*Matej KOVAČIČ**

IZVIRNI ZNANSTVENI ČLANEK

ZASEBNOST V INFORMACIJSKI DRUŽBI

If privacy is outlawed, only outlaws will have privacy.
(Če je zasebnost izven zakona, bodo zasebnost imeli samo tisti, ki so izven zakona.)

Philip R. Zimmerman, PGP(tm) User's Guide, 1994

Povzetek: *Članek obravnava problematiko zasebnosti v moderni informacijski družbi. V kompleksni moderni družbi je potreba po organiziranosti in s tem po zbiranju informacij o posameznikih vsak dan večja, posledica česar je ogroženost zasebnosti.*
Ogroženost zasebnosti se s pojavom moderne informacijsko komunikacijske tehnologije in predvsem interneta še potencira, obenem pa moderno tehnologijo - kriptografijo - lahko uporabimo tudi kot orodje zaščite zasebnosti. Ker pa je kriptografijo moč uporabiti tudi za prikrivanje kriminalnih aktivnosti, se je, večinoma na strani države in njenih represivnih organov, izoblikovala skupina nasprotnikov uporabe lete. Njim nasproti stojijo borci za človekove pravice in svoboščine, ki menijo, da je kriptografija eno temeljnih demokratičnih orodij informacijske družbe. Kljub vsemu pa kaže, da koristi pri uporabi kriptografije prevladujejo nad možnimi negativnimi posledicami. Ali kot bi rekli borci za uporabo kriptografije: če je svoboda govora eno temeljnih načel demokratične družbe, potem je uporaba kritografije njena naravna posledica.
Ključne besede: *zasebnost, kriptografija, informacijska družba.*

Med nadzorovanjem in zasebnostjo

Ena izmed pomembnih značilnosti življenja v modernih družbah je organiziranost. Webster ugotavlja, da je življenje danes mnogo bolj metodično urejeno kot kdajkoli prej, saj naše življenje načrtujejo in uravnavajo različne institucije na mnogotere načine (Webster, 1995: 53).

Večja organiziranost prinaša mnoge prednosti, predvsem predvidljivost in s tem večjo varnost - hkrati pa organiziranost terja tudi svoj davek. Dejstvo namreč

* *Matej Kovačič, mladi raziskovalec na Fakulteti za družbene vede.*

je, da če želimo uspešno uravnavati in načrtovati življenje ljudi (v družbi), moramo o ljudeh imeti ustrezne informacije. Družbena organizacija tako zahteva sistematično zbiranje informacij o ljudeh in njihovih aktivnostih. Webster ugotavlja, da je rutinski nadzor predpogoj uspešne družbene organizacije. "Organizacija in opazovanje sta siamska dvojčka, ki sta zrasla z razvojem modernega sveta", pravi Frank Webster (Webster, 1995: 54). Informacije o ljudeh so pogosto temeljnega pomena za delovanje modernih organizacij, saj mnogokrat služijo kot feedback. Interes za zbiranje, shranjevanje in obdelavo informacij imajo zato različni subjekti, poseben interes na področju nadzora pa (nacionalna) država oz. njena administracija. Ena izmed pomembnih nalog vsake države je zavarovanje njenih meja ter interesov, zato država načrtno zbira informacije o vsem, kar bi utegnilo prizadeti njene nacionalne interese (Webster, 1995: 58 - 64). Ni torej naključje, da so predvsem države in njene vojske razvile sisteme množičnega, rutinskega in nepretrganega nadzora ljudi in njihovih aktivnosti. Webster zato ugotavlja, da je informacijska tehnologija ena izmed ključnih vojaških tehnologij.

Nacionalni interes države pa je lahko ogrožen tudi od znotraj. Država ima zato posebne institucije (policijo, službe državne varnosti), ki spremljajo notranje življenje države. Država torej zbira informacije tako o subjektih zunaj, kot tudi znotraj njenih meja.

Trendi gredo v smer čedalje večjega nadzora, saj se procesi klasifikacije, zbiranja in zapisovanja informacij neprenehoma množijo. Ambicija države je videti in nadzorovati vse. "V moderni državi je nadzor maksimiziran", ugotavlja Giddens (v Webster, 1995: 70). Webster zato ugotavlja, da bi bilo morebiti namesto pojma informacijska družba bolje uporabljati pojem družba nadzora.

Ena izmed pomembnih značilnosti totalitarne države je, da posega na domala vsa področja družbenega udejstvovanja, njeno izhodišče pa je vzpostavitev skupnosti, ki se kot večvredna dobrina dviga nad posameznika in si ga podreja. V totalitarni državi je pomemben "interes skupnosti, nadrobno izdelana propaganda, skrbno nadzorovanje (vseh in vsakogar) in ne nazadnje še sredstva prisile" (Pavčnik v Kušej, Pavčnik, Perenič, 1992: 53).

Po drugi strani pa moderna demokratična družba visoko ceni človekovo individualnost. Ključna sestavina demokratične države so človekove pravice in državljanske svoboščine. Spoznanje, da so temeljne pravice univerzalne in da državne oblasti določajo meje, v katerih se lahko giblje, se je uveljavilo v času razsvetljenstva in meščanskih revolucij, predvsem v času francoske revolucije. Vsebinska sestavina demokracije se zrcali v človekovi emancipaciji (Pavčnik v Kušej, Pavčnik, Perenič, 1992: 50-52). Pogoj za to emancipacijo pa je zasebnost.

Zgodovinske izkušnje kažejo, da sta povečan nadzor in totalitarizem korakala z roko v roki (npr.: nacistična, fašistična in stalinistična država), po drugi strani pa je liberalna demokratična država visoko cenila pravice posameznika - tudi zasebnost - in omejevala nadzor nad posameznikom (Raab, 1997: 161). Stopnjo nadzora državljanov je zato mogoče povezati s stopnjo demokracije v družbi (povezanost je obratno sorazmerna). Charles D. Raab celo trdi, da sta odsotnost nadzorstva in varstvo zasebnosti nujna pogoja za liberalno in participativno demokracijo (Raab, 1997: 161). Nadzor in totalitarizem se torej postavljata nasproti zasebnosti in demokraciji.

Za moderno družbo je torej značilna dihotomna vloga države - sodobna država mora zaradi kompleksnosti sodobnega življenja izvajati nadzor nad državljani, hkrati pa liberalne demokratične vrednote visoko cenijo človekovo zasebnost. Očitno je torej, da mora biti v demokratični družbi doseženo pravo razmerje med stopnjo nadzora in zasebnostjo posameznika.

A zasebnost ni enodimenzionalen pojem. Čebulj navaja tri sestavine zasebnosti: zasebnost v prostoru (možnost posameznika, da je sam), zasebnost osebnosti (svoboda misli, opredelitve, izražanja) ter informacijska zasebnost (možnost posameznika, da obdrži informacije o sebi, ker ne želi, da bi bili z njimi seznanjeni drugi).

Prvi dve sestavini zasebnosti spadata med temeljne človekove pravice in svoboščine in v demokratični družbi nista sporni. Kritična, oz. v informacijski družbi potencialno ogrožena pa je tretja sestavina zasebnosti, ki vključuje tudi varstvo osebnih podatkov. V moderni družbi, ki je "prežeta" z informacijsko in komunikacijsko tehnologijo, je najbolj na udaru ravno informacijska zasebnost. Bistvena sestavina zaščite informacijske zasebnosti je zato kontrola pretoka in posredovanja podatkov, ki se nanašajo na nekega posameznika (Raab, 1997: 158).

Ker država oz. njene institucije potrebujejo informacije za učinkovito uravnavanje življenja posameznikov ter dobro funkcioniranje družbe, jim posameznik zbiranja ne more oz. včasih celo ne sme preprečiti. Je pa zato bistvena transparentnost uporabe osebnih podatkov. Mellors ugotavlja: "Najboljša zaščita ni ta, da oni (op. avt.: država) vedo manj o nas, pač pa da mi vemo več o njih: da vemo, kaj vedo o nas in kako te informacije o nas uporabljajo" (navedba v Raab, 1997: 158).

Pravica do zasebnosti se zato danes opredeljuje kot "pravica posameznika, da zahteva, da se podatki in informacije o njegovih zasebnih razmerjih ne sporočajo komurkoli" (Čebulj, 1992: 7) - to pomeni: tistim, ki za uporabo določene informacije niso pooblaščeni. Takšna je tudi vodilna misel modernih pravnih aktov in načel za zaščito zasebnosti, namreč, da se z večjo transparentnostjo uporabe osebnih podatkov ogroženost informacijske zasebnosti zmanjša. Moderna zakonodaja za zaščito zasebnosti se ukvarja predvsem s tranparentnostjo uporabe osebnih podatkov. Zakonodajalec ščiti posameznikovo informacijsko zasebnost predvsem z uzakonjanjem postopkov za zagotavljanje transparentnosti uporabe posameznikovih osebnih podatkov.

Informacijska zasebnost in informacijsko-komunikacijske tehnologije (IKT)

Država se je vedno trudila zbirati (osebne) podatke o posameznikih, vendar v preteklosti ni bilo na voljo ustrezne tehnologije za procesiranje, klasificiranje in povezovanje podatkov, ne nazadnje pa tudi za avtomatsko (rutinsko) zbiranje leteh. To se je spremenilo z razvojem informacijsko komunikacijske tehnologije (IKT), ki zaznamuje moderno družbo. Čebulj ugotavlja, da je bila zasebnost posameznika sicer ogrožena že pred uvedbo IKT in računalniških zbirk podatkov, da pa je nova tehnologija ogroženost zasebnosti še potencirala in privedla do tega, da

so se ljudje nevarnosti pričeli zavedati bolj kot v času ročno vodenih evidenc (Čebulj, 1992: 16). Sodobna IKT namreč omogoča rutinsko (namensko) pa tudi "naključno" zbiranje, hitro procesiranje, klasificiranje ter povezovanje podatkov.

Iz pravnega vidika za posameznika pomeni največjo nevarnost v zvezi z zbiranjem podatkov nenatančnost, napačnost, nepopolnost ali neažurnost zbranih podatkov (Čebulj, 1997: 8). Vendar je ob tem potrebno imeti v mislih tudi sam način zbiranja podatkov, ki lahko pomeni potencialno grožnjo zasebnosti. Vojske, obveščevalne službe ter policije držav namreč namenjajo ogromne količine denarja za nakup in razvoj sistemov za opazovanje akcij sovražnikov ter odkrivanje potencialnih nevarnosti in sovražnikov (Webster, 1995: 63) - vse v smislu "zaščite nacionalnih interesov". To pomeni, da se nadzor opravlja tudi preventivno, to pa že lahko ogroža svobodo in pravice posameznika. Leta 1994 je v ZDA npr. stopil v veljavo Zakon o digitalni telefoniji, ki od telefonskih družb zahteva, da v svoje telefonske centrale vgradijo "daljinske prisluškovalne priključke" (remote wiretapping port), ki bodo omogočili "prisluškovanje s klikom miške". Konkretno to pomeni, da agentom FBI-ja, ki bodo želeli prisluškovati, ne bo potrebno iti v samo telefonsko centralo, da bi tam priklopili prisluškovalno napravo, pač pa se bodo s pomočjo nove tehnologije na določeno telefonsko linijo priklopili kar izza svoje pisalne mize. Leto kasneje je FBI že objavil svoje načrte, po katerih naj bi od telefonskih družb zahteval, da v svojo infrastrukturo vgradijo naprave, ki bodo omogočale prisluškovanje enemu odstotku telefonskih pogovorov v vseh večjih ameriških mestih. Philip R. Zimmerman v svojem pričanju pred podkomitejem ameriškega Senata 26. junija 1996 o tem pravi takole:

"V prejšnjih letih so (ameriška) sodišča izdala samo okrog 1000 dovoljenj za prisluškovanje na leto. Težko si je predstavljati, kako bo država zaposlila dovolj sodnikov, da bodo izdali dovolj dovoljenj za prisluškovanje enemu odstotku naših telefonskih klicev, še težje pa si je predstavljati, kako bo država zaposlila dovolj agentov, ki bodo sedeli in te pogovore spremljali v realnem času. Edini mogoč način za spremljanje tako obsežnega telefonskega prometa v realnem času je mogočen Orwelovski program z vgrajeno tehnologijo prepoznavanja govora, ki bo med vsemi pogovori iskal zanimive besede ali glas določene osebe. In če država v prvem odstotku telefonskih klicev ne bo našla nič sumljivega, bo začela preiskovati naslednji odstotek, vse dokler cilj ne bo najden, oz. dokler ne bodo preverjeni vsi telefoni."[1]

Preventivno zbiranje podatkov ne predstavlja edinega problema; problem je tudi naključno zbiranje podatkov, ki bi ga lahko na primeru opisali z enim stavkom: "sateliti opazujejo vse, kar "pade" pod njihovo območje" (Webster, 1995: 69). Tak primer so na primer t.i. "sistemi razpoznavanja vozil" (Vehicle Recognition System), kakršen je naprimer Talon, ki ga je leta 1994 razvilo podjetje Racal iz Velike Britanije.[2] Sistem je sicer prvenstveno namenjen nadzoru prometa, vendar je sposoben razpoznati registrsko številko avtomobila in na tak način spremljati, ka-

[1] *Testimony of Phill Zimmerman, http://www.pgp.com/phil/phil-quotes.cgi, 19. januar 1998.*

[2] *STOA: Political control technologies - Summary of Interim Study, http://www.europarl.eu.int/dg4/stoa/en/publi/166499/execsum.htm, 2. februar 1999.*

ko se giblje neko vozilo.[3] Enako velja npr. tudi za kamere v veleblagovnici. Kot ugotavlja STOA (Scientific and Technological Options Assessment of the European Parliament) v svoji začasni študiji o tehnologijah politične kontrole, se je tehnologija vizualnega nadzora v zadnjih letih dramatično spremenila, saj so tovrstne naprave danes že izredno miniaturizirane, poleg tega pa je z moderno tehnologijo, predvsem z novimi algoritmi, mogoče posnetke (na primer demonstrantov) primerjati med sabo, (npr. primerjati osebe na posnetkih demonstracij s tistimi v policijskih kartotekah), shranjevati in povezovati. "Smo na začetku revolucije 'algoritmičnega nadzora' - učinkovite analize podatkov s pomočjo kompleksnih algoritmov, ki omogočajo avtomatsko razpoznavo in sledenje",[4] ugotavljajo avtorji te študije.

Da problem takega zbiranja podatkov dejansko obstaja, priča dejstvo, da je tovrsten sistem, lociran na Trgu nebeškega miru na Kitajskem, sicer namenjen kontroli prometa, leta 1989 kitajska vlada ob znanih študentskih demonstracijah, uporabila za iskanje voditeljev teh demonstracij. Podjetja tovrstne sisteme tudi dobro prodajajo v glavno mesto Tibeta, čeprav le-to nima nikakršnih prometnih problemov.[5]

Podobno je David Burnham leta 1983 opozoril na tako imenovano elektronsko sled, ki jo posamezniki puščajo za sabo. Vsakič, ko posameznik dvigne slušalko, uporabi bankomat ali plačilno kartico, gre na banko, obišče zdravnika, se poroči, rodi ali umre, avtomatski sistemi ali institucije ta dogodek zaznajo in zabeležijo. Elektronska sled je torej informacija, ki se shranjuje rutinsko in kaže na delovanje določenega posameznika.

Zbiranju teh vrst podatkov se danes tako rekoč ni več moč izogniti, saj so nujni za uspešno funkcioniranje zapletenih sistemov, ki nas obdajajo. Večina teh podatkov, Burnham jih je poimenoval tudi transakcijski podatki, se zapisuje in hrani. Tako zbrani podatki so lahko povsem nenevarni, dokler niso povezani. S povezavo in njihovo obdelavo pa lahko pridemo do novih podatkov in informacij s kvaliteto, ki je za posameznika lahko škodljiva ali celo nevarna (Čebulj, 1992: 8).

Problem IKT pa je ravno v tem, da poleg množične obdelave in kombiniranja omogočajo zelo eleganten prenos in povezovanje različnih podatkov. Tako se lahko zgodi, da naključno ali z določenim namenom zbrani podatki postanejo dostopni osebam ali institucijam, ki za njihovo uporabo niso pooblaščene, ali pa ti subjekti podatke začnejo uporabljati za drugačne namene, kot so bili zbrani.

---

[3] *Kanadsko Ministrstvo za promet uporablja podoben sistem: po celotnem območju avtoceste "Highway 401" so postavljene kamere za opazovanje prometnih razmer na tej avtocesti. Na njihovi spletni strani na internetu je dostopen zemljevid z vrisanimi lokacijami kamer, obiskovalec te spletne strani pa si lahko s klikanjem po tem interaktivnem zemljevidu ogleduje slike, ki jih posredujejo kamere nameščene po tej avtocesti. Na tak način je mogoče slediti gibanju nekega vozila po tej avtocesti. Spletna stran se nahaja na: http://www.mto.gov.on.ca/english/traveller/compass/camera/cammain.htm.*

[4] *STOA: Political control technologies - Summary of Interim Study, http://www.europarl.eu.int/dg4/stoa/en/publi/166499/execsum.htm, 2. februar 1999.*

[5] *STOA: Political control technologies - Summary of Interim Study, http://www.europarl.eu.int/dg4/stoa/en/publi/166499/execsum.htm, 2. februar 1999.*

Iz teh razlogov upravičeno obstaja bojazen, da imajo morda različne državne institucije dostop do podatkov zbranih za druge namene, poleg tega pa različne baze med seboj nepovezanih podatkov s pomočjo identifikacijskih oznak (v Sloveniji je to EMŠO (Enotna Matična Številka Občana), v ZDA pa Social Security Number) med seboj povezujejo in tako informacije med seboj kombinirajo (Webster, 1995: 68 ter Raab, 1993: 89).

Specifika problema zasebnosti na internetu

Organizacija Privacy Rights Clearinghouse ugotavlja, da "pravzaprav ne obstaja nobena on-line aktivnost, ki bi omogočila popolno zasebnost".[6] Da so baze osebnih podatkov - tudi o tem kaj posamezniki počnejo na internetu - čedalje bolj javno dostopne, ugotavljata tudi Allard in Kass (Allard in Kass, 1997: 572). V nadaljevanju si bomo ogledali nekaj primerov zbiranja (osebnih) podatkov na internetu.

Vsak uporabnik ima možnost, da na internetu postavi svojo predstavitveno stran. Ljudje na predstavitveni strani navadno objavljajo svoje osebne podatke, vendar se pri tem pogosto ne zavedajo, da je z današnjo IKT mogoče vse (na internetu) javno objavljene podatke elegantno avtomatsko zbrati in povezati. 6. oktobra 1997 je tako v Sloveniji pričel delovati Imenik elektronske pošte Slovenije (http://afna.telekom.si). Telekom Slovenije je v imeniku zbral 15.000 elektronskih naslovov, ki so že bili javno objavljeni na spletnih straneh slovenskega interneta. Poleg tega, da so podatki zbrani na enem mestu, so tudi lepo katalogizirani (strežnik Afna omogoča iskanje med podatki po različnih kiterijih), kar je tipičen primer obdelave podatkov, ki le-tem vnese novo kakovost.

Čeprav je tako zbiranje na prvi pogled nenevarno, pa se bo slovenski uporabnik interneta te nevarnosti zavedel najkasneje takrat, ko bo njegove podatke zbrala spretna marketinška agencija in mu v njegov elektronski predal pričela pošiljati reklamna sporočila oz. tako imenovani "junk mail" (pošto z elektronskimi "smetmi"). Nekaj podobnega se je zgodilo 18. januarja 1999, ko je anonimni posameznik, podpisan kot Vojaški Obveznik, na nekaj več kot 48.000 e-mail naslovov poslal odprto protestno pismo.

To pa ni edini možni način zbiranja podatov o uporabnikih interneta. Mnoge spletne strani na internetu namreč od uporabnikov v zameno za nekaj - informacije ali določene ugodnosti - zahtevajo osebne podatke. Na straneh, kjer se ti podatki zbirajo večinoma, ne piše oz. ni razvidno, v katere namene bodo tako zbrani podatki uporabljeni (večinoma marketinške).

15. decembra 1997 je ameriška Federal Trade Commision objavila rezultate raziskave Kids Privacy Surf Day (Dan zasebnosti otrok pri surfanju po internetu). V raziskavi so analizirali 126 med otroci najbolj popularnih spletnih strežnikov. Raziskovalci so ugotovili, da je približno 86 odstotkov strežnikov od otrok zbiralo osebne podatke (imena, naslove, telefonske številke, e-mail naslove), ob tem pa je bilo na manj kot 30 odstotkih teh strežnikov (ki so zbirali osebne podatke) objav-

[6] *Privacy in Cyberspace, http://www.privacyrights.org/fs/fs18-cyb.html, 19. januar 1998.*

ljeno opozorilo o zasebnosti, oz. za kakšen namen bodo zbrani podatki uporabljeni. Zaskbljujoče je tudi dejstvo, da je manj kot 4 odstotke strežnikov, ki so podatke zbirali, zahtevalo, da zbrane podatke avtorizirajo starši. Raziskava je pokazala, da je zasebnost otrok na internetu slabo varovana, raziskovalci pa so sklenili, da je potrebno na področju varovanja zasebnosti otrok na internetu še mnogo storiti.[7]

Elektronski kolački so majhni paketi podatkov, ki jih spletni strežnik pošlje spletnemu brskalniku, le-ta pa te podatke shrani na uporabnikov računalnik in jih vrne strežniku, ko ta to od njega zahteva. Strežnik lahko nastavi rok veljavnosti elektronskega kolačka in kdo ima dostop do njega. Elektronski kolaček navadno vsebuje interno identifikacijsko številko uporabnika; na elektronske kolačke lahko gledamo kot na bazo podatkov, ki je razpršena po računalnikih obiskovalcev spletne strani. Na ta način spletni strežnik ob naslednjem obisku uporabnika lahko ugotovi, ali je uporabnik na spletni strani že bil in kaj je na njej počel (na tak način delujejo elektronske trgovine).

Vendar pa nekateri strežniki elektronske kolačke uporabljajo za sledenje uporabnikov iz enega spletnega strežnika na drugega, lahko pa tudi razkrijejo identiteto uporabnika.

Na internetu namreč obstajajo podjetja, ki preprodajajo oglasni prostor znanih spletnih strani. Primer takega podjetja je DoubleClick. Ko uporabnik obišče npr. neko erotično spletno stran na internetu, oglas, ki se prikaže na tej spletni strani prihaja iz strežnika DoubleClick, hkrati z oglasom pa DoubleClick uporabniku pošlje tudi elektronski kolaček. Na ta način si strežnik podjetja DoubleClick zapomni, da je uporabnik z interno identifikacijsko številko, ki je zapisana v elektronskem kolačku, obiskal določeno erotično spletno stran. Ko ta uporabnik čez nekaj časa obišče npr. prodajalno CDjev CDNow DoubleClick, prek oglasa na tej spletni strani ugotovi, da je uporabnik pred tem obiskal erotično spletno stran in pošlje oglas z erotično vsebino. Ker je DoubleClick prisoten na mnogih spletnih straneh, lahko to podjetje uporabnika sledi, kako potuje po različnih straneh (elektronski kolački so bili prvotno sicer namenjeni sledenju gibanja uporabnika samo znotraj ene spletne strani).

To pa ni vse. Če uporabnik na kateri izmed spletnih strani, kjer je prisoten tudi DoubleClick, vtipka svoj elektronski naslov (ali druge podatke) in jih DoubleClick dobi, lahko njihovi analitiki povežejo uporabnikov elektronski naslov z njegovimi "brskalnimi navadami" (obiskovanjem spletnih strani). Dovolj je, da uporabnik svoje podatke vpiše samo enkrat. V začetku leta 2000 je časnik USA Today razkril, da DoubleClick zbira imena uporabnikov in skuša elektronske kolačke povezati tudi z identiteto uporabnikov v resničnem življenju (t.i. off-line identiteta).[8]

Nekateri strežniki pa celo pošiljajo reklamna elektronska sporočila z naslovom neke spletne strani (ali pa samo slike na spletni strani) in ko uporabnik obišče to povezavo, spletni strežnik poveže uporabnikov elektronskii naslov z elektronskim kolačkom. Tudi ta način je bil že uporabljen za sledenje obiskovalcev spletnih strani.

[7] *Kids Surf Day, http://www.ftc.gov/opa/9712/kids.htm, 19. januar 1998.*

[8] *Crypto-Gram, http://www.counterpane.com, 15. februar 2000.*

Naslednja stvar, s katero običajni uporabnik večinoma ni seznanjen, so tako imenovane datoteke aktivnosti (log files). Datoteke aktivnosti so posebne datoteke, kamor računalnik avtomatsko vpisuje aktivnosti uporabnikov. Konkretno to pomeni, da se vse aktivnosti posameznega uporabnika interneta (kdaj je prebral elektronsko pošto, katere spletne strani je obiskal in kdaj itd.) avtomatsko zapisujejo na strežniku uporabnikovega ponudnika dostopa do interneta (nekatere informacije pa zabeleži tudi spletni strežnik, ki ga uporabnik obišče). Dostop do teh elektronskih sledi, ki jih za seboj pušča uporabnik, ima vsaj upravitelj sistema, poleg njega pa verjetno še kdo. Te informacije so ob ustrezni statistični obdelavi marketinško zanimive in člani organizacije Privacy Rights Clearinghouse zato ugotavljajo, da se zbiranje tovrstnih informacij, predvsem informacij o obisku spletnih strani, povečuje.[9]

Tretja, in verjetno največja nevarnost je povezana s tajnostjo posameznikove elektronske pošte oz. elektronskih sporočil nasploh. Zimmerman ugotavlja, da je danes elektronska sporočila mogoče povsem enostavno prestreči ter v njih iskati določene (zanimive) besede. Današnja tehnologija omogoča, da je to narejeno "enostavno, rutinsko, avtomatsko in neopazno ter v velikem obsegu".[10] To lahko storijo posamezniki ali institucije, povsem enostavno pa je to za upravitelja internetnega strežnika, ki ima do elektronske pošte svojih uporabnikov načeloma povsem prost dostop, čeprav v večini držav velja načelo pisemske tajnosti. V ZDA je tako z zakonom Electronic Communications Privacy Act sicer prepovedano branje vsebine elektronskih sporočil, namenjenih nekomu drugemu, vendar pa obstajajo določene izjeme. Uporabnikovo elektronsko pošto lahko bere upravitelj sistema, ki sumi, da pošiljatelj načrtuje napad na sistem ali namerava škoditi drugim uporabnikom. Prav tako lahko delodajalec spremlja elektronsko pošto svojih uslužbencev - seveda v primeru, da uporabljajo poštni predal podjetja.[11]

Organizacija Privacy Rights Clearinghouse ugotavlja, da vse to pomeni grožnjo on-line zasebnosti.[12] Da bi morala biti zasebnost na internetu bolje zakonsko varovana, se strinja tudi mnogo uporabnikov interneta. GVU raziskovalni center (Graphics, Visualization & Usability Research Center) iz Atlante je v času od 10. oktobra do 16. novembra 1997 opravil (osmo) raziskavo med uporabniki interneta. Anketa je pokazala, da velika večina anketiranih uporabnikov interneta (72 %) meni, da bi morali obstajati novi zakoni, ki bi varovali zasebnost na internetu. Se pa večina uporabnikov (63 %) ne strinja s tem, da naj bi ponudniki dostopa do interneta smeli prodajati informacije o uporabnikih interneta tretjim osebam.[13] Podobnega mnenja so tudi slovenski uporabniki interneta: kar 47,7% se jih popolnoma strinja s trditvijo, da so zakoni za zaščito zasebnosti na internetu potrebni, povprečno strinjanje na lestvici od 1 do 5 pa je slabih 3,7.[14] Podatki iz slovenske raziskave ISPO'99, ki je bila narejena v okviru projekta Raba interneta v Sloveniji (RIS) leta 1999

[9] *Privacy in Cyberspace, http://www.privacyrights. org/fs/fs18-cyb.html, 19. januar 1998.*

[10] *Testimony of Phill Zimmerman, http://www.pgp.com/phil/phil-quotes.cgi, 19. januar 1998.*

[11] *Privacy in Cyberspace, http://www. privacyrights.org/fs/fs18-cyb.html, 19. januar 1998.*

[12] *Privacy in Cyberspace, http://www.privacyrights.org /fs/fs18-cyb.html, 19. januar 1998.*

[13] *GVU 8th WWW Survey, http://www.gvu.gatech.edu/user_surveys/survey-1997-10/, 19. januar 1998.*

[14] *Raziskava RIS '98, http://www.ris.org/rezultati/10.htm, 4. februar 1999.*

kažejo, da je nezaupanje v varnost eden glavnih razlogov za nezanimanje za elektronsko nakupovanje, isti razlog pa je na tretjem mestu po nerazlogih za uporabo bančnega poslovanja prek interneta (takoj po nepoznavanju in nerazmišljanju o tem). Uporabniki interneta torej čutijo, da je problem zasebnosti na internetu še kako pomemben.

Kriptografija kot orodje za zaščito elektronskih komunikacij

Kljub zakonodaji, ki ščiti zasebnost, je le-ta še vedno ogrožena, kar očitno čutijo tudi uporabniki elektronskih komunikacij. Korak naprej v zaščiti zasebnosti pomeni javno dostopna kriptografija.

Z besedo kriptografija označujemo metode za zaščito pred nepooblaščeno uporabo podatkov. Sporočilo zakrijemo z enkripcijsko metodo in enkripcijskim ključem in dobimo kriptogram, ki ga lahko pošljemo naslovniku. Naslovnik nato kriptogram s pomočjo dekripcijske metode in dekripcijskega ključa predela v izvorno obliko sporočila (Vidmar, 1997: 162 - 164).

Z vidika enkripcijskega in dekripcijskega ključa poznamo dve vrsti kriptografije: simetrično, ki za kodiranje in dekodiranje sporočila uporablja isti ključ (isto geslo), ter nesimetrično, kjer je ključ za kodiranje različen od ključa za dekodiranje.

Matematiki in računalničarji so razvili kar precej kodirnih algoritmov, leta 1978 pa so na Massachusetts Institute of Technology razvili kodirni algoritem RSA, ki omogoča praktično nezlomljivo kriptografijo, kar pomeni, da so podatki, zaščiteni s to kriptografsko metodo, izjemno varni (Vidmar, 1997: 181).

Metoda RSA namreč deluje tako, da imata tako tisti, ki sporočilo pošilja, kot tisti, ki sporočilo sprejema, vsak svoj par ključev. Zasebnega, ki je tajen, in javnega, ki je javno dostopen. Ključa sta med seboj povezana v posebnem matematičnem razmerju, ki omogoča, da oseba, ki sporočilo pošilja, le-to zakodira s svojim tajnim in naslovnikovim javnim ključem, tako zakodirano sporočilo pa lahko odkodira samo naslovnik, in sicer s svojim zasebnim in pošiljateljevim javnim ključem.

Čar RSA kriptografije je tako v tem, da ne potrebuje t.i. "varnih kanalov" za prenos ključev, saj so javni ključi lahko (oz. morajo biti) javno objavljeni, zasebne ključe pa posamezniki seveda obdržijo zase (v tajnosti). Za pošiljanje kodiranega sporočila torej potrebujemo samo naslovnikov javni ključ (svoj zasebni ključ že imamo), naslovnik pa potrebuje samo pošiljateljev javni ključ (svojega zasebnega že ima). Tak sistem kodiranja omogoča tudi verifikacijo pošiljatelja oz. t.i. "elektronski podpis".

Junija leta 1991 je Phil Zimmerman napisal program PGP (Pretty Good Privacy), ki vsebuje RSA algoritem za kodiranje sporočil na osebnih računalnikih. Razlog, zakaj je Phil Zimmerman napisal program PGP, je bil v tem, da je RSA kodirni algoritem, za razliko od ostalih do tedaj znanih algoritmov praktično onemogočal prisluškovanje (elektronskim) komunikacijam posameznika. S

splošno uporabo RSA kriptografije bi nadzorovanje elektronskih komunikacij, tako s strani posameznikov kot tudi države, postalo nemogoče. Ker Zimmerman meni, da sta demokracija in zaščita zasebnosti neločljivo povezani, "edini način za zaščito zasebnosti pa je močna kriptografija",[15] je sklenil, da mora omenjena tehnologija pripadati vsem ljudem.[16]

Istega leta, ko je Zimmerman napisal program PGP, je ameriški Senat obravnaval zakon, ki bi prepovedal tovrstno kriptografijo. Zimmerman je zato svoj program javno objavil in dovolil brezplačno kopiranje (tim. freeware program), neznanci pa so njegov program razširili po vsem svetu.[17] Program je v dveh letih postal de facto standard za učinkovito zaščito podatkov in elektronske pošte.[18]

Dve leti kasneje, natančneje februarja 1993, pa so na njegova vrata potrkali agenti FBI zaradi suma, da je omogočil nezakonit izvoz vojaške tehnologije.[19]

Napori za prepoved učinkovite kriptografije

Učinkovitost države izhaja iz dejstva, da ima država monopol nad sredstvi fizičnega prisiljevanja, ki jih uporablja zato, da ljudi prisiljuje k določenemu ravnanju (Perenič v Kušej, Pavčnik, Perenič, 1992: 29). Vendar pa si država prizadeva tudi za monopol nad poseganjem v zasebno sfero posameznika, kar opravičuje z nacionalnimi interesi. Zato so si države vedno prizadevale za nadzor nad kriptografijo (Bert-Jaap Koops, 1997).

Ni torej presenetljivo, da je odkritje učinkovite kriptografije v ameriški državni administraciji, predvsem med njenimi t.i. represivnimi organi (vojska, zvezna policija), sprožilo preplah. Do odkritja RSA je bilo namreč večino kriptografskih metod mogoče zlomiti,[20] de facto monopol nad razvojem novih kriptografskih metod pa je imela vojska, dostop do kriptografije pa so imeli poleg njih še akademiki. Z razvojem IKT, ki je omogočil nastanek in javno objavo PGP, pa se je to spremenilo. Ker je bil državni de facto monopol na področju kriptografije odpravljen, ga je država (ZDA) poizkusila vsiliti de iure. Z zakonom torej.

Vodilno vlogo pri naporih za prepoved ali vsaj omejevanje kriptografije v ZDA ima v zadnjih letih FBI (Federal Bureau of Investigation - zvezna ameriška polici-

[15] *Testimony of Phil Zimmerman, http://www.pgp.com/phil/phil-quotes.cgi, 19. januar 1998.*

[16] *Testimony of Phil Zimmerman, http://www.pgp.com/phil/phil-quotes.cgi, 19. januar 1998.*

[17] *InfoNation, The Phil Zimmerman Case, http://www.info-nation.com/philzima.html, 19. januar 1998.*

[18] *Testimony of Phil Zimmerman, http://www.pgp.com/phil/phil-quotes.cgi, 19. januar 1998.*

[19] *InfoNation, The Phil Zimmerman Case, http://www.info-nation.com/philzima.html, 19. januar 1998.*

[20] *Trenutno je najbolj razširjen kodirni algoritem DES (Data Encription Standard), ki se uporablja tudi v bancništvu. Vendar pa je DES izpeljanka enkripcijskega algoritma, ki ga uporablja ameriška vojska. Ker teoretično ozadje algoritma ni povsem pojasnjeno, obstaja sum, da vojska pozna bližnjico za razbijanje civilne različice DES-a (Vidmar, 1997: 179). Leta 1993 pa je Michael Wiener na konferenci o kriptografiji predstavil poseben čip, ki ga je razvil za razbijanje DES-a. Čip je leta 1993 stal 10 dolarjev in pol in Phil Zimmerman je izračunal, da bi za 100 milijonov dolarjev čipov - seveda povezanih med sabo - 65-bitni DES lahko razbili v 2 minutah. Zimmerman tudi ugotavlja, da lahko NSA s svojim proračunom DES razbije v sekundi. (Testimony of Phill Zimerman, http://www.pgp.com/phil/phil-quotes.cgi, 19. januar 1998.).*

ja), ki v zvezi s tem ciljem tesno sodeluje z NSA (National Security Agency - Nacionalna varnostna agencija).[21]

V ZDA imajo kriptografijo namreč za vojaško tehnologijo[22], izvoz take tehnologije pa je mogoč samo z dovoljenjem. Agenti FBI so zaradi suma, da je Zimmerman omogočil izvoz vojaške tehnologije, proti njemu uvedli preiskavo, ki je trajala kar dve leti. Januarja 1996 je bila preiskava ustavljena in sicer brez obtožbe, saj proti njemu niso našli dokazov za osumljeno kaznivo dejanje. Je pa ostal grenak priokus, da je šlo v Zimmermanovem primeru za poizkus zastraševanja. Danes je tako v ZDA mogoče uporabljati katerekoli kriptografske programe, vendar pa jih ni dovoljeno izvažati v tujino. Kljub temu si ZDA še vedno prizadevajo omejiti uporabo popolnoma varne kriptografije tudi doma. Zagovorniki omejevanja kriptografije ter ameriška administracija so v ta namen podali vrsto predlogov.

Uvedbo kriptografije z "zakonito avtorizacijo gesel" (key escrow) oz. vgrajenimi "stranskimi vrati". Že leta 1991 je predlog zakona Senate Bill 266 vseboval predlog, ki bi, če bi postal zakon, prisilil proizvajalce, da v svoje produkte vgradijo tim. stranska vrata (trap doors), da bi vlada lahko brala kodirana sporočila od kogarkoli. Leta 1993 je ameriška vlada objavila predlog tim. "key escrow" sistema. Omenjeni sistem vsebuje močno in varno kriptografijo, vendar pa morajo posamezniki svoje ključe "avtorizirati" pri za to pooblaščeni agenciji. Konkretno to pomeni, da uporabniki kopije svojih gesel shranijo pri neki tretji zaupanja vredni stranki, preiskovalni organi države pa imajo s tem - seveda na podlagi odredbe sodišča - omogočen dostop do teh gesel. ZDA so na podlagi te metode razvile kodirnik Clipper (za zaščito glasovnih komunikacij) ter Capstone za zaščito elektronskih podatkov.[23]

Kriptografski algoritem, uporabljen v Clipperju in Capstonu, se imenuje Skipjack, razvila pa ga je NSA in to kljub temu, da je leta 1987 ameriški Kongres z zakonom Computer Security Act poizkušal omejiti vlogo te agencije pri razvijanju standardov za civilne komunikacijske sisteme.[24]

Postavljanje kriptografskih standardov. Osnovna ideja tega pristopa je, da naj bi država (ZDA) računalniškemu trgu vsilila take kriptografske standarde, ki bi omogočali vladi dostop do kodiranih podatkov. Eden izmed takih standardov je npr. "key escrow". Ostali kriptografski pripomočki, ki tem standardom ne bodo ustrezali, ne bodo dobili licence, in kljub temu, da se bodo sicer verjetno še vedno razširjali po internetu, bo njihova uporaba zaradi nezdružljivosti z licenciranimi produkti omejena. S tem bi dosegli, da bi bili taki izdelki manj razširjeni (Denning, 1997: 188).

Uporaba šibke kriptografije. Šibka kriptografija omogoča, da ustrezna vladna agencija z dovolj zmogljivimi računalniki v nujnih primerih (npr. ugrabitvah) hitro razbije zaščito, zato avtorizacija gesel ni potrebna (Denning, 1997: 184). Problem je v tem, da šibka kriptografija uporabniku ne nudi ustrezne zaščite, saj lahko kripto-

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

[23] Denning, 1997: 180 - 181 ter The Clipper Chip, http://www.epic.org/crypto/clipper/, 19. januar 1998.

[24] The Clipper Chip, http://www.epic.org/crypto/clipper/, 19. januar 1998.

[21] Efforts to ban encryption, http://www.epic.org/crypto/ban/, 19. januar 1998.

gram zlomi vsakdo, ki ima malo bolj zmogljiv računalnik in ustrezno računalniško znanje.

Uporaba kriptografije znotraj zaprtih sistemov oz. uporaba "mrežne kriptografije". S terminom "mrežna kriptografija" (link encription) označujemo skupek metod, ki podatke kriptirajo samo znotraj nekega zaprtega sistema, ko pa podatki pridejo izven tega sistema, niso več zaščiteni. Primer takega sistema je npr. sistem GSM mobilne telefonije: podatki, ki se prenašajo preko radijskih povezav (od uporabnika do GSM centrale), so kodirani, ko pa podatki zapustijo centralo, niso več kodirani. Policija lahko prisluškuje pogovorom tako, da prisluškovalne naprave nastavi na izhodu iz centrale (Denning, 1997: 184).

Licenčno in zakonsko omejevanje. Država naj bi dovolila patentiranje kriptografskih metod, ne pa tudi njihove uporabe, če ne bi ustrezali postavljenim standardom. Konkretno to pomeni, da bi država prepovedala uporabo določenih kriptografskih metod (takih, ki bi ji onemogočale vpogled v kriptirane podatke). Posamezniki bi sicer še vedno lahko razvijali svoje lastne kriptografske metode, vendar samo za osebno uporabo in izobraževanje, brez dovoljenja pa jih ne bi smeli prosto razširjati (Denning, 1997: 187 - 188).

Da bi ne prihajalo do zlorab kriptografije s strani kriminalcev, so se pojavili tudi predlogi za **višje kazni ob uporabi kriptografije pri izvrševanju kaznivih dejanj.** V primeru, da bi si posameznik pri izvršitvi kaznivega dejanja pomagal s kriptografijo, naj bi se mu kazen podvojila.[25]

Strah pred kripto anarhijo

V ozadju naporov države za omejevanje kriptografije tiči predvsem strah pred tem, da bi država ne mogla več nadzorovati kriminala oz. sovražnih aktivnosti. V zvezi s tem se je izoblikoval izraz kripto anarhija.

V kripto anarhiji naj bi država, kot jo poznamo danes (nacionalna država torej), izginila, namesto nje pa naj bi se oblikovale virtualne skupnosti posameznikov, ki bi počele, kar bi hotele (Denning, 1997: 175). Napovedovalci kripto anarhije se strinjajo, da bi bila kripto anarhija neizogibna posledica širitve javno dostopne kriptografije. "Zaradi te tehnologije (kriptografije, m. op.) država ne bo mogla več nadzorovati informacij, sestavljati dosjejev, prisluškovati, regulirati 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), kar pa vodi v družbeni nered. Kriptografija naj bi bila torej uperjena predvsem proti državi,[26] s tem pa posredno tudi proti državljanom.

Gibanje za elektronsko zasebnost

Poizkusi ameriške vlade, da bi kriminalizirala kriptografijo, so na internetu sprožili močno gibanje, ki se zavzema za zaščito elektronske zasebnosti, predvsem

[25] *Omenjeni predlog za podvojitev kazni je bil dan v ameriškem trgovinskem parlamentarnem odboru, vir: http://epic.org/crypto/, 19. januar 1998.*

[26] *Denning, 1997: 187 ter Phill Zimmerman: PGP(tm) User's Guide, 1994*

pa za razširjanje uporabe kriptografije. Na internetu, pa tudi v realnem življenju se je oblikovala vrsta organizacij, ki se ukvarjajo z zaščito zasebnosti in pravicami posameznika. Člani teh organizacij z javnim pritiskom (podpisovanje peticij, pričanja pred ameriškim Kongresom, pritiski medijev) skrbijo za spoštovanje posameznikove zasebnosti in onemogočajo poizkuse prepovedi in omejevanja kriptografije. Prav tako si prizadevajo za odpravo prepovedi izvoza kriptografije iz ZDA.

Na vprašanje "Zakaj zasebnost?" Phil Zimmerman (eden najvidnejših borcev za neomejeno uporabo kriptografije ter član in ustanovitelj mnogih organizacij in gibanj za elektronsko zasebnost) slikovito odgovarja takole:

"Ker je osebno. Ker je zasebno. In ne briga nikogar drugega razen vas. Morda načrtujete politično kampanjo, se pogovarjate o svoji davčni napovedi ali počnete kaj nezakonitega. Ali pa počnete kaj, za kar mislite, da bi moralo biti zakonito, pa ni. Karkoli že je: ne želite, da bi vašo zasebno elektronsko pošto ali zaupne dokumente prebral nekdo drug. Nič ni narobe, če branite svojo zasebnost. Zasebnost je ustavna kategorija.

Morda mislite, da je vaša elektronska pošta ne vsebuje nič nezakonitega in da je enkripcija zato nepotrebna. Če ste resnično državljan, ki spoštuje zakone in nima ničesar skrivati - zakaj potem svojih pisem ne napišete na dopisnico? Zakaj se takoj, ko država od vas to zahteva, ne podvržete testom ugotavljanja uživanja mamil? Zakaj zahtevate odredbo sodišča, če želi policija preiskati vašo hišo? Ali poizkušate kaj skriti? Gotovo ste prevratniški trgovec z drogo, če svojo pošto skrijete v kuverto. Ali pa mogoče paranoičen norec. Ali navadni državljani, ki spoštujejo zakone, potrebujejo zaščito za svoje elektronske komunikacije?" [27]

Po mnenju organizacij za elektronsko zasebnost bomo v prihodnosti za medsebojno komuniciranje uporabljali predvsem elektronske komunikacije. Le-te pa je lahko neopazno in v velikem obsegu nadzorovati. Kriptografija je po njihovem mnenju torej instrument, ki zagotavlja zasebnost. Pravico do uporabe kriptografije te organizacije enačijo s pravico do zasebnosti.

Seveda je vsem jasno, da kriptografijo lahko zlorabijo tudi kriminalci. Vendar so prepričani, da bo z zavarovanjem zasebnosti skupni rezultat kljub temu pozitiven.[28]

Nasprotja med nasprotniki in zagovorniki kriptografije izvirajo iz njihovega različnega razumevanja vloge države. Medtem ko nasprotniki kriptografije državo vidijo kot "dobrega čuvaja", ki skrbi za varnost in blaginjo svojih državljanov, jo zagovorniki vidijo kot institucijo, ki posega v njihove pravice in svoboščine.[29] Phil Zimmerman, ki je bil zaradi svojega zavzemanja za javno dostopno kriptografijo leta 1995 razglašen za eno izmed petdesetih najbolj vplivnih oseb na internetu, državo vidi takole:

[27] *Testimony of Phil Zimmerman, http://www.pgp.com/phil/phil-quotes.cgi, 19. januar 1998.*

[28] *Testimony of Phil Zimmerman, http://www.pgp.com/phil/phil-quotes.cgi, 19. januar 1998.*

[29] *"Česar se, kot kaže, vlada resnično boji pri Zimmermanovem programu ni Precej Dobra Zasebnost (Pretty Good Privacy) - ime Zimmermanovega programa (m. op.)), pač pa zasebnost kot taka. The Zimmerman Case v The Ethical Spectacle, julij 1995, http://www.spectacle.org/795/zimm.html, 19. januar 1998.)*

"FBI-jev program COINTELPRO je zadeval skupine, ki so nasprotovale vladni politiki. Prisluškovali so Martinu Luthru Kingu. Nixon je imel spisek svojih sovražnikov. In potem je bila afera Watergate... ...Če ne bomo storili nič, bodo nove tehnologije dale državi moč nadzora, o kakršni je Stalin lahko samo sanjal... ...Nekateri Američani ne razumejo moje zaskrbljenosti v zvezi z močjo vlade. Toda če govorite z ljudmi iz Vzhodne Evrope, jim tega ni potrebno razlagati. Oni to že razumejo in ni jim jasno, zakaj tega ne razumemo tudi mi."[30]

Člani gibanj za elektronsko zasebnost so prepričani, da bo napačna oz. napačno uporabljena tehnologija lahko omogočila vladi nadzorovati vsakogar, ki ji bi utegnil nasprotovati. Ker so prepričani, da bi bila to zadnja vlada, ki bi bila izvoljena po demokratični poti, so mnenja, da državi določenih tehnologij (nadzora) ne bi smeli dovoliti uporabljati oz. da bi morala biti vsakomur omogočena uporaba dobre kriptografije.[31]

Zaključek

Kljub nevarnostim, ki jih kriptografija prinaša, da bi dobra kriptografija vseeno morala biti javno dostopna in ne bi smela biti samo v domeni države. Bolj konkretno: ker glavni razvoj na področju kriptografije poteka v ZDA in ker se ravno ZDA trudijo omejiti izvoz in uporabo kvalitetnih kriptografskih metod, nad uporabo kriptografije ne bi smele imeti patronata Združene države.

"Key escrow sistem" oz "sistem zakonite avtorizacije gesel", ki ga v zadnjem času poizkušajo ZDA vsiliti kot svetovni standard, namreč predvideva, da bodo posamezniki svoja gesla shranili pri neki tretji zaupanja vredni stranki, država pa bo imela dostop do gesel (na podlagi sodnega naloga). "Key escrow" sistem kriptografije bo mogoče tudi izvoziti iz ZDA, vendar se bodo kopije ključev shranjevale v ZDA ali v državah, ki bodo imele z ZDA ustrezen meddržavni sporazum (Denning, 1997: 183).

Leta 1991 je Stansfield Turner, v letih 1977 - 1981 direktor ameriške obveščevalne službe CIA, ki se sedaj ukvarja z spremenjeno vlogo omenjene agencije v času po padcu komunizma, napisal članek, v katerem se zavzema za to, da CIA še naprej opravlja svojo nalogo nadzorovanja drugih držav. Vendar pa Turner pravi, da je potrebno redefinirati pojem nacionalne varnosti ZDA. Po njegovem mnenju je potrebno v ospredje postaviti ekonomske interese, zato Turner predlaga, da se CIA, ki se je do sedaj ukvarjala z vojaškim in političnim vohunjenjem, začne ukvarjati z ekonomskim vohunjenjem (Webster, 1995: 66). Ameriška prizadevanja, da "key escrow" sistem postane svetovni standard, je treba gledati tudi v tej luči. S tem ko ZDA zahtevajo avtorizacijo (oz. shranjevanje) gesel v ZDA - pri tem ne smemo pozabiti, da je ameriška vlada "key escrow" sistem razvila predvsem za poslovne namene (Denning, 1997: 180) - dejansko dobijo ključ do vseh kriptiranih sporočil v ostalih delih sveta. In ker bodo poslovneži verjetno kriptografijo uporabljali pre-

[30] *Testimony of Phil Zimmerman, http://www.pgp.com/phil/phil-quotes.cgi, 19. januar 1998.*

[31] *Testimony of Phil Zimmerman, http://www.pgp.com/phil/phil-quotes.cgi, 19. januar 1998.*

dvsem za zaščito vsebin pomembnih poslovnih skrivnosti, to pomeni, da bi ZDA imele - če njihov predlog "key escrow" sistema postane svetovni standard - v bistvu ključe do poslovnih skrivnosti podjetij po vsem svetu. Če bi poleg tega obveljala nova Turnerjeva definicija nacionalnih interesov ZDA in vizija nove vloge CIE, lahko to pomeni, da bi "key escrow" sistem omogočal ohranjanje vloge ZDA kot ekonomske in siceršnje svetovne velesile. Ob poizkusih povezovanja ZDA in EU na področju prestrezanja komunikacij in boja proti globalnemu kriminalu se zdi ta bojazen še bolj upravičena.

LITERATURA

Allard, W. Nicholas in Kass, A. David (1997): Law and Order in Cyberspace: Washington Report v Hastings Communications and Entertainment Law Journal (Comm/Ent), vol. 19, No. 3., pomlad 1997. University of California: Hastings College of the Law.

A Statewatch report, http://www.freenix.fr/netizen/swreport.html, 2. februar 1999.

About CPSR (Computer Professionals for Social Responsibility),
http://cpsr.org/cpsr/about-cpsr.html, 19. januar 1998.

COMPASS - Highway 401 traffic camera homepage, http://www.mto.gov.on.ca/english/traveller/compass/camera/cammain.htm, 20. december 1998.

Crypto-Gram, http://www.counterpane.com, 15. februar 2000. Counterpane Internet Security, Inc.

Cryptography Policy, http://epic.org/crypto/, 19. januar 1998.

Cult of the Dead Cow, http://www.cultdeadcow.com, 15. avgust 1998.

Čebulj, Janez (1992): Varstvo informacijske zasebnosti v Evropi in Sloveniji. Ljubljana: Inštitut za javno upravo pri Pravni fakulteti v Ljubljani.

Denning, E. Dorothy (1997): The future of cryptography, v Brian D. Loader, The Governance of Cyberspace, str. 175 - 190. London, New York: Routledge.

Dunnett, Jim (1998): Secret Phone-Tap Plan, v DejaNews, http://www.dejanews.com/getdoc.xp?AN=419710899, 2. februar 1999.

Efforts to ban encryption, http://www.epic.org/crypto/ban/, 19. januar 1998.

GVU 8th WWW Survey, http://www.gvu.gatech.edu/user_surveys/survey-1997-10/. Atlanta. 1997.

Imenik elektronske pošte Slovenije, http://afna.telekom.si, 7. oktober 1998.

Key Escrow, http://www.epic.org/crypto/key_escrow/, 19. januar 1998.

Kids Surf Day (1997), http://www.ftc.gov/opa/9712/kids.htm, 19. januar 1998.

Koops, Bert-Jaap (1997): Crypo Law Survey, http://cwis.kub.nl/~frw/people/koops/lawsurvy.htm, 19. januar 1998.

Kušej, Pavčnik, Perenič (1992): Uvod v pravoznanstvo. ČZ Uradni list RS: Ljubljana.

Loader, D. Brian (1997): The Governance of Cyberspace. London, New York: Routledge.

More about the Privacy Rights Clearinghouse, http://www.privacyrights.org/fs/services.html, 19. januar 1998.

Pavčnik, v: Kušej, Pavčnik, Perenič (1992): Uvod v pravoznanstvo. ČZ Uradni list RS: Ljubljana.

Perenič, v: Kušej, Pavčnik, Perenič (1992): Uvod v pravoznanstvo. ČZ Uradni list RS: Ljubljana.

Raab, D. Charles (1993): The Governance of Data Protection, v Jan Kooiman, Modern Governance - New Government-Society Interactions. Sage publications: London.

Raab, D. Charles (1997): Privacy, democracy, information, v Brian D. Loader, The Governance of Cyberspace, str. 155 - 174. London, New York: Routledge.

Privacy in Cyberspace, http://www.privacyrights.org/fs/fs18-cyb.html, 19. januar 1998.
Statewatch Organisation (monitoring the state and civil liberties in the European Union), http://www.statewatch.org/, 5. februar 1999
STOA (1998): An Appraisal of the Technologies of Political Control (Summary of Interim Study), http://www.europarl.eu.int/dg4/stoa/en/publi/166499/execsum.htm, 2. februar 1999.
The Center for Democracy and Techology, http://www.cdt.org/, 19. januar 1998.
The Clipper Chip, http://www.epic.org/crypto/clipper/, 19. januar 1998.
The Phill Zimmerman Case. InfoNation, http://www.info-nation.com/philzima.html, 19. januar 1998.
The Zimmerman Case v The Ethical Spectacle (1995): http://www.spectacle.org/795/zimm.html, 19. januar 1998.
Zimmerman, Phill (1993): Testimony of Philip R. Zimmerman to the Subcommittee on Science, Technology, and Space of the US Senate Committe on Commerce, Science, and Transportation, http://www.pgp.com/phil/phil-quotes.cgi, 19. januar 1998.
Zimmerman, Phill (1994): PGP(tm) User's Guide, v datoteki PGPDOC1.TXT v programskem paketu PGP ver. 2.6.2.
Towards A European Framework for Digital Signatures And Encryption, http://www.ispo.cec.be/eif/policy/97503toc.html, 19. januar 1998.
Ustava RS (1991): Uradni list RS, št. 4/91. Uradni list: Ljubljana.
Vidmar, Tone (1997): Računalniška omrežja in storitve. Ljubljana: Atlantis.
Webster, Frank (1995): Theories of the Information Society. London: Routledge.