Press.
90. Empirica. 2003. SIBIS Pocket Book 2002/03 - Measuring the Information Society in the EU, the EU Accession Countries, Switzerland and the US. <http://www.sibis-eu.org>.
91. EPIC. 1994. EPIC Statement on Digital Telephony Wiretap Bill. Sporočilo za javnost z dne 22. avgusta 1994. <http://hotwired.wired.com/Lib/Privacy/epic.on.tele.html>. (Datum dostopa: 17. 5. 2004).
92. EPIC. 1997. »EC Rejects Key Escrow Encryption«. V EPIC alert 4.15, 10. november 1997. <http://www.epic.org/alert/EPIC_Alert_4.15.html>. (Datum dostopa: 22. 4. 2005).

93. EPIC. 1998a. 2001. Cryptography Policy. <http://epic.org/crypto/>. (19. januar 1998). (Datum dostopa: 19. 4. 2003).
94. EPIC. 1998b. 1998. Efforts to Ban Encryption. <http://www.epic.org/crypto/ban/>. (Datum dostopa: 19. 4. 2004).
95. EPIC. 1998c. 1998. Key Escrow. <http://www.epic.org/crypto/key_escrow/>. (Datum dostopa: 19. 4. 2004).
96. EPIC. 1998d. 1998. The Clipper Chip. <http://www.epic.org/crypto/clipper/>. (Datum dostopa: 19. 4. 2004).
97. EPIC. 2001. »Bush Administration Criticizes European Union Privacy Rules«. V EPIC Alert 8.06. 29. marec 2001. <http://www.epic.org/alert/EPIC_Alert_8.06.html>. (Datum dostopa: 2. 5. 2005).
98. EPIC. 2002a. Title III Wiretap Orders 1968-2002. <http://www.epic.org/privacy/wiretap/stats/wiretap_stats.html>. (Datum dostopa: 17. 4. 2005)
99. EPIC. 2002b. 2002. Microsoft Palladium Next Generation Secure Computing Base. <http://www.epic.org/privacy/consumer/microsoft/palladium.html>. (Datum dostopa: 9. 11. 2004).
100. EPIC. 2002c. Sign Out of Passport! <http://www.epic.org/privacy/consumer/microsoft/>. (Datum dostopa: 9. 11. 2004).
101. EPIC. 2003a. WHOIS Letter to ICANN (Javno pisno predsedniku ICANN, Paulu Twomeyu), poslano po e-pošti 25. oktobra 2003.
102. EPIC. 2004a. Comments Of the Electronic Privacy Information Center. <http://www.epic.org/privacy/us-visit/ADIS_comments.pdf>. (Datum dostopa: 22. 4. 2005).
103. EPIC. 2004b. »Congress Passes Law to Criminalize Inaccurate Domain Information«. EPIC Alert, Vol. 11.24, 23. december 2004. <http://www.epic.org/alert/EPIC_Alert_11.24.html>. (Datum dostopa: 22. 4. 2005).
104. EPIC. 2004c. Wiretapping. <http://www.epic.org/privacy/wiretap/>. (Datum dostopa: 22. 4. 2005).
105. EPIC. 2004d. Digital Rights Management and Privacy. <http://www.epic.org/privacy/drm/>. (Datum dostopa: 3. 6. 2004).
106. EPIC. 2004e. WHOIS. <http://www.epic.org/privacy/whois/>. (Datum dostopa: 10. 6. 2004).
107. EPIC. 2004f. Microsoft Passport Investigation Docket. <http://www.epic.org/privacy/consumer/microsoft/passport.html>. (Datum dostopa: 19. 11. 2004).
108. EPIC. 2005a. Carnivore. <http://www.epic.org/privacy/carnivore/>. (Datum dostopa: 22. 4. 2005).
109. EPIC. 2005b. The USA PATRIOT Act. <http://www.epic.org/privacy/terrorism/usapatriot/>. (Datum dostopa: 22. 4. 2005).
110. EPIC. 2006a. Foreign Intelligence Surveillance Act (FISA). <http://www.epic.org/privacy/terrorism/fisa/>. (Datum dostopa: 14. 8. 2006).

111. EPIC. 2006b. The Amy Boyer Case. <http://www.epic.org/privacy/boyer/>. (Datum dostopa: 15. 8. 2006).
112. EPIC. 2006c. Foreign Intelligence Surveillance Act Orders 1979-2005. <http://www.epic.org/privacy/wiretap/stats/fisa_stats.html>. (Datum dostopa: 14. 8. 2006).
113. Espiner, Tom. 2005. Security experts lift lid on Chinese hack attacks. CNET News.com, 23. november 2005. <http://news.zdnet.com/2100-1009_22-5969516.html>. (Datum dostopa: 8. 8. 2006).
114. Ettercap. 2005. Screenschots. <http://ettercap.sourceforge.net/screenshots.php>. (Datum dostopa: 2. maj 2005).
115. Etzioni, Amitai. 1999. The Limits of Privacy. ZDA: Basic Books.
116. Evron, Gadi. 2004. »Israeli Post Office Break-In«. Sporočilo na poštnem seznamu Bugtraq, 14. januarja 2004. <http://www.securityfocus.com/archive/1/349674>. (Datum dostopa: 29. 11. 2004).
117. FBI. 1995. »Implementation of the Communications Assistance for Law Enforcement Act«. V Federal Register, Vol. 60, No. 199 z dne 16. oktobra 1995. [Dostopno na: <http://www.epic.org/privacy/wiretap/calea/FR_10_16_95.pdf>. (Datum dostopa: 22. 4. 2005)].
118. FBI. 2003a. Carnivore/DCS 1000 Report to Congress, poročilo za leto 2002 z dne 24. februarja 2003. [Dostopno na: <http://www.epic.org/privacy/carnivore/2002_report.pdf>. (Datum dostopa: 22. 4. 2005)].
119. FBI. 2003b. Carnivore/DCS 1000 Report to Congress, poročilo za leto 2003 z dne 18. decembra 2003. [Dostopno na: <http://www.epic.org/privacy/carnivore/2003_report.pdf>. (Datum dostopa: 22. 4. 2005)].
120. FBI. 2004. Tiralica FBI za Echouafnijem, 7. 11. 2004. <http://www.fbi.gov/mostwant/alert/echouafni.htm>. (Datum dostopa: 7. 11. 2004).
121. Federal Trade Comission. 2000a. FTC Sues Failed Website, Toysmart.com, for Deceptively Offering for Sale Personal Information of Website Visitors. <http://www.ftc.gov/opa/2000/07/toysmart.htm>. (Datum dostopa: 8. 6. 2004).
122. Federal Trade Comission. 2000b. FTC Announces Settlement With Bankrupt Website, Toysmart.com, Regarding Alleged Privacy Policy Violations. <http://www.ftc.gov/opa/2000/07/toysmart2.htm>. (Datum dostopa: 8. 6. 2004).
123. Federal Trade Comission. 2002a. High School Student Survey Companies Settle FTC Charges. <http://www.ftc.gov/opa/2002/10/student1r.htm>. (Datum dostopa: 2. maj 2005).
124. Federal Trade Comission. 2002b. Eli Lilly Settles FTC Charges Concerning Security Breach. <http://www.ftc.gov/opa/2002/01/elililly.htm>. (Datum dostopa: 2. maj 2005).
125. Federal Trade Comission. 2002c Microsoft Settles FTC Charges Alleging False Security and Privacy Promises. <http://www.ftc.gov/opa/2002/08/microsoft.htm>. (Datum dostopa: 18. 4. 2005).

126. Federal Trade Comission. 2003. National Do Not Call Registry Opens. <http://www.ftc.gov/opa/2003/06/donotcall.htm>. (Datum dostopa: 2. maj 2005).
127. Federal Trade Comission. 2004. Compliance with Do Not Call Registry Exceptional. <http://www.ftc.gov/opa/2004/02/dncstats0204.htm>. (Datum dostopa: 2. maj 2005).
128. Felten, W. Edward. 2002. Keystone SpamKops. Freedom to Tinker, 16. avgust 2002. <http://www.freedom-to-tinker.com/archives/000014.html>. (Datum dostopa: 24. 4. 2005).
129. Felten, W. Edward in Schneider, A. Michael. 2000. »Timing Attacks On Web Privacy«. Proc. of 7th ACM Conference on Computer and Communications Security. <http://www.cs.princeton.edu/sip/pub/webtiming.pdf>. (Datum dostopa: 1. december 2001).
130. Figueroa, Liz. 2004. It's time to take a stand for online privacy. <http://www.gmail-is-too-creepy.com/liz.html>. (Datum dostopa: 29. 6. 2004).
131. Flaherty, H. David. 2001. »Controlling Surveillance«. V Agre E. Philip in Rotenberg Marc, (ur.). 2001. Technology and Privacy: The New Landscape, str. 167–192. Cambridge, Massachusetts, London, England: MIT Press.
132. Fleishman, Glenn. 2004. »WPA Cracking Proof of Concept Available«. Wi-Fi Net News. <http://wifinetnews.com/archives/004428.html>. (Datum dostopa: 23. 4. 2005).
133. Flexispy. 2006. Spletna stran podjetja Flexispy. <http://www.flexispy.com/>. (Datum dostopa: 8. maj 2006).
134. Foucault, Michael [Dolar Mladen (ur.)]. 1991. Vednost - oblast - subjekt. Krt: Ljubljana.
135. Foucault, Michael. 1984. Nadzorovanje in kaznovanje. Delavska enotnost: Ljubljana.
136. Foucault, Michael. 1997/2003. »Predavanje 17. marca 1976«. V Filozofski vestnik, št. 3, letnik XXIV, str, 151–169. Ljubljana: Filozofski inštitut ZRC SAZU.
137. Fraser, Nancy. 1997. »Rethinking the Public Sphere: A Contribution to the Critique of Actually Existing Democracy«. V Calhoun Craig (ur.). 1997. Habermas and the Public Sphere, str. 109–142. Cambridge, Massachusetts, London, England: MIT Press.
138. Frind, Markus. 2006. »AOL Search Data Shows Users Planning to commit Murder.« The Paradigm Shift blog, 7. avgust 2006. <http://plentyoffish.wordpress.com/2006/08/07/aol-search-data-shows-users-planning-to-commit-murder/>. (Datum dostopa: 8. 8. 2006).
139. Garfinkel, Simson. 1996. »Spam King«. Wired News, št. 4.02. <http://www.wired.com/wired/archive/4.02/spam.king_pr.html>. (Datum dostopa: 11. 6. 2004).
140. Geer Daniel, Pfleeger Charles P., Schneier Bruce, Quarterman John S., Metzger Perry, Bace Rebecca, Gutmann Peter. 2003. CyberInsecurity: The Cost of Monopoly. [Dostopno na <http://www.ccianet.org/papers/cyberinsecurity.pdf>. (Datum dostopa: 1. 5. 2004).]

141. Gellman, Robert. 2001. »Does Privacy Law Work?«. V Agre E. Philip in Rotenberg Marc, (ur.). 2001. Technology and Privacy: The New Landscape, str. 193–218. Cambridge, Massachusetts, London, England: MIT Press.
142. Georgia Tech Research Corporation. 1997a. GVU's 7th WWW User Survey. <http://www.gvu.gatech.edu/user_surveys/survey-1997-04>. (Datum dostopa: 1. 5. 2004).
143. Georgia Tech Research Corporation. 1997b. GVU Eight WWW User Survey: Most Important Issue Facing the Internet. <http://www.gvu.gatech.edu/user_surveys/survey-1997-10/graphs/general/Most_Import_Issue_Facing_the_Internet.html>. (Datum dostopa: 1. 5. 2004).
144. GILC. 1998. Cryptography and Liberty: An International Survey Of Encryption Policy. 1998. http://www.gilc.org/crypto/crypto-survey.html. (Datum dostopa: 2. 5. 2005).
145. Gimon, A. Charles. 1995. »The Phil Zimmermann Case«. Info Nation. <http://www.skypoint.com/members/gimonca/philzima.html>. (Datum dostopa: 19. 1. 2005).
146. Glasner, Joanna. 2002. DoubleClick to Open Cookie Jar. Wired News, 27. avgust 2002. <http://www.wired.com/news/business/0,1367,54769,00.html>. (Datum dostopa: 19. 4. 2004).
147. Glave, James. 1996. »AI Technology Watches What You Read, Sells Accordingly«. Wired News, 2. december 1996. <http://www.wired.com/news/technology/0,1282,751,00.html>. (Datum dostopa: 27. 4. 2004).
148. Glave, James. 1998. »'Sun Violated My Privacy'«. Wired News, 18. december 1998. <http://www.wired.com/news/politics/0,1283,16929,00.html>. (Datum dostopa: 26. 4. 2004).
149. Gonsalves, Antone. 2005. »Company Bypasses Cookie-Deleting Consumers«. InternetWeek, 31. marec 2005. <http://www.internetweek.com/showArticle.jhtml?articleID=160400749>. (Datum dostopa: 18. 4. 2005).
150. Google. 2004a. Gmail and Privacy. <http://gmail.google.com/gmail/help/more.html>. (Datum dostopa: 19. 6. 2004).
151. Google. 2004b. Gmail Terms of Use. <http://www.google.com/gmail/help/terms_of_use.html>. (Datum dostopa: 19. 6. 2004).
152. Google. 2005. Google Search: k-lite. <http://www.google.com>. (Datum dostopa: 24. 4. 2005).
153. Gottlieb, Bruce. 1999. HacK, CouNterHaCk. V New York Times Magazine, 3. oktober 1999. <http://www.nytimes.com/library/magazine/home/19991003mag-hackers.html>. (Datum dostopa: 3. 12 .2004).
154. Grossman, Wendy. 1998. »Rules, Britannia«. Wired News, 7. julij 1998. <http://www.wired.com/news/politics/0,1283,13509,00.html>. (Datum dostopa: 19. 5. 2004).

155. Gutmann, Ethan. 2006. »Human Rights in China«. Pričanje Ethana Gutmanna pred ameriškim House International Relations Committee, Subcommittee on Africa, Global Human Rights and International Operations, 19. april 2006. <http://wwwa.house.gov/international_relations/109/gut041906.pdf>. (Datum dostopa: 3. 6. 2006).
156. Gutwirth, Serge. 2002. Privacy and the Information Age. Rowman & Littlefield Publishers: Lanham, Boulder, New York, Oxford.
157. Habermas, Jürgen. 1962/1989. Strukturne spremembe javnosti. Ljubljana: Založba ŠKUC in Znanstveni inštitut Filozofske fakultete.
158. Habermas, Jürgen. 1990/1994. »Predgovor k novi izdaji (1990) Strukturnih sprememb javnosti«. V Javnost, Vol. 1 (1994), 1-2, str. 23–43. Ljubljana: Journal of the European Institute for Communication and Culture.
159. Hambridge, Sally. 1995. RFC 1855 - Netiquette Guidelines. The Internet Society. <http://www.faqs.org/rfcs/rfc1855.html>. (Datum dostopa: 11. 6. 2004).
160. 1.Harris, Andrew. 2006. Spy Agency Sought U.S. Call Records Before 9/11, Lawyers Say. Bloomberg.com, 30. junij 2006. <http://www.bloomberg.com/apps/news?pid=20601087&sid=abIV0cO64zJE&refer=#>. (Datum dostopa: 3. julij 2006).
161. Harrison, Ann. 2001. »Terror attacks revive crypto debate«. SecurityFocus, 20. september 2001. <http://www.securityfocus.com/news/256>. (Datum dostopa: 19. 4. 2004).
162. Heritage Media Corporation. 1999. Company profile: HNC Software Inc. <http://www.leavcom.com/hm_hnc.htm>. (Datum dostopa: 18. 4. 2005).
163. Heschong, Christopher. 2005. »ExitPolicy abuse«. Elektronsko sporočilo Christopherja Heschonga, poslano na poštni seznam uporabnikov orodja za anonimizacijo Tor <or-talk@seul.org>, dne 8. februarja 2005. <http://archives.seul.org/or/talk/Feb-2005/msg00066.html>.
164. Hoffman, D. Russell. 1996. Interview with author of PGP. <http://www.animatedsoftware.com/hightech/philspgp.htm>. (Datum dostopa: 26. 5. 2005).
165. Hughes, Eric. 1993. A Cypherpunk's Manifesto. <http://www.activism.net/cypherpunk/manifesto.html>. (Datum dostopa: 5. 3. 2004).
166. IDABC. 2004. EU-US agreement on transfer of air passenger data officially signed. V eGovernment News, 3. junij 2004. <http://europa.eu.int/idabc/en/document/2596/330>. (Datum dostopa: 19. 4. 2005).
167. IIT Research Institute. 2000. Independent Review of the Carnivore System - Final Report. IIT Research Institute: Lanham, Maryland. [Dostpno na: <http://www.usdoj.gov/jmd/publications/carniv_final.pdf>. (Datum dostopa: 5. 3. 2004).]
168. Ilett, Dan. 2004. »Richard Clarke: Straight talking on terror«. ZDNet, 16. november 2004. <http://www.zdnet.com.au/insight/security/0,39023764,39166796,00.htm>. (Datum dostopa: 18. 11. 2004).

169. Indymedia. 2004. »FBI Seizes IMC Servers in the UK«. Indymedia, 7. oktober 2004. <http://www.indymedia.org/en/2004/10/111999.shtml>. (Datum dostopa: 24. 4. 2005).
170. infiNity. 1997. The PGP Attack FAQ, Part 5. <http://www.stack.nl/~galactus/remailers/attack-5.html>. (Datum dostopa: 2. 3. 2004).
171. Inšpektorat za varstvo osebnih podatkov. 2004. Odločba Inšpektorja za varstvo osebnih podatkov št. 751-02-82/2004-o1 (0106) z dne 5. 10. 2004 [kopija odločbe je bila pridobljena na podlagi zakona o dostopu do informacij javnega značaja].
172. International Working Group on Data Protection in Telecommunications. 1998. Common Position on Essentials for privacy-enhancing technologies (e.g. P3P) on the WorlWideWeb. <http://www.datenschutz-berlin.de/doc/int/iwgdpt/priv_en.htm>. (Datum dostopa: 23. 4. 5).
173. Internet Security Systems. 2002. Wireless LAN Security - An ISS Technical White Paper. <http://documents.iss.net/whitepapers/wireless_LAN_security.pdf>. (Datum dostopa: 19. 4. 2004).
174. Jacques, Robert. 2004. »Hackers hit Italian Senate with gay porn worm«. Vunet.com, 25. november 2004. <http://www.infomaticsonline.co.uk/print/1159655>. (Datum dostopa: 27, 11. 2004).
175. Jalušič, Vlasta. 1995. Hannah Arendt: Politika kot možnost. V Vita Activa, str. VII–LII. Ljubljana: Krtina.
176. Jya.com. 1997. NSA and Crypto AG. <http://jya.com/nsa-sun.htm>. (Datum dostopa: 24. 5. 2004).
177. Kahn, David. 1973. The Codebreakers. New York: The New American Library.
178. Kawamoto, Dawn in Mills, Elinor. 2006. AOL apologizes for release of user search data. CNET News.com, 7. avgust 2006. <http://news.com.com/2100-1030_3-6102793.html?tag=nefd.top>. (Datum dostopa: 8. 8. 2006).
179. Kennedy, D. Peter. 1993. Steve Jackson Games v. US Secret Service - The Case and its Outcome. <http://www.sjgames.com/SS/pdk-article.html>. (Datum dostopa: 23. 11. 2004).
180. Kismet. 2005. Wireless Network Power Distribution Topology and Track Map. <http://nst.sourceforge.net/nst/docs/user/ch03s08.html>. (Datum dostopa: 3. 5. 2005).
181. Klemenčič, Goran. 2001. »Varstvo elektronske zasebnosti«. V Potrč, Matjaž (ur.). 2001. Internet in pravo, str. 129–191. Ljubljana: Pasadena.
182. Klemenčič, Goran. 2002. »37. člen (varstvo tajnosti pisem in drugih občil)«. V Šturm, Lovro (ur.). 2002. Komentar ustave republike Slovenije, str. 391–408. Ljubljana: Fakulteta za podiplomske državne in evropske študije.
183. Klemenčič, Goran. 2003. »Internet in pravica do zasebnosti«. V Bogataj, Maja (ur.). 2003. Internet in pravo, str. 101–141. Ljubljana: Pravna fakulteta.

184. Kovačič, Matej. 2004a. »Pogovor z Gorazdom Božičem, vodjo varnostnega centra SI-CERT«. Slo-Tech, 24. februar 2004. <http://www.slo-tech.com/clanki/04023/04023.shtml>. (Datum dostopa: 24. 2. 2004).
185. Kovačič, Matej in Koren, Gašper. 2004. »Botnet eksperiment«. Prosojnice iz še neobjavljenega predavanja.
186. Kovačič, Matej. 2003a. »Slovenski hekerji«. Prosojnice iz predstavitve na konferenci Infosek 2003, 3. december 2003, Nova Gorica.
187. Kovačič, Matej. 2003b. Zasebnost na internetu / Privacy on the Internet. Ljubljana: Mirovni inštitut.
188. Kovačič, Matej. 2004b. »Intervju z Darkotom Bulatom. Slo-Tech, 25. junij 2004. <http://www.slo-tech.com/clanki/04007/04007.shtml>. (Datum dostopa: 25. 6. 2004).
189. Labriola, Don. 2002. »Is Media Player Spyware?«. Extremetech.com, 6. marec 2002. http://www.extremetech.com/article2/0,1558,828150,00.asp. (Datum dostopa: 23. 4. 2005).
190. Lampe, Rok. 2004. Sistem pravice do zasebnosti. Ljubljana: Bonex založba.
191. Laurant, Cédric (ur.). 2003. Privacy & Human Rights. ZDA: EPIC in Privacy International.
192. Lemos, Rob. 1999. »How GUID tracking technology works«. ZDNet News. <http://www.zdnet.com/zdnn/stories/news/0,4586,2234550,00.html>. (Datum dostopa: 23. 4. 2005).
193. Leyden, John. 2003. »Suspected paedophile cleared by computer forensics«. The Register, 28. oktober 2003. <http://www.theregister.co.uk/2003/10/28/suspected_paedophile_cleared_by_computer/>. (Datum dostopa: 4. 11. 2004).
194. Leyden, Jonh. 2004. »Zombie PCs spew out 80% of spam«. The Register, 4. junij 2004. <http://www.theregister.co.uk/2004/06/04/trojan_spam_study/>. (Datum dostopa: 23. 4. 2005).
195. Lim, Louisa. 2004. »China to censor text messages«. BBC News. 2. julij 2004. <http://news.bbc.co.uk/1/hi/world/asia-pacific/3859403.stm>. (Datum dostopa: 23. 11. 2004).
196. Lindberg, Gunnar. 1999. RFC 2505 - Anti-Spam Recommendations for SMTP MTAs. The Internet Society. <http://www.faqs.org/rfcs/rfc2505.html>. (Datum dostopa: 23. 4. 2005).
197. Liston, Tom in Bambenek, John. 2004. BHO scanning tool and New Scam Targets Bank Customers, 29. junij 2004, <http://isc.sans.org/presentations/banking_malware.pdf> ter <http://isc.sans.org/diary.php?date=2004-06-29>. (Datum dostopa: 23. 4. 2005).
198. Loader, D. Brian (ur.). 1997. The Governance of Cyberspace. London, New York: Routledge.

199. Loney, Matt. 2002. »Want Wi-Fi? Learn the secret code«. CNET News.com, 26. junij 2002. <http://news.com.com/2102-1033-939546.html>. (Datum dostopa: 23. 4. 2005).
200. Lyon, David. 1994. The Electronic Eye. Cambridge: Polity Press.
201. Macavinta, Courtney. 1999. »Real Networks faced with second privacy suit«. CNET News.com, 10. november 1999. <http://news.com.com/2102-1001-232766.html>. (Datum dostopa: 3. 5. 2005).
202. Madsen, Wayne in Banisar, David. 2000. Cryptography & Liberty 2000. Washington: EPIC.
203. May, C. Timothy. 1988. The Crypto Anarchist Manifesto. Objavljeno na USENET julija 1988 in na različnih poštnih seznamih, <http://www.activism.net/cypherpunk/crypto-anarchy.html>. (Datum dostopa: 28. 5. 2004).
204. May, C. Timothy. 1995. Crypto Anarchy and Virtual Communities. Objavljeno na USENET v talk.politics.crypto, alt.politics.datahighway in alt.cyberpunk, 1. 4. 1995 @ 17:39:22 PST. <http://www.idiom.com/~arkuat/consent/Anarchy.html#cryptoanarchy>. (Datum dostopa: 28. 5. 2004).
205. Mayer-Schönberger, Viktor. 2001. »Generational Development of Data Protection in Europe«. V Agre E. Philip in Rotenberg Marc, (ur.). 2001. Technology and Privacy: The New Landscape, str. 219–241. Cambridge, Massachusetts, London, England: MIT Press.
206. McCue, Andy in Ilett, Dan. 2004. »Betting websites blackmailed with child pornography«. Silicon.com, 27. oktober 2004. <http://software.silicon.com/malware/0,3800003100,39125346,00.htm>. (Datum dostopa: 6. 12. 2004).
207. McCullagh, Declan. 2000. »FBI Hacks Alleged Mobster«. Wired News, 6. december 2000. <http://www.wirednews.com/news/print/0,1294,40541,00.html>. (Datum dostopa: 22. 4. 2005).
208. McCullagh, Declan. 2001a. »Senate OKs FBI Net Spying«. Wired News, 14. september 2001. <http://www.wired.com/news/print/0,1294,46852,00.html>. (Datum dostopa: 3. 5. 2005).
209. McCullagh, Declan. 2001b. »Bush Bill Rewrites Spy Laws«. Wired News, 19. september 2001. <http://www.wired.com/news/print/0,1294,46953,00.html>. (Datum dostopa: 3. 5. 2005).
210. McCullagh, Declan. 2001c. »Wiretap Bill Gets Third Degree«. Wired News, 26. september 2001. <http://www.wired.com/news/print/0,1294,47111,00.html>. (Datum dostopa: 3. 5. 2005).
211. McCullagh, Declan. 2001d. »Anti-Attack Feds Push Carnivore«. Wired News, 12. september 2001. <http://www.wired.com/news/print/0,1294,46747,00.html.>. (Datum dostopa: 3. 5. 2005).

212. McCullagh, Declan. 2001e. »'Lantern' Backdoor Flap Rages«. Wired News, 27. november 2001. <http://www.wired.com/news/conflict/0,2100,48648,00.html>. (Datum dostopa: 19. 5. 2004).
213. McGuire, David. 2001. »VeriSign has been selling customer data for a year«. ComputerUser.com, 20. februar 2001. <http://www.computeruser.com/news/01/02/20/news10.html>. (Datum dostopa: 11. 6. 2004).
214. McWilliams, Brian. 2003a. »North Korea's School for Hackers«. Wired News, 2. junij 2003. <http://www.wired.com/news/politics/0,1283,59043,00.html>. (Datum dostopa: 5. 12. 2004).
215. McWilliams, Brian. 2003b. »Cloaking Device Made for Spammers«. Wired News, 9. oktober 2003. <http://www.wired.com/news/business/0,1367,60747,00.html>. (Datum dostopa: 7. 12. 2004).
216. Miller, Jacques-Allain. 1981. »Despotizem koristnega«. V Problemi - razprave, št. 6–8, letnik XIX, str. 17–35. Ljubljana: Društvo za teoretsko psihoanalizo.
217. Ministrstvo za informacijsko družbo. 2004a. Prepis MID-ove klepetalnice 'Internet - iluzija varnosti in zasebnosti?' z dne 17.02.2004. Objavljen na <http://mid.gov.si>. (Datum dostopa: 17. 02. 2004).
218. Ministrstvo za informacijsko družbo. 2004b. Zapisnik sestanka "Izvedba zakonitega prestrezanja telekomunikacijskega prometa, ki poteka prek interneta", z dne 1. junija 2004.
219. Ministrstvo za zunanje zadeve. 2004. Odgovor glede iznosa osebnih podatkov. Elektronsko sporočilo MZZ - konzularni sektor, št. 921-92-2558/00 z dne 9. februarja 2004.
220. MIT. 2003. Jargonfile - različica 4.4.6. <http://jargon.watson-net.com/jargon.asp?w=hacker>. (Datum dostopa: 3. 5. 2005).
221. MIT. 2005. Reality Mining Project. <http://reality.media.mit.edu/>. (Datum dostopa: 8. maj 2006).
222. Mlinar, Zdravko. 1994. Individuacija in globalizacija v prostoru. Ljubljana: SAZU.
223. Mobitel. 2004. Odgovor Mobitelove Službe za odnose z javnostmi na moja vprašanja, 19. oktober 2004. Elektronsko sporočilo poslano iz naslova <PRMobitel@mobitel.si>, dne 19. oktobra 2004 ob 18:41:18.
224. Moskowitz, Robert. 2003. »Weakness in Passphrase Choice in WPA Interface«. Wi-Fi Net News, 3. november 2003. <http://wifinetnews.com/archives/002452.html>. (Datum dostopa: 23. 4. 2005).
225. Možina, Damjan. 2002. »Se Evropa odreka zasebnosti v korist varnosti?«. Informatika in pravo, (1): 3-5, priloga Pravne prakse, št. 43. Ljubljana: Gospodarski vestnik.
226. Sivaraman, Mukund. 2006. »Clearing cookies is not enough to save your privacy«. 11. september 2006. <http://www.mukund.org/blog/101/>. (Datum dostopa: 20. 9. 2006).

227. Niemelä, Jarno in Heikkilä, Juha-Pekka. 2006. F-Secure Trojan Information Pages: Flexispy.A. F-Secure, 29. marec 2006. <http://www.f-secure.com/v-descs/flexispy_a.shtml>. (Datum dostopa: 8. maj 2006).
228. Oakes, Chris. 1999. »Monitor This, Echelon«. Wired News, 22. oktober 1999. <http://www.wired.com/news/politics/0,1283,32039,00.html>. (Datum dostopa: 22. 4. 2005).
229. Orehar-Ivanc, Metoda. 2002. »35. člen (varstvo pravic zasebnosti in osebnostnih pravic)«. V Šturm, Lovro (ur.). 2002. Komentar ustave republike Slovenije, str. 370–386. Ljubljana: Fakulteta za podiplomske državne in evropske študije.
230. Page, Susan. 2006. NSA secret database report triggers fierce debate in Washington. USA Today, 11. maj 2006. <http://www.usatoday.com/news/washington/2006-05-11-nsa-reax_x.htm> (Datum dostopa: 3. julij 2006).
231. Palmer, Gareth. 2000. »The new spectacle of crime«. V Thomas, Douglas in Loader D. Brian, (ur.). 2000. Cybercrime, str. 85–102. London, New York: Routledge.
232. Pavčnik, Marijan. 1997. Teorija prava. Ljubljana: Cankarjeva založba.
233. Perenič, Anton (ur.). 1979. Zbornik znanstvenih razprav. Ljubljana: Univerza v Ljubljani, Pravna fakulteta.
234. Perry, Mike. 2006. »Holy shit I caught 1«. Elektronsko sporočilo Mikea Perrya, poslano na poštni seznam uporabnikov orodja za anonimizacijo Tor <or-talk@seul.org>, dne 27. avgusta 2006. <http://archives.seul.org/or/talk/Aug-2006/msg00261.html>.
235. PGP International. 2005. The PGPi Scanning Project. <http://www.pgpi.org/pgpi/project/scanning/>. (Datum dostopa: 22. 4. 2005).
236. Phillips, J. David. 2001. »Cryptography, Secrets, and the Structuring of Trust«. V Agre E. Philip in Rotenberg Marc, (ur.). 2001. Technology and Privacy: The New Landscape, str. 243–276. Cambridge, Massachusetts, London, England: MIT Press.
237. Plementaš, Miha in Sodja, Maja. 2004. »Podatki o številu prisluhov – javni ali ne?«. 24ur.com, 26. avgusta 2004. <http://24ur.com/naslovnica/slovenija/20040826_2045241.php>. (Datum dostopa: 2. 12. 2004).
238. PLS. 2004. Elektronsko pismo člana skupine PLS, 15. december 2004. Elektronsko sporočilo je bilo poslano 15. decembra 2004 ob 03:54:35.
239. Polen, Ben. 2001. »ACLU Exec Voices Concerns«. Wired News, 31. december 2003. <http://www.wired.com/news/politics/0,1283,49317,00.html>. (Datum dostopa: 19. 5. 2004).
240. Policija. 2004. Zahteva za dostop do informacij javnega značaja – odgovor. Pisni odgovor policije z dne 17. 9 2004, šifra dopisa: 205-1-005-1788/01.
241. Policija. 2006. Zahteva za dostop do informacij javnega značaja – odgovor. Pisni odgovor policije z dne 30. 8 2006, šifra dopisa: 100-1129/2006/8 (26-9).
242. Postel, Jon. 1975. RFC 706 - On the junk mail problem. The Internet Society. <http://www.faqs.org/rfcs/rfc706.html>. (Datum dostopa: 3. 5. 2005).

243. Potrč, Matjaž (ur.). 2001. Internet in pravo. Ljubljana: Pasadena.
244. Poulsen, Kevin. 2000. »Ex-CIA Chief: Beware Spy-Viruses«. Security Focus, 17. maj 2000. <http://online.securityfocus.com/news/38>. (Datum dostopa: 24. 4. 2005).
245. Poulsen, Kevin. 2003. »Slammer worm crashed Ohio nuke plant network«. Secrity Focus, 19. avgust 2003. <http://www.securityfocus.com/news/6767>. (Datum dostopa: 1. 8. 2006).
246. Poulsen, Kevin. 2004a. »Warspammer guilty under new federal law«. Security Focus, 29. september 2004. <http://www.securityfocus.com/news/9606>. (Datum dostopa: 24. 2. 2005).
247. Poulsen, Kevin. 2004b. »Wi-Fi hopper guilty of cyber-extortion«. The Register, 26. junij 2004. <http://www.theregister.co.uk/2004/06/26/wifi_hopper_extortion/>. (Datum dostopa: 29. 11. 2004).
248. Privacy International. 2004. Complaint: Google Inc - Gmail email service, 19. april 2004. (Datum dostopa: 19. 6. 2004).
249. Privacy Rights Clearinghouse. 1998. Privacy in Cyberspace. <http://www.privacyrights.org/fs/fs18-cyb.html>. (Datum dostopa: 23. 4. 2005).
250. quintessenz. 2005. Datamining the NSA. <http://www.quintessenz.at/cgi-bin/index?id=000100003123>. (Datum dostopa: 17. 4. 2005).
251. Raab, D. Charles. 1997. »Privacy, democracy, information«. V Loader, D. Brian (ur.). 1997. The Governance of Cyberspace, str. 155–174. London, New York: Routledge.
252. Reitinger, R. Philip. 2000. »Encryption, anonymity and markets«. V Thomas, Douglas in Loader D. Brian, (ur.). 2000. Cybercrime, str. 132–152. London, New York: Routledge.
253. Reuters. 2001. »FBI 'Fesses Up to Net Spy App«. Wired News, 12. december 2001. <http://www.wired.com/news/conflict/0,2100,49102,00.html>. (Datum dostopa: 19. 5. 2004).
254. Reuters. 2006. »Verizon to launch mobile chaperone service«. ZDNet, 10. junij 2006. <http://news.zdnet.com/2100-1040_22-6082472.html>. (Datum dostopa: 11. 11. 2006).
255. Richardson, Tim. 2004. »China snoops on text messages«. The Register, 2. julij 2004. <http://www.theregister.co.uk/2004/07/02/china_text_snoop/>. (Datum dostopa: 23. 11. 2004).
256. Rivest, Ronald. 1994. »Elektronsko pismo Ronalda Rivesta, 'Clipper Chip Will Block Crime', 25. februar 1994«. Computer underground Digest, 27. februar 1994, Vol. 6, Issue 19. <http://www.totse.com/en/zines/cud_a/cud619.html>. (Datum dostopa: 26. 5. 2004).
257. Rizman, Rudi (ur.). 1992. Sodobni liberalizem. Ljubljana: Krt.
258. Robinson, Colin. 2002. Military and Cyber-Defense: Reactions to the Threat. Center for Defense Information. <http://www.cdi.org/terrorism/cyberdefense-pr.cfm>. (Datum dostopa: 6. 12. 2004).

259. RSA Laboratories. 2000. RSA Laboratories' Frequently Asked Questions About Today's Cryptography, Version 4.1. RSA Security Inc.. <http://www.rsasecurity.com>. (Datum dostopa: 1. 4. 2004).
260. Ruffin, Oxblood. 2001. The Cult Of the Dead Cow Offers Helping Hand In America's Time Of Need. <http://www.cultdeadcow.com/archives/000870.php3>. (Datum dostopa: 4. 12. 2004).
261. Samarajiva, Rohan. 2001. »Interactivity as Though Privacy Mattered«. V Agre E. Philip in Rotenberg Marc, (ur.). 2001. Technology and Privacy: The New Landscape, str. 277–309. Cambridge, Massachusetts, London, England: MIT Press.
262. Sandberg, Jared. 2001. »Hackers poised to land at wireless AirPort«. ZDNet news, 4. februar 2001. <http://news.zdnet.com/2100-9595_22-527906.html>. (Datum dostopa: 23. 4. 2005).
263. SANS. 2004. Survival Time History. <http://isc.sans.org/survivalhistory.php>. (Datum dostopa: 6. 12. 2004).
264. SANS. 2006. Dnevni podatki o napadih. <http://isc2.sans.org/daily_summary.txt>. (Datum dostopa: 14. 8. 2006).
265. Schmieder, Stephan. 2005. tor.unixgu.ru. <http://tor.unixgu.ru/>. (Datum dostopa: 18. 8. 2006).
266. Schneier, Bruce in Banisar, David. 1997. The Electronic Privacy Papers. New York, Toronto: Jonh Wiley & Sons.
267. Schneier, Bruce. 1998. »The Secret Story of Non-secret Encryption«. V Crypto-Gram, 15. maj 1998, <http://www.schneier.com/crypto-gram-9805.html>. (Datum dostopa: 3. 5. 2005).
268. Schneier, Bruce. 1999. »European Cellular Encryption Algorithms«. V Crypto-Gram, 15. december 1999. <http://www.schneier.com/crypto-gram-9912.html>. (Datum dostopa: 3. 5. 2005).
269. Schneier, Bruce. 2000. »Cookies«. Crypto-Gram, 15. februar 2000. <http://www.schneier.com/crypto-gram-0002.html>. (Datum dostopa: 3. 5. 2005).
270. Schneier, Bruce. 2001a. »PGP broken«. Crypto-Gram, 15. januar 2001. <http://www.schneier.com/crypto-gram-0101.html>. (Datum dostopa: 3. 5. 2005).
271. Schneier, Bruce. 2001b. »802.11 Security«. Crypto-Gram, 15. marec 2001. <http://www.schneier.com/crypto-gram-0103.html>. (Datum dostopa: 3. 5. 2005).
272. Schneier, Bruce. 2002. »Secrecy, Security, and Obscurity«. V Crypto-Gram, 15. maj 2002. <http://www.schneier.com/crypto-gram-0205.html>. (Datum dostopa: 3. 5. 2005).
273. Schneier, Bruce. 2004a. »Virus wars«. V Crypto-Gram, 15. april 2004. <http://www.schneier.com/crypto-gram-0404.html>. (Datum dostopa: 3. 5. 2005).
274. Schneier, Bruce. 2004b. »News«. Crypto-Gram, 15. februar 2004. <http://www.schneier.com/crypto-gram-0402.html>. (Datum dostopa: 3. 5. 2005).

275. Schneier, Bruce. 2005. »T-Mobile Hack«. Crypto-Gram, 15. februar 2005. <http://www.schneier.com/crypto-gram-0502.html>. (Datum dostopa: 15. 2. 2005).
276. Schneier, Bruce. 2006a. »NSA and Bush's Illegal Eavesdropping«. Crypto-Gram, 15. januar 2006. <http://www.schneier.com/crypto-gram-0601.html#12>. (Datum dostopa: 15. 2. 2006).
277. Schneier, Bruce. 2006b. »Project Shamrock«. Crypto-Gram, 15. januar 2006. <http://www.schneier.com/crypto-gram-0601.html#14>. (Datum dostopa: 15. 2. 2006).
278. Schneier, Bruce. 2006c. »Dutch Botnet«. Crypto-Gram, 15. januar 2006. <http://www.schneier.com/crypto-gram-0601.html#4>. (Datum dostopa: 15. 2. 2006).
279. Schneier, Bruce. 2006d. »AOL Releases Massive Amount of Search Data«. Schneier.com, 8. avgust 2006. <http://www.schneier.com/blog/archives/2006/08/aol_releases_ma.html>. (Datum dostopa: 8. 8. 2006).
280. Schneier, Bruce. 2006e. »Security through Begging«. Crypto-Gram, 15. april 2006. <http://www.schneier.com/crypto-gram-0604.html#6>. (Datum dostopa: 15. 4. 2006).
281. Schneier, Bruce. 2006f. »Greek Wiretapping Scandal«. Schneier.com, 22. junij 2006. <http://www.schneier.com/blog/archives/2006/06/greek_wiretappi_1.html>. (Datum dostopa: 15. 7. 2006).
282. Schneier, Bruce. 2006g. »Updating the Traditional Security Model«. Schneier.com, 1. avgust 2006. <http://www.schneier.com/blog/archives/2006/08/updating_the_tr.html>. (Datum dostopa: 1. 8. 2006).
283. Schröder, Christian in Laurant, Cédric. 2005. Der Österreichische Verfassungsgerichtshof (Austrian Federal Constitutional Court) - VfGH, G 37/02 ua, February 27, 2003 - Outline - comments - relevant links. <http://www.epic.org/privacy/intl/austrian_vfgh-022703.html>. (Datum dostopa: 24. 4. 2005).
284. Schulman, Andrew. 2001a. Computer And Internet Surveillance in the Workplace: Rough Notes. <http://www.sonic.net/~undoc/survtech.htm>. (Datum dostopa: 17. 1. 2004).
285. Schulman, Andrew. 2001b. The Extent of Systematic Monitoring of Employee E-mail and Internet Use. <http://www.sonic.net/~undoc/extent.htm>. (Datum dostopa: 17. 1. 2004).
286. sci.crypt. 1994. The Cryptography FAQ (05/10: Product Ciphers). V USENET, oddelek: sci.crypt, <http://www.faqs.org/faqs/cryptography-faq/part05/>. (17. avgust 2002). (Datum dostopa: 19. 4. 2004).
287. Science Daily. 2000. Standard Feature Of Web Browser Design Leaves Opening For Privacy Attacks. Science Daily, 8. december 2000. <http://www.sciencedaily.com/releases/2000/12/001208074325.htm>. (Datum dostopa: 23. 4. 2005).

288. Shankland, Stephen. 2000. »German programmer “Mixter” addresses cyberattacks«. News.com, 14. februar 2000. <http://news.com.com/German+programmer+Mixter+addresses+cyberattacks/2100-1023_3-236876.html>. (Datum dostopa: 3. 12. 2004).
289. Shetty, Jitesh in Adibi, Jafar. 2004. The Enron Email Dataset Database Schema and Brief Statistical Report. Information Sciences Institute. <http://www.isi.edu/~adibi/Enron/Enron_Dataset_Report.pdf>. (Datum dostopa: 7. 12. 2004).
290. Shireen, J. Herbert. 1998. »A Brief History of Cryptography«. Cybercrimes. <http://cybercrimes.net/Cryptography/Articles/Hebert.html>. (Datum dostopa: 22. 4. 2005).
291. Singel, Ryan. 2003. »Congress Expands FBI Spying Power«. Wired News, 24. november, 2003. http://www.wired.com/news/politics/0,1283,61341,00.html. (Datum dostopa: 23. 1. 2005).
292. Singel, Ryan. 2004. »False Domain Info May Mean Jail«. Wired News, 7. februar 2003. http://www.wired.com/news/politics/0,1283,62198,00.html. (Datum dostopa: 11. 6. 2004).
293. Singel, Ryan. 2005. When Cell Phones Become Oracles. Wired, 25. julij 2005. <http://www.wired.com/news/wireless/0,1382,68263,00.html>. (Datum dostopa: 8. maj 2006).
294. Sinrod, J. Eric. 2004. »E-Legal: Employer Access to Employee E-Mails«. Law.com, 27. januar 2004. <http://www.duanemorris.com/articles/print/article1479.pdf>. (Datum dostopa: 11. 6. 2004).
295. Smith, M. Richard. 2003. »Microsoft Word bytes Tony Blair in the butt«. ComputerBytesMan.com, 23. september 2003. <http://www.computerbytesman.com/privacy/blair.htm>. (Datum dostopa: 1. 8. 2006).
296. Soo-Jeong, Lee. 2004. »North Korea has 600 computer hackers, South Korea claims«. Security Focus, 5. oktober 2004. <http://www.securityfocus.com/news/9649>. (Datum dostopa: 5. 12. 2004).
297. SOVA. 2004. Odločba o delni zavrnitvi zahteve za dostop do informacije javnega značaja. Pisni odgovor Slovenske varnostno obveščevalne agencije z dne 23. 8. 2004, šifra dopisa 071/3-2004.
298. Spamhaus. 2005. Virus and dDoS Attacks on Spamhaus. <http://www.spamhaus.org/cyberattacks/>. (Datum dostopa: 4. 11. 2004).
299. Splichal, Slavko. 2002. Principles of Publicity and Press Freedom. Lanham, Boulder, New York, Oxford: Rowman & Littlefield Publishers.
300. SPY. 2004. Odgovor podjetja SPY, 1. september 2004. Elektronsko sporočilo poslano iz naslova <agent@spy.co.za>, dne 1. sptember 2004 ob 13:34:44.

301. Srivastava, Anita. 2001. Dynamic Pricing Models: Opportunity for Action. Cap Gemini Ernst & Young Center for Business Innovation. <http://www.cbi.cgey.com/pub/bi-news/pdf/dynamic_pricing_models_with_cover.pdf>. (Datum dostopa: 15. 5. 2002).
302. Stallman, Richard. 2005. »Soft sell«. Guardian Unlimited, 2. avgust 2005. <http://technology.guardian.co.uk/online/comment/story/0,12449,1540984,00.html>. (Datum dostopa: 1. 8. 2006).
303. STAND. Operation Dear Jack (How the E-commerce Bill could send YOU to jail, pismo Jacku Strawu). <http://www.stand.org.uk/dearjack/>. (Datum dostopa: 19. 5. 2004).
304. Statewatch. 1997. European Union and FBI launch global surveillance system. <http://www.freenix.fr/netizen/swreport.html>. (2. februar 1999). (Datum dostopa: 22. 4. 2005).
305. Steinhardt, Barry. 2000. Statement Of Barry Steinhardt Associate Director American Civil Liberties Union On The Fourth Amendment And Carnivore Before The House Judiciary Committee Subcommittee On The Constitution, 24 julij 2000. <http://www.aclu.org/Privacy/Privacy.cfm?ID=8969&c=130>. (Datum dostopa: 3. 5. 2005).
306. StopCarnivore.org. 2000. <http://www.stopcarnivore.org/carnfreeisps.htm>. [Spletna stran ni več dostopna, kopija je dostopna na: Original Dissent. 2005. 'Carnivore free' ISPs. Original Dissent, 20. december 2000. <http://www.originaldissent.com/forums/showthread.php?t=3913>. (Datum dostopa: 20. 4. 2005).]
307. Stubblefield, Adam, Ioannidis, John in Rubin, D. Aviel. 2001. Using the Fluhrer, Mantin and Shamir Attack to break WEP. <http://www.isoc.org/isoc/conferences/ndss/02/proceedings/papers/stubbl.pdf>. (Datum dostopa: 3. 5. 2004).
308. Sykes, J. Charles. 1999. The End Of Privacy. New York: St. Martin's Press.
309. Šavnik, Janko. 2005. Računalniška kriminaliteta na področju PU Ljubljana. Predstavitev na konferenci Infosek 2005 – forum,10. maj 2005 v Ljubljani.
310. Šelih, Alenka. 1979. »Zasebnost in nove oblike njenega kazenskopravnega varstva«. V Perenič, Anton (ur.). 1979. Zbornik znanstvenih razprav, Let. 39, 1979 str. 149–181. Ljubljana: Univerza v Ljubljani, Pravna fakulteta.
311. Šturm, Lovro (ur.). 2002. Komentar ustave republike Slovenije. Ljubljana: Fakulteta za podiplomske državne in evropske študije.
312. Taylor, A. Paul. 2000. »Hackers - cyberpunks or microserfs?«. V Thomas, Douglas in Loader D. Brian, (ur.). 2000. Cybercrime, str. 36–55. London, New York: Routledge.
313. Tech Law Journal. 2001. An Analysis of How the Events of September 11 May Change Federal Law. <http://www.techlawjournal.com/terrorism/20010917.asp>. (Datum dostopa: 22. 4 .2005).

314. Temporary Committee on the ECHELON Interception System. 2001. Working document in preparation for a report on the existence of a global system for intercepting private and commercial communications (ECHELON interception system). European Parliament. [Dostopno na: <http://www.fas.org/irp/program/process/europarl_draft.pdf>. (Datum dostopa: 1. 4. 2004).]
315. Teranson, Alif. 2004. Elektronsko sporočilo Alifa Teransona z dne 25. aprila 2004, posredovano na poštni seznam PGP-USERS dne 28. aprila 2004. [Dostopno na: <http://lists.cryptorights.org/mailman/listinfo/pgp-users>. (Datum dostopa: 1. 4. 2005).]
316. The Ethical Spectacle. 1995. The Zimmermann Case. <http://www.spectacle.org/795/zimm.html>. (Datum dostopa: 22. 4. 2005).
317. The Pew Internet & American Life Project. 2000. Trust and Privacy Online: Why Americans Want to Rewrite the Rules. <http://www.pewinternet.org/reports/toc.asp?Report=19>. (Datum dostopa: 3. 5. 2005).
318. Thomas, Douglas. 2000. »Criminality on the electronic frontier«. V Thomas, Douglas in Loader D. Brian, (ur.). 2000. Cybercrime, str. 17–35. London, New York: Routledge.
319. Thomas, Douglas in Loader D. Brian, (ur.). 2000. Cybercrime. London, New York: Routledge.
320. Thomas, Jim. 1994. »Elektronsko pismo Jima Thomasa, 'Clipper Chip Will Block Crime', 25. februar 1994«. Computer underground Digest, 27. februar 1994, Vol. 6, Issue 19. <http://www.totse.com/en/zines/cud_a/cud619.html>. (Datum dostopa: 26. 5. 2004).
321. Thompson, Fred. 2000. Government Information Security Act of 1999 - Report of the Committee on Governmental Affairs, United States Senate, to accompany S. 1993, to reform government information security by strengthening information security practices throughout the federal government, 10. april 2000. Wahington: U.S. Government Printing Office. [Dostopno na strežniku <thomas.loc.gov>.]
322. Turkington, C. Richard in Allen, L. Anita. 1999. Privacy Law: Cases and Materials. ZDA: West Group.
323. Turkington, C. Richard in Allen, L. Anita. 2002. Privacy Law: Cases and Materials. ZDA: West Group.
324. US Department of Justice. 1996. FOIA Update, Vol. XVIII, No. 4, str. 2. <http://www.usdoj.gov/oip/foi-upd.htm>. (Datum dostopa: 19. 4. 2005).
325. Vehovar, Vasja, Jovan, Matej in Kragelj, Boris. 2003. Sibis Country Report: Slovenija. Ljubljana: Fakulteta za družbene vede.
326. Vidmar, Tone. 1997. Računalniška omrežja in storitve. Ljubljana: Atlantis.
327. Vodušek, Vladimir. 2005. Na Sovi s ponarejenimi spričevali. 24ur.com, 19. julij 2005. <http://24ur.com/bin/article.php?article_id=2059256>. (Datum dostopa: 20. julij 2005).

328. Voiskounsky, E. Alexander, Babveva D. Julia in Smyslova, V. Olga. 2000. »Attitudes towards computer hacking in Russia«. V Thomas, Douglas in Loader D. Brian, (ur.). 2000. Cybercrime, str. 56–84. London, New York: Routledge.
329. Vrhovno sodišče. 2004. Odločba o zavrnitvi zahteve za dostop do informacije javnega značaja. Pisni odgovor Vrhovnega sodišča Republike Slovenije z dne 20. 8. 2004, šifra dopisa Su 36-03/2004 - 19.
330. Wagner DeCew, Judith. 1997. In Pursuit of Privacy. Ithaca, London: Cornell University Press.
331. Wassenaar Secretariat. 2003. The Wassenaar Arrangement On Export Controls For Conventional Arms And Dual-Use Goods and Technologies - List Of Dual-Use Goods and Technologies And Munition List. <http://www.wassenaar.org/list/wa-listTableOfContents.htm>. (Datum dostopa: 22. 4. 2005).
332. Wearden, Graeme. 2001. »Virgin Mobile admits storing customer location records«. ZDNet, 29. oktober 2001. <http://news.zdnet.co.uk/hardware/emergingtech/0,39020357,2098193,00.htm>. (Datum dostopa: 5. maj 2006).
333. Wearden, Graeme. 2004. »Russia and China 'behind current spam deluge'«. ZDNet, 9. junij 2004. <http://www.zdnet.com.au/news/security/0,2000061744,39150051,00.htm>. (Datum dostopa: 23. 4. 2005).
334. Webster, Frank. 1995. Theories of the Information Society. London, New York: Routledge.
335. Whitaker, Reg. 1999. The End of Privacy. New York: The New Press.
336. White, C. James. 2003. People, Not Places - A Policy Framework for Analyzing Location Privacy Issues. EPIC. <http://www.epic.org/privacy/location/jwhitelocationprivacy.pdf>. (Datum dostopa: 1. 4. 2004).
337. Wi-Fi Toys. 2004. »New World Record for Bluetooth Link!«. Wi-Fi Toys, 30. julij 2004. <http://www.wifi-toys.com/wi-fi.php?a=articles&id=21>. (Datum dostopa: 24. 4. 2005).
338. Wienbar, Sharon. 2004. »The spyware inferno«. ZDNet, 16. avgust 2004. <http://www.zdnet.com.au/insight/security/0,39023764,39156395,00.htm>. (Datum dostopa: 8. 11. 2004).
339. Wikipedia, geslo: "Kerchoffs' law". <http://en.wikipedia.org/wiki/Kerchoffs%27_Law>. (Datum dostopa: 24. 4. 2005).
340. Wikipedia, geslo: "Morris worm". <http://en.wikipedia.org/wiki/Morris_worm>. (Datum dostopa: 3. 5. 2005).
341. Wikipedia, geslo: "Penet remailer". <http://en.wikipedia.org/wiki/Penet_remailer>. (Datum dostopa: 25. 4. 2005).
342. Willan, Philip. 2004. »EU seeks quantum cryptography response to Echelon«. Computerworld, <http://www.computerworld.com/printthis/2004/0,4814,93220,00.html>; [QuickLink: 46947]. (Datum dostopa: 18. 5. 2004).

343. Wired News. 2002. »U.S. v. Microsoft: Timeline«. Wired News. 4. november 2002. <http://www.wired.com/news/antitrust/0,1551,35212,00.html>. (Datum dostopa: 7. 12. 2004).
344. Woodcock, Mark. 1995. Improving Your Network Security Using SATAN. University of Maryland. <http://www.cs.umbc.edu/~woodcock/cmsc482/proj1/satan.html>. (Datum dostopa: 11. 4. 2005).
345. Young, Adam. 2004. »Mitigating Insider Threats to RSA Key Generation«. Cryptobytes, Volume 7, No. 1, Spring 2004. RSA Labolatories. <http://www.rsasecurity.com>.
346. Zetter, Kim. 2004a. »Outsourcing: Danger to Privacy«. Wired News, 20. februar 2004. <http://www.wired.com/news/business/0,1367,62356,00.html>. (Datum dostopa: 27. 4. 2004).
347. Zetter, Kim. 2004b. »Getting Naked for Big Brother«. Wired News, 17. maj 2004. <http://www.wired.com/news/privacy/0,1848,63450,00.html>. (Datum dostopa: 17. 5. 2004).
348. Zetter, Kim. 2004c. »E-Mail Snooping Ruled Permissible«. Wired News, 30. junij 2004. <http://www.wired.com/news/privacy/0,1848,64043,00.html>. (Datum dostopa: 1. 7. 2004).
349. Zimmermann, Phil. 1993. Testimony of Philip Zimmermann To the Subcommittee On Science, Technology, and Space of the US Senate Committe On Commerce, Science, and Transportation, 12. oktobra 1993. <http://www.pgp.com/phil/phil-quotes.cgi> ter <http://www.interesting-people.org/archives/interesting-people/199310/msg00026.html>. (Datum dostopa: 9. 6. 2004).
350. Zimmermann, Philip. 1999. Why I Wrote PGP. <http://www.philzimmermann.com/EN/essays/WhyIWrotePGP.html>. (Datum dostopa: 19. 1. 2005).
351. Zupančič, M. Boštjan. 2002. »36. člen (nedotakljivost stanovanja)«. V Šturm, Lovro (ur.). 2002. Komentar ustave republike Slovenije, str. 386–390. Ljubljana: Fakulteta za podiplomske državne in evropske študije.
352. Žerdin, Ali. 2001. »Sova v vašem računalniku«. Mladina, 8. oktobra 2001. <http://www.mladina.si/tednik/200140/clanek/sova2001/>. (Datum dostopa: 3. 5. 2005).

Odločbe Evropskega sodišča za človekove pravice

1. A. D. T. v. Veliki Britaniji, odločba z dne 31. 07. 2000.
2. Dudgeon v. Velika Britanija, odločba z dne 22. 10. 1981.
3. Gaskin v. Velika Britanija, odločba z dne 27. 3. 1983.
4. Guerra et. al. v. Italija, odločba z dne 19. 2. 1998.
5. Halford v. Velika Britanija, odločba z dne 25. 6. 1997.
6. Hatton in drugi v. Veliki Britaniji, odločba z dne 2. 10. 2001.
7. Klaas et. al v. ZR Nemčija, odločba z dne 6. 9. 1978.
8. Kopp v. Švica, odločba z dne 25. 3. 1998.
9. Lambert v. Francija, odločba z dne 24. 8. 1998.
10. Leander v. Švedska, odločba z dne 26. 03. 1987.
11. Lopez Ostra v. Španiji, odločba z dne 9. 12. 1994.
12. Lustig-Prean in Beckett v. Velika Britanija, odločba z dne 27. 09. 1999.
13. Malone v. Velika Britanija, odločba z dne 02. 08. 1984.
14. Modinos v. Cipru, odločba z dne 22.04.1993.
15. Niemietz v. ZR Nemčija, odločba z dne 16. 12. 1992.
16. Von Hannover v. Nemčija, odločba z dne 24. 6. 2004.

Odločbe ameriških sodišč

1. Ex parte Jackson, 96 U.S. 727 (1877).
2. Able v. United States, 155 F.3d 628 (1998).
3. Bernstein v. United States Department of Justice, 176 F.3d 1132 (1999).
4. Bonita P. Bourke, et. al. v. Nissan Motor Corporation, No. 68-705 (Cal. Ct.App.1993).
5. Bowers v. Hardwick, 478 U.S. 186 (1986).
6. Conboy v. AT&T, 84 F. Supp. 2d 492 (2000).
7. DeMay v. Roberts, 46 Mich. 160, 9 N.W. 146 (1881).
8. Eisenstadt v. Baird, 405 U.S. 438 (1972).
9. Goldman v. United States, 316 U.S. 129 (1942).
10. Griswold v. Conencticut, 381 U.S. 479 (1965).
11. Jaffee v. Redmond, 518 US 1 (1996).
12. Katz v. United States, 389 U.S. 347 (1967).
13. Kyllo v. United States, 533 U.S. 27 (2001).
14. Lawrence v. Texas, 539 US 558 (2003).
15. McLaren v. Microsoft, No. 05-97-00824 (Tex. Ct. App. 28. maj, 1999).
16. McVeigh v. Cohen, 983 F.Supp. 215 (1998).
17. Meyer v. Nebraska, 262 U.S. 390 (1923).

18. National Association for the Advancement of Colored People v. Alabama, 357 U.S. 449 (1958).
19. O'Connor v. Ortega, 480 U.S. 709 (1987).
20. Olmstead v. United States, 277 U.S. 438 (1928).
21. On Lee v. United States, 343 U.S. 747 (1952).
22. Pavesich v. New England Life Insurance Co., 122 Ga. 190, 50 S.E. 68 (1905).
23. Pierce v. Society of Sisters, 268 U.S. 510 (1925).
24. Reno v. American Civil Liberties Union, 521 U.S. 844 (1997).
25. Rhodes v. Graham, 37 S.W.2d 46 (1931).
26. Roe v. Wade, 410 U.S. 113 (1973).
27. Shoars v. Epson America Inc., No. (SWC) II2749 (Cal App. Dep't. Super. Ct. Dec 8, 1992)
28. Smith v. Maryland, 242 U.S. 735 (1979).
29. State v. Hunt, 91 N.J. 338, 450 A.2d 952 (1982).
30. Steve Jackson Games, Inc. v. United States Secret Service, 36 F.3d 457 (1994).
31. Talley v. California, 362 U.S. 60 (1960).
32. U.S. West v. F.C.C., 182 F.3d 1224 (1999).
33. United States of America v. Bradford C. Councilman, No. 03-1383 (1st Cir., June 29, 2004).
34. United States of America v. Bradford C. Councilman, 385 F.3d 793 (1st Cir. 2004).
35. United States v. Miller, 425 U.S. 435 (1976).
36. United States v. Nicodemo S. Scarfo, No. 00-404 (2001).
37. United States v. White, 401 U.S. 745 (1971).
38. Walls v. City of Petersburg, 895 F.2d 188, 192 (1990).
39. Whalen v. Roe, 429 U.S. 589 (1977).

Mednarodni dokumenti

Direktive in dokumenti EU

1. Direktiva 95/46/EC o varstvu posameznikov pri obdelovanju osebnih podatkov in svobodnem pretoku teh podatkov (Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data), sprejeta 24. oktobra 1995. Official Journal L 281, 23/11/1995 p. 0031 - 0050.
2. Direktiva 97/66/EC o obdelavi osebnih podatkov in varstvu zasebnosti v telekomunikacijskem sektorju (Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector), sprejeta 15. decembra 1997. Official Journal L 024, 30/01/1998 p. 0001 - 0008.

3. Direktiva 2002/58/EC o obdelovanju osebnih podatkov in varstvu zasebnosti na področju elektronskih komunikacij (Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector), sprejeta 12. julija 2002. Official Journal L 201, 31/07/2002 p. 0037 – 0047.
4. Direktiva 2006/24/ES Evropskega parlamenta in Sveta z dne 15. marca 2006 o hrambi podatkov, pridobljenih ali obdelanih v zvezi z zagotavljanjem javno dostopnih elektronskih komunikacijskih storitev ali javnih komunikacijskih omrežij, in spremembi Direktive 2002/58/ES (Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC), sprejeta 14. 12. 2005. Official Journal L 105, 13/04/2006, p. 0054 – 0063.
5. Resolucija o zakonitem prestrezanju telekomunikacij (Council Resolution of 17 January 1995 on the Lawful Interception of Telecommunications), sprejeta 17. januarja 1995. Official Journal, C 329, 04.11.1996, p. 1–6.
6. "Interception of communications", report to COREPER, ENFOPOL 40, 10090/93, Confidential, Brussels, 16.11.1993.; vir: Statewatch, 1997.
7. Odločba Komisije z dne 26. julija 2000 po Direktivi Evropskega parlamenta in Sveta 95/46/ES o primernosti zaščite, ki jo zagotavljajo načela zasebnosti varnega pristana in s tem povezana najpogosteje zastavljena vprašanja, ki jih je izdalo Ministrstvo za trgovino ZDA (notificirano pod dokumentarno številko K(2000) 2441) (Besedilo velja za EGP) (2000/520/ES). Official Journal L 215 , 25/08/2000 P. 0007 - 0047. [Dostopno na: <http://europa.eu.int/servlet/portail/RenderServlet?search=DocNumber&lg=sl&nb_docs=25&domain=Legislation&coll=&in_force=NO&an_doc=2000&nu_doc=520&type_doc=Legislation>. (Datum dostopa: 3. 5 .2005).]

Dokumenti Sveta Evrope

1. Svet Evrope. 1950. Evropska konvencija o varstvu človekovih pravic in mednarodnih svoboščin, spremenjene s protokoli št. 3, 5 in 8 ter dopolnjene s protokolom št. 2, ter njenih protokolov št. 1, 4, 6, 7, 9, 10 in 11 (Convention on Human Rights and Fundamental Freedoms as amended by Protocols Nos. 3, 5 and 8 and amended by Protocol No. 2 and its Protocols Nos. 1, 4, 6, 7, 9, 10 and 11), sprejel jo je Svet Evrope leta 1950. Uradni list RS, št. 33/1994, "Mednarodne pogodbe", št. 7/1994, 13. 6. 1994. Konvencijo je Državni zbor Republike Slovenije ratificiral 13. 6. 1994. Veljati je začela dne 28. 6. 1994.
2. Svet Evrope. 1981. Konvencija Sveta Evrope o varstvu posameznikov glede na avtomatsko obdelavo osebnih podatov (Convention for the Protection of Individuals

with Automatic Processing of Personal Data), sprejel jo je Svet Evrope 28. 1. 1981. Uradni list RS, Mednarodne pogodbe, št. 3/1994. Konvencijo je Državni zbor Republike Slovenije ratificiral dne 25. 1. 1994. Veljati je začela dne 1. 3. 1994.

3. Svet ministrov Sveta Evrope. 1989. Priporočilo Sveta Evrope št. R(89) 2, o varstvu osebnih podatkov, uporabljanih za zaposlovanje (Recommendation No. R (89) 2 on the protection of personal data used for employment purposes), sprejeto 18 januarja 1989.
4. Svet ministrov Sveta Evrope. 1995. Priporočilo Sveta Evrope št. R(95) 13, glede problemov kazensko procesnega prava povezanega z informacijskimi državami (Recommendation No. R(95) 13, Concerning Problems of Criminal Procedure Law Connected with Information states), sprejeto 11. septembra 1995.
5. Svet Evrope. 2001. Konvencija o kibernetski kriminaliteti (Convention on Cybercrime), sprejel jo je Svet Evrope, 23. novembra 2001. Uradni list RS, Mednarodne pogodbe, št. 17/2004. Konvencijo je Državni zbor Republike Slovenije ratificiral dne 20. 5. 2004. Veljati je začela dne 1. 1. 2005.

Dokumenti OECD

1. OECD. 1980. Smernice za zaščito zasebnosti in čezmejni pretok osebnih podatkov (Guidelines on the Protection of Privacy and Transborder Flows of Personal Data), sprejete 23. septembra 1980.
2. OECD. 1997. Smernice o kriptografski politiki (Guidelines on Cryptography Policy), sprejete 27. marca 1997.

Dokumenti OZN

1. Generalna skupščina Združenih narodov. 1948. Splošna deklaracija o človekovih pravicah (Universal Declaration of Human rights), 10. 12. 1948.
2. OZN. 1966. Mednarodni pakt o državljanskih in političnih pravicah (International Covenant on Civil and Political Rights), sprejeta v OZNa 1966. Uradni list SFRJ, št. 7/1971. Pakt je ratificiral Zvezni zbor skupščine SFRJ 30. 1. 1971. Veljati je začel 12. 2. 1971.
3. Resolucija Generalne skupščine OZN A/RES/45/95. 1990. Smernice o avtomatiziranih zbirkah osebnih podatkov. (Guidelines for the Regulation of Computerized Personal Data Files), sprejeta v Generalni skupščini OZN 14. decembra 1990.

Zakonodaja

Ameriška zakonodaja

1. Ustava Združenih držav Amerike (Constitution of United States of America), 1798.
2. Listina svoboščin (Bill of Rights), 1791.
3. Privacy Act of 1974, 5 U.S.C. (1974).
4. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001, 18 U.S.C. (2001).
5. Freedom of Information Act of 2002, 5 U.S.C. (2002).
6. Employee Polygraph Protection Act of 1988, 29 U.S.C. (1988).
7. Electronic Communication Privacy Act of 1986, 18 U.S.C. (1986).
8. Driver's Privacy Protection Act of 1994, 18 U.S.C. (1994).
9. Telecommunications Act of 1996, 47 U.S.C. (1996).
10. Video Privacy Protection Act of 1988, 18 U.S.C. (1988).
11. Fair Credit Report Act of 1970, 15 U.S.C. (1970).
12. Consumer Credit Reporting Reform Act of 1996, 15 U.S.C. (1997).
13. Bank Secrecy Act of 1970, 31 U.S.C. (1970).
14. Communications Assistance for Law Enforcement Act (Digital Telephony Act) of 1994, 47 U.S.C. (1994).
15. Invention Secrecy Act of 1951, 35 U.S.C. (1951).
16. Computer Security Act of 1987, 40 U.S.C. (1987).
17. Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. (1978).
18. The Homeland Security Act of 2002, 6 U.S.C. (2002).
19. Classified Information Procedures Act of 1980, 18 U.S.C. (1980).
20. Communications Decency Act of 1996, 47 U.S.C. (1996).
21. Children's Online Privacy Protection Act of 1998, 15 U.S.C. (1998).
22. Fraudulent Online Identity Sanctions Act of 2004, 15 U.S.C. (2004).
23. Intellectual Property Protection and Courts Amendments Act of 2004, 15 U.S.C. (2004).
24. Digital Millennium Copyright Act of 1998, 17 U.S.C. (1998).
25. Standards for Privacy of Individually Identifiable Health Information (HIPAA Privacy Rule), Department of Health and Human Services, 2001. <http://www.hhs.gov/ocr/hipaa/>.
26. Restatement of the Law (2d) of Torts, 1964.

Zakonodaja republike Irske

1. Electronic Commerce Act, 2000, Irska. <http://www.oireachtas.ie/documents/bills28/acts/2000/a2700.pdf>.

Zakonodaja Velike Britanije

1. Regulation of Investigatory Powers Act, 2000, Velika Britanija. <http://www.hmso.gov.uk/acts/acts2000/20000023.htm#aofs>.
2. Human Rights Act, 1998, Velika Britanija.

Slovenska zakonodaja

1. Odločba Ustavnega sodišča RS, št. Up-472/02, Uradni list, RS, št. 114/2004.
2. Odločba Vrhovnega sodišča RS, št. I Ips 264/2005. Dokument je bil maja 2006 na podlagi Zakona o dostopu do informacij javnega značaja pridobljen od Vrhovnega sodišča RS, št. Su 36-03/2006 – 78 – 2.
3. Odločba Vrhovnega sodišča RS, št. I Ips 292/2004. Dokument je bil maja 2006 na podlagi Zakona o dostopu do informacij javnega značaja pridobljen od Vrhovnega sodišča RS, št. Su 36-03/2006 – 78 – 2.
4. Zakon o varstvu osebnih podatkov (ZVOP), Uradni list RS, št. 52/99, 57/01, 59/01-popr., 52/02-ZDU-1 in 73/04-ZUP-C.
5. Zakon o varstvu osebnih podatkov (ZVOP-1), Uradni list RS, št. 86/04.
6. Zakon o Informacijskem pooblaščencu (ZInfP), Uradni list RS, št. 113/2005.
7. Zakon o elektronskih komunikacijah (ZeKOM), Uradni list RS, št. 43/04 in 86/04 – ZVOP-1.
8. Novela Zakona o varstvu potrošnikov (ZVPot-A), Uradni list RS št. 110/02.
9. Zakon o telekomunikacijah (ZTel), Uradni list RS, št. 30/01, 52/02-ZJA, 110/02-ZGO-1 in 43/04-ZEKom.
10. Zakon o kazenskem postopku (ZKP), Uradni list RS, št. 63/94, 70/94, 25/96-odl. US, 39/96-odl. US, 5/98-odl. US, 49/98, 66/98, 72/98, 6/99, 42/00-odl. US, 66/00, 111/01, 32/02 - odl. US, 110/02 - ZDT-B, 3/03 - odl. US, 21/03 - odl. US, 44/03 - odl. US, 56/03, 92/03-odl. US, 114/03-odl. US, 43/04, 68/04-odl. US in 83/04-odl. US.
11. Kazenski zakonik (KZ), Uradni list RS, št. 63/94, 70/94-popr., 23/99-KZ-A, 110/02-ZDT-B, 40/04-KZ-B in 95/04-KZ-UPB1.
12. Novela Kazenskega zakonika (KZ-B), Uradni list RS, št. 40/04.
13. Zakon o Slovenski obveščevalno varnostni agenciji (ZSOVA), Uradni list RS, št. 23/99, 56/02-ZJU, 26/03-ZPNOVS, 126/03 in 54/04-ZDoh-1, 56/2004, 62/2004, 63/2004 - popr., 61/2006.

14. Predlog Pravilnika o opremi in vmesnikih za zakonito prestrezanje komunikacij. Predlog je aprila 2005 pripravilo Ministrstvo za gospodarstvo. Kopijo predloga pravilnika so predstavniki Ministrstva za gospodarstvo poslali nekaterim slovenskim ponudnikom dostopa do interneta s prošnjo za komentiranje. Na spletnih straneh ministrstva za gospodarstvo je bil objavljen maja 2005.
15. Pravilnik o opremi in vmesnikih za zakonito prestrezanje komunikacij, Uradni list RS, št. 29/2006.
16. Pravilnik o programski opremi in vmesnikih za zakonito prestrezanje komunikacij, Uradni list RS, št. 73/03.
17. Zakon o zasebnem varovanju (ZZasV), Uradni list RS, št. 126/02.

Ostali internetni viri (necitirani)

1. Telekomov Imenik elektronske pošte Slovenije, <http://afna.telekom.si>.
2. Whoppix - distribucija Linuxa z orodji za odkrivanje varnostnih pomakljivosti, <http://www.whoppix.net/>.
3. Distributed.net - organizacija za razbijanje kriptogramov s pomočjo porazdeljenega procesiranja, <http://www.distributed.net>.
4. Kopija patenta št. 6,724,893 z dne 20. aprila 2004 za key-escrow sistem, <http://cryptome.org/pat6724893.pdf>).
5. Kopija 4. februarja 2004 izdane sodne odredbe, ki je ameriškemu ponudniku dostopa do interneta Earthlink nalagala namestitev Carnivora, <http://www.epic.org/privacy/carnivore/cd_cal_order.html>.
6. Keyghost - izdelovalec strojnih prestreznikov za prestrezanje signalov tipkovnice, <http://www.keyghost.com>.
7. Spletna stran organizacije Jihad On-line, ki so jo prevzeli ameriški hekerji, <http://www.jihadonline.org/>.
8. Spletna stran podjetja AOL, kjer so bili v začetku avgusta 2006 objavljeni iskalni nizi več kot 650.000 AOL-ovih uporabnikov interneta, <http://research.aol.com>.
9. Spletna stran Centra nevladnih organizacij Slovenije, ki je na internetu objavil osebne podatke udeležencev 2. foruma nevladnih organizacij iz leta 2003, <http://www.cnvos.si/grafi/Zemljevid/Forum%202.doc>.
10. Spletna stran Johnnya Longa, ki se ukvarja z "google hackingom", <http://johnny.ihackstuff.com/index.php>.
11. Kopija razsodbe, s katero je AOL leta 1998 proti Sanfordu Wallacu in njegovemu podjetju Cyber Promotion dosegel sodno prepoved pošiljanja elektronskih sporočil v svoje omrežje, <http://legal.web.aol.com/decisions/dljunk/bigfooto.html>.
12. Zahteva podjetja Sharman Networks po umiku prikaza najdenih zadetkov na iskalniku Google, <http://www.chillingeffects.org/dmca512/notice.cgi?action=image_410>.
13. Katalog zbirk osebnih podatkov na spletnih straneh ministrstva za pravosodje, <http://

www.sigov.si/mp/> (do uveljavitve ZVOP-1) oziroma katalog zbirk osebnih podatkov na spletni strani Informacijskega pooblaščenca, <http://www.ip-rs.si/> (po uveljavitvi ZVOP-1).

14. Kopija odločitve v primeru "United States of America v. Bradford C. Councilman, 385 F.3d 793 (1st Cir. 2004)", <http://www.ca1.uscourts.gov/pdf.opinions/03-1383EB-01A.pdf>.
15. Orkut - sistem za izgradnjo prijateljskih omrežij, <http://www.orkut.com>.
16. Ettercap - program za prestrezanje internetnega prometa v krajevnih omrežjih, <http://ettercap.sourceforge.net/>.
17. Kopija prošnje FBI za izdajo sodnega naloga, za tajni vstop v Scarfov urad in namestitev posebne programske opreme za prestrezanje gesla (naslovljena na okrožno sodišče v New Jerseyju, 8. maja 1999), <http://www2.epic.org/crypto/scarfo/application_5_99.pdf>.
18. Prosojnice predavanja Johnnyja Longa "You found that on Google?" na konferenci Defcon avgusta 2003, <http://www.defcon.org/images/defcon-12/dc-12-presentations/Long/dc-12-long.pdf>.
19. BackTrack - distribucija Linuxa z orodji za odkrivanje in zlorabo varnostnih pomanjkljivosti, <http://www.remote-exploit.org/index.php/BackTrack
20. Orodje "Echelon for Dummies" (objavljeno 31. decembra 1999, avtor Mixter), <http://packetstormsecurity.nl/groups/mixter/>.

STVARNO KAZALO

IMENSKO KAZALO

KAZALO PRAVNIH VIROV

W

KAZALO SLIK

KAZALO TABEL

KAZALO GRAFOV

POVZETEK

V knjigi Nadzor in zasebnost v informacijski družbi je obravnavan problem zasebnosti in nadzora na internetu ter vpliva tehnologije na spreminjanje meje med javnim in zasebnim. Avtor na začetku raziskuje, kdaj je zasebnost sploh nastala kot družbena kategorija in kako se je spreminjala skozi zgodovino. Hannah Arendt namreč ugotavlja, da zasebnost v antiki ni bila dojemana kot polje svobode, temveč kot polje prisile. Vsebina pojma zasebnosti, kot ga poznamo danes, začne nastajati šele v obdobju kapitalizma. Hkrati pa se začenja območje zasebnosti tudi ožiti. V prvi fazi se s področja zasebnosti loči sfera socialnega, zasebno pa se v končni fazi zoži na intimno, a tja skuša družba ravno tako posegati, in sicer z vplivom množičnih medijev ter reklamnih sporočil. Arendtova in Habermas izpostavljata dva vidika zasebnega: osebni prostor, torej prostor intime, ter prostor, ki omogoča interesno združevanje, torej delovanje posameznikov. Zato zasebnost danes ni več "nujno zlo", tako kot je bila v antiki, temveč je postala vrednota, predpogoj posameznikove svobode in emancipacije.

V nadaljevanju je obravnavana problematika nadzorovanja s pomočjo teorij Benthama, Foucaulta ter Deleuzeja. Podobno kot zasebnost tudi nadzorovanje skozi zgodovino doživi spremembe. Zamisel o nadzoru kot sredstvu izvajanja moči nad posamezniki je prvi izpostavi Bentham s svojo zamislijo o zaporu Panoptikon. Zaradi njegovega miselnega preskoka v kaznovanju, preskoka od modela, ki je zapornika izvrgel, v model, kjer je zapornik izpostavljen oblasti, ki gleda, Foucault označuje Benthama za "*enega najpomembnejših inovatorjev na področju tehnologije oblasti*" (Foucault, 1991: 48). Vendar pa se nadzorovanje skozi zgodovino spreminja, saj se poleg disciplinarne oblasti začne razvijati tudi regulacijska. Če je disciplinarna oblast osredotočena na posameznika, na njegovo "dresuro", na podrejanje in discipliniranje, se regulacijska oblast osredotoča na populacijo. Njen namen ni vplivati na konkretnega posameznika, temveč uvesti regulacijske mehanizme za ohranjanje ravnotežja na globalni ravni, in identifikacija tveganja ter priložnosti. Po Foucaultu in Deleuzeju obe vrsti oblasti, disciplinarna in regulacijska, v družbi nadzora delujeta hkrati. Regulacija ne nadomesti discipline, temveč jo nadgradi.

Nadzorovanje je mogoče v dveh smereh: v smeri proti posamezniku ali v smeri proti oblasti. Zamisel o nadzoru oblasti je v leta 1791 objavljenem delu *Of Publicity* razvil Bentham. Čeprav je bila prvotno usmerjena proti netransparentnosti oblasti, pa se pogosto uporablja kot argument proti zasebnosti posameznikov. Prišlo je torej do zaobrnjenega načela transparentnosti, saj so posamezniki, ki želijo zaščititi svojo zasebnost, pogosto soočeni z očitki o skrivanju in s tem o nemoralnosti. "*Biti dober državljan... pomeni biti merljiv in predvidljiv potrošnik*" (Palmer, 2000: 92), ugotavlja Gareth Palmer.

V nadaljevanju se delo posveča pravici do zasebnosti. Temeljni problem pravice do zasebnosti je v tem, da je zelo slabo definirana; poleg tega pravica do zasebnosti pogosto vstopa v kolizijo z drugimi pravicami in interesi. Posledično se zastavlja tudi vprašanje pod- in nadrejenosti posameznih pravic. Poleg vprašanja izvora pravice do zasebnosti so obravnavana tudi vprašanja povezanosti pravice do zasebnosti z nekaterimi drugimi koncepti (npr. s svobodo, avtonomijo,

medčloveškimi vidiki pravice do zasebnosti itd.), v nadaljevanju pa tudi vpliv družbenih in tehnoloških sprememb na njen razvoj.

Ob tem delo primerjalno obravnava tudi razvoj in obseg pravice od zasebnosti v ZDA in v Evropi. Pri tem se pokaže, da ima ameriški sistem varstva pravice do zasebnosti dve temeljni značilnosti, zaradi katerih je zasebnost posameznikov v ZDA v splošnem slabše varovana kot v Evropi. Kljub pomembnemu prispevku, ki ga ima ameriški pravni sistem za razvoj pravice do zasebnosti (uveljavitev načela upravičenega pričakovanja zasebnosti leta 1967), pa je v ZDA na nekaterih področjih še vedno opaziti lastninsko pojmovanje zasebnosti (npr. pri varstvu informacijske zasebnosti v zasebnem sektorju ter pri varstvu zasebnosti na delovnem mestu). Poleg tega v ameriški ustavi zasebnost ni izrecno omenjena in ni priznana kot pozitivna pravica. To hkrati z dejstvom, da prvi amandma k ameriški ustavi[439] vsakomur zagotavlja svobodo govora, pomeni, da ameriški pravni sistem že v temelju postavlja omejitve posameznim zveznim državam, ki želijo npr. regulirati obdelavo osebnih podatkov v zasebnem sektorju. Ta problem je viden zlasti v primeru *US West proti FCC*[440], v katerem je prizivno sodišče presodilo, da so osebni podatki, ki jih zbere podjetje, "*vrsta 'govora' in je zato uporaba potrošnikovih podatkov s strani tretje stranke v poslovnih transakcijah poslovni govor, ki je zaščiten s prvim amandmajem*" (White, 2003: 24).

V četrtem delu je obravnavan razvoj kriptografije kot tehnologije za zaščito zasebnosti. Kriptografija, ki je sicer znana že skoraj 4000 let, se je v preteklosti večinoma uporabljala v vojaške in diplomatske namene. Nastanek javno dostopne kriptografije v 60. letih 20. stoletja pa je uporabo kriptografije vsaj načeloma omogočil vsakomur. Zaradi tega so skušale države – vodilno vlogo pri tem so imele ZDA – raziskovanje, razvoj in uporabo kriptografije sistematično omejevati. To so skušale doseči tako s posrednimi kot tudi neposrednimi pritiski na raziskovalce, s sodelovanjem tajne službe *National Security Agency* pri razvoju in prilagajanju kriptografskih rešitev (npr. vgrajevanje stranskih vrat), pa tudi s poskusi uveljavljanja mednarodnih sporazumov o omejevanju kriptografije za civilne namene. Vsi poskusi so bili večinoma neuspešni, zato so se ZDA lotile drugačne taktike in si skušale zagotoviti možnosti za nadzorovanje kljub prosti uporabi kriptografije. Leta 1994 so v ZDA sprejeli *Communications Assistance for Law Enforcement Act*,[441] s katerim so dosegli, da so izdelovalci telefonskih central začeli v svoje izdelke vgrajevati zmožnosti za nadzorovanje komunikacij. Z drugimi besedami: dosegli so, da je komunikacijska tehologija že v osnovi zasnovana za nadzor. To se nadaljuje tudi pri uporabi internetnih tehnologij, kar dokazuje primer uvedbe sistema za nadzor interneta Carnivore v ZDA leta 2000 in pozneje tudi drugod po svetu.

Poskusi prepovedi in omejevanja kriptografije so sprožili nastanek močnega gibanja za elektronsko zasebnost, katerega člani so razvijali predvsem prosto dostopne kriptografske programe ter anonimizacijske sisteme. Hkrati se je oblikovalo tudi protigibanje, ki je poudarjalo predvsem negativne vidike splošne rabe kriptografije na preiskovanje kaznivih dejanj. Kljub temu

---

[439] 1. amandma, Listina svoboščin (Bill of Rights), 1791.

[440] U.S. West v. F.C.C., 182 F.3d 1224 (1999).

[441] Communications Assistance for Law Enforcement Act (Digital Telephony Act) of 1994, 47 U.S.C. (1994).

da je bilo gibanje za elektronsko zasebnost pri razvoju kriptografskih rešitev navidezno uspešno, pa je uporaba tehnologij, ki posamezniku omogočajo, da se izogne nadzoru na internetu, v praksi omejena. Ostaja zgolj kot možnost, ki pa jo izkoristi le malokdo.

V zadnjem delu je obravnavan problem zasebnosti na internetu. Osnovno vprašanje, ki se zastavlja, je, ali je internet "tehnologija svobode", kot so nekateri verjeli v začetku 90. let 20. stoletja, ali pa je panoptičnost že vgrajena v internet. V iskanju odgovora na to vprašanje avtor navaja številne konkretne primere, ki zadevajo informacijsko, komunikacijsko ter prostorsko zasebnost na internetu. Pri tem analizira tudi poskuse uvajanja nadzora nad internetom v Sloveniji ter predstavi nekatere možne smeri nadzora in zasebnosti na internetu v prihodnosti. Uvedba tehnologij za zaščito intelektualne lastnine, tehnologije t. i. zaupanja vrednega računalništva ("Trusted Computing") in nastanki monopolov ter posledično monokulture na področju operacijskih sistemov za zasebnost na internetu ne prinašajo nič dobrega. Enako velja za družbeni razvoj, predvsem razvoj neposrednega trženja in sodobnih modelov trženja in personalizacije storitev, ki zahtevajo zbiranje velikega števila osebnih podatkov.

Posamezniki postajamo kljub nastanku tehnologij varovanja zasebnosti čedalje bolj transparentni. Tehnologije varovanja zasebnosti nas v praksi sicer ščitijo pred kriminalom, ne pa tudi pred državo (kot so bili v 90. letih 20. stoletja prepričani pripadniki gibanja za elektronsko zasebnost) in družbeno sfero. Tehnologije varovanja zasebnosti ne onemogočajo tehnologij nadzora, njihova uporaba za zaščito medsebojnih komunikacij pa je v praksi zelo omejena. Tehnologije nadzora pa so, nasprotno, zelo razširjene in navadno veljajo za družbeno povsem sprejemljive.

ABSTRACT

The author addresses the problem of privacy and surveillance on the internet and the influence of technology on the changes of the boundary between public and private. The first part examines the question of when privacy emerged as a social category and how it has changed through history. As Hannah Arendt established, privacy in antique has not been perceived as a field of freedom, but rather as a field of coercion. Privacy as we know it today emerged with capitalism but, at the same time, began to diminish. First the sphere of social is separated from the private sphere, then privacy is shrunk to intimacy. But intimacy is not inviolated, it is subject to intervention by the social sphere, by mass media and advertising. Arendt and Habermas pointed out two aspects of the private: personal space - space of intimacy, and space which enables associations of individuals and their action. Therefore privacy today is a value, a precondition of human freedom and emancipation.

The next part examines the problem of surveillance through the theories of Bentham, Foucault and Deleuze. Similar to privacy, surveillance has been subject to changes through history. The idea of surveillance as a means of executing power over individuals was first introduced by Bentham in his work describing the idea of prison Panopticon. His mental leap from the model of punishment, which detached the prisoner to the model where prisoner is exposed to the authority which observes, made Foucault denote him as "*one of the most important inventors in the area of technology of power*" (Foucault, 1991: 48). But surveillance transformed through history, especially when regulatory authority emerged in addition to the disciplinary one. If the disciplinary authority is focused on the individual, his or her "training", coercion and reining, regulatory authority is focused on the population. It does not tempt to influence a specific individual but, rahter, tries to introduce regulatory mechanisms for preserving balance on a global scale and identify risks and opportunities. Foucault and Deleuze established that both authorities, disciplinary and regulatory, act together in the controlled society. Regulation does not replace discipline, it supersctructures it.

Surveillance and control could be directed in two ways: against individual or against authority (government). The idea of the control of the state authority has been introduced in 1791 in Bentham's essay *Of Publicity*. His idea has been directed against non-transparency and secrecy of authority, but today is often used as an argument against privacy of individuals. It came to the conversion of the principle of transparency, and the consequence is that individuals who want to protect their privacy are often faced with allegations of hiding and consecutive immorality. "*To be good citizens ... is to be measurable and predictable consumers*" (Palmer, 2000: 92), is the opinion of Gareth Palmer.

Next the right to privacy is analysed. The main problem of the right to privacy is that it is poorly defined and often collides with other rights and interests. Consequently, there is also a question of which right is superior and which is inferior when this collision emerges. This section also examines the connection of the right to privacy with some other concepts (such as

freedom, autonomy, interpersonal dimension of the right to privacy, etc.), and also the influence of social and technological changes to the development of the right to privacy.

In addition, this work brings forth an analysis of the development and content of the right to privacy in the United States and Europe. It is shown that the U. S. system of privacy protection has two fundamental characteristics whose consequence is that privacy protection of the individual is generally worse than in Europe. Despite the important contribution of the U. S. legal system to the protection of the right to privacy (recognition of reasonable expectation of privacy principle in 1967), privacy in some areas in the United States is still understood as inferior to the property right. This is especially true in case of information privacy and personal data in the private sector and protection of privacy in the workplace. The second characteristic is that privacy is not explicitly mentioned and recognized as a positive right in the U. S. Constitution.[442] The fact that the First Amendment[443] guarantees freedom of speech to everybody means that the American legal system sets some important restrictions to the regulation of personal data processing. This became evident in the case of *US West v. F.C.C.*[444] where Court of Appeals of the Tenth Circuit characterized private information as a sort of a speech, and the use of consumer-related information by third parties in commercial transactions as commercial speech protected by the First Amendment.

The next part of the book focuses on the emergence of the technology for protection of privacy - cryptography. Cryptography has been known for almost 4000 years and in the past has mostly been used for military and diplomatic purposes. But the phenomenon of publicly accessible cryptography in 1960's enabled everyone - at least in theory - to use it. Hence national states, most notably the United States, tried to ban or restrict research, development and use of cryptography. They used different kinds of tactics, including formal and informal pressures on the researchers, "assistance" of *National Security Agency* in the development and adaptation of cryptography products (for example with back doors, etc.) and attempts to enact international agreements to restrict the use of cryptography for civil purposes. All attempts were more or less unsuccessful, which led the USA to attempt to enable surveillance even if cryptography is allowed to be used. In 1994 *Communications Assistance for Law Enforcement Act*/,[445] was enforced, which required that all telecommunications operators use technology that enables government surveillance. In other words - they required that technology should be designed for surveillance. This trend is being continued in the area of internet technologies with the introduction of Carnivore in 2000 in the USA and later in other countries as well.

The attempts to ban or restrict cryptography triggered the formation of a strong movement for electronic privacy, whose members began to develop free cryptographic products and anonymization solutions. At the same, an opponent movement was formed, which mostly emphasized the negative aspects of the free use of cryptography in crime investigations. But

---

442 Constitution of United States of America, 1798.
443 First Amendment , Bill of Rights, 1791.
444 U.S. West v. F.C.C., 182 F.3d 1224 (1999).
445 Communications Assistance for Law Enforcement Act (Digital Telephony Act) of 1994, 47 U.S.C. (1994).

despite the apparent success of the movement for electronic privacy, the use of technologies for enhancing privacy and avoiding surveillance on the internet is limited today. It is merely a possibility that is rarely used.

The last part of this work is dedicated to the problem of privacy on the internet. The main question is whether the internet is a "technology of freedom", as it has been believed in 1990's, or panopticism is already built-in. In search of the answer to this question, several cases concerning information, communication and space privacy on the internet are examined. A part of the analysis is devoted to the introduction of surveillance of the internet in Slovenia and some likely future trends of the development of surveillance and privacy issues on the internet. The development of technologies for intellectual property protection, technology of "Trusted Computing", monopolies and consequent monoculture in the market of computer operating systems, are bad news for privacy on the internet. The same could be said regarding social and economic development, especially the development of direct marketing, modern marketing models and personalisation of services, which all require collecting large amounts of personal data.

Despite the emergence of the technologies of freedom, individuals are becoming more and more transparent. The technologies of freedom in everyday reality protect us against cybercrime, but not against the government (recognised as the main threat by privacy activists in 1990's) and the social sphere. The technologies of freedom do not hinder the technologies of surveillance, and their use for protection of everyday interpersonal communications is limited. On the other hand, the technologies of surveillance are wide-spread and have become socially acceptable.

ZNANSTVENA KNJIŽNICA FDV

1. Tine Hribar, Teorija znanosti in organizacija raziskovanja, 1991
2. Ivan Bernik, Dominacija in konsenz v socialistični družbi, 1992
3. Danica Fink Hafner, Nova družbena gibanja - subjekti politične inovacije, 1992
4. Pavle Gantar, Sociološka kritika teorij planiranja, 1993
5. Bojko Bučar, Mednarodni regionalizem, 1993
6. Helmut Willke, Sistemska teorija razvitih družb, 1993
7. Jan Makarovič, Logika dela, 1993
8. Drago Kos, Racionalnost neformalnih prostorov, 1993
9. Mitja Hafner Fink, Sociološka razsežja razpada Jugoslavije, 1994
10. Marko Lah, Efektivno povpraševanje, 1994
11. Franc Mali, Znanost kot sistemski del družbe, 1994
12. P. Phillips, B. Ferfila, Political Economic System of Canada and Slovenia, 1995
13. Andrej Sušjan, Postkeynesianska ekonomska teorija, 1995
14. Maca Jogan, Sodobne smeri v sociološki teoriji, 1995
15. Vlado Miheljak, Camera obscura psihologije, 1995
16. Dana Mesner-Andolšek, Vpliv kulture na organizacijsko strukturo, 1995
17. Zdravko Mlinar, ur., Osamosvajanje in povezovanje v evropskem prostoru, 1995
18. D. Fink-Hafner, T. Cox, ured., Into Europe? Perspectives from Britain and Slovenia, 1996
19. Janez Štebe, Resnična in navidezna dejstva iz družboslovnih anket, 1996
20. Brina Malnar, Zaznava družbene neenakosti, 1996
21. Alojzija Židan, Metadidaktično poučevanje in učenje družboslovja, 1996
22. Zlatko Jančič, Celostni marketing, 1996
23. Ivan Bernik, Dvojno odčaranje politike, 1997
24. Andrej Škerlep, Komunikacija v družbi, družba v komunikaciji, 1997
25. Adolf Bibič, Politološki preseki, Civilna družba in politični pluralizem, 1997
26. Samo Uhan, Prava in neprava mnenja, Vpliv konteksta v raziskovanju javnega mnenja, 1998
27. Dean Komel, Diagrami bivanja, 1998
28. Dimitrij Rupel, Svoboda proti državi, Osvobodilni in prosti čas, 1998
29. Samo Kropivnik, Slovenski volivci v geografskem, družbenem in ideološkem prostoru, 1998
30. Ida Hojnik Zupanc, Samostojnost starega človeka v družbeno-prostorskem kontekstu, 1999
31. Boštjan Zalar, Privatizacija in človekove pravice, 1999
32. Darko Lubi, Jedrsko širjenje po hladni vojni, 1999
33. Aleksandra Kanjuo-Mrčela, Lastništvo in ekonomska demokracija, 1999

34. Zlatko Šabič, Voting in international organisations: Mere formality or a matter of substance?, 1999
35. Anton Kramberger, Poklici, trg dela in politika, 1999
36. Angelca Ivančič, Izobraževanje in priložnosti na trgu dela, 1999
37. Andrej Rus, Social Capital, Corporate Governance, and Manageria Discretion, 1999
38. Ferfila Bogomil, Lance Leloup: Budgeting, management and Policymaking: A comparative perspective, 1999
39. Niko Toš, Peter Ph. Mohler, Brina Malnar, ured., Modern Society and Values, 1999
40. Srna Mandič, ured., Kakovost življenja, 2000
41. Slavko Kurdija, Družbene identitete in pomen potrošnje, 2000
42. Janko Berlogar, Managerska etika ali Svetost preživetja, 2000
43. Marjan Hočevar, Novi urbani trendi, Prizorišča v mestih - omrežja med mesti, 2000
44. Urban Vehovar, Sodstvo na Slovenskem, Političnosociološki esej o položaju in vlogi sodstva na Slovenskem v času trojnega prehoda, 2001
45. Branko Ilič, Socioekonomska analiza spodbude za inoviranje v podjetju, 2001
46. Maca Jogan, Seksizem v vsakdanjem življenju, 2001
47. Miroljub Ignjatović, Družbene posledice povečanja prožnosti trga delovne sile, 2002
48. Tomo Korošec, ured., Razžalitve v tiskanih medijih, 2002
49. Igor Kotnik-Dvojmoč, Od obvezniške do poklicne vojske, Preoblikovanje oboroženih sil razvitih industrijskih držav, 2002
50. Alenka Krašovec, Oblikovanje javnih politik, 2002
51. Srna Mandič, Maša Filipović, Stanovanjske študije, 2002
52. Stanislav Andolšek, Družbeni odnos kot proces (iz)menjave, 2003
53. Tomaž Krpič, Kognitivno delovanje človeškega telesa, 2004
54. Anja Kopač, Aktivacija – obrat v socialni politiki, 2004
55. Matej Kovačič, Zasebnost in nadzor v informacijski družbi, 2006

Podrobnejša informacija o knjižnih izdajah v okviru programa Znanstvene knjižnice FDV in o izdajah v okviru zbirke Dokumenti SJM je dostopna na http://www.cjm.si/.

Popoln pregled revij, knjižnih zbirk in knjig, ki izhajajo v okviru Založbe FDV je dostopen na http://www.fdv.uni-lj.si/.