Matej Kovačič

ZASEBNOST NA INTERNETU

Mirovni inštitut
Inštitut za sodobne družbene in politične študije

Matej Kovačič
ZASEBNOST NA INTERNETU

Lektura: Nevenka Škrlj
Risba na zunanji strani ovitka: A. Stewart in R. Mendez, RSA kripto-sardina
Risba na notranji strani ovitka: J. Bentham, Panoptikon (1791) in V. Ćosić,
Internetni zemljevid vojne v Jugoslaviji
Oblikovanje: Irena Wölle
Tisk: Stane Peklaj

Recenzenti: Goran Klemenčič, Anton Kramberger in Franc Trček

Izid knjige je omogočil Open Society Institute

Zbirka Politike POLITIKE

Izdajatelj: Mirovni inštitut
Inštitut za sodobne družbene in politične študije
Metelkova 6
SI-1000 Ljubljana
E: info@mirovni-institut.si
www.mirovni-institut.si

Urednik: Aldo Milohnić

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

342.721:004.738.5
004.738.5:342.71

KOVAČIČ, Matej, 1974
Zasebnost na internetu / Matej Kovačič. - Ljubljana : Mirovni inštitut, Inštitut za sodobne družbene in politične študije, 2003. - (Zbirka Politike)

Vsebuje tudi prevod, tiskan v obratni smeri: Privacy on the internet / [translation Olga Vuković]

ISBN 961-6455-09-5
1. Kovačič, Matej: Privacy on the internet

123847680

Kazalo

Za mentorsko pomoč, ki je omogočila nastanek te knjige, se zahvaljujem red. prof. dr. Slavku Splichalu s Fakultete za družbene vede. Prav tako se zahvaljujem za pomoč pri nastajanju knjige Matjažu Robinšaku, Gorazdu Kovačiču, nekaterim članom Slo-Techa ter Jerneju iz aufbix.org.

Za kritični pregled prve različice besedila se zahvaljujem mag. Jožetu Bogataju in mag. Jožefu Šantavcu z Inšpektorata za varstvo osebnih podatkov, mag. Marku Bonaču, direktorju Akademske in raziskovalne mreže Slovenije ARNES, Gorazdu Božiču, vodji varnostnega centra SI-CERT, dr. Tonetu Krambergerju in dr. Francu Trčku s Fakultete za družbene vede ter Vuku Ćosiću. Za kritično branje in mnoge koristne napotke pa se zahvaljujem predvsem mag. Goranu Klemenčiču iz Sveta Evrope.

UVOD

Leta 1976 sta matematika Whitfield Diffie in Martin E. Hellman v reviji *IEEE Transactions on Information Theory* objavila desetstranski članek z naslovom »New Directions In Cryptography«. V članku sta opisala protokol za varno izmenjavo šifrirnih ključev prek nezaščitenega medija in rodila se je zamisel o sistemu šifriranja z javnimi ključi.

Leto pozneje, neke aprilske noči, se je Ronald L. Rivest med hudim glavobolom (Dupuis 1999) domislil novega šifrirnega algoritma, ki bi temeljil na sistemu javnih ključev, omogočal pa bi tudi digitalno podpisovanje. Algoritem si je zapisal in ga zjutraj poslal kolegoma Adiju Shamirju in Leonardu M. Adlemanu. Vsi trije avtorji, ki so bili tedaj popolni novinci v kriptografiji, so opisali problem v znanstvenem članku, ki so ga poslali reviji *Scientific American*. Članek je bil objavljen septembra 1977, avtorji pa so v njem 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 šeststranski članek z naslovom »A Method for Obtaining Digital Signatures and Public-Key Cryptosystems«. V članku 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, kar pomeni, da je sporočila, zašifrirana z njim, izjemno težko zlomiti.

Minilo je štirinajst let in leta 1991 je računalniški programer Philip R. Zimmerman 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 je bil za tedanje standarde uporabniške prijaznosti razmeroma preprost, predvsem pa zelo učinkovit. Ker je tega leta ameriški senat obravnaval zakon,

ki bi močno omejil uporabo kriptografije v civilne namene, je Zimmerman – da bi izničil učinke tega zakona, če bi bil sprejet – program javno objavil na internetu in dovolil njegovo brezplačno kopiranje. V razmeroma kratkem času se je program razširil po vsem svetu.

Tako so se v petnajstih letih zgodili trije na videz nepomembni dogodki, ki bi praviloma morali zanimati le peščico matematikov in računalničarjev. Ampak obrnilo se je drugače. Na videz drobno matematično odkritje je v resnici imelo veliko večji pomen, kakor bi si konec 70. let kdo lahko mislil. Kajti po odkritju, predvsem pa računalniški implementaciji algoritma RSA, so se v ZDA aktivirali pravosodni sistem in tudi tajne službe. In potem ni bilo nič več tako kot prej.

ZASEBNOST, NADZOR IN TEHNOLOGIJA

Živimo v družbi, v kateri po eni strani opažamo čedalje večje poudarjanje posameznikove individualnosti in zasebnosti, po drugi strani pa smo priča čedalje višji stopnji nadzorovanja. Ni dvoma, da se nadzor pogosto povezuje z demokratičnostjo oziroma avtoritarnostjo družbe. Prav tako tudi ni dvoma, da obstaja močna povezanost med nadzorom in zasebnostjo, pa tudi varnostjo in organizacijo. Toda, ali lahko rečemo, da je vsak nadzor že sam na sebi dober ali slab?

Pri preučevanju zasebnosti in nadzora namreč nujno trčimo na paradoksalno dvojnost. Nadzor je hkrati dober in slab. Danes je namreč nadzorovanje posameznikov sredstvo družbenega nadzora kakor tudi sredstvo za zagotavljanje pravic družbene participacije. Prav tako tudi ne moremo mimo tega, da je nadzor tesno povezan s tehnologijo. Informacijske tehnologije so namenjene zbiranju in obdelavi vseh vrst podatkov in informacij. Tako podatkov in informacij o okolju, družbi, v kateri živimo, in posameznikih, ki nas obdajajo. Informacijska družba *je* družba nadzora. Zato ni presenetljivo, da imajo informacijske tehnologije danes izjemen pomen za nacionalno varnost, z vprašanji zasebnosti pa se čedalje bolj ukvarjajo politični aktivisti, civilna družba in delavski sindikalisti.

Pri preučevanju nadzora in zasebnosti nujno trčimo tudi ob tehnologijo. Tudi ta sama na sebi ni dobra ali slaba: pomembno je v kakšne namene jo uporabljamo. Marsikatero tehnologijo je mogoče uporabiti za namene, o katerih ob njeni uvedbi ni nihče razmišljal. Pri tem pa ne gre samo za specializirane tehnologije, pač pa za tehnologije, ki so že ali pa bodo kmalu v množični rabi.

Identifikacija dohodnih klicev (ang. *caller ID*) je v Sloveniji postala javno poznana šele z nastopom GSM mobilne telefonije ter ISDN stacionarne telefonije, čeprav so to tehnologijo razvili v ZDA že leta 1987. Identifikacija dohodnih klicev ima nekaj očitnih prednosti. Po

poskusni uvedbi v Kanadi leta 1991 je policija zaznala drastičen upad opolzkih anonimnih telefonskih klicev in nadlegovanja po telefonu (Lyon 1994, 149). Vendar pa je bila ta tehnologija v ZDA sprejeta z deljenimi mnenji, saj so se kmalu pokazale možnosti njene zlorabe. Kmalu po popolni digitalizaciji telefonskega omrežja v ZDA in uvedbi ISDN telefonije v 90. letih so ameriška podjetja začela povezovati klicoče telefonske številke s socioekonomskimi in geodemografskimi podatki. Tako so podjetja ob sprejemu telefonskega klica lahko iz svoje baze podatkov dobila profil klicočega in celo njegove potrošniške preference. To je sprožalo proteste potrošnikov, saj so bili po eni strani zbrani podatki mnogokrat zastareli ali netočni, po drugi strani pa je prihajalo tudi do diskriminacije nekaterih skupin potrošnikov zaradi njihovih demografskih značilnosti, predvsem rase in kraja bivanja.

Znano je, da je izvor radijskega signala mogoče dokaj natančno določiti s pomočjo triangulacije. Metoda je dobro poznana in uporabljana npr. za odkrivanje ilegalnih radijskih postaj, pri reševanju ponesrečenih ladij, med radioamaterji itd. Ker mobilni telefoni oddajajo radijske signale, je seveda mogoče prostorsko locirati tudi njih. V grobem sta mogoča dva načina ugotavljanja lokacije mobilnega telefona in sicer terminalska rešitev (ang. *terminal-based* oz. *handset-based*), kjer lokacijo ugotovi in v omrežje sporoči mobilni telefon sam, ter omrežna rešitev (ang. *network-based*), kjer lokacijo mobilnega telefona ugotovi omrežje (Leskovšek 2001, 19). Terminalske rešitve so zelo natančne (od 50 do 5 metrov), vendar razmeroma drage in počasne, saj predvidevajo zamenjavo vseh mobilnih telefonov z novimi, ki bodo imeli vgrajeno podporo ugotavljanja lokacije (npr. s pomočjo satelitskega navigacijskega sistema GPS). Veliko cenejše in hitrejše so omrežne storitve. Nekatere so že na voljo, vendar je njihova natančnost ugotavljanja lokacije tudi manjša, saj niha od 100 do 1100 metrov (Leskovšek 2001, 20).

T. i. mobilne storitve so pomembna tržna niša za operaterje GSM mobilne telefonije, saj poznavanje lokacije mobilnega uporabnika omogoča lokalizacijo informacijskih storitev, izvajanje storitev sledenja, navigacijskih storitev, storitev upravljanja z razpršenimi viri po prostoru itd. (Leskovšek 2001, 21). Podjetje Streetbeam iz ZDA na primer že trži pošiljanje oglasnih SMS sporočil uporabnikom mobi-

lnih telefonov, ki se približajo njihovim oglasnim točkam.[1] Razvoj tovrstnega oglaševanja bo šel zagotovo v smer interaktivnih oglasnih panojev, ki bodo zaznali in prepoznali uporabnika ter mu predstavili personificiran oglas. Seveda pa ima poznavanje in zaznavanje lokacije lahko za mobilnega uporabnika tudi negativne posledice.

Novembra 1996 je bila v evropskem uradnem listu Official Journal objavljena *resolucija o zakonitem prestrezanju telekomunikacij* (ang. *resolution on the lawful interception of communications*). Resolucija v prvem delu navaja, da je »z zakonom podprto prestrezanje telekomunikacij pomembno orodje za zaščito nacionalnega interesa, nacionalne varnosti in preiskovanje resnih kaznivih dejanj«, v drugem delu pa podaja zbirko podrobnih zahtev, ki jih bodo morala izpolniti telekomunikacijska podjetja. Ena izmed njih je tudi zahteva po posredovanju podatkov o lokaciji uporabnika mobilnega telefona (Council Resolution 1996, 1–6).[2] Pri tem pa dodaten problem predstavlja hramba podatkov, saj 15. člen direktive EU 2002/58 o obdelovanju osebnih podatkov in varstvu zasebnosti na področju elektronskih komunikacij državam članicam omogoča hranjenje prometnih podatov za določen čas (Možina 2002, 4). Države članice EU imajo tako možnost operaterjem mobilne telefonije predpisati rok obveznega hranjenja prometnih podatkov (med drugim tudi podatkov o lokaciji uporabnika), kar državnim organom potencialno omogoča *vedeti za vsak premik tako rekoč vsakega posameznika*. Nekateri pravni strokovnjaki zato opozarjajo da bi tim. lokacijska zasebnost zaslužila enako pravno varstvo kot vsebina komunikacije (Možina 2002, 5).

Današnjega življenja si brez identifikacijskih (ang. *ID card*) in pametnih kartic (ang. *smart card*) skorajda ne moremo zamisliti, saj nam omogočajo opravljanje vsakodnevnih dejavnosti, kot npr. nakupovanje, uporabo zdravstvenih storitev itd. Vendar pa so bile identifikacijske izkaznice prvotno namenjene registraciji za državo nezaželenih posameznikov (Banisar et al. 1999). Prve osebne izkaznice, ki so vsebovale tudi fotografijo, prstni odtis in lastnoročni podpis posameznika, so na predlog nizozemskega statistika

[1] Več o podjetju na http://www.streetbeam.com.

[2] Enaka zahteva je zapisana tudi v 6. točki 4. člena predloga *Pravilnika o programski opremi in vmesnikih za zakonito prestrezanje komunikacij*, ki ga je 20. decembra 2002 pripravilo in v javno obravnavo dalo Ministrstvo za informacijsko družbo.

Jacobusa Lambertusa Lentza uvedli na Nizozemskem med nacistično okupacijo, na njih pa je bilo tudi označeno, ali je oseba Jud ali ne. Black ugotavlja, da so bile omenjene osebne izkaznice prvi korak do izvedbe holokavsta na Nizozemskem, saj so identifikaciji sledile deportacije (Black 2002, 388–389).

Poleg osebne izkaznice lahko štejemo med identifikacijske kartice tudi različne bančne, nakupovalne itd. kartice, ki imajo zapisane podatke o identiteti uporabnika. Za razliko od navadnih identifikacijskih kartic, na katerih so zapisani samo vnaprej pripravljeni podatki, pa pametne kartice vsebujejo pomnilnik, kamor se lahko podatki zapisujejo tudi pozneje. Argument za uporabo inteligentnih kartic je predvsem ta, da naj bi imeli imetniki teh kartic z njihovo uporabo večji nadzor nad svojimi osebnimi podatki (Lyon 1994, 150). Vendar pa, kot ugotavlja Lyon, uporaba pametnih kartic omogoča zlivanje javnih, državnih in zasebnih komercialnih baz podatkov. V Sloveniji se je pred časom že razmišljalo o tem, da bi zdravstvene kartice uporabljali tudi za identifikacijo študentov. Tehnično za kaj takega ni večjih ovir, vendar pa zamisel zaradi zakonskih omejitev verjetno ne bi bila izvedljiva. Chaum zato ugotavlja, da je zasebnost posameznikov, ki uporabljajo tovrstne kartice, čedalje bolj ogrožena (Chaum 1996, 235).

Biometrija je proces zbiranja, procesiranja in shranjevanja podatkov o posameznikovih fizičnih lastnostih z namenom identifikacije. Najbolj priljubljene oblike biometrije so skeniranje očesne mrežnice, geometrije rok, odtisov palca, prstnih odtisov, prepoznava glasu in prepoznava obraza, razvijajo pa se tudi drugi načini, npr. sistemi za prepoznavo vzorcev tipkanja, uporabe pisala (hitrost pisanja, pritisk pisala...), itd. Da ne gre za znanstveno fantastično tehnologijo, dokazujeta mednarodno letališče Ben Gurion v Tel Avivu, kjer biometrični sistem za skeniranje geometrije rok že uporabljajo (Mesenbrink 2002) in amsterdamsko letališče Shiphol, kjer za identifikacijo uporabljajo sistem za skeniranje očesne šarenice (Amsterdam 2001). Po terorističnih napadih 11. septembra v ZDA so na nekaterih ameriških letališčih začeli razmišljati tudi o uporabi sistemov za prepoznavo obrazov (ang. *face-recognition system*). Tak sistem je že bil uporabljen januarja 2001 v mestu Tampa na Floridi, julija 2001 pa so podoben projekt, ki naj bi pomagal pri iskanju kriminalcev in pogrešanih otrok, začeli v mestu Virginia Beach (EPIC 2002).

Še bolj kontroverzna biometrična metoda pa je identifikacija genetskega zapisa (ang. *DNA identification*). Kakor navaja poročilo Privacy & Human Rights 1999, vzpostavljajo policije več držav, med drugim tudi ZDA, Nemčije in Kanade, nacionalne baze odtisov DNA (Banisar et al. 1999). Ni dvoma, da biometrija izrazito povečuje možnosti nadzora posameznikov, zato ne preseneča, da so se kmalu po terorističnih napadih na New York 11. septembra 2001 pojavile ideje o splošni uvedbi biometrije na letališčih (Manjoo 2001).

Kljub temu da je nezakonito prisluškovanje in nezakonito tajno video snemanje v zasebnih prostorih prepovedano, pa v marsikateri državi – tudi v Sloveniji – ni omejena prodaja audio in video prisluškovalnih naprav. Te naprave so razmeroma poceni in zato dostopne tudi širšemu krogu potrošnikov. Poročilo Privacy & Human Rights navaja oceno iz leta 1996, da v Veliki Britaniji vsako leto prodajo približno 200.000 prisluškovalnih naprav, še več pa v azijskih državah (Banisar et al. 1999).

Podobno so danes v splošni rabi tudi videokamere (*CCTV – Closed Circuit Television* sistemi), ki jih množično uporabljajo v javnih zgradbah in na javnih mestih. Kot ugotavlja študija STOA (*Scientific and Technological Options Assessment of the European Parliament)* v svojem vmesnem poročilu iz študije o tehnologijah političnega nadzora, se je tehnologija vizualnega nadzora v zadnjih letih dramatično spremenila, saj so te naprave danes že izredno miniaturizirane, poleg tega pa je s sodobno tehnologijo, predvsem z novimi algoritmi, mogoče posnetke nadzornih videokamer primerjati med sabo, shranjevati in povezovati. Primer take tehnologije so sistemi samodejnega razpoznavanja vozil (ang. *Vehicle Recognition System*), ki so na trgu že od leta 1994 (STOA 1998). Namenjeni so nadzoru prometa, vendar so sposobni razpoznati registrsko številko avtomobila in tako spremljati gibanje vozila.[3]

»Smo na začetku revolucije 'algoritmičnega nadzora' – učinkovite analize podatkov s pomočjo kompleksnih algoritmov, ki omogočajo avtomatsko razpoznavo in sledenje« (STOA 1999), ugotavljajo avtorji te študije. Po ugotovitvah študije se tovrstni sistemi tudi dobro pro-

[3] Na spletnih straneh kanadskega ministrstva za transport si je mogoče ogledati interaktivne zemljevide treh avtocest in slike, ki jih posredujejo kamere, nameščene na teh avtocestah. Spletna stran je na naslovu http://www.mto.gov.on.ca/english/traveller/compass/.

dajajo v glavno mesto Tibeta, čeprav le-to nima nikakršnih težav s prometom. Kitajska vlada je podoben sistem uporabila leta 1989 med znanimi študentskimi demonstracijami na Trgu nebeškega miru na Kitajskem za iskanje voditeljev demonstracij (STOA 1999).

Moč video nadzora se v kombinaciji z uporabo nekaterih drugih tehnologij, na primer detekcije gibanja, uporabe povečave in infrardečega snemanja, lahko še poveča. Za vizualni nadzor se lahko uporabljajo tudi sateliti. Satelitski nadzor se že uporablja na številnih področjih, na primer pri poročanju s kriznih žarišč, ugotavljanju obsega in škode ob naravnih nesrečah ter celo pri odkrivanju črnih gradenj (Banisar et al. 1999). Satelitski nadzor ni omejen samo na državne organe, pač pa so na voljo tudi komercialne različice.[4] Poleg tega pa omogoča tudi povezavo satelitskih posnetkov z geografskimi informacijskimi sistemi (t. i. *GIS* bazami), prek njih pa tudi povezovanje z drugimi bazami podatkov.

Prav tako osupljiv je tudi razvoj tehnologije za nadzor komunikacijskih sredstev. Le-ta namreč omogoča t. i. »prijazno prisluškovanje« (ang. *to wiretap friendly*), kar pomeni predvsem to, da je prisluškovanje prijazno oz. preprosto za prisluškovalca (Banisar et al. 1999). Leta 1994 je namreč v ZDA stopil v veljavo *zakon o digitalni telefoniji*, ki je od telefonskih družb zahteval, da v svoje telefonske centrale vgradijo zmožnosti za oddaljeno prisluškovanje (t. i. *remote wiretapping port*), kar je agentom FBI močno olajšalo prisluškovanje. Danes imajo vse nove telefonske centrale že vgrajene tehnične možnosti za prisluškovanje, problem pa je seveda nastal, ker so telefonske centrale z vsemi tehničnimi zmožnostmi vred danes dostopne tudi zasebnikom (npr. podjetjem), nad katerimi pa se izvaja precej manj strog nadzor kot nad operaterji javne telefonije.

Seveda so tehnologije prestrezanja in prisluškovanja razvite tudi v virtualnem svetu. Phil Zimmerman je že junija 1996 v svojem priča-

[4] Leta 1998 je računalniško podjetje *Microsoft* na internetu postavilo strežnik *Terraserver* (http://terraserver.microsoft.com/). Na strežniku je mogoče dobiti satelitske posnetke Zemlje, ki so jih leta 1992 posneli ruski vohunski sateliti iz višine 230 km (posnetke, ki niso več označeni kot zaupni, je podjetje *Microsoft* odkupilo od rusko-ameriškega podjetja SPIN-2). Posnetke je možno tudi kupiti, najbolj pa sta presenetljivi njihova čistost in visoka kvaliteta; na njih so namreč jasno razpoznavni predmeti do velikosti dveh metrov. V Sloveniji pa je Agencija RS za okolje postavila Interaktivni naravovarstveni atlas, dostopen na naslovu http://212.103.140.243/nvatlas/, kjer je ravno tako mogoče pregledovanje zračnih posnetkov celotne Slovenije. Atlas omogoča iskanje in prikaz kateregakoli objekta s stalnim naslovom v Sloveniji.

nju pred podkomitejem ameriškega senata svaril pred prestrezanjem elektronskih sporočil, saj je ugotavljal, da je elektronska sporočila mogoče čisto preprosto prestreči in nato analizirati, tehnologija pa omogoča, da je to narejeno »preprosto, rutinsko, avtomatsko in neopazno ter v velikem obsegu« (Zimmerman 1993). Danes je takšna tehnologija nadzora na internetu – to je sistem Carnivore, o katerem bo govor pozneje – že v uporabi. Obstajajo pa tudi računalniški programi za masovni nadzor elektronske pošte, pri čemer računalniški program za vsako elektronsko sporočilo določi stopnjo verjetnosti, da gre za potencialno sumljivo sporočilo, najbolj sumljiva sporočila pa potem analizira človek.[5]

Poročilo Privacy & Human Rights iz leta 1999 navaja, da so leta 1998 člani evropskega parlamenta dobili dokaze, da je ameriška agencija National Security Agency v sodelovanju z britansko vlado vzpostavila sistem, ki omogoča »prestrezanje skoraj vsakega faxa, elektronskega sporočila ali telefonskega klica v Evropski uniji« (Banisar et al. 1999). To je sistem ECHELON, ki je bil zgrajen z namenom, da bi prestrezal komunikacije Sovjetske zveze, Kitajske in drugih držav, ki bi lahko ogrožale nacionalno varnost zahodnih držav in ZDA. Odbor Evropske unije *Temporary Committee on the ECHELON Interception System* je 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 in ne vojaških komunikacij« (Temporary Committee 2001, 88).[6]

Kljub razburjenju, ki ga je poročilo o obstoju sistema ECHELON povzročilo v evropskem parlamentu, pa ostaja cilj Evropske unije

[5] SpamAssasin (http://spamassassin.taint.org/) je računalniški program namenjen odkrivanju ti. spam pošte (nezaželene/nenaročene elektronske pošte). Program označi vsako sporočilo s točkami, pri čemer pomeni večje število točk večjo verjetnost, da je sporočilo spam. S preusmeritvenimi filtri je nato sporočilo glede na število točk mogoče posredovati na različne naslove. Program omogoča točkovanje po poljubnih merilih.

[6] V protest proti sistemu globalnega nadzorovanja so 21. oktobra 2001 na internetu organizirali *Jam Echelon Day*. Organizatorji so uporabnike interneta pozivali naj pošljejo čim več elektronskih sporočil z besedami, ki naj bi sistem Echelon aktivirale (npr. »orožje«, »droga«, »terorizem«, »Bush«, itd.), s čimer naj bi dosegli njegovo preobremenitev. Da bi do kakšne večje preobremenitve zares prišlo je sicer malo verjetno, kljub temu pa takšne akcije pomagajo povečati zavedanje uporabnikov interneta o tem problemu (Oakes 1999).

uskladitev zakonodaje o prisluškovanju,[7] kar pomeni, da se nadzor komuniciranja globalizira. To potrjuje tudi poročilo *delovne skupine za policijsko sodelovanje* iz junija 1995, ki pravi, da so novi telekomunikacijski sistemi »globalni problem, ki je lahko rešen le z globalnim sodelovanjem« (Statewatch report 1999). Po mnenju uradnikov Evropske unije je namreč »z zakonom podprto prestrezanje telekomunikacij pomembno orodje za zaščito nacionalnega interesa, nacionalne varnosti in preiskovanje resnih kaznivih dejanj« (Council Resolution 1996, 1–6).

Ni torej dvoma, da živimo v družbi, kjer je stopnja nadzora visoka. Zato je vsekakor umestno vprašanje, kakšen je pomen nadzora in kakšne so njegove pozitivne in negativne posledice. V tej študiji se bomo posvetili vprašanjema nadzora in zasebnosti v sodobni informacijski družbi, predvsem pa njuni specifiki na internetu. Ogledali si bomo tudi, kakšno je stanje na področju zasebnosti v Sloveniji, in skušali predlagati nekaj smernic za njeno učinkovitejše varstvo.

[7] S tem v zvezi je zanimiv tudi članek v prvi številki *Evropskega dialoga* v letu 1999, revije, ki jo izdaja evropska komisija in izhaja v desetih jezikih. Članek govori o boju proti resnemu kriminalu: »Kriminalci lahko izkoriščajo razlike med zakonodajami posameznih držav ... Komisija v okviru prizadevanj za zapiranje pravnih vrzeli priporoča dogovor vseh vlad EU o enotnem obravnavanju kriminalnih prestopkov ...« (Watson 1999, 26).
Februarja 1999 sta evropska komisija in Svet Evrope začela izvajati program »Octopus II«, ki naj bi pomagal državam srednje in vzhodne Evrope ter Rusiji pri boju proti organiziranemu kriminalu. Program je nadaljevanje programa »Octopus I«, ki se je izvajal v letih 1996–1998. Namen Octopusa II je predvsem *poenotenje zakonodaje s področja pravosodja in notranjih zadev*. V okviru programa bodo med drugim potekali tudi *seminarji o tehnikah raziskovanja kaznivih dejanj* (Agence Europe 3. 2. 1999, Bruselj).

DRUŽBA NADZORA

Vprašanje (družbenega) nadzora je bilo eno pomembnih vprašanj v sociologiji 19. stoletja. Družbeni nadzor so sociologi videli kot nekaj pozitivnega, nekaj, kar omogoča red in sobivanje posameznikov v družbi. Ross trdi, da uspešno sodelovanje posameznikov zahteva visoko stopnjo družbenega reda (Ross 1969, 2), visoka stopnja družbene organizacije pa predpostavlja nadzor. Hkrati je v družbi potrebna še kakšna avtoriteta, ki razmejuje konfliktne interese posameznikov. Ross trdi, da to avtoriteto v statičnih družbah lahko predstavljajo navade, v spreminjajočih se družbah pa mora biti ta avtoriteta eksterna (Ross 1969, 40). Po njegovem pa so institucije umetnega reda potrebne zaradi družbene neenakosti in ekonomske diferenciacije (Ross 1969, 42, 56). Podobno pravi tudi Cooley, ki meni, da če obstaja neka celota, neka skupnost, mora biti cilj posameznika služiti tej skupnosti, življenje v večji skupnosti pa potegne za sabo disciplino v organizaciji in samonadzor (Cooley 1993, 39, 152).

Cooley tako pravi, da ni posameznika zunaj družbe in svobode mimo organizacije. Po njegovem mnenju obstajata dva tipa individualnosti, individualnost izolacije in individualnost izbire, v družbi pa je zaželena slednja, saj dela življenje racionalno in svobodno, namesto naključno in lokalno (Cooley 1993, 47, 93). Zato nekateri sociologi vidijo predvsem pozitivno funkcijo nadzora. »Ideji resnice in razumnosti v človeških zadevah težko prevladata v sistemu brez opazovanja (nadzorovanja), ki bi ju krepilo,« pravi Cooley (Cooley 1993, 185). Po njegovem je »cilj moderne demokracije organizirati pravico, kjer resnica preživi, hinavščina pa pogine« (Cooley 1993, 184). Nadzor posameznikov v tej perspektivi nima negativne konotacije, saj Ross pravi, da je družbeni nadzor zgoščen ali razpršen v razmerju, kakor ljudje čutijo potrebo po vodstvu in zaščiti (Ross 1969, 78).

Tako pri Rossu kakor pri Cooleyu se pojavlja ideja o samozavedajočem se posamezniku in samonadzoru. Cooleyjev ideal je posa-

meznik, ki se zaveda samega sebe in je predan svojemu delu, vendar pa se čuti kot del velike celote.

Sociologi so obravnavali nadzor tudi kot nekaj, kar izvajajo družbeni subjekti, predvsem državni organi in kapitalistični podjetniki, za dosego svojih ciljev. Marx je tako nadzor obravnaval z vidika boja med delom in kapitalom; nadzorovanje delavcev je obravnaval kot sredstvo vzdrževanja menedžerskega nadzora v prid kapitalu z namenom zagotoviti konkurenčnost posla oziroma maksimirati produkcijo ob čim manjših stroških.[8] Marx torej v zvezi z nadzorom delavcev govori o zagotavljanju njihove poslušnosti in disciplin iranju, zato ima pri njem nadzor negativno konotacijo. Po drugi strani pa je Weber povezoval nadzor z organizacijo in učinkovitostjo birokracije. Zanj je racionalna administracija skupek znanja in discipline, racionalnost sodobnih organizacij pa se kaže v knjigovodstvu oziroma vodenju evidenc, ki temeljijo na pisnih dokumentih (Lyon 1994, 7, 25–26).

Marx in Weber sta tako nadziranje obravnavala kot sredstvo nadzora. Izkazalo pa se je, da ga je mogoče obravnavati tudi v povezavi z močjo in disciplino.

Eno pomembnejših teoretskih sprememb v obravnavi nadzora je namreč povzročil francoski filozof Michel Foucault. Če Marx govori o nadzoru kot o nečem, s čimer kapitalistični menedžer *sili* delavce k povečanju produkcije, Foucault govori o »urjenju teles« (Foucault 1984, 138) in razlaga, da so od 17. in 18. stoletja dalje discipline postale splošne formule gospodovanja. Po njem so sodobne družbe razvile sredstva disciplin iranja, v njih so vedno navzoče tehnike in strategije moči, zato jih Foucault imenuje tudi »disciplinske družbe«. Foucault pravi, da je cilj discipline »izdelati podrejena in izurjena telesa, 'krotka' telesa« (Foucault 1984, 137–138). Disciplinski mehanizmi, ki so jih razvile sodobne družbe, subtilno in posredno vsiljujejo normativno delovanje posameznikov in ker se za disciplin iranje posameznikov uporablja nadzor, je po Foucaultu le-ta sredstvo podrejanja.

Svoj zelo odmevni teoretski pogled na nadzor je Foucault zgradil na modelu načrta za zapor Panoptikon, ki ga je britanski vladi leta

[8] Takšno vrsto nadzora je skoraj do skrajnosti pripeljal taylorizem oz. znanstveni menagement, ki je temeljil na natančnem opazovanju in beleženju dela in delovnih gibov, pisanju poročil itd., njegov namen pa je bilo povečati produktivnosti delavcev.

1791 predstavil Jeremy Bentham. Glavni učinek Panoptikona je nadzor, ki se vzdržuje s pomočjo stalnega občutka, da zapornike opazujejo nevidne oči. Najpomembnejša je nevidnost opazovalcev, kar zapornike spravi v negotovost, ta pa vzpostavi mehanizme samonadzora. Foucault tako pravi: »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« (Foucault 1984, 202).

Po njem moč ni posest, pač pa strategija. Pri panoptičnem učinku nadzora gre torej predvsem za to, da se z uporabo negotovosti doseže prostovoljno podrejanje posameznikov. Opazovanje mora biti zato nesimetrično oziroma hierarhično. Lyon ugotavlja, da je nesimetrično opazovanje postalo del sodobnega projekta uničevanja gotovosti (Lyon 1994, 65). Zavest, da smo nenehno vidni, zagotavlja samodejno delovanje oziroma vzpostavitev oblasti na mikroravni. Vidnost je zato neke vrste past.[9] Panoptikon je po Foucaultovem mnenju politična tehnologija, ki deluje na podlagi subtilnih prisil in omogoča vzdrževanje oblasti. Panoptično delovanje v samem temelju družbe ohranja ravnotežje, zato se sodobna družba boji odpraviti nadzorovanje.

Foucaultov teoretski pogled zelo neposredno govori o nadzoru v povezavi s podrejanjem posameznikov in njihovim discipliniranjem. Ta panoptični učinek je prikazal pisatelj George Orwell v svojem znanem delu z naslovom *1984*, kjer opisuje totalitarno družbo, v kateri skrivnostni Veliki Brat ljudi nadzoruje prek telekranov, vendar tako, da posameznik nikoli ne ve, kdaj je nadzorovan in kdaj ni. Posledica takega nadzora je visoka stopnja samocenzure in navsezadnje skrajno totalitarna družba. Ali kot pravi Servan v predgovoru Foucaultove knjige *Nadzorovanje in kaznovanje*:

»Bedast despot lahko prisiljuje sužnje z železnimi verigami, toda pravi politik jih precej krepkeje zveže z verigo njihovih lastnih idej; na trdno raven razuma pripne prvi konec; ta vez je toliko bolj trdna, ker ne poznamo njene teksture in ker mislimo, da je naše delo ... na mehkih vlaknih možganov pa stoji neomajen temelj najtrdnejših cesarstev« (J. M. Servan v Foucault 1984, 102).

[9] Primer panoptičnega učinka je denimo nadzor anketarjev ali pa video nadzor v veleblagovnicah.

Nadzor v obliki popisovanja posesti in preštevanja prebivalstva se je, kot ugotavlja Lyon, v zgodovini začel, da bi vzpostavil pregled in red, pa tudi zaradi utrjevanja moči. Hkrati pa je izvor nadzora tudi tesno povezan z dojemanjem časa v sodobni družbi, saj so za razliko od tradicionalnih družb delovne rutine v sodobnih družbah vezane na uro, ki uravnava človeške dejavnosti. Urnik in ura kapitalističnemu menadžerju že zgodaj omogočata vsakodnevno opazovanje in nadzorovanje delavcev (Lyon 1994, 34–35, 46), danes pa se povezanost nadzora z uro nadaljuje v povezanost nadzora z računalnikom, saj vlogo koordinatorja človeških dejavnosti v prostoru in času danes čedalje bolj prevzema računalnik.

Sistematični in množični nadzor, kakršnega poznamo v sodobni družbi, se je tako pojavil šele s pojavom in rastjo vojaške organizacije, industrijskih mest, vladne administracije in kapitalističnega podjetništva, predvsem pa s pojavom informacijskih in mikroprocesorskih tehnologij, kar je povzročilo, da je tudi zasebnost posameznikov postala resen problem prav v dvajsetem stoletju.

Beniger pravi, da je procesiranje informacij temeljno za vse k cilju usmerjene dejavnosti (Beniger 1986, 434), zato ne preseneča povezanost nadzora s sodobnimi organizacijami. Frank Webster tako ugotavlja, da sta »organizacija in nadzorovanje siamska dvojčka, ki sta zrasla z razvojem modernega sveta« (Webster 1995, 54). Beniger zato govori o *revoluciji nadzora* v 20. stoletju, ki jo primerja z industrijsko revolucijo iz 19. stoletja. Pri revoluciji nadzora gre predvsem za zmožnost izrabe informacij (Beniger 1986, 427), povezana pa je z organizacijo in tudi s tehnološkim razvojem.

Pomembni element nadzora je danes proizvodnja dosjejev o posameznikih (baze podatkov), zato Lyon govori o *družbi dosjejev* (Lyon 1994, 29–30). Ljudje čedalje bolj postajamo svoji dosjeji, posameznik pa v sodobni družbi praktično ne more obstajati, ne da bi bil nadzorovan. In če obstaja, o njem obstaja tudi kakšna evidenca. Zato smo posamezniki že s samo participacijo v družbi (uveljavljanje državljanskih, zdravstvenih, zaposlitvenih in drugih pravic) izpostavljeni nadzoru. S pomočjo dosjejev lahko nadzorujemo dejavnost in potrebe ljudi, zapisovanje pa omogoča tudi nadzor nad preteklimi dogodki. Ker je nadzorovanje značilno za vse vrste organizacij, ga izvajata tako država kakor tudi zasebni sektor, pri čemer je treba ugotoviti, da lokomotiva tega procesa čedalje bolj postaja

zasebni sektor. Podrobnosti o posameznikih zbirajo kapitalistične korporacije in tudi vladne službe, zato nadzorovanje zadeva tako posameznike potrošnike, kot posameznike državljane. Država se poslužuje nadzora za zagotavljanje zunanje in notranje varnosti ter izvajanje administrativnih nalog; kapitalistične korporacije pa izhajajo iz predpostavke o posameznikovi svobodi, zato skušajo čim bolj natančno ugotoviti potrošnikove želje ter jim prilagoditi ponudbo. Zato se nadzor pojavlja tako v obliki »nadzorovanja ljudi«, ki se ga v glavnem poslužujejo države in nosilci oblasti, ter v obliki »zbiranja podatkov«, ki je podlaga za potrošniško nadzorovanje (Lyon 1994, 11).

Čeprav so pri nadzoru največkrat izpostavljene predvsem njegove negativne plati, pa ima nadzor tudi pozitivne strani, saj pomaga pri zagotavljanju varnosti in vzdrževanju reda, v povezavi z organizacijo pa služi tudi urejanju življenja v družbi. Pri preučevanju nadzora torej naletimo na zanimiv paradoks, saj je danes nadzorovanje posameznikov tako sredstvo družbenega nadzora kakor tudi sredstvo za zagotavljanje pravic družbene participacije. Lyon ugotavlja da se je nadzor razrasel skupaj z demokracijo, saj je tesno povezan z zahtevo po enakosti. Zahteva po enaki obravnavi vseh državljanov in uveljavljanju njihovih pravic namreč potegne za seboj tudi zahtevo po individualni ločljivosti teh posameznikov (Lyon 1994, 24, 31).

Trendi kažejo, da se nadzor še povečuje, saj se procesi klasifikacije, zbiranja in zapisovanja podatkov in informacij neprenehoma množijo, življenja navadnih posameznikov pa postajajo čedalje bolj transparentna. Ambicija države je videti in nadzorovati vse, enako ambicijo pa imajo tudi zasebna podjetja. »V moderni državi je nadzor maksimiran,« ugotavlja Giddens (Giddens v Webster 1995, 70), zato Webster predlaga, da bi bilo morebiti namesto pojma *informacijska družba* bolje uporabljati pojem *družba nadzora*.

Nadzor na delovnem mestu in nadzor potrošnikov

Kot že rečeno, nadzor ni samo domena države, pač pa ga izvajajo tudi zasebna podjetja. Eden izmed ključnih delov menedžmenta v 20. stoletju je tako neposredni nadzor podrejenih na kapitalističnem delovnem mestu, to doktrino pa je skoraj do skrajnosti pripeljal taylorizem. Pri delodajalčevem nadzoru zaposlenih je več nasprotujočih si interesov. Klemenčič navaja interese treh subjektov. Prvi je

interes delodajalca. Ta je navadno lastnik delovne opreme (računalnikov in telekomunikacijskih omrežij ter naprav), ki je bila zaposlenemu dana v uporabo. Delodajalec ima interes, da je oprema uporabljena skladno z namenom uporabe, da preprečuje zlorabo opreme, in da odkriva ter preganja disciplinske prekrške zaposlenih. Končni cilj je seveda zmanjšanje stroškov in povečanje produkcije. Na drugi strani obstaja *interes zaposlenega*, ki pričakuje določeno stopnjo zasebnosti in avtonomije tudi na delovnem mestu. To še posebej velja takrat, ko zaposleni ni seznanjen oz. se ni predhodno strinjal z nadzorom npr. telefona ali elektronske pošte. Poleg tega je za razliko od ZDA, kjer pravo načeloma ne ščiti zasebnosti zaposlenega na delovnem mestu pred delodajalcem, pač pa je to prepuščeno notranji politiki podjetja, evropska pravna ureditev zaposlenim veliko bolj naklonjena. Znan je primer Halford vs. Združeno kraljestvo, o katerem je evropsko sodišče za človekove pravice izrecno zapisalo, da zaposleni na delovnem mestu upravičeno pričakuje zasebnost, prav tako pa je znano tudi priporočilo Sveta Evrope št. R(89) 2, ki določa, da imajo zaposleni na delovnem mestu pravico do vzpostavljanja osebnih in socialnih stikov. Ker sta v procesu medsebojnega komuniciranja udeležena vsaj dva, obstaja tudi *interes tretjih oseb*, ki komunicirajo z zaposlenim in morda niti ne vedo, da gre za službeno komunikacijsko sredstvo ter da delodajalec nadzoruje komunikacije zaposlenega, s katerim so v stiku (Klemenčič et al. 2001, 188–189).

Nadzorovanje na delovnem mestu je danes tehnično in organizacijsko čedalje laže izvedljivo, posebej še v primerih, ko delodajalci uporabljajo lastno telekomunikacijsko opremo (npr. lastne telefonske centrale, lastne poštne strežnike itd.), ki ima vgrajene enake možnosti nadzora, kakršnih smo vajeni v javnih telekomunikacijskih omrežjih. Nadzor nad uporabo teh možnosti nadzora je namreč v zasebnih telekomunikacijskih omrežjih veliko manjši (če sploh obstaja) kot v javnih omrežjih. Kljub temu zakonodaja in sodna praksa določata, da zaposleni na delovnem mestu upravičeno pričakuje neko stopnjo zasebnosti, da mora biti zaposleni vnaprej seznanjen in se mora vnaprej strinjati s posegi v zasebnost, katerih obseg in oblika morata biti prilagojena najmanjšemu mogočemu posegu, s katerim se še da zagotoviti namen nadzora, ter da je treba upoštevati varstvo zasebnosti tretjih oseb.

Vendar pa se podjetja ne omejujejo samo na nadzor zaposlenih na delovnem mestu. Zaradi zahtev po čim boljši organizaciji poslovanja so začela zbirati tudi podatke o strankah oziroma potrošnikih. Začetki zbiranja podatkov o potrošniških navadah segajo že v leto 1920, ko je v ZDA Alfred Sloan začel za General Motors zbirati podatke o potrošnikih in graditi potrošniške profile. Raziskave trga so začele vključevati tudi zbiranje socioekonomskih in geodemografskih podatkov (Lyon 1994, 139). Že leta 1930 je IBM kot eno izmed prvih podjetij na svetu predstavilo in začelo tržiti komercialne rešitve za tovrstno nadzorovanje potrošnikov (uporaba predhodnikov računalnikov pri analizi zbranih podatkov). Z zahtevo po svobodi informacij (v ZDA so sprejeli *Freedom of Information Act*) so postali javno dostopni tudi podatki iz popisov prebivalstev; te podatke pa so nato povezovali s komercialno zbranimi podatki. Batagelj na primer navaja, da je eden največjih ponudnikov podatkovnih baz o potrošnikih Abacus Alliance iz ZDA leta 1997 združeval podatke o nakupih potrošnikov, ki so v tem letu opravili več kot dve milijardi transakcij (Batagelj 1997).

S pojavom postfordističnih modelov proizvodnje, kjer se pomembna okolica organizacije vse bolj širi, in novih menedžerskih konceptov je nadzor potrošnikov postal še pomembnejši. Koncept *Just in Time*, ki skuša zagotoviti natančno preskrbo trga glede na potrebe, ter odpravlja potrebe po vzdrževanju zalog, prav zahteva potrošniški nadzor. Podobno zahteva tudi koncept *Total Quality Control*, ki skuša v izdelek že med samim proizvodnim procesom vgraditi želje potrošnikov.

Pomena zbiranja čim več podatkov o potrošnikih pa so se podjetja začela še bolj zavedati v letih 1980 do 1992, ko je pošiljanje oglasov po pošti v ZDA tako naraslo, da je postal učinek direktnega marketinga zaradi zasičenosti potrošnikov z oglasno pošto premajhen. Podjetja so zato začela potrošnike ločevati po geografskih značilnostih, saj so ugotovila, da poštna številka potrošnike v ZDA dokaj dobro ločuje po premožnosti; revno in bogato prebivalstvo namreč v ZDA živita precej bolj narazen kot npr. v Sloveniji. Pozneje so začeli potrošnike deliti še glede na socialne, psihološke in demografske značilnosti ter tudi voditi statistike o njihovi odzivnosti (t. i. *responsegraphics*) (Batagelj 1997). Današnja gibanja se bližajo čedalje bolj individualni obravnavi potrošnikov, na primer pošiljanju personificiranih pisem

oz. reklam, to pa seveda potegne za sabo potrebo po zbiranju čim več podatkov o posameznem potrošniku. Kljub temu, da je zbiranje podatkov o potrošnikih na videz namenjeno potrošnikom v prid, saj služi prilagajanju ponudbe podjetja potrošnikovim okusom in željam, pa lahko na podlagi zbranih podatkov prihaja do njihove diskriminacije. Tako zaradi kupne moči, kakor tudi zaradi zaznanega potrošniškega okusa.

Pri tovrstnem zbiranju in analizi podatkov je uporaba informacijske tehnologije nepogrešljiva. Posebej nepogrešljiva pa je uporaba informacijske tehnologije pri t. i. razpršenem (decentraliziranem) nadzoru, saj je z njeno pomočjo mogoče podatke izjemno učinkovito povezovati.

Nadzor in informacijska tehnologija

Nadzor bi obstajal tudi brez informacijske tehnologije, vendar pa je le-ta nadzorovanje poglobila in okrepila. Značilen primer prednosti uporabe tehnologije je popis prebivalstva.

Popisi prebivalstva so bili za države vedno izjemno pomembni, vendar tudi izjemno zapleteni. Največji problem ni bilo zbiranje podatkov, pač pa njihova analiza. Razvrščanje, katalogizacija in preštevanje podatkov je bila pred izumom računalnika izjemno dolgotrajna naloga, saj so morali vse analize opravljati ročno. Konec 19. stoletja pa je Herman Hollerith izumil posebno napravo za obdelavo podatkov. Poimenovali so jo Hollerithov stroj (ang. *Hollerith machine*) in velja za predhodnika računalnika. Hollerithov izum so za analizo popisnih podatkov prvič uporabili pri ameriškem popisu prebivalstva leta 1890 in pri tem prihranili okrog pet milijonov dolarjev. Uporaba Hollerithovih strojev je torej analizo podatkov pocenila in pospešila. To so kmalu spoznale ne samo vlade drugih držav, pač pa tudi različna podjetja, ki so začela za analizo svojih podatkov (o strankah in potrošnikih) uporabljati tovrstne naprave.

Vendar pa hitrejša in cenejša analiza ni prinesla samo kupa prednosti, pač pa tudi nove nevarnosti, ki se jih pred pojavom te tehnologije ni nihče dobro zavedal. Dvanajstega aprila 1933 so namreč v tretjem rajhu začeli popisovati prebivalstvo, eden izmed namenov popisa je bil tudi identifikacija judovskega prebivalstva. Pri tej identifikaciji so si nacisti pomagali s Hollerithovimi stroji,

identifikaciji pa so pozneje sledile zaplembe premoženja in deportacije (Black 2002, 70, 77).

Gary T. Marx zaznava pri sodobnih elektronskih tehnologijah za nadzor tele značilnosti: so nevidne oz. malo vidne, nenamerne (niso usmerjene k nekemu natančno določenemu cilju), so bolj kapitalsko kot delovno intenzivne, decentralizirane ter niso usmerjene k specifičnemu posamezniku, pač pa vključujejo obravnavanje posameznikov po kategorijah (Lyon 1994, 68).

Benthamov načrt Panoptikona iz leta 1791 je predvideval optični nadzor, v informacijski družbi pa vidnost ni več samo optična. Večina današnjega nadzora je nevidnega, kajti pojavlja se na območju digitalnih signalov. Pojavlja se v vsakodnevnem življenju, pri opravljanju vsakdanjih opravil. Leta 1983 je David Burnham 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, uporabi mobilni telefon ..., avtomatski sistemi ali institucije ta dogodek *zaznajo* in *zabeležijo*. Elektronska sled je torej informacija, ki se shranjuje rutinsko in kaže dejavnost nekega posameznika. Večina teh podatkov, Burnham jih je poimenoval tudi *transakcijski podatki*, se zapisuje in vsaj nekaj časa tudi hrani. Pomembno je poudariti, da imajo sodobni nadzorovalni sistemi poleg shranjevanja tudi zmožnost kreacije in destrukcije podatkov ter informacij, zato ob tem seveda nastaja vprašanje, ali zaupati shranjenim podatkom (Lyon 1994, 59).

Vendar pa je povečana moč nadzorovanja v tem, da je tako zbrane podatke mogoče *povezati*. S povezavo in njihovo obdelavo lahko pridemo do novih vrednih podatkov in informacij, kar je za posameznika lahko škodljivo ali celo nevarno – zaradi ogrožanja njegovih pravic (Čebulj 1992, 8). Prav povezavo in kombiniranje različnih podatkov pa omogočajo sodobne informacijsko-komunikacijske tehnologije. Zato se lahko zgodi (če podatki niso ustrezno zavarovani), da naključno ali z nekim namenom zbrani podatki postanejo dostopni osebam ali institucijam, ki jih niso pooblaščene uporabljati, ali pa ti subjekti začnejo podatke uporabljati za drugačne namene. Zaradi tega med državljani upravičeno obstaja bojazen, da imajo morda različne državne institucije ali posamezniki dostop do podatkov, zbranih za druge namene, poleg tega pa

različne baze med seboj nepovezanih podatkov s pomočjo identifikacijskih oznak[10] povezujejo in tako podatke ter informacije med seboj kombinirajo (Webster 1995, 68 ter Raab 1993, 89). Vsekakor nadaljnji razvoj informacijske tehnologije možnost zapisovanja in povezovanja elektronskih sledi samo še stopnjuje.

Rule ugotavlja, da spremljata razvoj nadzorovalnih sistemov dva nevarna trenda, zaradi katerih se posamezniki ne zavedajo obsega nadzorovanja v tolikšni meri, kot bi se ga lahko sicer. Po eni strani posamezniki s svojimi dejanji samodejno sprožajo te sisteme (npr. z nakupom s kreditno kartico, vstopom v vidno polje nadzorne kamere ...), hkrati pa ti sistemi podatke in informacije tudi iščejo in preverjajo sami, predvsem iz sekundarnih virov (v Lyon 1994, 40–42). Posredno zbiranje osebnih podatkov je zaradi mogočih netočnosti in napak, predvsem pa zaradi tega, ker posamezniku ne omogoča pregleda nad uporabo njegovih osebnih podatkov, problematizirano tudi v 8. členu slovenskega *zakona o varstvu osebnih podatkov*, ki določa, da se smejo osebni podatki načeloma zbirati samo neposredno od posameznika.

Poleg tega računalniki skupaj z naprednimi statističnimi tehnikami in tehnikami izkopavanja podatkov (ang. *data mining*) vzpostavljajo nove razsežnosti nadzora. Uporaba računalniške tehnologije pa ta proces lahko nadgradi tudi s sistemi umetne inteligence, kar pomeni preskok na novo raven, na raven *preventive* in *predvidevanja*. Panoptična tehnologija tako ne čaka, da se zgodi neko dejanje oz. dogodek, pač pa ukrepa že vnaprej na podlagi podatkov in predvidevanj. S tem pa je ogroženo eno temeljnih pravnih demokratičnih načel, namreč domneve nedolžnosti, odpirajo pa se tudi nove možnosti za različne oblike diskriminacije na podlagi zaznav in ocen sistemov umetne inteligence. Kljub vsemu pa ni dvoma da postaja preventiva čedalje bolj pomembna usmeritev v razvoju sodobnih nadzorovalnih sistemov.

[10] V Sloveniji je to v nekaterih primerih npr. *EMŠO* – enotna matična številka občana, v ZDA *Social Security Number*, v Kanadi *Social Insurance Number*, v Veliki Britaniji uporabljajo *British National Insurance Number*, v Avstraliji *Tax File Number* itd. Zanimivo je, da je bila marsikatera izmed teh identifikacijskih oznak prvotno razvita za zagotavljanje družbenih pravic, šele pozneje pa so se zavedeli, da jih je mogoče uporabiti za povezovanje podatkov.

Elektronski panoptikon

James Rule ugotavlja, da so za omejitev sodobnih sistemov nadzora pomembne štiri stvari: velikost datotek, ki jih sistem lahko hrani, stopnja, do katere so lahko ti sistemi centralizirani, hitrost pretoka podatkov in informacij med točkami v sistemu in število stičnih točk med sistemom in subjektom. Uporaba računalnikov je moč nadzorovalnih sistemov izjemo povečala zato je Rule prepričan, da nas od družbe popolnega nadzora loči samo omejena zmogljivost nadzorovalnih sistemov (v Lyon 1994, 51–57).

Če se vrnemo k Foucaultovi teoriji, lahko ugotovimo, da je najpomembnejša značilnost panoptičnega nadzora njegova nezaznavnost in asimetričnost. Nadzor, ki ga posamezniki ne morejo zaznati, vedo pa, da je mogoč, ima namreč učinek podrejanja s pomočjo negotovosti. Zato je zanimiva tudi Mertonova teorija samoizpolnjujoče se prerokbe. Merton namreč pravi, da se »ljudje ne odzivajo samo na objektivne značilnosti določenih razmer, temveč in v določenih trenutkih predvsem na pomen (smisel), ki ga imajo razmere za njih« (v Gantar 1993, 62). Po Mertonu samoizpolnjujoča se prerokba deluje tako, da napačno ali nerealno opredeljene razmere povzročijo novo obnašanje, to pa povzroči, da se napačna opredelitev razmer uresniči. Ni torej pomembno, kakšne razmere v resnici so, pač pa, kako jih ljudje dojemajo (v Gantar 1993, 63). Močnik gre tu še dlje. V analizi razmerja med vednostjo in verovanjem podobno kot Merton ugotavlja, da lahko popolnoma neresnična izjava postane resnična če »zadosti ljudi verjame v njeno resničnost« (Močnik 1985, 21). Za naivneže, ki naj bi verjeli tej neresnični izjavi, Močnik uporabi izraz »hipotetični idioti«. Po njegovem neresnična izjava ne postane resnična samo v primeru, če ti hipotetični idioti zares obstajajo, ampak tudi, če je dovolj ljudi, ki *domnevajo,* da obstajajo hipotetični idioti – in rezultat je enak, kot če bi hipotetični idioti tudi zares obstajali. Ni torej nujno, da posameznik verjame neresnični izjavi – lahko se zaveda njene neresničnosti – dovolj je že njegova domneva, da vsi drugi verjamejo v njeno resničnost in nato deluje na podlagi svojih predvidevanj o njihovem ravnanju. Po Močniku je namreč »verovanjska funkcija izpolnjena tudi, če se omejuje zgolj na vero v subjekt, ki se zanj verjame, da verjame« (Močnik 1985, 23).

In prav v tem se kaže totalitarni potencial sodobnih nadzorovalnih tehnologij, saj lahko podobno deluje tudi prepričanje o obstoju nadzora, ki ga te tehnologije omogočajo. Kakor namreč ugotavlja poročilo Privacy & Human Rights 1999, imajo sodobne tehnologije nadzora močan samocenzurni učinek (t.i. »*chilling effect*«), saj lahko ljudi odvrnejo od »izstopanja« oz. uveljavljanja nekaterih pravic, na primer pravice do demokratičnega protesta (Banisar et al. 1999). Zato je upravičeno vprašanje, ali je elektronsko nadzorovanje oziroma že sam njegov obstoj panoptična moč.

Vsekakor računalniška informacijsko-komunikacijska tehnologija potencialno ogroža pravice in svoboščine posameznikov, predvsem pa lahko njena uporaba spremeni ravnotežje moči v družbi. Po eni strani je namreč dostop do baz podatkov povezan z močjo oziroma je monopoliziran, po drugi strani pa vzpostavitev velikega decentraliziranega nadzorovalnega sistema tudi zahteva finančni in časovni vložek. Kakor ugotavljajo avtorji poročila Privacy & Human Rights 1999, se nadzor redno izrablja in to celo v najbolj demokratičnih državah. »Glavne tarče so politični nasprotniki, novinarji in borci za človekove pravice,« ugotavlja omenjeno poročilo (Banisar et al. 1999). Kakor navaja poročilo o kršitvah človekovih pravic, več kot 90 držav nezakonito nadzoruje komunikacije političnih nasprotnikov, borcev za človekove pravice, novinarjev in sindikalistov. Posebej zaskrbljujoče je tudi čedalje večje število kršitev zasebnosti v zasebnih podjetjih, pri čemer imajo, kakor ugotavlja poročilo, vodilno vlogo podjetja iz ZDA.

Množični podatkovni nadzor se ponavlja rutinsko in je namenjen odkrivanju oseb, ki bi utegnile koristiti kakšni organizaciji oz. za katere organizacija ugotovi, da jim je vredno posvetiti posebno pozornost. Gre za to, da posameznika uvrstijo v neko kategorijo, kjer je na podlagi svojih karakteristik, ne pa dejanj, označen za sumljivega oz. vrednega pozornosti. Postopek – imenuje se *profiliranje* – so začeli na veliko uporabljati tudi v ZDA po 11. septembru. To sproža mnoga vprašanja, recimo že omenjeni problem domneve nedolžnosti, saj je neki posameznik tako označen za krivega, dokler ne dokaže svoje nedolžnosti (namesto da bi bilo nasprotno).

Ker je nadzorovanje čedalje bolj obsežno, nezaznavno, instrumentalizirano, neselektivno in preventivno, lahko spodkopava človekove pravice in svoboščine. Zaradi panoptičnih učinkov sodobnega, s

tehnologijo podprtega nadzora Charles D. Raab trdi, da sta odsotnost (oblastnega) nadzorstva (posameznikov) in varstvo zasebnosti *nujna pogoja* za liberalno in participacijsko demokracijo (Raab 1997, 161). Vsekakor je nadzor značilen primer kolizije med svobodo in omejevanjem svobode. Omejevanje svobode je v življenju v skupnosti do neke mere nujno, po drugi strani pa je nadzor posameznikov tesno povezan z močjo. Vendar pa mora biti moč v demokratični družbi podvržena demokratičnemu nadzoru, da ne prihaja do zlorab.

Nadzor in zasebnost

Razvoj tehnologije je omogočil povečanje in pocenitev zbiranja in obdelave podatkov ter informacij, zato je nadzor lahko postal večji. Hkrati je, predvsem zaradi nadzorovanja potrošnikov, prišlo do tega, da imajo podatki in informacije, ki so bili včasih popolnoma vsakdanji in nezanimivi, zdaj veliko tržno vrednost.

Poleg tega se nadzor globalizira. Predvsem v zadnjem času je opaziti globalizacijo mednarodnih varnostnih in administrativnih sistemov, pa tudi globalizacijo komercialnega nadzorovanja. Napačno je tudi mišljenje, da je uporaba sodobnih tehnologij nadzora omejena samo na gospodarsko razvite države (ki imajo večinoma razvite tudi demokratične in pravne standarde), saj poročilo Privacy & Human Rights 1999 z zaskrbljenostjo ugotavlja, da se povečuje izvoz tehnologij nadzora v države tretjega sveta.

Če je po eni strani v sodobni družbi opaziti močne težnje po čim večjem ali celo popolnem nadzoru, pa po drugi strani sodobna demokratična družba visoko ceni človekovo individualnost. Ključna sestavina demokratične države so *človekove pravice in temeljne državljanske svoboščine*. Spoznanje, da so temeljne pravice univerzalne in da državni oblasti določajo *meje*, v katerih se lahko giblje, se je uveljavilo v času razsvetljenstva in meščanskih revolucij, predvsem med francosko revolucijo. Če je torej po eni strani demokratična država omejena pri poseganju v pravice in svoboščine posameznikov, pa je izhodišče totalitarne države vzpostavitev skupnosti, ki se kot več vredna dobrina dviga nad posameznika in si ga podreja. V totalitarni državi je pomemben »*interes skupnosti*, nadrobno izdelana propaganda, *skrbno nad-*

zorovanje (*vseh in vsakogar*) in ne nazadnje še sredstva prisile« (Kušej, Pavčnik in Perenič 1992, 53).

Čeprav stopnjo nadzora državljanov mnogi avtorji povezujejo s stopnjo demokracije v družbi (povezanost je obratno sorazmerna), je paradoksalno panopticizem 19. in 20. stoletja rasel hkrati z naraščanjem družbenih pravic (Lyon 1994, 76). Po drugi strani pa zgodovinske izkušnje kažejo, da sta povečan nadzor in totalitarizem korakala z roko v roki (npr.: nacistična, fašistična in stalinistična država), liberalna demokratična država pa je – vsaj deklarativno – visoko cenila pravice posameznika in omejevala nadzor nad njim (Raab 1997, 161). To je med drugim tudi razlog za to, da civilna družba in politični aktivisti povezujejo nadzor (države) s totalitarizmom in varovanje zasebnosti z demokratičnostjo države. Vendar se pri tem mnogokrat pozablja, da so panoptični učinki nadzora prisotni tudi ali pa celo še v večji meri v t.i. demokratični državi. Po Foucaultu je panoptikon politična tehnologija, ki deluje na podlagi subtilnih prisil, ponotranjenja oblasti in omogoča vzdrževanje oblasti. Foucault pravi, da je sodobna oblast disciplinska oblast, katere cilj so krotka telesa, nadzorovanje pa je zato namenjeno discipliniranju in podrejanju posameznikov. Zato se lahko upravičeno zdi, da ima panoptikon sodobne disciplinske oblasti podobne učinke kot odkriti totalitarizem, le da nekako deluje bolj prikrito, hinavsko.

Za razliko od nadzora kot politične tehnologije za discipliniranje posameznikov pa sta t.i. administrativni in potrošniški nadzor na videz precej bolj prijazna do posameznika. Pri prvem ima opazovanje posameznikov namen uravnavati njihove dejavnosti in njihovo življenje, značilen primer je na primer določanje obsega različnih socialnih pravic ali določanje prednosti zadovoljevanja potreb državljanov, nadzor potrošnikov pa je na videz še bolj prijazen do posameznika, saj predvideva njegovo svobodo in postavlja v ospredje njegove želje. Nadzor potrošnikov pogosto vključuje tudi izgradnjo t.i. skupnosti potrošnikov, prek raznih kartic zaupanja in klubov zvestobe. Dokument *Privacy on the Internet – An Integrated Approach to On-line Data Protection* tako navaja, da spletne strani pogosto uporabljajo t.i. programe zvestobe, kot npr. igre, anketne vprašalnike in spletne biltene, s pomočjo katerih pridobivajo osebne podatke o svojih obiskovalcih (Data Protection Working Party 2000, 18). 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 primer so reklame prilagojene zaznanemu okusu in predvidenim potrebam potrošnika.

Vendar pa ima tudi ta vrsta nadzora, posebej še v povezavi z analizo podatkov in poznejšim profiliranjem, lahko negativne posledice. Na področju potrošniškega nadzorovanja namreč lahko prihaja do diskriminacije potrošnikov. Takšna diskriminacija se lahko dogaja na primer pri izdaji kreditnih kartic ali kartic ugodnosti, predvsem pa pri uporabi marketinškega koncepta dinamičnega določanja cen (ang. *dynamic pricing*). Dinamično določanje cen je definirano kot »kupovanje in prodaja blaga in storitev na prostih trgih, kjer so cene odvisne od ponudbe, povpraševanja in spreminjajočih se potrošniških preferenc« (Srivastava 2001, 1–2). Ta model 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.

Eden izmed poučnih primerov posledic uporabe takšnega modela za potrošnike se je zgodil konec leta 2000. Nekateri uporabniki spletne trgovine Amazon.com so namreč ugotovili, da za enake izdelke plačujejo več kot drugi in pojavil se je sum, da je cena odvisna od njihovih potrošniških preferenc (bolj zvestim kupcem naj bi zaračunavali višje cene). Amazon je priznal, da so testirali vpliv cene na nakupne navade potrošnikov, vendar pa naj bi bilo to testiranje omejeno, potrošniki pa izbrani povsem naključno in ne na podlagi njihovih potrošniških preferenc (Bicknell 2000). A dinamično določanje cen že obstaja v fizičnem svetu, zato ne preseneča napoved analitika organizacije Forrester Research, da bo »personalizirano določanje cen (zagotovo) del naravnega razvoja spleta« (Bicknell 2000). Ta pristop pa bo zaradi zagotavljanja čimvečje učinkovitosti zagotovo temeljil na analizi podatkov o potrošnikih.

Dodatni problem potrošniškega in administrativnega nadzorovanja pa je tudi ta, da si posamezniki izstopa (zanj se pogosto uporablja tudi angleški izraz *opt-out*) iz tovrstnega 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 izstop 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 podjetja. Potrošniki in državljani tako živimo v svetu, v katerem se moramo nujno odpovedati delu svoje zasebnosti na račun večje funkcionalnosti in obvladovanja kompleksnosti življenja v sodobni družbi.

Varstvo zasebnosti

Zasebnost je temelj človeškega dostojanstva in drugih vrednot, kot npr. svobode združevanja in svobode govora, nekateri avtorji pa celo trdijo, da so vse človekove pravice neke vrste posamični vidiki pravice do zasebnosti. Pravica do zasebnosti je sicer temeljna, vendar pa ne absolutna. V sodobni družbi pa je postala ena najpomembnejših človekovih pravic, ugotavlja poročilo Privacy & Human Rights 1999.

Pravica do zasebnosti je najpogosteje določena kot »meja, do katere družba lahko vdre v posameznikove zadeve« (Banisar et al. 1999). Vendar pa zasebnost ni enodimenzionalen pojem; različni avtorji vidijo več dimenzij zasebnosti. Čebulj navaja tri sestavine zasebnosti: *zasebnost v prostoru* (možnost posameznika, da je sam), *zasebnost osebnosti* (svoboda misli, opredelitve, izražanja) in *informacijska zasebnost* (možnost posameznika, da obdrži podatke in informacije o sebi, ker ne želi, da bi bili z njimi seznanjeni drugi) (Čebulj 1992, 7). Poročilo Privacy & Human Rights 1999 pa loči tele vrste zasebnosti: *informacijsko zasebnost*, *zasebnost telesa*, *zasebnost komunikacij* in *prostorsko zasebnost*. V sodobni družbi sta najbolj ogroženi informacijska zasebnost in zasebnost komunikacij.

Po poročilu Privacy & Human Rights 1999 ogrožajo zasebnost trije pomembni trendi: *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 hitro lahko spremenijo v drugo obliko).

Vsi ti procesi so privedli do potrebe po učinkoviti zakonodaji za zaščito zasebnosti. Danes skoraj vsaka država na svetu priznava v ustavi pravico do zasebnosti[11], se pa po posameznih državah ra-

[11] Slovenska ustava opredeljuje v členih od 35. do 38. varstvo pravic zasebnosti in osebnostnih pravic, nedotakljivost stanovanja, varstvo tajnosti pisem in drugih občil ter varstvo osebnih podatkov.

zlikuje obseg priznavanja te pravice. Minimum, ki ga zakonodaja priznava, je nedotakljivost stanovanja in tajnost komunikacij, čedalje več držav pa razširja pravico do zasebnosti tudi na dostop in obravnavo osebnih podatkov o posameznikih.

Začetki zakonodaje, ki ščiti zasebnost, segajo že v leto 1361, ko je zakon *Justices of the Peace Act* predvidel kazni za osebe, ki so skrivaj opazovale druge posameznike ali jim prisluškovale. Leta 1765 je britanski lord Camden protestiral, ker so preiskovalci želeli vstopiti v njegovo hišo in zaseči neke listine. Parlamentarec William Pitt je ob 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.« (Banisar et al. 1999)

Leta 1776 je švedski parlament sprejel *zakon o dostopnosti javnih zapisov*, ki je določal, da morajo biti vsi podatki, ki jih zbere država, uporabljeni izključno za zakonite namene. Leta 1890 pa sta ameriška pravnika Samuel Warren in Louis Brandeis opredelila zasebnost kot pravico posameznika, da se ga pusti pri miru (Warren in Brandeis 1890).

Temelje varovanja zasebnosti v sodobnem času je postavila *splošna deklaracija človekovih pravic*, ki jo je sprejela in razglasila generalna skupščina Združenih narodov leta 1948.[12] Potreba po učinkoviti zaščiti zasebnosti se je pojavila predvsem zaradi razvoja informacijsko-komunikacijskih tehnologij, zato ni naključje, da je interes za zaščito zasebnosti narasel v 60. in 70. letih prejšnjega stoletja s pojavom sodobne informacijske tehnologije. Čebulj ugotavlja, da je bila zasebnost posameznika sicer ogrožena že pred pojavom informacijsko-komunikacijskih tehnologij in računalniških zbirk podatkov, da pa je nova tehnologija ogroženost zasebnosti samo stopnjevala in privedla do tega, da so se ljudje začeli zavedati nevarnosti bolj kot v času ročno vodenih evidenc (Čebulj 1992, 16). Tehnologija je namreč pospešila zbiranje in tudi obdelavo podatkov, zmožnosti nove tehnologije so zato zahtevale posebna pravila za obravnavo osebnih podatkov. Prvi zakon o varstvu osebnih podatkov je leta 1970 sprejela Zvezna republika Nemčija, pozneje pa

[12] »Nikogar se 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 takšnim vmešavanjem ali takšnimi napadi.« 12. člen *splošne deklaracije človekovih pravic*.

še Švedska (1973.), ZDA (1977.) in Francija (1978.). Močan pritisk na oblikovanje ustrezne zakonodaje za zaščito zasebnosti v drugih državah izvajajo danes direktive Evropske unije.

Kakor ugotavlja poročilo Privacy & Human Rights 1999, so razlogi za sprejem zakonodaje za zaščito zasebnosti želja po popravi starih krivic (z namenom, da bi preprečili ponovno vzpostavitev totalitarizma), spodbujanje elektronskega poslovanja in uskladitev zakonodaje s evropsko zakonodajo. EU tako spodbuja predvsem model vzpostavitve sistema krovne zakonodaje, sprejem področnih zakonov in samoregulacijo s sprejemom ustreznih praks (ang. *codes of practice*) pa podpirajo ZDA, Japonska in Singapur. Rezultati tega so, da so npr. zaposleni v ZDA na veliko slabšem glede zasebnosti na delovnem mestu. Prihaja celo do tega, da si podjetja na podlagi dejstva, da so zbrala osebne podatke posameznikov, te podatke lastijo in celo skušajo omejevati pravice posameznikov v zvezi njimi (npr. vpogled in brezplačno posredovanje, popravljanje zastarelosti in netočnosti itd.).

Pravno so največja nevarnost pri zbiranju podatkov zlasti nenatančnost, napačnost, nepopolnost ali neažurnost zbranih podatkov (Čebulj 1997, 8), poleg tega pa se lahko podatki zbirajo preventivno, »za vsak primer«, kar lahko prejudicira pravni proces (npr. policijske baze ali baze varnostnih služb). Problematičen je tudi obstoj baz osebnih podatkov, za katere posamezniki niti ne vedo, da obstajajo, ali pa vanje nimajo vpogleda.

Zato je leta 1974 generalni sekretar OZN v poročilu *Človekove pravice in znanstveni in tehnološki razvoj – Uporaba elektronike, ki lahko vpliva na pravice oseb, in omejitve, ki bi morale biti podane v demokratični družbi pri takih uporabah*,[13] priporočil predvsem tri načela, ki naj bi jih vsebovala zakonodaja s področja varovanja informacijske zasebnosti: *načelo relevantnosti*, ki zahteva, da se o posamezniku zbirajo samo tisti podatki, ki so nujno potrebni za dosego namena, zaradi katerega se zbirajo; *načelo notifikacije*, ki zahteva, da bo posameznik predhodno seznanjen o tem, kateri podatki se o njem zbirajo, shranjujejo in obdelujejo; ter *načelo privolitve*, ki pravi, da naj se zbirajo samo tisti podatki, za katere je posameznik privolil, da se zbirajo.

[13] Omenjeno poročilo je generalni sekretar OZN leta 1974 pripravil za ekonomsko socialni svet.

Pri vzpostavljanju zakonskega varstva posameznikove zasebnosti seveda nujno trčimo na že omenjeno kolizijo med svobodo in poseganjem vanjo. Vsekakor pretirano omejevanje posegov v zasebnost iz različnih vzrokov ni mogoče, morda pa tudi ni smiselno. Mellors zato ugotavlja, da »najboljša zaščita ni ta, da oni (op.p.: 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« (Mellors v Raab 1997, 158). Glavna sestavina zaščite informacijske zasebnosti je torej *nadzor pretoka in posredovanja podatkov, ki se nanašajo na nekega posameznika*. Zato se sodobna zakonodaja za zaščito zasebnosti ukvarja predvsem s transparentnostjo *uporabe* osebnih podatkov. Zbiranje podatkov se torej ne omejuje, vendar mora imeti zakonsko podlago, namen zbiranja in uporaba podatkov pa morata biti vnaprej znana in transparentna.

Zaradi tega se pravica do informacijske zasebnosti, ki je ena izmed najbolj ogroženih, 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 določenih podatkov in informacij niso pooblaščeni. Načelo transparentnosti uporabe osebnih podatkov se čedalje bolj uporablja tudi na internetu, predvsem v obliki izjave 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.[14]

[14] Seveda pa sama izjava o zasebnosti ne zagotavlja, da bo zasebnost obiskovalca spletne strani res močno varovana. Nekatere izjave so namreč namenoma zapisane zelo dvoumno, lahko pa je v njih celo preprosto zapisano, da bodo zbrani podatki uporabljeni za katerekoli potrebe in namene.

ZASEBNOST V VIRTUALNEM PROSTORU

Če so računalniki prinesli kakovostno spremembo v nadzorovanje, to še toliko bolj velja za računalniška omrežja, predvsem za internet.

Na začetku 90. let prejšnjega stoletja so bili nekateri sociologi prepričani – še bolj pa uporabniki interneta – da je internet zaradi svojih lastnosti[15] že po svoji naravi odporen proti nadzorovanju države. Po njihovem mnenju naj bi se tehnologija razvijala proti čedalje večji svobodi in neodvisnosti od državnega nadzora (Boyle 1997). To je seveda veljalo samo na začetku, ko internet še ni bil močno razširjen in je bil za državo ter njene organe pa tudi za kapitalistične korporacije nekaj novega in neobvladljivega. Vendar pa Boyle ugotavlja, da je pojav »tehnologij svobode« vedno potegnil za sabo poostritev mehanizmov nadzora. Danes različne državne zakonodaje obvladujejo internet čedalje bolj, državni organi in podjetja pa celo na novo odkrivajo privlačnost nadzorovanja po internetu. Če so bili prvi zakonski posegi v internet razumljeni kot omejevanje svobode, lahko predvidevamo, da bodo uporabniki sami čedalje bolj zahtevali zakonodajno regulacijo interneta zaradi zaščite svojih pravic. Če je na začetku kazalo, da je na internetu neobstoj s strani države postavljenih pravil priložnost za razvoj svobode, pa se danes že kaže, da popolna neregulacija – predvsem uporabe nadzorovalnih mehanizmov – dopušča možnost različnih zlorab in s tem omejitev svobode posameznikov. Do tega prihaja zaradi možnosti razmaha kiberkriminala, pa tudi zaradi nevarnosti privatizacije nadzorovalnih sistemov s strani ponudnikov dostopa, predvsem pa ponudnikov storitev in vsebin.

Glede panoptične moči interneta je treba opozoriti na dve pomembni lastnosti računalniške tehnologije. Računalniška omrežja nam-

[15] Te lastnosti so: tehnologija medija, geografska razpršenost in vsebina; Boyle jih imenuje »internetna sveta trojica« (Boyle 1997).

reč omogočajo decentraliziran nadzor, saj lahko omogočijo povezovanje formalno ločenih nadzornih sistemov prek telekomunikacijskih sredstev, prav tako pomembna lastnost računalnikov pa je tudi njihova zmožnost shranjevanja oziroma arhiviranja podatkov, kar omogoča gradnjo arhivov oziroma dosjejev. Če se je še pred nekaj leti zdelo, da je internet tehnologija svobode, se danes zdi, da je panoptičnost že vgrajena vanj.

Podobno kot v fizičnem svetu tudi na internetu izvajajo nadzor različni subjekti. Čedalje bolj aktivno vlogo pri nadzoru na internetu imajo države in njihovi organi, sploh po terorističnih napadih 11. septembra na ZDA. Nadzorovanje potrošnikov oziroma zbiranje podatkov o potrošnikih po internetu je prav tako zanimivo za podjetja. Ta imajo tudi velik interes za nadzorovanje *on-line* aktivnosti svojih zaposlenih, poleg tega pa se nadzorovanja po internetu poslužujejo tudi *hekerji*[16]. V nasprotju z državo in podjetji, ki se nadzora poslužujejo z natančno določenimi nameni in cilji, pa hekerji navadno ne vdirajo v računalnike nujno samo zaradi finančne koristi, pač pa bolj za zabavo, zaradi samodokazovanja ali povzročanja škode.

Organizacija Privacy Rights Clearinghouse ugotavlja, da »pravzaprav ne obstaja nobena *on-line* aktivnost, ki bi omogočila popolno zasebnost« (Privacy in Cyberspace 1998). Na internetu obstajajo različni načini ogrožanja zasebnosti. V nadaljevanju bomo bolj podrobno obravnavali številne načine, kako se lahko ogroža zasebnost na internetu.

Problem računalniške tehnologije in interneta je predvsem v tem, da tehnologija že sama na sebi, zaradi svojih lastnosti, omogoča nekatere zlorabe zasebnosti. Pri tem sploh ne gre za to, da bi bila

[16] Za t. i. računalniške znalce, ki vdirajo v sisteme, se poljudno uporablja izraz hekerji (ang. *hacker*). Ta izraz opisuje osebo, ki ima o računalnikih veliko znanja, vendar tega znanja ne izkorišča za slabe namene, medtem ko se za osebe, ki to znanje zlorabljajo za napade na sisteme uporablja izraz kreker (ang. *cracker*). Poleg njih pa se vdorov v sisteme poslužujejo še t. i. skriptarji (ang. *script kiddie*). Gre za osebe, ki nimajo pretiranega računalniškega znanja, pač pa za vdore izkoriščajo znane varnostne luknje, ki so jih odkrili drugi ali uporabljajo javno dostopna vdiralska orodja. Navadno ne iščejo točno določenih žrtev, pač pa po internetu povsem naključno iščejo slabo zaščitene strežnike v katere potem poiskušajo vdreti. Vdiralci v sisteme sicer lahko vdirajo tudi s kriminalnimi ali terorističnimi nameni, zaradi industrijskega vohunjenja ali iz maščevanja, vendar gre pri večini teh oseb za samodokazovanje, zabavo ali vandalizem.

tehnologija že vnaprej zasnovana z namenom nadzorovanja (čeprav se je dogajalo tudi to), pač pa le za uporabo tehnoloških lastnosti, na način, ki omogoča nadzorovanje. Zaradi tovrstnih »stranskih učinkov« internetne tehnologije se tako danes na internetu zbira velikansko število osebnih podatkov in to brez privolitve oziroma celo brez vednosti posameznikov (Data Protection Working Party 2000, 19). Obstaja pa tudi nevarnost, da se zbrani podatki ne uporabijo za tisto, za kar so bili zbrani, temveč za druge namene. Pri bankrotu nekega podjetja namreč obstaja nevarnost, da bodo za poplačilo dolgov uporabili denar od prodaje osebnih podatkov, pa čeprav so bili podatki zbrani z zagotovilom, da ne bodo nikoli posredovani tretjim osebam brez izrecne privolitve posameznikov. Znan je primer podjetja Toysmart.com, ki je šlo v stečaj, za poplačilo dolgov pa so v stečajno maso vključili ravno tako zbrane osebne podatke (Morehead 2000).

Zbiranje podatkov in nadzor oziroma zlorabe zasebnosti so v virtualnem prostoru mogoči na več načinov. Posamezniki z uporabo računalniške in telekomunikacijske tehnologije v virtualnem prostoru puščamo sledove, tako namerno (npr. na svoji spletni strani, v javnem forumu itd.) kakor tudi nevede (npr. z obiskom spletne strani, z uporabo neke storitve ...). Hkrati pa obstaja tudi nevarnost prestrezanja podatkov in informacij, ki se prenašajo prek telekomunikacijskih sredstev, nevarnost vdora v računalniški sistem. Obstajajo tudi tehnike za prestrezanje informacij v neposredni okolici računalniškega oziroma telekomunikacijskega sistema. Vse te tehnologije nadzora si bomo v nadaljevanju ogledali nekoliko podrobneje, kljub temu pa se je treba zavedati, da zlorabe zasebnosti niso povzročene samo s tehničnimi sredstvi, pač pa tudi z različnimi goljufijami, ko skušajo napadalci žrtev prepričati oziroma pretentati, da jim posreduje dostop do sistema ali posreduje želene podatke oziroma informacije, ali pa se do želenih podatkov dokopljejo s tajnim opazovanjem (v zvezi s tem se uporablja angleški izraz *social engineering*). Tovrstno goljufanje navadno poteka tako, da se napadalci lažno predstavljajo oziroma si pridobijo zaupanje uporabnika, pozneje pa to zaupanje zlorabijo. Znani so primeri, ko so se napadalci lažno predstavili kot osebje tehnične pomoči in se tako dokopali do uporabniških gesel, zgodilo pa se je celo, da so postavljali lažne

spletne strani[17]. Uporabniki namreč večinoma ne vedo, da lokacija spletne strani v splošnem zapisu lahko vsebuje tudi uporabniško ime in geslo za dostop do strani v obliki http://ime:geslo@www.streznik.com. Seveda večina spletnih strani tega ne zahteva, saj je dostop prost za vse. Ker je do javno dostopnih spletnih strani mogoče dostopati z vpisom kateregakoli imena in gesla, seveda obstaja nevarnost, da uporabnik zamenja uporabniško ime s spletnim mestom. Hkrati je do spletnih strani mogoče dostopati tudi z vpisom IP številke strežnika, kar lahko uporabnika dodatno zmede.[18]

Pridobivanje informacij o računalniku, vključenem v omrežje

V omrežju se računalniki predstavljajo z IP številko oz. IP naslovom (ang. *IP address)*,[19] ki predstavlja virtualni naslov računalnika. IP naslov namreč pove, kje v omrežju se nahaja določen računalnik, s tem pa je znana tudi pot do njega. Računalnik je lahko vključen v internet neposredno, torej s svojim IP naslovom, lahko pa je »skrit« za posebnim vmesnikom NAT (ang. *Network Address Translation*), ki vključuje skupino več računalnikov v internet prek istega zunanjega IP naslova. IP naslov posameznega računalnika je lahko stalen (včasih se uporablja tudi izraz fiksni IP naslov), kar pomeni, da če se računalnik izključi iz omrežja, bo pri ponovni vključitvi ohranil isti

[17] Decembra 2002 se je pojavila spletna stran ebayupdates.com. Uporabniki nakupovalnega spletišča eBay so bili po elektronski pošti naprošeni, naj na spletno stran ebayupdates.com vpišejo številko svoje kreditne kartice in geslo. Seveda je bila spletna stran lažna in ni bila nikakor povezana s podjetjem eBay, namenjena pa je bila izključno kraji številk kreditnih kartic (Internet 2002).

[18] Uporabnik namreč lahko namesto npr. http://www.arnes.si vpiše tudi http://193.2.1.66/ oziroma celo http://www.trgovina.com@193.2.1.66/ – in v vseh treh primerih se mu bo prikazala Arnesova spletna stran. Seveda pa v nasprotju s prvim primerom, kjer je jasno, za katero spletno stran gre, v tretjem primeru na prvi pogled že ni več tako. Niz »www.trgovina.com« namreč pomeni uporabniško ime in ne naslova spletnega mesta. V nekaterih starejših različicah spletnih brskalnikov se je dalo uporabnika še bolj zmesti z zapisom znaka »@« v heksadecimalnem zapisu kot »%40« ter pretvorbo IP naslova v t.i. »dword« format. S takšnim preprostim trikom bi bilo povsem mogoče narediti kopijo kakšne znane spletne trgovine in tako zbirati osebne podatke zapeljanih uporabnikov. Več o tem v *How to Obscure Any URL*, http://www.pc-help.org/obscure.htm.

[19] IP številke so 32-bitne številke, najpogosteje predstavljene v decimalni obliki (ang. *dotted decimal notation*, v obliki xxx.xxx.xxx.xxx). Vsaka decimalna številka predstavlja 8 bitov binarnih podatkov, zato lahko zavzame vrednosti od 0 do 255.

IP naslov; lahko pa je dinamičen, kar pomeni, da mu bo pri vsaki vključitvi v omrežje dodeljen drugačen IP naslov, iz neke skupine prostih IP naslovov. Dinamični IP naslovi se večinoma uporabljajo pri klicnih dostopih do interneta (ang. *dial-up*), stalni IP naslovi pa večinoma za različne strežnike in računalnike, ki so v internet vključeni prek lokalnega omrežja, najete linije, ADSL povezave ali podobne stalne povezave. Očitno je, da je laže identificirati uporabnika s stalnim IP naslovom, saj je pri dinamično dodeljenih IP naslovih treba najprej ugotoviti, kateremu uporabniku je bil v danem trenutku dodeljen neki IP naslov, medtem ko je uporabnik stalnega IP naslova vedno enak. Po drugi strani pa identifikacija uporabnika za vmesnikom NAT ni tako preprosta, saj IP naslov predstavlja le vmesnik, ne pa tudi konkretnega uporabnika za njim.

Del internetne infrastrukture je tudi protokol za izmenjavo kontrolnih sporočil ICMP (ang. *Internet Control Message Protocol*), ta protokol pa je implementiran v ukazu *ping*, ki se uporablja za preverjanje funkcionalnosti povezave med dvema točkama v internetu. S pomočjo tega ukaza lahko uporabnik preveri, ali obstaja povezava med njegovim in nekim drugim računalnikom v internetu. Vendar pa je ukaz *ping* mogoče uporabiti tudi za preverjanje, ali je neki računalnik v nekem trenutku vključen v internet ali ne, posebej še v primeru, ko ima računalnik stalni IP naslov. Ni si težko predstavljati, da bi s pomočjo povsem preprostega periodičnega izvajanja ukaza *ping* delodajalec v podjetjih, kjer zaposleni pri delu uporabljajo računalnike, lahko preverjal, kdaj so zaposleni prižgali in kdaj ugasili računalnik, ter na podlagi tega lahko sklepal o času njihovega prihoda in odhoda iz službe. Še več, enako bi lahko za zaposlenega s stalnim IP naslovom lahko počel kdorkoli v internetu, od ljubosumnega partnerja do konkurence.

Vendar pa pri računalnikih, ki jih uporablja več uporabnikov ali ki so skriti za vmesnikom NAT, natančna identifikacija uporabnika z ukazom *ping* ni mogoča. To pomanjkljivost odpravljajo interaktivni sistemi, kot npr. ICQ, Yahoo Messenger, MSN Messenger itd., ki celo nekoliko podrobneje obveščajo o statusu uporabnika (ali je vključen v omrežje, ali je za računalnikom itd.). Seveda pa so to specializirani programi, ki jih uporabnik sam naloži na računalnik in se (oziroma naj bi se) tudi zavedal njihovih zmožnosti.

Elektronske sledi pri ponudniku dostopa do interneta

Med gibanjem po virtualnem prostoru puščajo uporabniki veliko elektronskih sledi, največ pa jih pustijo pri svojem ponudniku dostopa do interneta. Le-ta namreč lahko zapisuje *vse* dejavnosti posameznega uporabnika interneta (kdaj in katere storitve interneta je uporabljal), hkrati pa se vanj lahko zapiše tudi uporabniško ime (kar je pozneje mogoče povezati z uporabnikovo fizično identiteto), IP številka, ki jo je uporabljal in telefonska številka oziroma druga vstopna točka, prek katere se je povezal v internet. Ti podatki se zbirajo v t.i. datotekah aktivnosti (ang. *log files*). Pomen teh podatkov je spoznala tudi država. Tako od junija 2000 v ZDA deluje sistem *Carnivore* (uradno se imenuje DCS1000). To je poseben program, ki ga državni organi namestijo na strežnike ponudnika dostopa do interneta, sposoben pa je prestrezati vsa uporabnikova elektronska sporočila in beležiti vse njegove internetne dejavnosti (StopCarnivore 2000). Uvedba sistema je sprožila huda nasprotovanja ameriških uporabnikov interneta pa tudi ponudnikov dostopa do interneta, kljub temu pa je organizacija Privacy International takrat ocenila, da bo sistem v letu ali dveh nameščen na vse ponudnike interneta v ZDA (Privacy International 2000). Do tega je prišlo še hitreje, saj so ameriške vladne agencije teroristične napade 11. septembra 2001 hitro izkoristile za povečanje nadzora na internetu (McCullagh 2001a, Analysis 2001). Spletni časopis Wired News je že 12. septembra 2001 poročal, da so samo nekaj ur po terorističnem napadu agenti FBI začeli obiskovati ponudnike dostopa do interneta in elektronske pošte z zahtevami po namestitvi sistema Carnivore, pri tem pa sploh niso naleteli na veliko nasprotovanja (McCullagh 2001a).

Navadno imajo ponudniki dostopa do interneta v lasti tudi DNS strežnike (ang. *Domain Name System*, sistem, ki skrbi za pretvorbo imen domen v ustrezne IP naslove). To pomeni, da si lahko ponudnik dostopa do interneta beleži, katere spletne strani obiskuje neki uporabnik, in na podlagi tega izdela profiliranje uporabnikov. Obstaja še ena možnost za zbiranje podatkov o uporabniših okusih. Ponudniki dostopa do interneta imajo lahko v lasti tudi portale[20]

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

prek katerih zapisujejo, do katerih vsebin dostopa posamezni uporabnik. Danski 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 portal, 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).

Elektronske sledi pri ponudniku internetnih storitev in vsebin

Poleg datotek aktivnosti, ki jih vzdržujejo ponudniki dostopa do interneta, poznamo še datoteke aktivnosti, ki jih vzdržujejo ponudniki različnih storitev interneta (predvsem spletnih strani) beležijo pa dejavnosti svojih uporabnikov. V te baze podatkov se lahko zapišeta vsaj IP naslov uporabnika in spletna stran (oziroma podstran), ki jo uporabnik obiskuje, lahko pa tudi nekatere spremenljivke o uporabnikovem virtualnem okolju (ang. *environment variables*). Upravitelji spletnih strani tako lahko zapišejo npr. tip uporabnikovega spletnega brskalnika, operacijski sistem, ki teče na njegovem računalniku, vrsto vključenih jezikovnih podpor, s katere spletne strani je uporabnik prišel do njihove spletne strani itd. Sicer je res, da je nekatere od teh podatkov mogoče spremeniti ali zabrisati, vendar večina uporabnikov s temi postopki ni seznanjena. Poleg tega nekateri spletni brskalniki, na primer *Microsoft Internet Explorer* pošiljajo spletnim stranem nekoliko več podatkov o uporabnikovem okolju kot drugi. V zvezi s tem se uporablja izraz klepetavost brskalnikov (ang. *browser's chattering)*. V poročilu z naslovom *Privacy on the Internet – An integrated EU Approach to Online Data Protection* je bilo s primerjalno analizo različnih spletnih brskalnikov ugotovljeno, da *Internet Explorer* razkrije celo, ali ima uporabnik na svojem računalniku nameščene programske pakete Word, Excel in PowerPoint (Data Protection Working Party 2000, 14–15).

Dodatne možnosti odpira uporaba JavaScripta.[21] Na spletno stran je mogoče vključiti poseben program – ta deluje le takrat, kadar

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

uporabnik v spletnem brskalniku nima onemogočenega izvajanja JavaScripta – ki med obiskom spletne strani le-tej pošlje še več podatkov o uporabnikovem okolju, npr. resolucijo zaslona, nastavljeni časovni pas, ali ima uporabnik vključeno podporo za Javo,[22] katere priključne module (ang. *plug-in*) ima naložene, oceno hitrosti dostopa do interneta itd.

Te podatke večinoma uporabljajo za spremljanje obiskanosti spletnih strani oziroma drugih strežnikov, pa tudi za določanje tipa vsebine, ki jo bo spletna stran pošiljala uporabniku. S pomočjo teh podatkov namreč spletni strežnik lahko ugotovi stopnjo multimedijske opremljenosti uporabnikovega računalnika in glede na te podatke pošlje uporabniku spletno vsebino v ustreznem formatu (npr. ali lahko pošlje *flash* animacijo ali pa raje film v AVI formatu itd.). Iskalniki lahko na podlagi teh podatkov in podatkov o uporabljenih iskanih pojmih izvajajo profiliranje svojih uporabnikov (Data Protection Working Party 2000, 44). Hkrati pa pri zlorabah ali poskusih zlorab upravitelj spletne strani oziroma ogroženega sistema skupaj s ponudnikom dostopa do interneta na podlagi IP naslova in časa dostopa lahko ugotovi fizično identiteto zlonamernega uporabnika.

Upravitelj spletne strani s prej opisanimi tehnikami lahko ugotovi tudi število *obiskov* na posamezni spletni strani, ta podatek pa je pomemben za oglaševalce. Vendar pa pri uporabnikih, ki dostopajo prek klicnega dostopa, prehoda (ang. *gateway*), ali anonimnega zastopniškega programa (ang. *anonymous proxy*), ne more ugotoviti števila *različnih obiskovalcev*, saj posamezni obiskovalec lahko dostopa večkrat oziroma prek ene IP številke dostopa več različnih uporabnikov, kaj šele, da bi te obiskovalce natančno identificiral. Zato je Lou Montulli leta 1994 za podjetje *Netscape* razvil piškotke (ang. *cookies*).

Piškotki so majhni paketi podatkov, ki jih spletni strežnik pošlje spletnemu brskalniku, le-ta pa jih shrani na uporabnikov računalnik in jih vrne strežniku, ko ta to od njega zahteva. 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 vztrajne piškotke (ang. *persistent cookies*).

[22] Java je objektno orientiran programski jezik, ki ga je razvilo podjetje Sun Microsystems, zaradi svoje razširjenosti pa je primeren za izvajanje spletnih aplikacij.

Prvi potečejo na koncu brskalne seje, torej ko uporabnik zapre spletni brskalnik, drugi pa imajo čas trajanja daljši, lahko tudi več desetletij. Piškotek je strežniku dostopen ves čas trajanja (če ga seveda uporabnik prej ne izbriše). Razen 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 v zadnjem času, pomembno pa je, da piškotke tretjih spletnih strani večinoma uporabljajo oglaševalska omrežja, namenjeni pa so sledenju uporabnikov (Data Protection Working Party 2000, 52).

Piškotek navadno vsebuje interno identifikacijsko številko uporabnika in ko se uporabnik giblje po spletnem mestu, lahko spletni strežnik te identifikacijske številke beleži. Seveda pa se da to identifikacijsko številko povezati tudi s kakšnimi drugimi podatki. Tako lahko spletni strežnik pri naslednjem obisku uporabnika ugotovi, če je uporabnik na spletni strani že bil in kaj je na njej počel. Piškotki so bili razviti z namenom, da bi omogočili spletne nakupne košarice, danes pa jih množično uporabljajo na vseh vrstah spletnih strani.

Na piškotke zato lahko gledamo kot na razpršeno bazo podatkov, saj so podatki o obiskovalcih razpršeni po računalnikih obiskovalcev spletne strani. Vendar pa, kot smo že omenili, nekateri strežniki uporabljajo piškotke za sledenje uporabnikov z enega spletnega strežnika na drugega, lahko pa tudi razkrijejo identiteto uporabnika. Eden najbolj znanih primerov domiselne uporabe piškotkov je povezan s podjetjem DoubleClick.

Neposredno trženje oglasnega prostora na internetu je nepraktično, zato 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. Pri podjetju so ugotovili, da lahko za vsak prikazani oglas določijo, na kateri spletni strani je bil prikazan, ta podatek pa lahko povežejo z identifikacijsko številko piškotka, ki ga po celotnem oglaševalskem omrežju pošilja njihov strežnik.[23] Namesto oglasa je lahko

[23] Na spletnih straneh podjetja DoubleClick (http://www.doubleclick.com), je bilo 25. oktobra 2002 objavljeno sporočilo za javnost DOUBLECLICK AD SERVING DATA SHOWS RICH MEDIA CLICK-THROUGH RATES TO BE SIX TIMES HIGHER THAN STANDARD ADS, v katerem je objavljen podatek, da so v maju 2001 prikazali 55 milijard oglasov.

uporabljena majhna slika, navadno velika 1 x 1 *pixel*, kar pomeni, da je skorajda nevidna, zato se za ta postopek uporablja tudi izraz sledenje s *pixel tehnologijo*, slikam pa pravimo *spletni hrošči* (ang. *web bugs*). Ta postopek jim omogoča ugotoviti, po katerih spletnih straneh v oglaševalskem omrežju se giblje posamezni uporabnik, s čimer so zaobšli prvotno zamišljeno omejitev dostopnosti do piškotka izključno za spletne strani znotraj strežnika. Če je oglaševalsko omrežje dovolj veliko, lahko na podlagi zbranih podatkov ugotovimo brskalne navade posameznega uporabnika.

Vendar pa tudi to ni vse. Te podatke lahko povežemo z elektronskim naslovom posameznika in celo s t.i. *off-line* identiteto. Fizično, *off-line* identiteto uporabnika je mogoče ugotoviti tako, da uporabnik svoje podatke posreduje katerikoli spletni strani v omrežju, ti podatki pa se potem povežejo z identifikacijsko številko piškotka.

Povezovanje brskalnih navad z elektronskim naslovom posameznika pa lahko poteka tako, da podjetje razpošlje množico elektronskih sporočil s personaliziranimi povezavami, prejemniki elektronskih sporočil pa so vabljeni, naj kliknejo na povezavo. Personalizirana povezava pomeni, da je na vsak elektronski naslov poslana drugačna povezava, po možnosti taka, da za vsakega prejemnika vsebuje enolično identifikacijsko oznako. Pošiljatelj torej natančno ve, na kateri elektronski naslov je poslal katero povezavo. Ko torej uporabnik klikne na personalizirano povezavo, lahko prejemnik ta klik zabeleži in tako s pomočjo piškotka poveže elektronski naslov 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, pač pa je dovolj, da jih uporabnik samo prebere. Takšna sporočila so prirejena tako, da vsebujejo povezavo na neopaznega *spletnega hrošča* in ko uporabnik takšno sporočilo prebere, skupaj s sliko dobi tudi piškotek. Seveda ta način deluje le, če so izpolnjeni določeni pogoji (v trenutku branja sporočila mora biti uporabnik povezan v internet, program za branje elektronske pošte mora podpirati prikaz HTML oblikovanih sporočil, imeti mora omogočeno sprejemanje piškotkov ...), vendar je v povezavi z drugimi načini nadzora lahko izjemno učinkovit. Da taki načini identifikacije uporabnikov ne obstajajo samo v teoriji, je postalo jasno vsaj v začetku leta 2000, ko je časnik USA Today razkril, da je DoubleClick zbiral imena uporabnikov in

skušal piškotke povezati tudi z identiteto uporabnikov v resničnem življenju[24] (ang. *off-line* identiteto) (Schneier 2000).

Iz teh razlogov nekateri uporabniki interneta onemogočajo uporabo piškotkov in JavaScripta, kljub temu da to povzroči zmanjšano funkcionalnost spleta.[25] Tudi če uporabnik privoli v zmanjšano funkcionalnost spleta, to še ne pomeni, da bo v zameno zares dobil večjo zasebnost. Felten in Schneider iz 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*). Tehniko sta poimenovala 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 ter celo če uporablja sisteme za anonimizacijo (Felten in Schneider 2000, Standard Feature 2000).

Dostop do tako zbranih elektronskih sledi ima vsaj upravitelj sistema, lahko pa še kdo drug. Na primer oddelek tržnih raziskav ali pa specializirano podjetje, ki za zunanje naročnike izvaja analize spletne obiskanosti (Data Protection Working Party 2000, 43). Zaradi marketinške zanimivosti teh podatkov člani organizacije Privacy Rights Clearinghouse ugotavljajo, da se njihovo zbiranje, predvsem informacij o obisku spletnih strani, povečuje (Privacy in Cyberspace 1998). Zato tudi ni presenetljiv podatek, ki ga navaja poročilo *Privacy on the Internet – An Integrated EU Approach to On-line Data Protection*, da mnoge iskalnike financirajo marketinška podjetja (Data Protection Working Party 2000, 18). Ravno tako so močno sponzorirani tudi spletni ponudniki brezplačnih elektronskih naslovov, ni pa tudi presenetljiva ugotovitev, da pri slednjih obstaja celo možnost razkritja elektronskega naslova osebe marketinškemu podjetju (Data Protection Working Party 2000, 36).

[24] Podjetje DoubleClick se je povezalo s podjetjem Abacus Alliance, ki je v ZDA vodilno podjetje za zbiranje podatkov o potrošnikih, novembra 1999 pa sta podjetji začeli združevati podatke o potrošnikih iz obeh svojih baz (Data Protection Working Party 2000, 45).

[25] Nekoliko več možnosti ponuja selektivno onemogočanje piškotkov. Program *Bugnosis* je namenjen odkrivanju spletnih hroščev, ki pošiljajo piškotke, nekateri spletni brskalniki, na primer *Mozilla* pa omogočajo selektivno blokiranje in uničevanje piškotkov.

Marsikomu se takšno početje zdi sporno, nekaterim celo takrat, ko te podatke zbirajo neodvisni raziskovalci ali akademske ustanove, ki so zbrane podatke pred objavo dolžni anonimizirati in ki zbranih podatkov načeloma ne prodajajo naprej. Vendar pa zbiranje teh podatkov in njihova uporaba za marketinške namene nista nujno samo škodljiva, saj prihodek od oglaševanja nekaterim spletnim stranem omogoča obstoj oziroma brezplačno ponujanje spletne vsebine, poleg tega opisane tehnologije omogočajo personalizacijo spletnih strani, kar je ravno tako lahko koristno za uporabnike.[26] Vsekakor pa bi popolno onemogočanje tovrstnega zbiranja podatkov precej zmanjšalo funkcionalnost spleta, verjetno pa tudi zaustavilo razvoj internetne ekonomije. Zato direktiva EU 2002/58 takšno zbiranje podatkov dovoljuje, vendar pod pogojem, da je uporabnik o tem zbiranju in uporabi zbranih podatkov ustrezno obveščen, poleg tega pa mora imeti možnost takšno obdelovanje odkloniti (Možina 2002, 3). Pravzaprav se zdi, da je edina smiselna zaščita pred tovrstnim posegom v zasebnost strog nadzor nad zbiranjem in uporabo elektronskih sledi. Žal Allard in Kass ugotavljata, da so baze osebnih podatkov in *on-line* aktivnosti čedalje bolj javno dostopne (Allard in Kass 1997, 572).

Povezovanje in zbiranje razpršenih podatkov

Na internetu je dostopnih velikansko število podatkov in informacij, večina pa jih je nepovezanih, kar pa ne pomeni, da se jih ne da povezovati. Baze je mogoče povezovati s pomočjo tehnik računalniškega ujemanja in povezovanja zapisov (ang. *computer matching and record linkage*), lahko pa so podatkovne baze že v izhodišču zasnovane kot relacijske, kar omogoča povezovanje med njimi. Te tehnike so prvi uporabili vladni oddelki v ZDA v poznih 70. letih, njihova uporaba pa se je razširila v 90. letih (Lyon 1994, 9).

Danes so baze podatkov eno glavnih orodij množičnega nadzora, saj so lahko izjemno kompaktne in po začetnem vložku tudi poceni za vzdrževanje, kar jih dela še posebno privlačne. Clarke zato gov-

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

ori 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 univerzalne identifikacijske sheme, po možnosti s pomočjo telekomunikacijskih omrežij. Internet pa je za to vrsto nadzora prav idealno okolje, značilen primer podatkovnega nadzora pa je povezovanje elektronskih sledi.

Posebno privlačno je zbiranje javno dostopnih in prostovoljno posredovanih osebnih podatkov. Zbiranje in klasifikacija na spletnih straneh objavljenih osebnih podatkov že dolgo časa nista več večja tehnična problema, sta pa izjemno učinkovita in poceni. Tehnologija za zbiranje podatkov, objavljenih na spletnih straneh je javno dostopna, nekoliko večji poblem sta le samodejna klasifikacija in prepoznavanje pomembnih podatkov. Programi za zbiranje podatkov, imenujejo se roboti, pajki ali črvi (ang. *spider, worm, [ro]bot*, včasih tudi *harvester*), so velikokrat namenjeni zbiranju elektronskih naslovov. Programi iščejo po spletnih straneh pa tudi po spletnih forumih, novičarskih skupinah in arhivih poštnih seznamov. Upravitelji, ki takšno zbiranje želijo preprečiti, sicer lahko določijo področje spletnega strežnika, kjer je vstop robotom prepovedan,[27] vendar ni nujno, da se roboti teh navodil držijo.[28] Zato se pri objavi nekaterih podatkov, predvsem elektronskih naslovov, mnogokrat uporabljajo različni triki, ki robote zmedejo tako zelo, da podatka niso več sposobni prepoznati kot elektronski naslov.[29]

V Sloveniji se je že 6. oktobra 1997 pojavil *Imenik elektronske pošte Slovenije* (http://afna.telekom.si), pozneje pa še e-mail imenik iskalnika Najdi.si (http://www.najdi.si). Sodobni spletni iskalniki, kakor npr. Najdi.si, imajo vgrajene tudi sisteme umetne inteligence,

[27] Gre za t.i. *robot exclusion protocol*, seznam za robote prepovedanih spletnih strani. Shrani se ga v datoteko robots.txt na spletnem strežniku.

[28] Robot se obnaša kot povsem običajen 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 običajen spletni brskalnik.

[29] Obstajajo pa tudi skripte, ki generirajo naključne elektronske naslove, ki seveda ne obstajajo. Njihov namen je robota oskrbeti z lažnimi podatki, baza elektronskih naslovov, ki jo ustvari tak robot, pa je zato neuporabna.

ki so do neke mere sposobni prepoznati, v katerem jeziku je napisano neko besedilo in samodejno izločiti ter zabeležiti nekatere podatke, kot na primer javno objavljen elektronski naslov, telefonsko številko ali sliko.

Seveda pa so tudi drugačni, predvsem pa učinkovitejši načini zbiranja podatkov. Mnoge spletne strani ali storitve na internetu namreč od uporabnikov v zameno za nekaj – informacije, nekatere ugodnosti ali uporabo – zahtevajo osebne podatke. Pogosto uporabijo tudi trik s kakšno nagradno igro ali žrebanjem. Na straneh, kjer se ti podatki zbirajo, velikokrat ne piše oz. ni razvidno, v katere namene bodo tako zbrani podatki uporabljeni, včasih pa se podatki kljub drugačnim zagotovilom uporabijo za drugačne namene kot za tiste, za katere so bili zbrani. Zbiranje podatkov lahko poteka tudi preko registracije različnih brezplačnih programov, lahko pa tudi s pomočjo na spletni strani podtaknjene zlonamerne JavaScript kode (Data Protection Working Party 2000, 32) ali s pomočjo računalniških virusov, o čemer bo nekoliko več besed pozneje.

Ameriška zvezna trgovinska komisija je 15. decembra 1997 objavila rezultate raziskave *Kids Privacy Surf Day*. V raziskavi so analizirali 126 med otroki najbolj priljubljenih spletnih strežnikov. Raziskovalci so ugotovili, da je približno 86 odstotkov strežnikov od otrok zbiralo osebne podatke (imena, naslove, telefonske številke, e-mail naslove), pri tem pa je bilo na manj kot 30 odstotkih teh strežnikov objavljeno opozorilo o zasebnosti, oziroma za kakšen namen bodo zbrani podatki uporabljeni. Skrb zbujajoče je bilo tudi to, da so manj kot 4 odstotki stežnikov, ki so podatke zbirali, zahtevali, da zbrane podatke avtorizirajo starši. Raziskava je pokazala, da je zasebnost otrok na internetu slabo varovana in da je treba za varovanje zasebnosti otrok na internetu še mnogo storiti (Kids Surf Day 1998).

Prestrezanje podatkov po omrežju

Prestrezanje podatkov po omrežju je v računalniških omrežjih podobno prisluškovanju v telefonskem omrežju. Izpeljati ga je mogoče s pomočjo tehnike prestrezanja paketkov (ang. *packet sniffing*). S pomočjo te tehnike napadalec prestreza in analizira promet tujih računalnikov (ker se podatki na internetu izmenjujejo v obliki

paketkov, napadalec prestreza te paketke – od tod ime za opisano tehniko).[30] Ker navadno ne gre za aktivni vdor, pač pa je prestrezanje paketkov pasivno, prisluškovalec namreč samo *spremlja* promet, je to tehniko težko odkriti. Hekerji jo pogosto uporabljajo za prestrezanje in krajo gesel (ang. *password sniffing*).

S pojavom cenovno dostopnih brezžičnih lokalnih omrežij (ang. *wireless LAN network*, navadno temelječih na protokolu 802.11b) so se ravno tako pojavile številne možnosti zlorab: kraja dostopa do interneta (s pomočjo neavtoriziranega vstopa v omrežje ali kraje gesel za dostop do omrežja), prestrezanje omrežnega prometa pa tudi napadi na omrežje oziroma na druge računalnike v brezžičnem omrežju (Wireless 2002). Raziskovalci berkeleyske univerze, ki jim je uspelo v realnem času razbiti šifrirni algoritem WEP[31] (*Wired Equivalent Privacy*) – uporabljajo ga brezžična omrežja – so celo ugotovili, da je ta varnostni protokol tako slabo zasnovan, da omogoča neopazno ponarejanje paketkov, ki se prenašajo po brezžičnem omrežju (Sandberg 2001). Pomembno je tudi, da je uporabnik od bazne postaje lahko oddaljen do 120 metrov (z usmerjeno anteno še dlje, tudi več kilometrov), predvsem pa za razliko od uporabnikov navadnih omrežij ni fizično povezan v omrežje. To pomeni, da ga je veliko teže, navadno celo nemogoče locirati. Če napadalec prek pomanjkljivo zavarovanega brezžičnega omrežja

[30] Prestrezanje paketkov (tim. *promisc sniffing*) je bilo včasih posebej priljubljeno na lokalnih Ethernet omrežjih, ki so temeljila na tehnologiji koncentratorjev (ang. *hub*). Takšna 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. »*promisc* način«, je lahko prisluškoval prometu ostalih računalnikov v omrežju. Vendar pa je to tehniko mogoče zaznati. Današnje prestrezanje podatkov poteka predvsem preko spremljanja prometa na usmerjevalnikih (ang. *router*) oziroma podatkovnih povezavah.

[31] WEP je sistem za šifriranje in nadzor dostopa (avtentikacijo). Trenutno sta na voljo t.i. 64-bitni in t.i. 128-bitni WEP, vendar gre v resnici za 40-bitni in 104-bitni RC4 algoritem. Ostalih 24 bitov tvorijo sistemsko generirani podatki, t.i. »inicializacijski vektor«, ki služi za zagotavljanje nemotenega toka oz. sinhronizacijo podatkovnih paketov. Raziskovalci so leta 2001 dokazali, da je mogoče z minimalnimi stroški (pod 100 dolarjev) v nekaj urah obnoviti 128-bitni ključ v brezžičnem omrežju (Stubblefield et al. 2001). Vendar pa pomanjkljivosti WEP-a ne izhajajo iz algoritma RC4 (ta se uporablja tudi v implementaciji SSL), pač pa iz slabe zasnove samega sistema. Dodatna varnostna pomanjkljivost sistema je tudi dejstvo, da si vsi uporabniki omrežja delijo isti dostopni ključ (Schneier 2001b). Nekatere teh pomankljivosti 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*).

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. Takšna nevarnost je še posebej velika, kadar dostop do omrežja sploh ni zavarovan z geslom.[32] V hekerski skupnosti se je že izoblikoval poseben sistem oznak, ki v fizičnem svetu označujejo točke, kjer je mogoč dostop do brezžičnih omrežij. To je t.i. *warchalking*, kjer hekerji s kredo (ali s sprejem) na javnih mestih označijo prisotnost in način vključitve v brezžično omrežje (Loney 2002), za take točke pa se je uveljavil angleški izraz *hotspot*.

Prestrezanje elektronske pošte

Iz povedanega se seveda da sklepati, da je za razliko od navadne pošte ali telefonskih komunikacij elektronska sporočila mogoče veliko bolj preprosto prestrezati in v njih iskati nekatere besede, saj se elektronska pošta po internetu načeloma prenaša nešifrirano, torej kot navadno besedilo (ang. *plain text*). Poleg tega imajo do elektronske pošte svojih uporabnikov načeloma povsem prost dostop upravitelji poštnih strežnikov in tudi upravitelji posredniških poštnih strežnikov (ang. *relay server*), preko katerih se sporočilo posreduje od enega poštnega strežnika do drugega v internetu, čeprav v večini držav velja načelo pisemske tajnosti. Pri prenosih elektronske pošte tako velja, da mora biti sporočilo s posredniškega poštnega strežnika izbrisano takoj, ko je bilo posredovano naprej (Data Protection Working Party 2000, 33), enako pa velja tudi za končni poštni strežnik uporabnika, razen če se uporabnik sam odloči, da bo sporočilo ohranil na svojem poštnem strežniku. Pomembno je tudi ločevanje med prometnimi podatki, ki so nujni za prenos sporočila in zaračunavanje stroškov, osebnimi podatki in vsebino sporočila. Poštni strežnik namreč o sporočilu samodejno zabeleži nekaj tehničnih podatkov, in sicer velikost sporočila, elektronski naslov pošiljatelja in sprejemnika, datum in čas pošiljanja sporočila ter še

[32] Dostop do brezžičnega omrežja je mogoče zavarovati tudi s kontrolo dostopa na ravni serijskih številk omrežnih vmesnikov, t.i. strojnih MAC naslovov (ang. *Media Access Control Address*). Upravitelj omrežja namreč lahko dovoli uporabo brezžičnega omrežja samo uporabnikom z določenimi MAC naslovi (ti naj bi se razlikovali za vsako omrežno kartico). Vendar je mogoče MAC naslove programsko ponarejati, nekatere brezžične mrežne kartice pa uporabnikom celo omogočajo, da sami vpišejo poljubno serijsko MAC številko. Ni odveč poudariti, da takih goljufij ni enostavno odkrivati.

nekaj tehničnih podatkov o poteku prenosa sporočila. S posebno programsko opremo, oziroma posebnimi nastavitvami pa je seveda mogoče beležiti še veliko drugih podatkov, na primer, število in velikost datotečnih prilog, uporabljeni nabor znakov, temo (ang. *subject*) ter 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 in jih zato shranjujejo (Data Protection Working Party 2000, 33). Protislovje elektronske pošte je pravzaprav v tem, da je videti tehnično bolj kot razglednica, uporabniki pa jo razumejo kot zasebno pošto pa tudi zakonodaja jo obravnava kot zaprto pisemsko ovojnico.

Pri elektronski pošti (pa tudi pri podatkih o uporabi drugih internetnih storitev) se pojavljajo še dodatna vprašanja. Nekateri poštni strežniki imajo namreč nameščene posebne programe, ki pošto pregledujejo in skušajo ugotoviti, ali je sporočilo okuženo z virusom oziroma ali gre za t.i. *spam* (nezaželeno/nenaročeno elektronsko pošto). Vsekakor velja, da programi ne smejo posredovati okužene ali *spam* pošte nobeni tretji osebi (Data Protection Working Party 2000, 34). Kadar so ti programi nameščeni brez soglasja ali celo vednosti uporabnikov, nastajajo tudi zanimiva pravna vprašanja, ali je to dopustno ali ne. Če je filtriranje virusov načeloma še sprejemljivo (kljub temu da so mogoči tudi lažni preplahi, ki prizadenejo neokužena sporočila), pa je filtriranje (brisanje) *spam* pošte po merilih, ki jih uporabnik morda ni odobril, pravno že nekoliko bolj sporno.

Na dodatni problem opozarja vprašanje, ali je elektronska pošta osebna v vseh primerih ali samo v nekaterih. V ZDA je z zakonom *Electronic Communications Privacy Act* sicer prepovedano branje vsebine elektronskih sporočil, namenjenih nekomu drugemu, vendar pa so določene izjeme. Ena izmed njih je, da delodajalec lahko spremlja elektronsko pošto svojih uslužbencev – seveda kadar uporabljajo poštni predal podjetja (Privacy in Cyberspace 1998). Za razliko od ZDA, bi moral biti v Sloveniji uslužbenec v podobnem primeru prej seznanjen s takšno možnostjo oziroma bi se z njo moral predhodno strinjati. Podobna vprašanja o omejitvah zasebnosti elektronske pošte se včasih pojavljajo celo pri ponudnikih brezplačnih elektronskih naslovov.

Kljub nekaterim pravnim prazninam pa imajo uporabniki elektronske pošte možnost le-to zavarovati s kriptografijo. O tem bo nekoliko več besed v nadaljevanju.

Vdiranje v sisteme

Poleg vdiranja v zasebnost komunikacij in zlorabe informacijske zasebnosti v virtualnem prostoru poznamo tudi zlorabo prostorske zasebnosti.

Vdiranje v računalniške sisteme je eden izmed najbolj neposrednih napadov na zasebnost. Do njega sicer lahko pride zaradi malomarnosti pri postavitvi in vzdrževanju sistemov, npr. zaradi nepravilno nastavljenih pravil za dostop do datotek (ang. *file permission*) ali slabo napisanih programov (značilen primer so npr. spletni programi, ki ne preverjajo ukazov za delo z bazami), navadno pa gre pri vdiranju v sisteme bolj za sofisticirane načine iskanja varnostnih pomanjkljivosti (ang. *vulnerability*) in njihovo izkoriščanje. Praviloma to zahteva veliko računalniškega znanja, vendar pa se je to v zadnjih letih začelo korenito spreminjati.

Leta 1995 sta računalniška programerja Wietse Venema in Dan Farmer objavila na internetu program SATAN (*Security Administrator's Tool for Analyzing Networks*), ki po internetu ali lokalnem omrežju išče varnostne luknje v računalniškemu sistemu (What SATAN is 2002). Program je namenjen odkrivanju, ne pa tudi izkoriščanju varnostnih lukenj, avtorja pa sta ob njegovi brezplačni objavi na internetu zatrdila da je namenjen predvsem upraviteljem računalniških sistemov za izboljšanje varnosti njihovega lastnega sistema (Improving 2002). Tri leta pozneje, leta 1998, pa je skupina računalniških hekerjev, zbranih v skupini Cult of the Dead Cow, na svoji spletni strani objavila *trojanskega konja*[33] *Back Orifice*, ki je namenjen oddaljenemu nadzorovanju računalnikov, na katerih teče operacijski sistem *Windows*. *Back Orifice* je sistem za oddaljeno upravljanje z računalnikom oziroma programski paket, ki na računalniku odpre t. i. stranska vrata (ang. *back door*), skozi katera sta

[33] 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 običajni programi (od tod tudi njihovo ime), njihove skrite funkcije pa so najbolj pogosto namenjene odpiranju t.i. stranskih vrat na žrtvinem računalniku, kraji gesel ali povzročanju druge škode.

napadalcu omogočeni oddaljeno nadzorovanje in upravljanje z računalnikom prek interneta, ne da bi lastnik tega nadzorovanega računalnika to opazil. Program je zelo preprost za uporabo, saj ne zahteva kakšnega posebnega računalniškega znanja, poleg tega pa je popolnoma brezplačen. Edini problem je le, kako podtakniti ta program na računalnik žrtve. Hkrati s pojavom programa *Back Orifice* se je na internetu pojavil tudi konkurenčni program *NetBus*, ki je prav tako namenjen oddaljenemu nadzorovanju računalniških sistemov. Danes je na internetu brezplačno dostopnih čedalje več orodij za nadzorovanje in vdiranje v računalniške sisteme, ki od uporabnika ne zahtevajo skoraj nobenega znanja.[34]

Če so zgoraj omenjena orodja za vdiranje v računalniške sisteme namenjena za vdor v neki natanko določeni sistem, pa se računalniški virusi od njih razlikujejo po tem, da se širijo brez natančno določenega cilja. S pojmom računalniški virus včasih poljudno označujemo vse programe ali programske kode, namenjene povzročanju škode ali obremenjevanju računalniških sistemov, ki so se hkrati sposobni sami širiti. Virusi pa niso nujno le destruktivni. Maja 2000 je bivši direktor CIE R. James Woolsey opozoril na novo vrsto virusov – instruktivne viruse (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 (recimo seznama elektronskih naslovov iz uporabnikovega adresarja), spreminjanje vsebine datotek ali elektronsko prisluškovanje.

Decembra 2001 je prišlo na dan, da enega takšnih programov pri svojem delu uporablja FBI. Agenti FBI so namreč leta 1999 med preiskavo proti domnevnemu mafijcu Nicodemu S. Scarfu ugotovili, da le-ta uporablja šifrirni program PGP, kar jim je onemogočilo dostop do vsebine njegovih datotek. Zato so 10. maja 1999 tajno stopili v Scarfov urad v New Jerseyju, na njegov računalnik namestili program za prestrezanje tipkanja (ang. *keyboard-sniffing device*) in tako prestregli njegovo geslo za šifriranje elektronskih sporočil (McCullagh 2000 in Schneier 2001a). Izkazalo se je da je FBI

[34] Na tem mestu ni odveč opozorilo, da imajo nekateri tovrstni programi vgrajena tudi posebna stranska vrata, skozi katera lahko avtorji programa nadzorujejo računalnik uporabnika tovrstnega orodja in tudi računalnik njegove žrtve. Zato previdnost pri »*preskušanju*« tovrstnih orodij ni odveč, odveč pa je poudarjati, da je njihova *uporaba* in celo posedovanje seveda nezakonita (309. člen kazenskega zakonika RS).

razvil posebno orodje za prestrezanje gesel z imenom *Magic Lantern*. To je trojanski konj, ki izkorišča varnostne luknje in pomanjkljivosti v računalniškem sistemu in ga je v nekaterih primerih mogoče namestiti na računalnik celo na daljavo – po elektronski pošti ali kar po internetu. Kmalu po tistem, ko je FBI odkril in potrdil obstoj tega orodja, se je razvnela debata 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*. Protivirusna podjetja so se pozneje – verjetno tudi zaradi pritiska javnosti – odločila, da z FBI ne bodo sodelovala in da se bodo trudila še naprej odkrivati vse viruse, ne glede na njihov izvor (FBI 2002).

A namestitev takšne pogramske opreme ni edina možnost za nadzor posameznikov. Včasih imajo programi že vnaprej vgrajene skrite nadzorovalne zmogljivosti. Pogosto so to tako imenovani vohunski programi (ang. *spyware*), ki zberejo neke podatke (največkrat s tržno vrednostjo, kot npr. elektronski naslov in brskalne navade), nato pa jih pošljejo na strežnik avtorjev programa. Za take programe se včasih uporablja tudi izraz E. T. aplikacije, ker potem, ko zberejo podatke, »pokličejo domov« (izraz se je razvil na podlagi zgodbe iz filma *E. T.*).[35]

Vendar pa mehanizmi nadzora niso vgrajeni samo v proizvode manj znanih podjetij, pač pa tudi v najbolj razširjene računalniške aplikacije. Na začetku leta 1999 se je namreč pojavil 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 *MS Office* okolja, je seveda takoj nastalo vprašanje, kako je FBI uspelo med milijoni uporabnikov *MS Officea* odkriti pravega avtorja. Izkazalo se je, da je *Microsoft* v *Office 97* potihem vgradil t.i. GUID, globalni univerzalni identifikator (ang. *Global Unique Identifier*), ki se zapiše v vsak *MS Office* dokument. Če ima uporabnik na svojem računalniku vgrajeno mrežno kartico, serijska številka te kartice postane del GUID, na podlagi česar je mogoče

[35] Med vohunske programe naj bi spadale tudi nekatere različice programov *RealPlayer* (Macavinta 1999) ter *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 obstajale.

natančno ugotoviti, na katerem računalniku je dokument nastal (Lemos 1999). Zaradi tega so nastala resna vprašanja, ali ni mogoče takšno tehnologijo zlorabiti tudi v drugačne namene, ne samo za odkrivanje piscev virusov, pač pa, na primer, tudi za odkrivanje političnih oporečnikov (Joel 1999). Tudi zato direktiva EU 2002/58 o obdelovanju osebnih podatkov in varstvu zasebnosti na področju elektronskih komunikacij 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 (Možina 2002, 3).

Poleg tega imajo današnji računalniški sistemi veliko varnostnih lukenj[36], za katere se sicer hitro najdejo ustrezni popravki, vendar si jih njihovi uporabniki ne namestijo dovolj hitro, včasih pa si jih sploh ne, ker zanje niti ne vedo. Ker so varnostne luknje navadno dobro dokumentirane (čeprav je res, da je prave informacije včasih težko najti), uporabniki pa popravkov ne namestijo, lahko od hekerjev, zasebnih podjetij in tudi državnih organov pričakujemo naraščanje vdorov in poskusov vdorov v računalniške sisteme.

Prestrezanje podatkov in informacij v okolici sistema

Prestrezanje podatkov in informacij v okolici sistema je ena najmanj znanih tehnik nadzorovanja, saj je na voljo zelo malo javno objavljenih raziskav s tega področja, kljub temu da je bila ta tehnologija prvič opisana že leta 1967 (Kuhn in Anderson 1998, 125). Temelji na dejstvu, da računalniške naprave oddajajo v okolje elektromagnetne signale, imenuje pa se TEMPEST – *Transient Electromagnetic Pulse Emanation Surveillance Technology* (tehnika prestrezanja oddanih začasnih elektromagnetnih signalov; *tempest* pa v angleščini pomeni vihar). Leta 1985 je nizozemski znanstvenik Wim van Eck v članku »Electromagnetic Radiation from Video Display Units: An Eavesdropping Risk?« opisal tovrstni problem za video naprave. Van Eck je namreč ugotovil, da je mogoče z razmeroma poceni in s komercialno dostopno opremo zgraditi prisluškovalni sistem, ki lahko

[36] O varnostnih luknjah v okolju Windows skoraj redno poročajo internetni časopisi, kot npr. Crypto-Gram (http://www.counterpane.com/crypto-gram.html) ali Security Focus (http://www.securityfocus.com), veliko tovrstnih informacij pa je dostopnih tudi na spletnih strežnikih podjetja *Microsoft* (http://www.microsoft.com/technet/security/).

obnovi sliko s TV-zaslona v odaljenosti več sto metrov, v nekaterih primerih pa celo v oddaljenosti več kot enega kilometra (Van Eck 1985, 2, 3). Seveda je med zaslonom in prestrezno napravo lahko tudi zid ali kakšna druga ovira.

Kuhn in Anderson z univerze v Cambridgeu opisujeta še več primerov uporabe tempest tehnike. Tako je na primer mogoče prestrezati in prepoznati signale, ki se pretakajo po različnih kablih (iz tipkovnice, po telefonskem kablu, po kablih lokalnega omrežja, itd.). Pri tem je mogoče uporabiti tudi analizo električne aktivnosti (ang. *Differential Power Analysis*), ki so jo opisali Kocher, Jaffe in Jun iz podjetja Cryptography Research. Odkrili so, da je mogoče na podlagi opazovanja električne aktivnosti naprave (npr. pametne kartice) ugotoviti nekatere skrite informacije, na primer šifrirni ključ ali PIN kodo (Kocher, Jaffe in Jun 1999). Podobno nevarna je tehnika časovnega napada (ang. *Timing Attack*), ki jo je odkril Paul Kocher. Tehnika na podlagi merjenja časa, ki ga naprava porabi za procesiranje, omogoča napadalcu razkritje šifrirnih ključev (Kocher 1996).

Kuhn in Anderson ugotavljata, da je s pomočjo teh tehnik mogoče tudi zaobiti zaščito na pametnih karticah, ki onemogoča neomejeno preskušanje gesel oz. PIN kod. Večina pametnih kartic se pri večkratnem vnosu napačnega gesla (PIN kode) zaklene. Na podlagi elektromagnetnega sevanja pa se da ugotoviti, ali je PIN geslo, ki ga nekdo vnese v pametno kartico, pravilno, še preden se kartica pri vnosu napačnega gesla zaklene, in ob napačnem geslu kartico resetirati. To pa omogoča neomejeno preskušanje gesel oziroma napad z grobo silo.

Avtorja celo opisujeta možnost, da bi nekdo razvil poseben virus, ki bi s pomočjo povečane aktivnosti, npr. procesorja ali trdega diska oziroma prek ohranjevalnika zaslona, oddajal sporočila v obliki elektromagnetnega sevanja. Avtorja sta tako predlagala razvoj posebne programske opreme v obliki virusa za ugotavljanje piratstva v podjetjih. Tak program naj bi s pomočjo opisanega generiranja elektromagnetnega sevanja v časovnih intervalih oddajal licenčne številke programske opreme skupaj z naključno številko, kar bi prisluškovalcem omogočilo ugotoviti, koliko različnih kopij nekega programa uporablja preiskovano podjetje, ne da bi fizično sploh vstopili v njegovo stavbo (Kuhn in Anderson 1998, 125–126, 136).

VARSTVO ZASEBNOSTI V VIRTUALNEM PROSTORU

Glede varstva zasebnosti na internetu je najprej treba ločiti različne akterje, ki sodelujejo v procesu izmenjevanja podatkov in informacij na internetu. Akterji so operater telekomunikacij, ponudnik dostopa do interneta, ponudnik internetnih storitev in uporabnik (Data Protection Working Party 2000, 11–12). Vsak od njih ima na voljo svoje mehanizme nadzora, o katerih smo govorili v prejšnjem poglavju. V nadaljevanju si bomo pogledali, kako se zavarujemo pred posameznimi tehnikami nadzora.

Zakonodaja, ki ureja varovanje zasebnosti v realnem svetu, načeloma velja tudi v virtualnem svetu. Vendar pa se je treba zavedati da internet ni prostorsko zamejen, kar ima lahko pri uveljavljanju uporabnikovih pravic zelo konkretne posledice. Posebej še v primerih, kjer zakonodaja med državami ni usklajena, uporabnik pa se med uporabo interneta giblje na območju jurisdikcije različnih držav ali vstopa v interakcijo z globalno razpršenimi subjekti. Pot podatkovnih paketov namreč lahko poteka čez ozemlje različnih držav, tudi takih z nizko stopnjo varstva podatkov, in to celo, kadar sta oba udeleženca komunikacijskega procesa iz iste države. Prenos podatkov namreč poteka po najmanj obremenjeni povezavi in včasih ta pač poteka čez tujino.

Zaradi tega pa tudi zato, ker se je ustrezna regulativna zakonodaja interneta v 90. letih prejšnjega stoletja začela šele razvijati, so se nekateri uporabniki hitro zavedeli pomena samozaščitnega ravnanja in razvoja ustrezne varnostne kulture. Vendar pa organizacija International Working Group on Data Protection in Telecommunications ugotavlja, da samozaščitno ravnanje samo na sebi ne more zagotoviti zasebnosti na internetu, pač pa je potreben tudi celovit pravni okvir, ki zagotavlja učinkovito varstvo zasebnosti (International Working Group 1998). Problem varnosti in s tem tudi zasebnosti namreč ni samo tehnični, pač pa je družbeni problem. To tudi

pomeni, da bi se morali uporabniki računalnikov bolj zavedati nevarnosti različnih zlorab, predvsem pa, kako se proti njim kar najbolje zavarovati. Kljub temu da noben sistem ni stoodstotno varen, pa je s samozaščitnim ravnanjem mogoče varnost precej povečati. Predvsem se je treba zavedati, da varnost ni izdelek oziroma nekaj, kar lahko kupimo, pač pa je *proces*. Varnostno kulturo je treba razvijati in gojiti neprestano. Pri tem si lahko veliko pomagamo že z razumnim ravnanjem pa tudi s specializiranimi programi, ki so večinoma poceni, marsikateri izdelek pa je na internetu dostopen tudi povsem brezplačno.

Anonimizacija

Eno izmed zaščit zasebnosti na internetu omogoča anonimizacija. Seveda popolna anonimizacija razen v izjemnih primerih ni mogoča, saj mora uporabnik, kadar želi dobiti dostop do interneta, z nekim ponudnikom skleniti pogodbeno razmerje in že zaradi tega ne more ostati anonimen. Popolna anonimnost bi bila mogoča le v primeru (nezakonite) vključitve v internet prek brezžičnega ali lokalnega omrežja[37] ali pa s sklenitvijo naročniške pogodbe s ponudnikom dostopa do interneta z lažnimi podatki, kar ravno tako ni zakonito. A celo v tem primeru se je treba zavedati, da ponudnik dostopa do interneta lahko zapisuje, prek katerih vstopnih točk (telefonskih številk) se je uporabnik povezoval v internet, zato bi uporabnik, ki bi želel ostati popolnoma anonimen, moral za priklop na internet uporabiti npr. mobilni telefon iz predplačniškega paketa. Anonimizacija pride tako bolj v poštev za obiskovanje spletnih strani in drugih spletnih storitev, kakor pa za anonimno uporabo interneta v odnosu do ponudnika dostopa do interneta.

Če torej želimo uporabljati internet kar najbolj anonimino, lahko za pošiljanje elektronske pošte uporabimo posebne strežnike, ki izbrišejo podatke o izvoru elektronskega sporočila (ang. *remailer*), pri obiskovanju spletnih strani pa lahko uporabimo anonimni zastopniški program (ang. *anonymous proxy*). To je neke vrste vmesnik med lokalnim računalnikom in internetom, saj v upora-

[37] Ni odveč dodati, da je v tem primeru mogoče zabeležiti serijsko številko omrežnega vmesnika, t.i. strojni MAC naslov (ang. *Media Access Control address*), na podlagi katerega bi bilo v nekaterih primerih mogoče odkriti identiteto uporabnika (glej opis *Microsoftovega* GUID v prejšnjem poglavju).

bnikovem imenu pošilja zahtevke za dostop do spletnih strani, prejete podatke pa nato posreduje uporabniku. Zastopniški program nekatere pogosto prenesene podatke (npr. slike) shranjuje v svoj medpomnilnik (ang. *cache*) in jih po potrebi od tam posreduje do lokalnega računalnika, s čimer se zmanjša obremenitev omrežja. Vendar pa se dajo zastopniški programi uporabiti tudi za drugačne namene. Zastopniški programi se namreč v internetu predstavljajo s svojim IP naslovom, zato lahko skrijejo identiteto pravega uporabnika interneta.[38] T.i. anonimni zastopniški programi tako podatkov o svojih uporabnikih ne posredujejo nikamor in ne shranjujejo in s tem 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*). Seveda pa zastopniški programi skrijejo identiteto uporabnika samo obiskanemu spletnemu strežniku, medtem ko ponudnik dostopa do interneta oziroma morebitni prisluškovalec še vedno lahko spremlja promet uporabnika. Temu se izognemo s šifriranjem povezave med lokalnim računalnikom in anonimnim zastopniškim programom. Vendar pa je tudi v tem primeru mogoče analizirati promet, predvsem kateri anonimni zastopniški program je bil uporabljen, in količino prenesenih podatkov. Poleg tega je treba biti pri uporabi anonimnih zastopniških programov previden, saj nekateri od njih niso anonimni, kljub temu da trdijo drugače. Načeloma je anonimizacija za udeležbo na kakšnih spletnih forumih povsem zadovoljiva (uporaba pač temelji na zaupanju), s policijsko preiskavo pa se lahko izkaže, da marsikateri izmed anonimnih zastopniških programov v resnici ni povsem anonimen.

Poleg tovrstne anonimizacije IP naslova obstajajo tudi programi, ki blokirajo v prejšnjem poglavju opisano sledenje obiskovalcev spletnih strani s piškotki oziroma *spletnimi hrošči*, splača pa se tudi razmisliti o tem, kakšne naj bodo nastavitve glede sprejemanja piškotkov, predvsem tistih s spletnih strani tretjih strank (ang. *third-*

[38] Običajen zastopniški program sicer zahtevke za dostop do podatkov spletnim strežnikom pošilja iz svojega IP naslova, vendar pa spletni strani (s pomočjo spremenljivke *X-Forwarded-for*) sporoči IP naslov kateremu bo posredoval prejete podatke. Anonimni zastopniški programi pa tega podatka ne sporočajo dalje s čimer zagotavljajo anonimnost IP naslovov svojih uporabnikov.

party cookies), in uporabe Jave ter JavaScripta. Treba se je zavedati, da lahko prestroga varnostna pravila včasih otežijo normalno delo z računalnikom in internetom, zato je treba vedno poiskati pravo mero. Žal izklop piškotkov in onemogočanje JavaScripta zmanjšata funkcionalnost spleta, zato v praksi umik v zasebnost ni vedno možnost, ki bi jo uporabniki lahko enakovredno izbrali.

Zaščita pred prestrezanjem

Kot rečeno, je podatke, ki se prenašajo prek omrežij, mogoče prestrezati. Če podatki potujejo prek nezaščitenih in javnih omrežij, seveda neposredna zaščita pred prestrezanjem ni mogoča. Lahko pa podatke spremenimo v tako obliko, da si prisluškovalec, ki jih prestreže, z njimi ne more pomagati.

Ena izmed najbolj znanih in učinkovitih tehnik zaščite zasebnosti je kriptografija. Kriptologija je veda o tajnosti, šifriranju, zakrivanju sporočil (kriptografija) in o razkrivanju šifriranih podatkov (kriptoanaliza). *Kryptos logos* pomeni po grško skrita beseda. Šifriranje sporočil uporabimo za to, da prisluškovalcu, ki sporočilo prestreže, preprečimo dostop do njegove vsebine.

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 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. Poleg simetričnih in asimetričnih algoritmov poznamo tudi zgostitvene algoritme (ang. *hash algorithms*, včasih tudi *message digests* ali *fingerprints*),[39] ki poljubno dolg niz znakov preslikajo v število fiksne dolžine, kar pomeni, da izračunajo t.i. prstni odtis (ang. *fingerprint*) tega niza znakov, kar je osnova za digitalni podpis (ang. *digital signature*). Z uporabo kombinacije kriptografskih metod, metod za digitalno podpisovanje in z uporabo potrdil (ang.

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

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.[40]

Matematiki in računalničarji so razvili precej šifrirnih algoritmov, enega pomembnejših mejnikov v razvoju kriptografije, ki je bil omenjen že v uvodu, pa so konec 70. let prejšnjega stoletja postavili Rivest, Shamir in Adleman z inštituta Massachusetts Institute of Technology, ko so razvili kodirni algoritem RSA. Podatki, zaščiteni s to kriptografsko metodo, so namreč izjemno varni (Vidmar 1997, 181). RSA je asimetrični šifrirni algoritem in predvideva, da imata pošiljatelj in prejemnik vsak svoj par ključev, javnega, ki je javno objavljen, in zasebnega, ki ga obdržita v tajnosti. Prednost te metode je med drugim tudi ta, da ne potrebuje t.i. »varnih kanalov« za prenos ključev, saj so javni ključi javno objavljeni, zasebne ključe pa posamezniki obdržijo zase. Za pošiljanje šifriranega sporočila namreč potrebuje pošiljatelj naslovnikov javni ključ in svoj zasebni ključ, prejemnik pa potrebuje pošiljateljev javni ključ in svoj zasebni ključ.

Junija leta 1991 je računalniški programer Phil Zimmerman napisal program PGP (*Pretty Good Privacy*), ki je vseboval implementacijo RSA algoritma za šifriranje sporočil na osebnih računalnikih. Zimmerman je bil prepričan, da obstaja močna povezanost med demokracijo in zasebnostjo ter da je »edini način za zaščito zasebnosti močna kriptografija« (Zimmerman 1993). Zato je sklenil, da mora biti omenjena tehnologija dostopna vsem ljudem, in svoj program brezplačno objavil na internetu, njegovi simpatizerji pa so ga razširili po vsem svetu (Phil Zimmerman Case 1998). Program se je razvijal dalje in danes omogoča še digitalno podpisovanje, izmenjavo javnih ključev preko 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.

Vsekakor je Zimmermanov program v dveh letih postal dejanski standard za učinkovito zaščito podatkov in elektronske pošte (Zimmerman 1993). Zato so februarja 1993 na njegova vrata potrkali agenti FBI zaradi suma, da je omogočil nezakonit izvoz vojaške tehnologije (Phil Zimmerman Case 1998). V ZDA kriptografijo nam-

[40] Poleg tega mora varnostna aplikacija zagotoviti še preprečevanje tajenja (ang. *nonrepudiation*) in nadzor dostopa (ang. *access control*) do podatkov.

reč štejejo za vojaško tehnologijo,[41] izvoz take tehnologije pa je mogoč samo z dovoljenjem. Januarja 1996 je bila preiskava ustavljena, in sicer 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.

Seveda pa se šifriranje ne uporablja samo za skrivanje vsebine elektronskih sporočil. Šifrirati se da tudi datoteke in celo diskovne pogone. Šifriranje lahko uporabimo za zaščito vsebine sporočil, ki se prenašajo prek telekomunikacijskih omrežij, in tudi za zaščito vsebine sporočil znotraj samega sistema.

Pri uporabi šifriranja je najbolj pomembno, katero kriptografsko metodo uporabljamo. Uporaba šibkih kriptografskih metod sicer lahko da občutek varnosti, vendar je v resnici ne zagotavlja. Poleg tega je treba vedeti, da so bile nekatere kriptografske metode razvite s »pomočjo« ameriških državnih organov (predvsem *National Security Agency*) in zato morda niso tako varne, kot so videti na prvi pogled. Večkrat so določene metode razvila neznana podjetja in v tajnosti, zato v njihovo zanesljivost ni mogoče zaupati. Argument oziroma marketinški trik, da tajnost metode zagotavlja njeno varnost, je popolnoma napačen in navadno kaže le na to, da metoda ni bila javno preskušena, ali pa, da celo sploh ni bila preskušena. V kriptologiji se je namreč izoblikovalo načelo, da morajo biti vse kriptografske metode javno objavljene in jih morajo preskusiti vodilni kriptoanalitiki, in da le to zagotavlja njihovo kakovost. Dobro izbrana metoda namreč potencialnemu napadalcu onemogoča izvajanje znanih in učinkovitih napadov, navadno se le-ta lahko poslužijo samo metode grobe sile (ang. *brute force attack*, preskušanje vseh možnih kombinacij gesel), ki pa je zaradi svoje zahtevnosti razmeroma neučinkovita.[42]

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

[42] Metoda grobe sile namreč zahteva veliko procesorske moči, vendar pa je treba opozoriti, da je procesorsko moč mogoče dobiti tudi s pomočjo distribuiranega procesiranja. Obstajajo namreč volonterski projekti, eden bolj znanih je npr. *RC5 Challenge* iz leta 1997, kjer uporabniki na svojem računalniku, ko ni zaseden, procesirajo podatke, ki jih dobijo iz omrežja. Obdelane podatke potem pošljejo nazaj na centralni stežnik. Tako darujejo nekaj svojega prostega procesorskega časa, in če je takih uporabnikov veliko, lahko dobimo velikansko procesorsko moč. S projekti razbijanja šifriranih sporočil z metodo grobe sile se med drugim ukvarja organizacija distributed.net (http://www.distubuted.net).

Poleg tega je dobro vedeti, da imajo tudi dobre kriptografske metode lahko nekatere omejitve. Varnost metode RSA je tako na primer odvisna tudi od dolžine uporabljenega ključa (ang. *key length*). Znano je tudi, da je mogoče RSA zašifrirano sporočilo razbiti s pomočjo faktorizacije. Faktorizacija 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 pomočjo distribuiranega procesiranja podatkov prek interneta ta čas mogoče skrajšati na nekaj dni (RSA Laboratories 2000, 48, 52).

Poleg metode je pomembna tudi izbira gesla. Gesla morajo biti sestavljena tako, da jih ni mogoče hitro uganiti. Najboljša je kombinacija številk in črk. Gesla, ki so enaka uporabniškemu imenu, imenu partnerja ali najljubše glasbene skupine, zagotovo niso dobra, saj potencialnemu napadalcu omogočajo, da s pomočjo napada s slovarjem (ang. *dictionary attack*, iskanje gesla v vnaprej pripravljenih vrednostih, navadno najbolj pogostih besedah v danem jeziku) takšno geslo hitro odkrije. Prav tako je tudi pomembno, da uporabimo geslo, ki ni prekratko, saj z dolžino gesla število vseh mogočih kombinacij znakov eksponentno narašča. Pomembno je tudi, da si geslo zapomnimo, ne pa, da si ga zapišemo, npr. na listek, ki ga odložimo poleg računalnika, in da za različne sisteme uporabljamo različna gesla. Zaradi zmanjšanja možnosti zlorab strokovnjaki priporočajo redno menjavanje gesel, obstajajo pa tudi sistemi, ki uporabljajo enkratna gesla (ang. *one-time password*), torej gesla, ki so uporabna samo enkrat, drugič pa je treba za vstop v sistem vnesti drugo geslo.

K samozaščitnem ravnanju sodi poleg tega tudi zavedanje o možnosti zlorab in tudi dejanska uporaba šifrirnih metod povsod, kjer je to potrebno. Tako na primer ni vseeno, ali občutljive podatke po internetu prenašamo prek varnih povezav, pri uporabi spletnih storitev s pomočjo protokola SSL (ang. *Secure Sockets Layer* – pro-

tokol ki omogoča šifrirano povezavo med odjemalcem in strežnikom), pri prenosu prek elektronske pošte ali kakšnih interaktivnih sistemov, kot npr. ICQ in podobno, pa z uporabo močnega šifriranja ali ne. Niso redki primeri, ko so posamezniki ali podjetja imeli na voljo zelo kakovostno šifrirno tehnologijo, vendar je iz malomarnosti preprosto niso uporabljali ali pa pri uporabi niso bili dovolj natančni in je zato prišlo do zlorabe.

Zaščita pred vdori in zasegom podatkov

Seveda pa je šifriranje mogoče uporabiti tudi za zaščito vsebine informacij v računalniškem sistemu, s čimer se izognemo zlorabi v primeru, da dobi napadalec fizični ali pa virtualni dostop do računalnika. Danes že poznamo programske rešitve, ki na fizičnem disku ustvarijo posebno šifrirano datoteko. Ta se v operacijskem sistemu predstavi kot virtualni disk. Delo z njim je povsem običajno, a s to razliko, da se vsi podatki zapisujejo v šifrirano datoteko, ki se v sistemu predstavlja kot disk. Dostop do virtualnega diska pa seveda ni mogoč brez ustreznega gesla. Poleg šifriranja je sporočila mogoče tudi skrivati (npr. v slikovne, zvočne ali tekstovne datoteke), s čimer se ukvarja *steganografija* (ang. *steganography*), vendar je skrivanje sporočil uporabno bolj za implementacijo t.i. digitalnega vodnega tiska (ang. *digital watermark*) ali označevanje datotek z digitalnimi serijskimi številkami (ang. *digital serial numbers*), kakor pa za skrivanje občutljivih sporočil. Mogoča pa je uporaba kombinacije šifriranja in skrivanja sporočil.

Kljub uporabi šifriranja pa se da včasih podatke zaseči še pred šifriranjem ali neposredno po dešifriranju. Najbolj značilen primer, ki je bil že omenjen, je uporaba instruktivnega virusa, s katerim lahko prisluškovalec prestreže geslo ali pa kar gole podatke v času, ko se vnašajo v računalnik oziroma če so v nešifrirani obliki na trdem disku. Nekateri virusi pa podatke (npr. datoteke ali elektronske naslove iz adresarja) kradejo in razpošiljajo po omrežju povsem naključno. Ena najpomembnejših stvari, na katero opozarjajo strokovnjaki za računalniško varnost, je zato vsekakor dobra zaščita pred virusi. Ker pa se novi virusi pojavljajo vsak dan, je pomembno, da uporabnik svoj protivirusni program redno dopolnjuje z novimi protivirusnimi vzorci. Današnji protivirusni programi veči-

noma omogočajo dopolnjevanje virusnih vzorcev prek interneta s pomočjo tehnologije t. i. samoposodobitve (ang. *live update*),[43] kar uporabniku olajša skrb za redno posodabljanje protivirusnih vzorcev. Protivirusni programi in dopolnjevanje virusnih vzorcev seveda niso brezplačni, vendar strošek zagotovo odtehta tveganje okužbe z virusom, s tem pa zmanjša možnost kraje ali izgube podatkov.

Najbolj temeljna zaščita pred nezaželenimi vdori je vsekakor redno posodabljanje programske opreme s popravki (v mislih imamo predvsem operacijski sistem Windows in *Microsoftovo* storitev *Windows Update*, čeprav tudi drugi sistemi niso izjeme). Verjetnost možnosti vdora v računalnik pa je mogoče zmanjšati tudi s t. i. požarnim zidom (ang. *firewall*).[44] Požarni zid je neke vrste vmesnik med uporabnikovim računalnikom in omrežjem, na katero je priključen ta računalnik. Požarni zid preverja vso komunikacijo lokalnega računalnika z zunanjim omrežjem in obratno, zato lahko preprečuje neželeno vhodno ali izhodno komunikacijo. Požarni zid se lahko pojavlja kot poseben računalnik, včasih je celo strojno implementiran, lahko tudi kot poseben program, ki se, podobno kot protivirusni program, zažene in pritaji pri vsakem zagonu računalnika. Omejitve dostopa so mogoče zaradi IP naslova in zaradi vrat (ang. *port*), skozi katera poteka komunikacija. Ker grozi nevarnost, da bi se neki virus ali trojanski konj pretvarjal za program, kateremu požarni zid dovoljuje komunikacijo z zunanjim omrežjem, nekateri programski požarni zidovi s pomočjo digitalnega podpisa vsakič preverjajo tudi pristnost programa, ki želi vzpostaviti dovoljeno povezavo.

Brisanje elektronskih sledi

Med elektronskimi sledmi, ki jih uporabniki puščajo v virtualnem prostoru, je treba ločiti med elektronskimi sledmi v lokalnem sistemu in elektronskimi sledmi zunaj njega. Izven lokalnega sistema

[43] Tehnologja samoposodobitve po eni strani zmanjša skrb za posodabljanje programske opreme računalnika, po drugi strani pa omogoča nove zlorabe. Storitev samoposodabljanja namreč omogoča namestitev zlonamerne programske opreme, namestitev lažne zaščite pred virusi (kadar napadalec pošlje prazno datoteko z definicijami virusov), lahko pa napadalec celo obremeni omrežje s pošiljanjem velikih količin (naključnih) podatkov prek te storitve.

[44] Kljub temu da je uporaba požarnega zidu na lokalnem računalniku hitra in poceni rešitev, se je treba zavedati, da pred varnostno luknjo v operacijskem sistemu požarni zid zelo verjetno ne bo zagotavljal ustrezne zaščite.

uporabnik sam seveda ne more posegati. Vse, kar lahko stori, je le, da pušča čim manj sledi, oziroma da sledi zabrisuje. O tem je bil govor v poglavju o anonimizaciji uporabe interneta.

Uporabnik pa ima načeloma prost dostop do elektronskih sledi v svojem lokalnem sistemu. Na trdi disk računalnika se namreč med drugim zapisujejo tudi podatki o uporabi računalnika in spletnih storitev, zato morda ni odveč pomisliti na brisanje sledov uporabe računalnika, posebej takrat, ko en računalnik uporablja več oseb ali ko namerava uporabnik računalnik prodati. To vključuje brisanje piškotkov, čiščenje zastarelih zapisov v registru računalnika (za uporabnike operacijskega sistema Windows), brisanje morebitnih lokalnih datotek aktivnosti, nepovratno brisanje vsebine datotek in t.i. praznega prostora na disku. Običajno brisanje datotek namreč ne izbriše trajno, zato je mogoče vsebino že izbrisanih datotek z različnimi orodji obnoviti deloma ali v celoti. Trajno brisanje (ang. *wiping*) vsebine datotek poteka s prepisovanjem novih (navadno naključnih) podatkov *čez* stare. Navadno gre za večkratno prepisovanje (ang. *number of passes*), saj je v nekaterih primerih samo enkratno (oziroma tudi večkratno) prepisane podatke zaradi temperaturnega krčenja in širjenja diska mogoče rekonstruirati s pomočjo elektronskega mikroskopa. Metodo mikroskopiranja magnetnih sil (ang. *magnetic force microscopy*) in postopek nepovratnega brisanja podatkov je opisal Peter Gutmann z Univerze v Aucklandu v članku »Secure Deletion of Data from Magnetic and Solid-State Memory«,[45] zato se ena od metod brisanja podatkov imenuje po njem. Ta metoda zahteva 35-kratno prepisovanje podatkov po posebnem postopku. Brisanje sledov uporabe računalnika pa seveda zajema tudi brisanje začasnega pomnilnika (ang. *swap file*) pri zaustavitvi računalnika, kar onemogoča poznejšo obnovitev vsebine pomnilnika pri izklopu računalnika.

Zaščita pred tempest napadi

Kljub že opisanim zmožnostim tempest tehnologije – tehnologije prestrezanja elektromagnetnih signalov, ki jih oddajajo elektronske

[45] Članek je bil predstavljen konferenci USENIX Security Symposium Proceedings v Kaliforniji leta 1996, dostopen pa je prek interneta na naslovu http://www.safedelete.com/a-gutmann.phtml.

naprave – pa je mogoča vsaj delna zaščita pred tovrstnim prisluškovanjem. Strojne rešitve so oklepljanje kablov, elektronskih naprav ali celo celih stavb s kovino, kar prepreči »uhajanje« elektromagnetnih signalov, vendar pa so razmeroma drage. Za pametne kartice Kocher in sodelavci iz podjetja Cryptography Research predlagajo več rešitev, ki pa ravno tako zahtevajo posege v samo zasnovo pametnih kartic. Te rešitve niso poceni, pa tudi hitro dosegljive ne.

Za preprečevanje tempest napada na računalniški zaslon opisujeta Kuhn in Anderson neprimerno cenejšo programsko rešitev, in sicer uporabo posebnih tempest pisav (ang. *tempest prevention font*), s katerimi preprečimo, da bi prisluškovalcu uspelo rekonstruirati dovolj jasno sliko z nadzorovanega zaslona. Signal torej lahko prestreže, vendar si z njim ne more veliko pomagati. Poleg tega sta odkrila še dve metodi, s katerima bi bilo mogoče preprečiti prestrezanje signalov s tipkovnice in trdega diska, metodi pa bi bilo mogoče implementirati z manjšimi stroški z nadgraditvijo gonilnikov (Kuhn in Anderson 1998, 139). Za običajne uporabnike je danes na voljo le zaščita proti tempest napadu s tempest pisavami; vgrajena je v programski paket PGP.

Kriptografija in gibanje za elektronsko zasebnost

Če je v ozadju zahtev po čedalje večjem nadzoru potreba po maksimalno varni in predvidljivi družbi, pa se je s pojavom kriptografije pojavil strah pred tem, da bi država ne mogla več nadzorovati kriminala oz. sovražnih dejavnosti proti njej sami. Ker samozaščitno ravnanje vključuje med drugim tudi tehnike, ki morebitnemu nadzorovalcu, tako nezakonitemu kakor tudi zakonitemu, izjemno otežijo oziroma onemogočijo nadzorovanje, je vprašanje, ali naj ima država zgolj *možnost,* da posameznike nadzoruje, ali pa naj ima *absolutno pravico* do njihovega nadzorovanja. Glede tega si v slovenski pravni ureditvi velja zapomniti dve določbi *zakona o kazenskem postopku*. Prva določba (5. člen) določa, da obdolženec ni dolžan pričati proti sebi ali svojim bližnjim ali priznati krivde. Posledice te določbe za obdolženca, ki je uporabljal šifriranje, pomenijo, da mu v postopku proti njemu ni treba povedati gesel, na podlagi katerih bi preiskovalci lahko odprli zašifrirano sporočilo, ter tako prišli do

kakšnih obremenilnih dokazov. Vendar pa druga določba predpisuje, da se pričanju ne more izogniti oseba, ki ni obdolženec, razen če je priča v sorodstvu z obdolžencem, in če je verjetno, da bi s pričanjem spravila sebe ali svojega bližnjega sorodnika v hudo sramoto, znatno materialno škodo ali v kazenski pregon (238. člen zakona o kazenskem postopku).

Poleg tega je ena izmed značilnosti sodobne informacijske družbe izjemno povečana možnost ubikvitete, povsodprisotnosti. Teritorialne meje postajajno čedalje bolj prepustne in imajo čedalje manjšo vlogo pri omejevanju pretoka podatkov in informacij. Vendar pa, če po eni strani prostor odpravljamo kot oviro, po drugi strani izgubljamo zaščitno vlogo prostora (Mlinar 1994, 11).

Denningova in Baugh navajata, da teroristična organizacija Hamas prek interneta in z uporabo kriptografije razpošilja zemljevide, slike in ostale podrobnosti, potrebne za načrtovanje terorističnih napadov, podobno pa sta internet in kriptografija uporabljana tudi pri širjenju otroške pornografije, pri kraji številk kreditnih kartic, v trgovini z mamili, pri vdiranju v računalniške sisteme, pranju denarja in vohunjenju (Denning in Baugh 1999, 252–274). Po terorističnih napadih 11. septembra 2001 v ZDA pa so se pojavljali tudi mnogi sumi (pozneje niso bili dokazani), da je bila kriptografija uporabljena pri njihovem načrtovanju (Harrison 2001). Po mnenju teh avtorjev največji problem ni uporaba interneta, pač pa uporaba kriptografije.

Ameriški FBI je že konec 20. let prejšnjega stoletja, v času prohibicije, ustanovil poseben oddelek, ki se je ukvarjal z dešifriranjem sporočil, ki so jih uporabljali tihotapci alkohola (Shireen 1998). Razvoju računalniške tehnologije je sledil tudi organizirani kriminal in že leta 1998 je oddelek računalniških strokovnjakov ameriške zvezne policije FBI obravnaval 299 primerov, v katerih so bili v kriminalne namene uporabljeni računalniki, pri štirih odstotkih primerov pa so zaznali uporabo kriptografije (Denning in Baugh 1999, 259). Denningova in Baugh ugotavljata, da se povečuje uporaba takšnih vrst šifriranja, ki je nezlomljivo, torej popolnoma onemogoča prisluškovanje. Avtorja navajata, da ameriški zvezni policiji v letu 1995 ni uspelo zlomiti pet, v letu 1996 pa dvanajst šifriranih informacij (Denning in Baugh 1999, 253). Poleg tega sta Denningova in Baugh ugotovila, da visoka cena in nezdružljivost

posameznih vrst naprav za šifriranje telefonskih pogovorov upočasnjujeta razširitev uporabe kriptografije v telefoniji, sta pa opozorila na internetno telefonijo, ki je izjemno poceni, omogoča pa šifriranje zvočnih komunikacij z minimalnimi stroški.

V zvezi s širjenjem javno dostopne kriptografije in njene zlorabe v kriminalne namene se je izoblikoval izraz *kriptoanarhija*. »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), kar naj bi vodilo v družbeni nered. Kriptografija naj bi bila torej uperjena predvsem proti državi (Denning 1997, 187 in Zimmerman 1994), s tem pa posredno tudi proti državljanom.

Države so si vedno prizadevale nadzorovati kriptografijo (Bert-Jaap Koops 1997), zatorej ni 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 kriptografskih metod mogoče zlomiti.

V civilni sferi, med drugim tudi v bančništvu, je (bil) eden najbolj razširjenih kodirnih algoritmov DES (*Data Encription Standard*), ki so ga razvili pri IBM. DES je izpeljanka enkripcijskega algoritma *Lucifer*, ki ga je uporabljala ameriška vojska. Ker teoretično ozadje algoritma ni bilo povsem pojasnjeno, je obstajal sum, da vojska pozna bližnjico za razbijanje civilne inačice DES (Vidmar 1997, 179). Izkazalo se je, da je bila civilna različica algoritma resnično prirejena, saj je namesto 128-bitnega šifrirnega ključa, ki ga je uporabljala vojska, uporabljala 64-bitni ključ. Pa še za tega se je pozneje izkazalo, da je v resnici 56-bitni, saj je bilo 8 bitov kontrolnih. Poleg tega se je v 90. letih prejšnjega stoletja tudi izkazalo, da so pri IBM že med razvojem algoritma odkrili matematično bližnjico za razbijanje civilne različice DES-a, vendar je zaradi zahtev ameriške NSA to odkritje ostalo v tajnosti. Izraelska kriptografa Eli Biham in Adi Shamir sta v letih 1990 in 1991 predstavila novo vrsto kriptoanalize in jo poimenovala diferencialna kriptoanaliza (ang. *differential cryptanalysis*). Pojavil se je sum, da je bila *civilna* različica DES namerno prirejena tako, da je bila učinkovitost do tedaj neznanega napada z diferencialno kriptoanalizo povečana (Bach et al. 1999).

Leta 1993 je Michael Wiener na konferenci o kriptografiji predstavil načrt za napravo za razbijanje 56-bitne različice DES. Naprava bi stala milijon dolarjev in bi DES lahko razbila povprečno v treh urah in pol. Phil Zimmerman je izračunal, da bi nekoliko kompleksnejši napravi za 100 milijonov dolarjev uspelo zlomiti 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 sekundi (Zimmerman 1993). Julija 1998 je John Gillmore iz fundacije Electronic Frontier predstavil napravo DES Cracker, ki je s pomočjo metode grobe sile (ang. *brute-force*) in s pomočjo distribuiranega procesiranja podatkov prek interneta razbila DES v 22 urah (RSA Laboratories 2000, 64). Od takrat dalje je znano, da DES ni več varen.[46]

Do odkritja in javne objave RSA je *de facto* monopol nad razvojem novih kriptografskih metod dejansko imela vojska, deloma pa tudi akademiki. Z razvojem informacijsko komunikacijske tehnologije, ki je omogočila nastanek in javno objavo kakovostnih in poceni šifrirnih programov, pa se je to spremenilo. Ker je bil državni *de facto* monopol na področju kriptografije odpravljen, ga je država poskusila vsiliti *de iure*. Zagovorniki omejevanja kriptografije in ameriška administracija so v ta namen predlagali več ukrepov.

Eden prvih predlogov, ki se je pojavil že leta 1991, je bil, da bi morali proizvajalci v svoje kriptografske proizvode vgraditi t.i. »bližnjico« (ang. *trap door*), skozi katera bi imeli državni organi dostop do šifriranih sporočil. Zakon ni bil sprejet, je pa leta 1993 ameriška vlada objavila predlog sistema avtorizacije gesel (t.i. *key escrow* sistem), ki bi od posameznikov zahteval, da svoje ključe avtorizirajo pri za to pooblaščeni agenciji, kar bi državnim organom omogočilo dostop do teh ključev (EPIC 1998c in EPIC 1998d).

Podoben predlog se je nanašal na postavljanje kriptografskih standardov. Njegova temeljna zamisel je, naj bi država vsilila trgu take

[46] Na civilnem področju, predvsem v bančništvu, uporabljajo tudi prirejene različice DES, npr. *Triple DES*, ki je sicer močnejši, vendar še vedno temelji na DES algoritmu. V kratkem pa naj bi DES zamenjal AES – *Advanced Encryption Standard*. 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 AES standard so bili javno objavljeni, preiskusili pa so jih vodilni svetovni kriptoanalitiki.

kriptografske standarde, 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. S tem bi dosegli, da bi bili taki izdelki manj razširjeni (Denning 1997, 188). Nesmiselnost takega predloga je kmalu postala očitna, saj je bilo pričakovati, da kriminalci ne bodo uporabljali programske opreme s takšno licenco (Denning 1996, 216). Ena izmed različic tega predloga je celo predvidevala zakonsko prepoved uporabe nekaterih kriptografskih metod. Po tem predlogu bi posamezniki sicer še vedno lahko razvijali svoje lastne kriptografske metode, vendar samo za osebno uporabo in izobraževanje, brez dovoljenja pa jih ne bi smeli prosto širiti (Denning 1997, 187–188).

Prav tako zelo pomanjkljiv je bil tudi predlog, naj se dovoli samo uporaba šibke kriptografije, kar bi ustrezno opremljenim državnim organom omogočilo, da v nujnih primerih (npr. ugrabitvah) hitro razbijejo zaščito (Denning 1997, 184). Žal takšna kriptografija uporabniku ne daje ustrezne zaščite, saj lahko šifropis zlomi vsakdo, ki ima zmogljivejši računalnik in ustrezno računalniško znanje.

Večina ter predlogov je bila hudo pomanjkljivih, predvsem zaradi tega, ker so omejevali svobodo govora. Pravno pa tudi z varnostnega vidika je zato še najbolj sprejemljiv predlog za uporabo kriptografije v zaprtih sistemih oziroma uporaba mrežnega šifriranja (ang. *link encription*). Ta predlog predvideva šifriranje podatkov v zaprtem omrežju, podatki pa sistem zapustijo nešifrirani, kar državnim organom omogoča prestrezanje pri izhodu iz sistema (Denning 1997, 184, Denning in Baugh 1999, 253–254). Podoben sistem uporabljajo v GSM omrežju mobilne telefonije za podatke, ki se prenašajo preko radijskih povezav od telefona do bazne postaje.[47]

Da bi omejili zlorabo kriptografije v kriminalne namene, se je pojavila tudi predlagana višja kazen za uporabo kriptografije pri

[47] Glede GSM mobilne telefonije je treba opozoriti, da so GSM šifrirne algoritme že razbili, kar pa ne preseneča, saj so bili razviti s »pomočjo« ameriške NSA. GSM telefoni 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 pa 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 vsaj s 128 Mb RAM ter dvema 73 Gb trdima diskoma (Schneier 1999).

storitvah kaznivih dejanj. Če bi si posameznik pri kaznivem dejanju pomagal s kriptografijo, naj bi se mu kazen podvojila.[48]

Vodilno vlogo pri naporih za prepoved ali vsaj omejevanje kriptografije v ZDA je imel FBI, ki pa tesno sodeluje tudi z agencijo *National Security Agency* in drugimi državnimi organi (EPIC 1998b). Kljub temu da je danes v ZDA dovoljena uporaba katerekoli kriptografske opreme (izvažanje v tujino je omejeno), pa ameriški državni organi izrabijo vsako priložnost za omejitev uporabe kriptografije ali povečanje svoje pristojnosti pri prisluškovanju in prestrezanju elektronskih sporočil. Tako so se že kmalu po 11. septembru v ZDA pojavile zahteve po prepovedi kriptografskih izdelkov, ki bi državnim organom onemogočali dostop do vsebine šifriranih sporočil (Harrison 2001), in celo predlogi, da naj ima policija pristojnost odrediti nadzor internetnih komunikacij brez odločbe sodišča za 48 ur (McCullagh 2001b, 2001c in 2001d).

Poskusi ameriške vlade, da bi kriminalizirala kriptografijo, pozneje pa tudi nadzorovanje, ki so ga povečevale marketinške organizacije, so na internetu sprožili nastanek močnega gibanja za zaščito elektronske zasebnosti. Aktivisti skušajo povečati zavedanje posameznikov o tem, kje in kako so lahko izpostavljeni nadzoru, delijo praktične nasvete in programsko opremo za zaščito zasebnosti, predvsem pa javno predstavljajo uporabo kriptografije. Poleg tega te organizacije in posamezniki skušajo onemogočati poskuse prepovedi in omejevanja kriptografije.

Po mnenju organizacij za elektronsko zasebnost bomo v prihodnosti za medsebojno komuniciranje uporabljali predvsem elektronske komunikacije. Le-te pa je mogoče nadzorovati neopazno in v velikem obsegu. Kriptografija je po njihovem mnenju instrument, ki zagotavlja zasebnost, zasebnost pa je ustavna kategorija, zato pravico do uporabe kriptografije te organizacije enačijo s pravico do zasebnosti. Kljub temu, da se zavedajo nevarnosti zlorabe kriptografije, so prepričane, da bi njena prepoved povzročila večjo škodo, kot pa to, da je dovoljena (Zimmerman 1993).

Trenja med nasprotniki in zagovorniki neomejene uporabe kriptografije izvirajo iz njihovega različnega razumevanja vloge

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

države. Medtem ko nasprotniki neomejene uporabe kriptografije vidijo državo kot dobrega čuvaja, ki skrbi za varnost in blaginjo svojih državljanov, jo zagovorniki vidijo kot foucaultovsko institucijo, ki omejuje njihove pravice in svoboščine.[49] Phil Zimmerman tako pravi, da »če ne bomo storili nič, bodo nove tehnologije dale državi moč nadzora, o kakršni je Stalin lahko samo sanjal.« (Zimmerman 1993).

[49] »Česar se, kot kaže, vlada resnično boji pri Zimmermanovem programu, ni Precej Dobra Zasebnost (*Pretty Good Privacy* – ime Zimmermanovega programa, op. p.) pač pa zasebnost kot taka« (The Zimmerman Case 1995).

SLOVENSKA ZAKONODAJA IN PRAKSA

V slovenskem pravu se pravica do zasebnosti pojavlja v dveh oblikah in sicer kot osebnostna pravica, in je torej zasebnega značaja, ter kot človekova pravica, in je torej tudi javnega značaja (Šturm et al. 2002, 369). Pravica do zasebnosti namreč posameznika varuje tako pred posegi drugih posameznikov, kakor tudi pred posegi države. Pravica do zasebnosti je v Sloveniji ustavna kategorija, saj slovenska ustava v drugem poglavju zagotavlja varstvo različnih vidikov zasebnosti. Čeprav je pravica do zasebnosti razdrobljena na različne kategorije, je to zgolj zaradi posebnih pogojev, ki so jih razvili za posege vanje, ugotavlja Klemenčič, in dodaja, da je treba vsako pravico s področja varstva zasebnosti vedno tolmačiti skozi prizmo splošnega in celovitega varstva zasebnosti in osebnostnih pravic (Šturm et al. 2002, 392).

Ustava tako v 35. členu določa nedotakljivost človekove zasebnosti in njegovih osebnostnih pravic, v 36. členu opredeli nedotakljivost stanovanja, v 37. členu varstvo pisem in drugih občil, kamor lahko štejemo tudi zvočne in digitalne komunikacije, v 38. členu pa je opredeljeno varstvo osebnih podatkov. Ustava določa samo okvir varovanja in uveljavljanja teh pravic, podrobneje pa jih določajo zakoni in sodna praksa. Seveda pa obseg varovanja pravic zasebnosti ni absoluten.

Prostorska zasebnost

Nedotakljivost stanovanja oziroma prostorska zasebnost zgodovinsko izvira iz angleške domneve o nedotakljivosti državljanovega in državljankinega doma, vendar pa 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 (Šturm et al. 2002, 387). Zato se je uveljavilo načelo zaščite razumno pričakovane

zasebnosti (ang. *reasonable expectation of privacy*), na podlagi katerega se besede »stanovanje« ne razume v ožjem smislu, pač pa kot vse prostore, v katerih državljan lahko razumno pričakuje zasebnost, torej tudi razne hotelske sobe, počitniške hišice itd. »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 (Šturm et al. 2002, 401).

Kazenski zakonik Republike Slovenije v 149. in 152. členu sankcionira posege v prostorsko zasebnost. Prvi od členov prepoveduje neupravičeno slikovno snemanje druge osebe ali njenih prostorov, če se pri tem občutno poseže v njeno zasebnost, drugi pa določa sankcije pri kršitvi nedotakljivosti stanovanja, ki se nanaša na nezakonit vstop ali preiskavo zasebnih prostorov, kazniv pa je tudi poskus.

Kakšna bi bila obravnava virtualnega prostora, je nekoliko manj jasno. Vsekakor je vdor v računalniški sistem in preiskovanje računalniškega sistema prek telekomunikacijskega omrežja (s tem ni mišljeno prestrezanje) virtualno vstop v tuj (virtualni) prostor. O vdoru v računalniški sistem sicer govori 242. člen *kazenskega zakonika*, vendar pa določa, da je vdor kazniv samo pri gospodarskem poslovanju, in če je povzročen z namenom, da bi storilec sebi ali komu drugemu pridobil protipravno premoženjsko korist ali drugemu povzročil premoženjsko škodo. Takšna dikcija zakona žal lahko privede do primera, da vdor v računalniški sistem pri katerem ni povzročena nobena škoda, niti storilec ni pridobil nobene koristi, ni sankcioniran. V tem primeru bi bilo treba uporabiti 152. člen, ki prepoveduje neupravičen vstop v tuje prostore (če bi sodišče seveda sprejelo dikcijo virtualnega prostora), in 309. člen, ki sankcionira izdelavo ali pridobitev pripomočkov za vdor v računalniški sistem.

Komunikacijska zasebnost

Ustava v 37. členu zagotavlja tajnost pisem in drugih občil, pri čemer pa je občila treba pojmovati zelo široko. Med občila lahko štejemo telefonske komunikacije, tudi elektronsko pošto, SMS sporočila itd., saj oblika in vsebina sporazumevanja ni pomembna. Poleg tega tudi

ni nujno, da se za prenos sporočila uporabi javno telekomunikacijsko omrežje, pač pa je komunikacijska zasebnost varovana tudi takrat, ko se sporočilo prenaša preko zasebnih ali zaprtih telekomunikacijskih sistemov (Šturm et al. 2002, 395). Seveda je v omenjenem primeru, kar velja predvsem, ko npr. zaposleni uporablja telekomunikacijsko omrežje podjetja, obseg varovanja komunikacijske zasebnosti manjši.

Poleg same vsebine komunikacije so varovani tudi t.i. prometni podatki, ki so integralni del komunikacije (Šturm et al. 2002, 396). To pomeni, da se določbe o varovanju komunikacijske zasebnosti nanašajo tudi na razne izpiske telefonskih številk, podatke o dolžini komunikacije, količini prenesenih podatkov itd.

Ustava zagotavlja pravico vsakomur, ki pri svojem ravnanju razumno upravičeno pričakuje zasebnost, pri tem pa je vseeno, ali gre za prestrezanje v realnem času ali pa za zaseg (npr. poštne pošiljke). Poseg v pravico nastane že s tem, da nekdo nezakonito prestreže komunikacijo in se seznani z njeno vsebino, pa čeprav te informacije pozneje ne uporablja (Šturm et al. 2002, 398).

Vendar pa Klemenčič 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« (Šturm et al. 2002, 395). Odločitev Kasacijskega sodišča Francije št. 99–42.942 z dne 2. 10. 2001 izrecno pravi, da »delodajalec, ki bere sporočila, ki jih zaposleni pošilja ali sprejema preko 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, kjer bi delodajalci arbitrarno in brez omejitev izvajali svoje diskrecijske pravice; ne smejo postati okolja totalnega nadzora, kjer temeljne človekove pravice nimajo veljave ... Menimo, da je splošna popolna prepoved uporabe e-pošte v neslužbene namene nerealna in krši pravno načelo sorazmernosti.« (Šturm et al. 2002, 402.) Zato bi tudi vsak poseg države, ki bi nesorazmerno prepovedal uporabo kriptografije ali anonimnih poštnih strežnikov, lahko pomenil poseg v ustavno zajamčeno komunikacijsko zasebnost (Šturm et al. 2002, 395).

O pravici do zasebnosti komunikacij govori tudi 150. člen *kazenskega zakonika*, ki določa sankcije zaradi kršitve tajnosti občil. Ta člen prepoveduje neupravičeno odpiranje tujih pisem oziroma drugih pošiljk in prestrezanje sporočil, ki se prenašajo po telekomunikacijskem omrežju, oziroma seznanjanje z njihovo vsebino, tudi če se pisma ali pošiljke ne odpre. Prav tako je prepovedano tudi neupravičeno seznanjanje s sporočilom, ki se prenaša po telefonu ali po kakšnem drugem telekomunikacijskem sredstvu. V istem členu je sankcionirano tudi neupravičeno posredovanje tujega pisma tretjim osebam, 151. člen pa prepoveduje javno objavo zasebnega pisanja brez dovoljenja pooblaščene osebe.

Zakoniti poseg v zasebnost komunikacij je mogoč izključno na podlagi odredbe sodišča, če je to potrebno zaradi uvedbe ali poteka kazenskega postopka ali zaradi varnosti države, v Sloveniji pa ga na podlagi *zakona o kazenskem postopku* in *zakona o Slovenski obveščevalno-varnostni agenciji* izvajata policija in Sova. Nezakoniti posegi v zasebnost komuniciranja so prepovedani in sankcionirani. O nadzoru telekomunikacijskega prometa govori 130. člen *zakona o telekomunikacijah*, kjer je med drugim navedeno tudi, da morajo operaterji na lastne stroške zagotoviti ustrezno programsko opremo in primerne vmesnike. *Zakon o poštnih storitvah* pa v 50. členu od izvajalcev poštnih storitev zahteva, da na podlagi sodne odredbe pristojnemu organu omogočijo dostop do vsebine poštnih pošiljk. Hkrati morajo operaterji telekomunikacijskih storitev in tudi izvajalci poštnih storitev zagotoviti neizbrisno registracijo posegov.

Vendar pa se pristojnosti državnih organov glede posegov v zasebnost razlikujejo. *Zakon o kazenskem postopku* v 151. členu določa, da so nadzor komuniciranja, sporočil, prisluškovanje in tajno opazovanje, sledenje ter snemanje dovoljeni za naslednja kazniva dejanja:

- za kazniva dejanja zoper varnost Republike Slovenije in njeno ustavno ureditev in za kazniva dejanja zoper človečnost in mednarodno pravo, za katera je v zakonu predpisana kazen zapora petih ali več let;
- za kaznivo dejanje ugrabitve, neopravičene proizvodnje in prometa z mamili, omogočanja uživanja mamil, izsiljevanja, neupravičenega sprejemanja ali dajanja, daril, ponarejanja denarja, pranja denarja, tihotapstva, jemanja ali dajanja podkupnine,

hudodelskega združevanja, nedovoljene proizvodnje in prometa orožja ali razstrelilnih snovi ter ugrabitve letala ali ladje;
- za druga kazniva dejanja, za katera je v zakonu predpisana kazen zapora osmih ali več let.

(151. člen *zakona o kazenskem postopku*)

Zakon o Slovenski obveščevalno-varnostni agenciji pa predvideva nadzor pisem in nadzorovanje ter snemanje telekomunikacij v Republiki Sloveniji (prisluškovanje v prostorih je izključeno), če je podana verjetnost, da obstaja nevarnost za varnost države, ki se kaže v:
- tajnih aktivnostih zoper suverenost, neodvisnost, državno celovitost in strateške interese Republike Slovenije;
- tajnih aktivnostih, načrtih in pripravah za izvedbo mednarodnih terorističnih akcij zoper Republiko Slovenijo ter drugih nasilnih dejanjih proti državnemu organu in nosilcem javnih funkcij v Republiki Sloveniji ter tujini;
- posredovanju podatkov in dokumentov, ki so v Republiki Sloveniji opredeljeni kot državna tajnost, nepooblaščeni osebi v tujini;
- pripravah na oborožen napad na Republiko Slovenijo;
- obveščevalni dejavnosti posameznikov, organizacij in skupin v korist tujine;
- mednarodni organizirani kriminalni dejavnosti;

in je utemeljeno pričakovati, da se v zvezi s to aktivnostjo uporablja določeno telekomunikacijsko sredstvo ali bo to sredstvo uporabljeno, pri tem pa je mogoče utemeljeno sklepati, da podatkov ni mogoče pridobiti drugače oziroma bi njihovo pridobivanje na drug način lahko ogrozilo življenje in zdravje ljudi.

(24. člen *zakona o Slovenski obveščevalno-varnostni agenciji*)

Zakon o kazenskem postopku tako zelo natančno določa, za katera kazniva dejanja in v katerih primerih je mogoče posegati v zasebnost komunikacij. *Zakon o Slovenski obveščevalno-varnostni agenciji* pa ni tako natančen, saj določa da se nevarnost za varnost države lahko kaže v »tajnih aktivnostih zoper ... strateške interese Republike Slovenije«. Poznavalci opozarjajo, da je ta člen zakona problematičen zato, ker je za razliko od kaznivih dejanj, ki so zelo natančno opredeljena, »strateške interese« mogoče opredeliti bolj

ohlapno, kar bi lahko imelo za posledico, da Sova laže pride do zakonitega sodnega naloga za prestrezanje komunikacij.[50]
Pomembno je tudi, da je dolžnost Sove o njenih ugotovitvah obveščati predsednika vlade, kadar gre za zadeve v njihovi pristojnosti, pa tudi predsednika republike, državnega zbora in ministre (6. člen *zakona Slovenski obveščevalno-varnostni agenciji*). Sova se namreč ne ukvarja s pregonom storilcev kaznivih dejanj, pač pa mora vselej, kadar naleti na sum kaznivega dejanja, o tem obvestiti generalnega direktorja policije in pristojnega državnega tožilca, kar je določeno v 8. členu istega zakona. Zdi se, da so ravno zaradi dikcije 24. člena zakona o Slovenski obveščevalno-varnostni agenciji mogoče morebitne zlorabe.

Informacijska zasebnost

S komunikacijsko zasebnostjo je močno povezano tudi varstvo osebnih podatkov oziroma informacijska zasebnost. Žal se zdi, da je to področje precej slabše urejeno. Zakonodajno je sicer urejeno razmeroma dobro, problem pa je, ker je kljub inšpekcijskemu nadzorstvu na njem še vedno precej nereda.

Varstvo informacijske zasebnosti je prav tako ustavna kategorija, sankcionirano pa je tudi v *kazenskem zakoniku*, ki v 154. členu prepoveduje zlorabo osebnih podatkov in sicer za vsakogar, ki v nasprotju z zakonom uporabi osebne podatke ter za vsakogar, ki vdre v računalniško vodeno zbirko podatkov z namenom, da bi zase ali koga drugega pridobil kakšen osebni podatek. Poleg tega 225. člen prepoveduje neupravičen vstop v zaščiteno bazo podatkov, spreminjanje in kopiranje podatkov iz nje ter vnašanje virusov. Vendar pa pogoje zbiranja, obdelovanja in uporabe osebnih podatkov določa poseben zakon.

Zakon, ki konkretizira varstvo informacijske zasebnosti, je *zakon o varstvu osebnih podatkov*, poleg tega pa se v Sloveniji neposredno uporabljajo tudi določbe *konvencije o varstvu posameznikov glede na avtomatsko obdelavo osebnih podatkov*, ki je bila ratificirana leta 1994. Konvencija in zakon določata, da je v zvezi z zbiranjem in

[50] Lahko pa tudi teže, saj ohlapna dikcija lahko daje širši manevrski prostor tudi predsedniku okrožnega sodišča, ki tako laže zavrne zahtevek za nadzor pisem in telekomunikacij. S stališča varovanja zasebnosti pa ni problematična le sama zloraba, pač pa že *možnost* zlorabe.

obdelavo osebnih podatkov prepovedano vse, kar ni izrecno dovoljeno. Prva različica zakona je bila sprejeta že leta 1990, zakon pa je bil dopolnjen leta 1999 in 2001. Zakon govori izključno o osebnih podatkih, torej podatkih, ki kažejo na lastnosti, stanje ali razmerja *posameznika*, med drugim pa določa tudi pogoje za zakonito obdelavo osebnih podatkov, pravice posameznika v zvezi z njegovimi osebnimi podatki, pogoje za iznos podatkov iz države ter nadzor nad varstvom osebnih podatkov.

Tretji člen zakona določa, da se smejo osebni podatki zbirati, shranjevati in obdelovati samo, če je tako določeno z zakonom (in ne s podzakonskimi predpisi) ali če ima upravljavec zbirke osebnih podatkov pisno privolitev posameznika. Osebe, o katerih se zbirajo osebni podatki, morajo biti predhodno seznanjene z namenom zbiranja (s pisno privolitvijo ali pa mora biti ta namen določen z zakonom), osebni podatki pa se smejo zbirati samo za ta namen (9. člen). Osebni podatki se lahko načeloma shranjujejo in uporabljajo samo toliko časa, kolikor je potrebno za dosego tega namena (10. člen), nato pa jih je treba izbrisati ali blokirati. Morebitne izjeme morajo biti določene z zakonom.

Konvencija o varstvu posameznikov glede na avtomatsko obdelavo osebnih podatkov je pri teh vprašanjih še strožja, saj zahteva celo *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 (Šturm et al. 2002, 411).

Zakon tudi natančno določa dolžnosti upravljavca zbirke osebnih podatkov. Osmi člen uzakonja načelo, da se smejo osebni podatki zbirati samo neposredno od posameznika, razen v posebnih primerih, ki pa morajo biti vnaprej določeni z zakonom. Glede povezovanja osebnih podatkov iz različnih baz je prav tako v 8. členu zapisana prepoved uporabe istega povezovalnega znaka v zbirkah podatkov s področja javne varnosti, državne varnosti, obrambe države, pravosodja in zdravstva, sicer pa velja, da je takšno povezavanje dovoljeno le, če je za to zakonska podlaga ali če se je posameznik s tem predhodno pisno strinjal. Poleg tega mora upravljavec zbirke osebnih podatkov v najmanj 15 dneh po prejemu zahteve posamezniku brezplačno omogočiti vpogled v njegove osebne podatke ter njihovo prepisovanje, oziroma mu na podlagi zahteve v

30 dneh posredovati njihov izpis. Če tega ne stori, ga mora v tem času pisno obvestiti o razlogih za to. Enak 30-dnevni rok velja za posredovanje seznama tistih, ki jim je posredoval njegove osebne podatke (18. člen).

Če posameznik dokaže, da so bili osebni podatki zbrani nezakonito, mora upravljavec osebnih podatkov le-te izbrisati oziroma jih dopolniti ali popraviti, če se izkaže, da so nepopolni, netočni ali zastarani. Tudi te stroške nosi upravljavec zbirke osebnih podatkov. Poleg tega mora upravljavec zbirke osebnih podatkov za vsako zbirko zagotoviti poseben katalog, v katerem mora biti med drugim natančno zapisano, kateri osebni podatki se zbirajo in kako, namen njihove uporabe in čas njihovega shranjevanja, uporabnike zbranih podatkov, opis zavarovanja osebnih podatkov itd. (15. člen). Ministrstvo za pravosodje, ki je pristojno za varstvo osebnih podatkov, vodi poleg tega katalog zbirk osebnih podatkov, podatke za ta katalog pa mora ministrstvu ravno tako posredovati upravljavec zbirke (16. člen).[51]

Iznos osebnih podatkov iz države je mogoč samo v države, ki imajo urejeno varovanje osebnih podatkov, ki obsega tudi tuje državljane, razen če se posameznik pisno strinja z iznosom in je seznanjen s posledicami (24. člen). Prenašanje nekaterih občutljivih vrst osebnih podatkov (tistih, ki se nanašajo na rasno in drugo poreklo, politična, verska in druga prepričanja, pripadnost sindikatu, spolno vedenje, kazenske obsodbe in zdravstvene podatke) prek telekomunikacijskih sredstev pa 4. člen zakona dovoljuje samo, če so podatki zavarovani s kriptografskimi metodami in digitalnim podpisom.

Zakon za izjemne primere s področja nacionalne varnosti, obrambe, javne varnosti, preprečevanja, odkrivanja in preganjanja kaznivih dejanj, ki pa morajo biti določeni z zakonom, lahko omeji pravice posameznika do vpogleda ali prepisa zbranih podatkov. Poleg tega pa določa tudi inšpekcijsko nadzorstvo nad izvajanjem določb tega zakona, inšpektorat pa je o svojem delu dolžan ministrstvu za pravosodje in varuhu človekovih pravic predložiti letno poročilo o svojem delu.

[51] Katalog zbirk osebnih podatkov je javno dostopen na spletnih straneh ministrstva za pravosodje (http://www.sigov.si/mp/) in se dnevno dopolnjuje.

V letnem poročilu inšpektorata za varstvo osebnih podatkov za leto 2001[52] Jože Bogataj ugotavlja, da je v letih 1996 do 2001 prišlo do povečanega števila prijav, pritožb in pobud posameznikov, kar kaže na to, da se posamezniki vedno bolj zavedajo pravic iz zasebnosti. Poročilo ugotavlja, da je večina kršitev posledica nezadostnega poznavanja oziroma nerazumevanja posameznih določb *zakona o varstvu osebnih podatkov* (Bogataj 2001, 18). Inšpekcijsko poročilo je opozorilo predvsem na te kršitve: upravljavci zbirk osebnih podatkov informacij o svojih zbirkah ne posredujejo v katalog ministrstva za pravosodje, osebni podatki so pogosto neustrezno zavarovani, pomanjkljivo je tudi evidentiranje posredovanja osebnih podatkov drugim uporabnikom, včasih so osebni podatki posredovani tudi nepooblaščenim uporabnikom (npr. v bolnišnicah in zdravstvenih zavodih), inšpekcijski nadzor je odkril več primerov obdelave osebnih podatkov brez ustrezne pravne podlage oziroma brez pisne privolitve (posebej izpostavljen je npr. video nadzor v javnih zgradbah, če se seveda video posnetki shranjujejo in se s tem formira zbirka osebnih podatkov), osebni podatki se shranjujejo predolgo ali pa se zbira čezmerno število osebnih podatkov. Javni sektor načeloma lahko obdeluje le osebne podatke, določene z zakonom, razen kadar zakon določa pisno privolitev posameznikov. Za zasebni sektor pa velja, da lahko obdeluje tudi tiste vrste osebnih podatkov, ki v zakonu niso ustrezno določene, vendar pa si mora za to pridobiti ustrezno pisno privolitev posameznika. Inšpektorat za varstvo osebnih podatkov zato ugotavlja, da zaradi tega v praksi pogosto prihaja do izsiljevanja posameznika in čezmernega zbiranja osebnih podatkov (Bogataj 2002, 20–21). Upravljavci tudi pogosto kršijo pravice posameznika, saj po ugotovitvah inšpektorata posamezniku pogosto ne dovolijo vpogleda, prepisa in izpisa podatkov, prav tako pa ravnajo tudi kadar posameznik zahteva popravek ali izbris podatkov.

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

[52] Poročilo o delu inšpektorata za varstvo osebnih podatkov v letu 2001 je dostopno na spletnih straneh ministrstva za pravosodje, pripravil pa ga je Jože Bogataj, v. d. glavnega inšpektorja za varstvo osebnih podatkov.

ministrstvu posredoval samo en ponudnik dostopa do interneta, pozneje pa se mu je pridružil še eden.

Ponudniki dostopa imajo sicer na podlagi sklenjene pogodbe z uporabnikom pravico do zbiranja osebnih podatkov, vendar bi morali kljub temu uporabnike seznaniti s tem, katere osebne podatke bodo zbirali (in pri tem ne pozabiti na podatke, ki se zbirajo v datotekah aktivnosti), kakšen je namen zbiranja in obdelave teh podatkov ter kolikšen je čas shranjevanja teh podatkov. Po naših informacijah je splošno stanje na tem področju takšno, da uporabniki s tem večinoma niso seznanjeni. Drugi odstavek 131. člena *zakona o telekomunikacijah* določa, da za potrebe obračunavanja storitev operater do plačila storitve ali preteka zastaralnega roka lahko shranjuje (prometne) podatke, na podlagi katerih lahko uporabniku obračuna svojo storitev, po naših informacijah pa se podatki iz datotek aktivnosti hranijo dlje časa, poleg tega se hranijo tudi pri tistih uporabnikih, ki dostopa do interneta ne plačujejo ali pa plačujejo fiksno ceno. Nova direktiva EU 2002/58 o obdelovanju osebnih podatkov in varstvu zasebnosti na področju elektronskih komunikacij državam članicam že omogoča hranjenje katerihkoli prometnih podatkov za določen čas, v pripravi pa je tudi »ukrep, ki bo državam članicam naložil uzakonitev obveznosti ponudnikov telekomunikacijskih storitev, da hranijo prometne podatke 12 do 24 mesecev« (Možina 2002, 4). Ti podatki pa bodo (oziroma so) državnim organom dostopni na podlagi sodnega naloga. Problem takšnega hranjenja je seveda v tem, da se državi s tem omogoča »(pre)velik vpogled v aktivnost uporabnikov, ki niso ničesar osumljeni« (Možina 2002, 4).

V zvezi z internetom tudi nastaja vprašanje, kaj je nepretirano zbiranje osebnih podatkov, sploh če namen zbiranja osebnih podatkov ni znan. Nekateri ponudniki dostopa do interneta oziroma internetnih storitev (elektronska pošta, spletno gostovanje...) zbirajo veliko število osebnih podatkov, tudi take, ki lahko kažejo socialno in ekonomsko ozadje posameznika. Ni tudi odveč opozoriti, da zakon dovoljuje le zbiranje podatkov neposredno od osebe, zato zbiranje podatkov npr. o sorodnikih osebe ni zakonito. Prav tako je vprašanje, kakšno je varovanje zbranih osebnih podatkov, predvsem pa ni znano ali imajo ponudniki dostopa do interneta v notranjih aktih predpisane ustrezne organizacijske in logično-tehnične postopke za njihovo zavarovanje.

Do sedaj še ni znan primer, da bi kdo izmed uporabnikov zahteval vpogled ali prepis svojih osebnih podatkov, 18. člen *zakona o varstvu osebnih podatkov* pa določa, da stroške v zvezi z zahtevo in izpisom teh podatkov nosi upravljavec zbirke. Zato se je treba vprašati, ali so ponudniki dostopa do interneta organizacijsko in tehnično sploh pripravljeni na izpolnjevanje *zakona o varstvu osebnih podatkov*. Zaradi tehničnih značilnosti interneta morda tudi ne bi bilo odveč razmisliti o spremembi zakonodaje, ki bi določala, da bi bilo treba prenos osebnih podatkov po nezaščitenem internetu *vedno* zavarovati s kriptografskimi metodami in morda tudi z digitalnim podpisom.

Podobna vprašanja se porajajo tudi pri zbiranju osebnih podatkov po internetu in pri t.i. *on-line* registraciji programske opreme. Poleg tega da uporabniki pogosto niso seznanjeni z namenom zbiranja in časom hranjenja tako zbranih osebnih podatkov, se ti prek interneta pogosto prenašajo nezavarovani, prenašajo pa se tudi v tuje države. Poleg tega zakon izrecno zahteva pisno privolitev, ki pa jo je prek interneta težko izpeljati. *Zakon o elektronskem poslovanju in elektronskem podpisu* v 15. členu sicer določa, da je t.i. varni elektronski podpis,[53] ki je overjen s kvalificiranim potrdilom, enakovreden lastnoročnemu podpisu, vendar uporaba elektronskega podpisa v Sloveniji v praksi še ni zaživela.

Zaradi vsega tega bi bilo treba nujno zagotoviti čimprejšnjo in dosledno varstvo osebnih podatkov na internetu, potrebne pa bi bile tudi nekatere spremembe zakonodaje, predvsem določbe o pisni privolitvi, saj jo je ob sedanjih zakonskih rešitvah preko interneta preveč zapleteno izvajati. Hkrati pa bi bilo tudi smiselno za nekatere vrste podatkov na internetu določiti drugačne pogoje varstva, saj morajo biti nekateri podatki zaradi svoje narave javno dostopni, nadzor dostopa pa iz praktičnih razlogov ni mogoč (v mislih imamo predvsem podatke o lastnikih spletnih domen iz DNS zapisov), po drugi strani pa bi bilo treba zakonsko zaščititi tudi tiste vrste osebnih podatkov, ki niso strogo osebni, na primer elektronske sledi javno dostopnih računalnikov.

[53] Zakon v 2. členu določa, da je varen elektronski podpis tisti, ki izpolnjuje tele zahteve: da je povezan izključno s podpisnikom; da je na njegovi podlagi mogoče zanesljivo ugotoviti podpisnika; da je ustvarjen s sredstvi za varno elektronsko podpisovanje, ki so izključno pod podpisnikovim nadzorom; da je povezan s podatki, na katere se nanaša, tako da je opazna vsaka poznejša sprememba teh podatkov ali povezava z njimi.

Hkrati bi bilo treba razmisliti o mehanizmih, ki bi zasebnemu sektorju onemogočali izsiljevanje z zbiranjem nepotrebnih osebnih podatkov in z njimi povezano kartelno dogovarjanje. Sedanja ureditev namreč lahko privede do položaja, v katerem bi se podjetja, ki ponujajo neke storitve, med seboj lahko dogovorila, da bodo svoje storitve ponujala samo uporabnikom, ki bodo dali pisno soglasje za zbiranje in obdelavo osebnih podatkov v velikem obsegu. Uporabniki, ki takšne privolitve ne bi želeli podpisati, pa zaradi kartelnega dogovora ne bi imeli možnosti dostopa do storitve.

Glede varovanja osebnih podatkov bi bilo treba razmisliti o standardizaciji organizacijskih in logično-tehničnih postopkov za njihovo varovanje. Poročilo inšpektorata za varstvo osebnih podatkov ugotavlja, da ima policija dokaj dobro urejeno področje varstva osebnih podatkov (Bogataj 2002, 10), zato morda ne bi bilo odveč, če bi se zgledovali po njihovih postopkih. Postopki bi morali vključevati tudi nadzor dostopa in omogočati poznejše ugotavljanje, kdo je dostopal do katerih podatkov, kako, kdaj in s kakšnim namenom. Poleg tega bi bilo z uporabo kriptografije in fizičnega varovanja mogoče preprečevati tudi nepooblaščene dostope.

Zaradi organizacijskih zahtev na nekaterih področjih preprečevanje zbiranja osebnih podatkov ni uresničljivo. Zato bi bilo treba doseči transparentnost zbiranja in uporabe osebnih podatkov ter s tem možnost njune zlorabe kar najbolj zmanjšati. Naloga zakonodaje je določanje pravil igre, ki jih je treba dosledno spoštovati. Zato tudi ne bi bilo odveč premisliti o kadrovski okrepitvi inšpektorata za varstvo osebnih podatkov.

SKLEP

Po Benigerju se revolucija nadzora vzdržuje sama na sebi, to pa omogočajo trije dejavniki. Izraba energije, hitrost procesiranja informacij in tehnologije nadzora sobivajo v pozitivni spirali – napredek enega faktorja povzroči ali vsaj omogoči napredek preostalih. Ne smemo tudi pozabiti na tehnološki napredek, saj tehnološke inovacije sprožajo potrebe po novih in novih tehnoloških inovacijah (Beniger 1986, 433–434), kar odpira nove možnosti, s tem pa se ustvarjajo tudi nove potrebe po nadzoru. Značilen primer so tehnologije zbiranja podatkov, ki so s seboj prinesle potrebo po tehnologijah shranjevanja podatkov, povečane zmogljivosti pomnilnih sistemov pa ustvarjajo možnosti za še bolj izpopolnjene in ekstenzivne metode zbiranja podatkov.

Zaradi tega se bo stopnja nadzora v družbi samo še povečevala in zelo verjetno teh teženj ne bo mogoče zaustaviti, vprašanje pa je tudi, ali bi bilo to smiselno. Problem zasebnosti neprestano niha med totalitarizmom in anarhijo, zato ni vprašanje, ali naj ga bolj obtežimo na eno ali drugo stran, pač pa je vprašanje, kako ujeti ravnotežje. Pomembno pa je, da družba nadzora ne postane totalitarna družba – in tu je treba opozoriti na izjemni pomen sprejema in uveljavitve ustrezne zaščitne zakonodaje, ki bo nadzorovanje naredila transparentno, predvsem pa je treba opozoriti na pomen demokratičnega nadzora nadzorovanja. Kakor je bilo prikazano, je eden najbolj nevarnih učinkov nadzorovanja panoptični učinek in proti njemu se v družbi nadzora lahko borimo predvsem z visoko stopnjo zaščite državljanskih in političnih svoboščin, predvsem svobode govora in svobode politične akcije. Zasebnosti nikakor ne smemo omejevati zgolj na individualno oziroma individualistično raven, pač pa jo je treba gledati skozi širšo optiko državljanskih svoboščin. Zasebnost je eden izmed temeljnih pogojev za aktivno državljanstvo, vendar pa končni cilj zakonodaje za zaščito zase-

bnosti ne sme postati zasebnost, ki vodi zgolj v individualizem in ograjevanje od družbe, pač pa zasebnost, ki vodi v aktivno državljanstvo. Če nekateri razumejo pravico do zasebnosti v splošnem kot pravico izrazito negativnega statusa, torej kot pravico posameznika, da se ga pusti pri miru, je pravica do komunikacijske zasebnosti, ki je močno povezana tudi z informacijsko zasebnostjo, enako pomembna vrednota. Namreč vzpostavljanje in vzdrževanje stikov z drugimi. Vrhovno sodišče ZDA je leta 1891 zapisalo, da je pravica do zasebnosti pomembna zato, ker pospešuje izmenjavo informacij z drugimi, ne pa zgolj zaradi zagotavljanja neodvisnosti in izolacije od drugih (Šturm et al. 2002, 392). Prav to pa je eden izmed pogojev za aktivno državljanstvo.

Določitev meje, do katere družba in posamezniki lahko vdrejo v posameznikove zadeve, je tako eden izmed izzivov, s katerimi se bo treba v prihodnje neprestano spopadati. Boj za pravice posameznika, razvoj demokratične kulture in razvoj tehnologije bodo tehtnico vedno obteževali na eni ali drugi strani, in teh obtežitev ne bo mogoče preprečiti, saj bodo notranje povezane s spremembami in razvojem. Zato bo najpomembnejše neprestano loviti ravnotežje in prav tu bosta morala pravo in družba nujno slediti tehnologiji.

LITERATURA

Allard, Nicholas W. in Kass, David A. 1997. Law And Order In Cyberspace: Washington Report. V *Hastings Communications and Entertainment Law Journal (Comm/Ent)*, 19 (3): pomlad 1997.

»Amsterdam Schiphol Launches 'Iris Scan' Trial«. 2001. *Airwise News*. <http://news.airwise.com/stories/2001/10/1004008821.html>. (17. avgust 2002).

»An Analysis of How the Events of September 11 May Change Federal Law«. 2001. *Tech Law Journal*. <http://www.techlawjournal.com/terrorism/20010917.asp>. (17. september 2001).

Bach, E., et al. 1999. »The Cryptography FAQ (05/10: Product Ciphers)«. <http://www.faqs.org/faqs/cryptography-faq/part05/>. (17. avgust 2002).

Banisar, David et al. 1999. *Privacy & Human Rights 1999*. <http://www.privacyinternational.org/survey/index99.html>. (23. maj 2000).

Batagelj, Zenel. 1997. »Direktni marketing, oglaševanje in internet«. <http://www.cati.si/papers/zbymm0003.html>. (23. maj 2000).

Beniger, James R. 1986. *The Control Revolution*. Cambridge, Massachusetts and London: Harvard University Press.

Bicknell, Craig. »Online Prices Not Created Equal«. 2000. Wired News. <http://www.wired.com/news/print/0,1294,38622,00.html>. (17. avgust 2002).

Black, Edwin. 2002. *IBM and the Holocaust*. London: Time Warner Paperbacks.

Bogataj, Jože. 2002. *Poročilo o delu Inšpektorata za varstvo osebnih podatkov v letu 2001*. Ljubljana: Ministrstvo za pravosodje Republike Slovenije.

Boyle, James. 1997. *Foucault In Cyberspace: Surveillance, Sovereignity, And Hard-Wired Censors*. <http://www.wcl.american.edu/pub/faculty/boyle/foucault.htm>. (19. januar 1998).

Raab, Charles D. 1997. »Privacy, democracy, information«. V *The Governance of Cyberspace,* Loader, Brian D., 155–174. London, New York: Routledge.

The Center for Democracy and Techology. <http://www.cdt.org/>. (19. januar 1998).

Chaum, David. 1996. »Achieving Electronic Privacy«. V *High Noon On the Electronic Frontier*, Ludlow, Peter. 1996. Cambridge, London: The MIT Press.

Clarke, Roger A. 1988. »Information Technology and Dataveillance«. V *Communications of the ACM*. 498–512. <http://www.anu.edu.au/people/Roger.Clarke/DV/CACM88.html>.

Compass. 1998. Government of Ontario. <http://www.mto.gov.on.ca/english/traveller/compass/>. (20. december 1998).

Cooley, Charles Horton. 1993. *Social Organization: A Study Of The Larger Mind; introduction by Philip Rieff*. New Brunswick and London: Transaction Publishers.

Council Resolution of 17. January 1995 On the Lawful Interception of Telecommunications. 1996. Bruselj : *Official Journal*, C 329. 1–6.

Macavinta, Courtney. 1999. »Real Networks faced with second privacy suit«. CNET News.com, <http://news.com.com/2102-1001-232766.html>. (17. avgust 2002).

Cult of the Dead Cow.1998. <http://www.cultdeadcow.com>. (23. maj 2000).

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

Data Protection Working Party. 2000. *Privacy on the Internet – An integrated EU Approach to On-line Data Protection*. <http://www.europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wpdocs_2k.htm>. (21. november).

Denning, Dorothy E. 1996. »The Clipper Chip Will Block Crime«. V *High Noon On the Electronic Frontier,* Ludlow, Peter. 215–216. Cambridge, London: The MIT Press.

——. 1997. »The Future of Cryptography«. V *The Governance of Cyberspace,* Loader, Brian D., 1997. 175–190. London, New York: Routledge.

Denning, Dorothy E. in Baugh, William E. 1999. »Hiding Crimes In Cyberspace«. V *Information, Communication & Society*, (2) 3. 251–276.

DoubleClick. 2002. »Doubleclick ad serving data shows rich media click-through rates to be six times higher than standard ads«. <http://www.doubleclick.com>. (26. oktober 2002).

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

Dupuis, Clement. 1999. *A Short History Of Crypto*. <http://webhome.idirect.com/jproc/crypto/crypto_hist.html>. (25. julij 2002).

E-mail imenik iskalnika Najdi.si. 2000. Noviforum. <http://www.najdi.si>. (1. oktober 2002).

EPIC. 1998a. *Crptography Policy*. <http://epic.org/crypto/>. (19. januar 1998).

———. 1998b. *Efforts to Ban Encryption*. <http://www.epic.org/crypto/ban/>. (19. januar 1998).

———. 1998c. *Key Escrow*. <http://www.epic.org/crypto/key_escrow/>. (19. januar 1998).

———. 1998d. *The Clipper Chip*. <http://www.epic.org/crypto/clipper/>. (19. januar 1998).

———. 2002. *Face Recognition*. <http://www.epic.org/privacy/facerecognition/>. (9. avgust 2002).

»FBI 'Fesses Up to Net Spy App«. 2000. Wired News. <http://www.wired.com/news/print/0,1294,49102,00.html>. (12. december 2000).

Felten, Edward W. in Schneider, Michael A. 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>. (1. december 2001).

Foucault, Michel. 1984. *Nadzorovanje in kaznovanje*. Ljubljana: Delavska enotnost.

Gantar, Pavel. 1993. *Sociološka kritika teorij planiranja*. Ljubljana: Znanstvena knjižnica FDV.

Glasner, Joanna. 2002. »DoubleClick to Open Cookie Jar«. Wired News. <http://www.wired.com/news/print/0,1294,54769,00.html>. (27. avgust 2002).

Gutmann, Peter. 1996. »Secure Deletion of Data from Magnetic and Solid-State Memory«. USENIX Security Symposium Proceedings. <http://www.safedelete.com/a-gutmann.phtml>. (1. december 2001).

Harrison, Ann. 2001. »Terror attacks revive crypto debate«. SecurityFocus. <http://www.securityfocus.com/news/256>. (19. september 2001).

Hastings Communications and Entertainment Law Journal (*Comm/Ent*). 1998. 19 (3). San Francisco: Hastings College of the Law.

How To Obscure Any URL. <http://www.pc-help.org/obscure.htm>. (13. januar 2002).

»Internet Watchdog Warns of Fake eBay Web Site«. 2002. Yahoo News. <http://story.news.yahoo.com/news?tmpl=story2&cid=575&ncid=738&e=6&u=/nm/20021211/wr_nm/crime_ebay_email_dc>. (11. december 2002).

Imenik elektronske pošte Slovenije. 1998. Telekom Slovenije. <http://afna.telekom.si>. (7. oktober 1998).

Improving Your Network Security Using SATAN. 2000. <http://www.cs.umbc.edu/~woodcock/cmsc482/proj1/satan.html>. (23. maj 2000).

Informacijski servis Agence Europe. 1999. Bruselj. <http://www.agenceurope.com/>. (3. februar 1999).

Information, Communication & Society. 1999. 2 (3). London: Sage Publications.

Interaktivni naravovarstveni atlas. 2002. Agencija RS za okolje.<http://212.103.140.243/nvatlas/>. (1. december 2002).

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>.

Joel, Deane. »Melissa manhunt creates precedent«. 1999. ZDNet News. <http://www.zdnet.com/zdnn/stories/news/0,4586,2237838,00.html>. (7. april 1999)

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

Kocher, C. Paul, Jaffe, Joshua in Jun, Benjamin. 1999. »Differential Power Analysis«. Konferenca Crypto '99, 15-19 avgust 1999. University of California, Santa Barbara. <http://www.cryptography.com/resources/whitepapers/DPA.pdf>. (1. december 2001).

Kocher, C. Paul. 1996. »Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems«. Advances in Cryptology

– CRYPTO '96, 16th Annual International Cryptology Conference, Santa Barbara, California, USA, August 18-22, 1996, Proceedings. V *Lecture Notes in Computer Science*, ur. Neal Koblitz. Vol. 1109, Springer. <http//www.cryptography.com/resources/whitepapers/TimingAttacks.pdf>.

Klemenčič, Goran et al. 2001. *Internet in pravo*. Ljubljana: Pasadena.

Kooiman, Jan. 1993. *Modern Governance – New Government-Society Interactions*. London: Sage publications.

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

Kuhn, Markus G. in Anderson, Ross J. 1998. »Soft Tempest: Hidden Data Transmission Using Electromagnetic Emanations«. V *Information Hiding, Second International Workshop*, ur. David Aucsmith, 124–142. IH'98, Portland, Oregon, USA, April 15–17, 1998, Proceedings, LNCS 1525, Springer-Verlag. <http://www.cl.cam.ac.uk/~mgk25/ih98-tempest.pdf>.

Kušej Gorazd, Marijan Pavčnik in Anton Perenič. 1992. *Uvod v pravoznanstvo*. Ljubljana: ČZ Uradni list RS.

Labriola, Don. 2002. »Is Media Player Spyware?«. Ziff Davis Media Inc. <http://www.extremetech.com/article2/0,3973,9615,00.asp>. (20. december 2002).

Lemos, Rob. 1999. »How GUID tracking technology works«. ZDNet News. <http://www.zdnet.com/zdnn/stories/news/0,4586,2234550,00.html>. (30. marec 1999).

Leskovšek, Tomaž. 2001. »Poznavanje lokacije uporabnika – Locating mobile users«. V *Razkrij svojo digitalno substanco : zbornik predavanj: telekomunikacije OI telecommunications mednarodna konferenca: človeku prijazna / tehnološko popolna / informacijska družba, Nova Gorica, 19.–21. september 2001,* 18–22. Ljubljana: Inštitut za telekomunikacije.

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

Loney, Matt. 2002. »Want Wi-Fi? Learn the secret code«. CNET News.com. <http://news.com.com/2102-1033-939546.html>. (26. junij 2002).

Ludlow, Peter. 1996. *High Noon On the Electronic Frontier*. The MIT Press: Cambridge, London.

Lyon, David. 1994. *The Electronic Eye*. Cambridge: Polity Press.

Manjoo, Farhad. 2001. »Making It Harder for Hijackers«. Wire News. <http://www.wired.com/news/print/0,1294,46782,00.html>. (13. september 2001).

McCullagh, Declan. »FBI Hacks Alleged Mobster«. 2000. Wired News. <http://www.wirednews.com/news/print/0,1294,40541,00.html>. (6. december 2000).

———. 2001a. »Anti-Attack Feds Push Carnivore«. Wired News. <http://www.wired.com/news/print/0,1294,46747,00.html.>. (12. september 2001).

———. »Senate OKs FBI Net Spying«. 2001b. Wired News. <http://www.wired.com/news/print/0,1294,46852,00.html>. (14. september 2001).

———. »Bush Bill Rewrites Spy Laws«. 2001c. Wired News. <http://www.wired.com/news/print/0,1294,46953,00.html>. (19. september 2001).

———. »Wiretap Bill Gets Third Degree«. 2001d. Wired News. <http://www.wired.com/news/print/0,1294,47111,00.html>. (26. september 2001).

McKay, Nial. 1998. »Europe Is Listening«. WiredNews. <http://www.wired.com/news/news/politics/story/16588.html>. (23. marec 2000).

Mesenbrink, John. 2002. »Biometrics Plays Big Role with Airport Security«. Security Magazine. <http://www.securitymagazine.com/CDA/ArticleInformation/features/BNP__Features__Item/0,5411,69728,00.html>. (20. december 2002).

Mlinar, Zdravko. 1994. *Individuacija in globalizacija v prostoru*. Ljubljana: SAZU.

Močnik, Rastko. 1985. *Beseda ... besedo*. Ljubljana: ŠKUC.

More About the Privacy Rights Clearinghouse. 1998. <http://www.privacyrights.org/fs/services.html>. (19. januar 1998).

Morehead, Nicholas. 2000. »Toysmart: Bankruptcy Litmus Test«. Wired News, <http://www.wired.com/news/business/0,1367,37517,00.html>. (20. december 2000)

Možina, Damjan. 2002. »Se Evropa odreka zasebnosti v korist varnosti?« *Informatika in pravo*, (1): 3-5, priloga *Pravne prakse*, št 43. Ljubljana: Gospodarski vestnik.

Oakes, Chris. »Monitor This, Echelon«. 1999. Wired News. <http://www.wired.com/news/politics/0,1283,32039,00.html>. (22. oktober 1999)

»The Phil Zimmerman Case«. InfoNation <http://www.info-nation.com/philzima.html>. (19. januar 1998).

Poulsen, Kevin. 2000. »Ex-CIA Chief: Beware Spy-Viruses«. Security Focus on-line. <http://online.securityfocus.com/news/38>. (20. december 2000).

Privacy in Cyberspace. 1998. <http://www.privacyrights.org/fs/fs18-cyb.html>. (19. januar 1998).

Raab, Charles D. 1993. »The Governance of Data Protection«. V Kooiman, Jan, *Modern Governance: New Government–Society Interactions,* 89–103. London: Sage publications.

Ross, Edward Alsworth. 1922. *Social Control: a survey of the foundations of order*. New York, London: The Macmillan Company.

RSA Laboratories. 2000. *RSA Laboratories' Frequently Asked Questions About Today's Cryptography, Version 4.1*. RSA Security Inc. <http://www.rsasecurity.com/rsalabs/faq/index.html>.

Sandberg, Jared. 2001 (4. februar). »Hackers poised to land at wireless AirPort«. The Wall Street Journal Online. <http://zdnet.com.com/2100-11-527906.html?legacy=zdnn>. (20. december 2002).

Schneier, Bruce. 1999. »European Cellular Encryption Algorithms«. Crypto-Gram. <http://www.counterpane.com/crypto-gram-9912.html>. (15. december 1999).

———. 2000. »Cookies«. Crypto-Gram. Counterpane Internet Security, Inc. <http://www.counterpane.com/crypto-gram-0002.html>. (15. februar 2000).

———. 2001a. »PGP broken«. Crypto-Gram. <http://www.counterpane.com/crypto-gram-0101.html>. (15. januar 2001).

———. 2001b. »802.11 Security«. Crypto-Gram. Counterpane Internet Security, Inc. <http://www.counterpane.com/crypto-gram-0103.html>. (15. marec 2001).

Shireen, Herbert J. 1998. *A Brief History of Cryptography*. Cybercrimes. <http://cybercrimes.net/Cryptography/Articles/Hebert.html>. (25. julij 2002).

Srivastava, Anita. 2001. »Dynamic Pricing Models – Opportunity for Action«. Center for Business Innovation. <http://www.cbi.cgey.com/pub/bi-news/pdf/dynamic_pricing_models_with_cover.pdf>

»Standard Feature Of Web Browser Design Leaves Opening For Privacy Attacks«. 2000. Science Daily. <http://www.sciencedaily.com/releases/2000/12/001208074325.htm>. (20. december 2000).

Statewatch Organisation (Monitoring the State and Civil Liberties in the European Union). 1999. <http://www.statewatch.org/>. (5. februar 1999).

A Statewatch Report. 1999. <http://www.freenix.fr/netizen/swreport.html>. (2. 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).

StopCarnivore.org. 2000. <http://www.stopcarnivore.org>. (20. december 2000).

StreetBeam. 2002. <http://www.streetbeam.com>. (17. oktober 2002).

Stubblefield et. al. 2001. »Using the Fluhrer, Mantin and Shamir Attack to break WEP«. AT&T Labs, <http://www.cs.rice.edu/~astubble/wep_attack.pdf>.

Šturm, Lovro ur. 2002. *Komentar Ustave Republike Slovenije*. Ljubljana: Fakulteta za podiplomske državne in evropske študije.

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. <http://www.fas.org/irp/program/process/europarl_draft.pdf>

Terraserver. 2001. Microsoft Corporation. <http://terraserver.microsoft.com/>. (1. december 2001).

»Towards A European Framework For Digital Signatures And Encryption«. <http://www.ispo.cec.be/eif/policy/97503toc.html>. (19. januar 1998).

Van Eck, Wim. 1985. »Electromagnetic Radiation from Video Display Units: An Eavesdropping Risk?«. Computers & Security. 296–286. <http://jya.com/emr.pdf>.

Vidmar, Tone. 1997. *Računalniška omrežja in storitve*. Ljubljana: Atlantis.

Watson, Rory. 1999. »Unija ukrepa proti nevarnosti kriminala«. V *Evropski dialog: revija za evropsko integracijo* [Slovenska izd.]. 1999. (januar–februar). Bruselj: Evropska komisija, Generalna direkcija za informiranje.

Webster, Frank. 1995. *Theories of the Information Society*. London: Routledge.

»What SATAN Is« 2000. <http://www.cs.ruu.nl/cert-uu/satan.html>. (30. april 2000).

»Wireless LAN Security«. 2002. An ISS Technical White Paper. Internet Security Systems. <http://documents.iss.net/whitepapers/wireless_LAN_security.pdf>.

»The Zimmerman Case«. 1995. The Ethical Spectacle. <http://www.spectacle.org/795/zimm.html>. (19. januar 1998).

Zimmerman, Phil. 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™ User's Guide«. V datoteki PGPDOC1.TXT v programskem paketu PGP ver. 2.6.2.

V knjigi je bila obravnavana naslednja slovenska zakonodaja, ki je, vključno s spremembami in dopolnitvami, dostopna po internetu:

- *kazenski zakonik*
- *konvencija o varstvu posameznikov glede na avtomatsko obdelavo osebnih podatkov*
- *ustava Republike Slovenije*
- *zakon o kazenskem postopku*
- *zakon o poštnih storitvah*
- *zakon o Slovenski obveščevalno-varnostni agenciji*
- *zakon o telekomunikacijah*
- *zakon o varstvu osebnih podatkov*
- predlog *pravilnika o programski opremi in vmesnikih za zakonito prestrezanje komunikacij*, ki ga je 20. decembra 2002 pripravilo in v javno obravnavo dalo ministrstvo za informacijsko družbo.

SLOVAR UPORABLJENIH POJMOV

Algoritmični nadzor: analize podatkov s pomočjo kompleksnih algoritmov, ki omogočajo avtomatsko razpoznavo in sledenje.

Analiza električne aktivnosti (ang. *Differential Power Analysis*): ena izmed *tempest tehnik*, ki na podlagi električne porabe omogoča napadalcu razkritje šifrirnih ključev.

Biometrija: proces zbiranja, procesiranja in shranjevanja podatkov o posameznikovih fizičnih lastnostih z namenom identifikacije.

Brezžična lokalna omrežja (ang. *wireless LAN network*): omrežja za brezžično povezovanje računalnikov. Navadno temeljijo na protokolu 802.11b.

Brisanje začasnega pomnilnika (ang. *swap file*): ob zaustavitvi računalnika na disku ostane vsebina začasnega pomnilnika, njegovo brisanje pa onemogoča poznejšo obnovitev vsebine pomnilnika, kakršna je bila ob izklopu računalnika.

CCTV (*Closed Circuit Television*): nadzorne videokamere.

Carnivore: računalniški program, ki ga ameriški državni organi uporabljajo za prestrezanje vsega uporabnikovega internetnega prometa. Uradno se sistem imenuje DCS1000. V ZDA deluje od junija 2000.

Cult of the Dead Cow: hekerska skupina, ki je leta 1998 na svoji spletni strani objavila trojanskega konja Back Orifice, ki je namenjen nadzorovanju računalnikov prek interneta.

Časovni napad (ang. *Timing Attack*): ena izmed *tempest tehnik*, ki na podlagi merjenja časa, ki ga naprava porabi za procesiranje, napadalcu omogoča razkritje šifrirnih ključev.

Čistopis (ang. *cleartext, plaintext*): osnovno, nešifrirano sporočilo.

Datoteka aktivnosti (ang. *log file*): datoteka, kamor se beležijo dejavnosti uporabnika interneta. Vzdržujejo jih ponudniki dostopa do interneta in ponudniki različnih storitev interneta (predvsem spletnih strani).

DES (*Data Encription Standard*): eden najbolj razširjenih kodirnih algoritmov, ki se je uporabljal v civilni sferi, predvsem v bančništvu. Ameriška vojska pozna bližnjico za njegovo razbijanje.

Distribuirano procesiranje podatkov prek interneta: procesiranje podatkov v omrežju računalnikov, povezanih prek interneta, kjer vsak računalnik sprocesira le košček informacije. Skupna procesorska moč tako povezanih računalnikov je zelo velika.

DNS (*Domain Name System*): sistem, ki skrbi za pretvorbo imen domen v ustrezne IP naslove. Zasnovali so ga leta 1983 na Univerzi Wisconsin v ZDA.

Družba dosjejev: družba, v kateri o vsakem posamezniku obstaja neki zapis, neki dosje. Ljudje tako čedalje bolj postajamo svoji dosjeji, saj ti tvorijo našo podobo.

Družba nadzora: družba, v kateri je nadzor maksimiran. Webster je namesto uporabe pojma informacijska družba predlagal uporabo pojma družba nadzora.

ECHELON: sistem, ki je bil prvotno zgrajen za prestrezanje komunikacij Sovjetske zveze, Kitajske in drugih držav, danes pa se uporablja tudi za prestrezanje civilnih komunikacij.

Elektronska sled: informacija, ki se shranjuje rutinsko in kaže na akcije določenega posameznika, tudi informacija, ki jo posamezniki za seboj puščamo v virtualnem prostoru.

Enkratno geslo (ang. *one-time password*): geslo, ki je uporabno samo za enkraten vstop v sistem.

Faktorizacija: poseben matematični postopek iskanja praštevilčnih faktorjev danega števila. Napadalec, ki bi mu uspela faktorizacija, bi lahko na podlagi tega postopka odkril zasebni ključ in tako dešifriral sporočilo.

GIS baze: podatkovne baze geografskih informacijskih sistemov. Z njimi se lahko poveže druge baze podatkov in satelitske posnetke.

Groba sila, napad z grobo silo (ang. *brute force attack*): preskušanje vseh možnih kombinacij gesel. Metoda grobe sile zahteva veliko procesorskega časa in je zato razmeroma neučinkovita.

GUID, globalni univerzalni identifikator (ang. *Global Unique Identifier*): identifikacijska številka, ki se zabeleži v vse dokumente programskega paketa *Microsoft* v *Office 97*, kar omogoča poznejšo identifikacijo avtorja dokumenta.

Hollerithov stroj: predhodnik računalnika, ki ga je konec 19. stoletja izumil Herman Hollerith za obdelavo podatkov, prvič pa so ga uporabili v ameriškem popisu prebivalstva leta 1890.

ICMP (*Internet Control Message Protocol*): protokol za izmenjavo kontrolnih sporočil v internetu.

Identifikacija genetskega zapisa (ang. *DNA identification*): ena izmed najbolj kontroverznih biometričnih tehnik. Policije več držav skušajo vzpostaviti nacionalne baze odtisov DNA.

IP naslov (ang. *IP address*): virtualni naslov računalnika, s katerim je le-ta predstavljen v omrežju. IP naslov posameznega računalnika je lahko stalen (t.i. stalni IP naslov) ali pa dinamičen.

Izjava o zasebnosti (ang. *privacy statement*): izjava lastnika spletne strani, v kateri navadno pove kakšni osebni podatki se zbirajo, kakšen je namen zbiranja in kakšna bo uporaba zbranih osebnih podatkov.

Izkopavanje podatkov (ang. *data mining*): skupek statističnih in matematičnih tehnik za analizo velikih količin podatkov in iskanje vzorcev v njih.

Java: objektno orientiran programski jezik, ki ga je razvilo podjetje Sun Microsystems, zaradi svoje razširjenosti pa je primeren za izvajanje spletnih aplikacij.

JavaScript: skriptni programski jezik, ki ga je razvilo podjetje Netscape, namenjen pa je uporabi na spletnih straneh.

Klepetavost brskalnikov (ang. *browser's chattering*): pošiljanje podatkov o uporabnikovem virtualnem okolju s spletnih brskalnikov spletnim strežnikom.

Ključ: geslo, vrednost parametra v šifrirnem algoritmu, s katerim čistopis spremenimo v tajnopis. Pri asimetrični kriptografiji ločimo zasebne (ang. *private key*) in javne (ang. *public key*) ključe.

Kriptoanarhija: izraz, ki se je izoblikoval v zvezi s širjenjem javno dostopne kriptografije. Nekateri avtorji menijo, da zaradi te tehnologije država ne bo mogla več nadzorovati informacij, sestavljati dosjejev, prisluškovati, itd.

Kriptologija: veda o tajnosti, šifriranju, zakrivanju sporočil (kriptografija) in o razkrivanju šifriranih podatkov (kriptoanaliza). *Simetrična kriptografija:* za šifriranje in dešifriranje sporočila uporablja isti ključ (isto geslo). *Asimetrična kriptografija:* ključ za šifriranje je različen od ključa za dešifriranje.

Mikroskopiranje magnetnih sil (ang. *magnetic force microscopy*): metoda, pri kateri je prepisane podatke zaradi temperaturnega krčenja in širjenja diska mogoče rekonstruirati s pomočjo elektronskega mikroskopa.

Napad s slovarjem (ang. *dictionary attack*): iskanje gesla v vnaprej pripravljenih vrednostih, navadno gre za najpogostejše besede v danem jeziku.

NAT (*Network Address Translation*): vmesnik, ki omogoča vključitev skupine več računalnikov v internet prek istega zunanjega IP naslova. Včasih se za NAT vmesnik uporablja tudi izraz maškarada (ang. *masquerade*).

Navadno besedilo (ang. *plain text*): nešifrirano besedilo; v taki obliki se po internetu navadno prenaša elektronska pošta.

Nepovratno brisanje podatkov: posebna metoda, s katero podatke trajno uničimo tako, da jih ni mogoče obnoviti niti z metodo mikroskopiranja magnetnih sil. Metodo je razvil Peter Gutmann, zahteva pa 35-kratno prepisovanje po posebnem postopku.

Panoptični učinek nadzora: če je opazovanje nesimetrično oziroma hierarhično, ima za posledico negotovost, s čimer se doseže prostovoljno podrejanje posameznikov.

Panoptikon: zapor, katerega načrt je britanski vladi leta 1791 predstavil Jeremy Bentham. Zapor v resnici ni bil nikoli zgrajen, vendar je Foucault iz Benthamove ideje razvil idejo panoptikona kot politične tehnologije, ki deluje na podlagi subtilnih prisil in omogoča vzdrževanje oblasti.

Personalizirana povezava: povezava na isto spletno stran, ki je drugačna za vsakega uporabnika. Navadno se personalizirane povezave povezuje z elektronskimi naslovi, kar omogoča vodenje statistik odzivnosti.

PGP (*Pretty Good Privacy*): računalniški program, ki ga je leta 1991 napisal računalniški programer Phil Zimmerman in ki je namenjen šifriranju sporočil na osebnih računalnikih.

Piškotki (ang. *cookies*): 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. *Sejni piškotki* (ang. *session cookies*) potečejo ob zaključku brskalne seje, torej ko uporabnik zapre spletni brskalnik, *vztrajni piškotki* (ang. *persistent cookies*) pa imajo čas trajanja določen dlje, lahko

tudi več desetletij. *Piškotki obiskane spletne strani* (ang. *first-party cookies*) so piškotki, ki jih pošilja obiskana spletna stran, *piškotki, ki jih pošiljajo tretje spletne strani* (ang. *third-party cookies*), pa pošiljajo strani, ki so vključene v obiskano spletno stran, na primer strani oglaševalskih omrežij.

Podatkovni nadzor (ang. *dataveillance*): nadzor s pomočjo razpršenega zbiranja podatkov, ki jih kasneje lahko povežemo.

Portal: razširjena vstopna točka; spletna stran, na kateri je zbrano večje število povezav in koristnih informacij. Je uporabnikovo izhodišče za surfanje po internetu.

Posredniški poštni strežnik (ang. *relay server*): strežnik za posredovanje elektronske pošte na poti od pošiljatelja do naslovnika. Zakonodaja EU zahteva, da mora posredniški poštni strežnik sporočilo izbrisati takoj, ko je bilo uspešno posredovano dalje.

Požarni zid (ang. *firewall*): vmesnik med uporabnikovim računalnikom in omrežjem, ki lahko preprečuje neželeno vhodno ali izhodno komunikacijo.

Prehod (ang. *gateway*): točka v omrežju, prek katere se računalnik poveže iz lokalnega omrežja v internet.

Prestrezanje in kraja gesel (ang. *password sniffing*): prestrezanje paketkov, ki vsebujejo uporabniška imena in gesla.

Prestrezanje paketkov (ang. *packet sniffing*): s pomočjo te tehnike napadalec spremlja in analizira promet tujih računalnikov. Prestrezanje paketkov (tim. *promisc sniffing*) je bilo včasih posebej priljubljeno na lokalnih Ethernet omrežjih, ki so temeljila na tehnologiji koncentratorjev (ang. *hub*). Takšna 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. »*promisc* način«, je lahko prisluškoval prometu ostalih računalnikov v omrežju. Vendar pa je to tehniko mogoče zaznati. Današnje prestrezanje podatkov poteka predvsem preko spremljanja prometa na usmerjevalnikih (ang. *router*) oziroma podatkovnih povezavah.

Prijazno prisluškovanje (ang. *to wiretap friendly*): izraz označuje prisluškovalne zmogljivosti sodobnih telefonskih central, ki omogočajo tehnično preprosto prisluškovanje. Problem je, ker so sodobne telefonske centrale z vsemi prisluškovalnimi zmogljivostmi vred danes dostopne tudi posameznikom in podjetjem, ne samo operaterjem javne telefonije.

Priključni modul (ang. *plug-in*): dodatek, ki spletnim brskalnikom omogočajo prikaz nekaterih vsebin.

Profiliranje: postopek uvrstitve posameznika v neko kategorijo na podlagi njegovih zaznanih karakteristik.

Program za prestrezanje tipkanja (ang. *keyboard-sniffing device*): program, ki prestreza vse pritiske uporabnika na tipkovnico, najpogosteje pa je namenjen kraji gesel. *Magic Lantern:* posebno orodje za prestrezanje tipkanja, ki ga je razvil in ga pri svojem delu uporablja FBI.

Prstni odtis niza znakov (ang. *fingerprint*): unikatno število fiksne dolžine, ki ga s pomočjo zgostitvenega algoritma izračunamo iz poljubno dolgega niza znakov. Uporablja se za izračun digitalnega podpisa (ang. *digital signature*).

Računalniški virus: širše s tem izrazom označujemo vse programe ali programske kode, namenjene povzročanju škode ali obremenjevanju računalniških sistemov in z zmožnostjo, da se sami širijo. Ločimo destruktivne in instruktivne viruse.

Računalniško ujemanje in povezovanje zapisov (ang. *computer matching and record linkage*): tehnike za povezovanje različnih baz podatkov.

Revolucija nadzora: pri njej gre predvsem za zmožnost izrabe informacij in ima v 20. stoletju enak pomen, kot ga je imela v 19. stoletju industrijska revolucija.

Roboti, pajki ali črvi (ang. *spider, worm, [ro]bot,* včasih tudi *harvester*): programi za zbiranje podatkov iz spleta, pogosto so namenjeni zbiranju elektronskih naslovov.

RSA: asimetrični šifrirni algoritem, ki so ga leta 1977 razvili Rivest, Shamir in Adleman. Je eden izmed najbolj znanih šifrirnih algoritmov, implementiran pa je v programu PGP.

Samocenzurni učinek (ang. *chilling effect*): učinek, ki posameznika odvrne od »izstopanja« oz. uveljavljanja določenih pravic, na primer pravice do demokratičnega protesta.

Samoposodobitev (ang. *live update*): tehnologija za samodejno posodabljanje programske opreme in protivirusnih vzorcev.

SATAN (*Security Administrator's Tool for Analyzing Networks*): eden prvih javno dostopnih brezplačnih programov, ki prek interneta ali lokalnega omrežja išče varnostne luknje v računalniškemu sistemu.

Satelitski nadzor: opazovanje s pomočjo satelita, uporablja se na številnih področjih, tako v vojaške kakor civilne namene.

Sistem samodejnega razpoznavanja vozil (ang. *Vehicle Recognition System*): sistem, ki omogoča samodejno identifikacijo vozila na podlagi slike iz nadzorne kamere.

Sistem za prepoznavo obrazov (ang. *face-recognition system*): ena izmed biometričnih tehnik, ki se v ZDA uporablja za iskanje kriminalcev in pogrešanih.

»*Social engineering*«*:* goljufije, ko skušajo napadalci žrtev pretentati, da jim posreduje dostop do sistema ali želene podatke.

SpamAssasin: računalniški program, namenjen odkrivanju t.i. *spam* pošte (nezaželene/nenaročene elektronske pošte). Program označi vsako sporočilo s točkami, pri čemer pomeni večje število točk večjo verjetnost, da je sporočilo *spam*. Program omogoča točkovanje po poljubnih merilih.

Spletni hrošč (ang. *web bug*): majhna slika, navadno velikosti 1 x 1 *pixel*, ki uporabniku pošlje piškotek. Tehnologija se uporablja za sledenje uporabnikov spletnih strani, za postopek se uporablja tudi izraz sledenje s »*pixel* tehnologijo«.

Spletni medpomnilnik (ang. *browser's cache, web caching*): pomnilnik spletnega brskalnika, kamor se shranjujejo pogosto uporabljani statični podatki s spletnih strani (npr. slike). Tehnika časovnega napada (ang. *timing attack*) meri čas nalaganja spletne strani, s čimer je mogoče ugotoviti, ali je del poljubne spletne strani že naložen v medpomnilniku.

Spremenljivke o uporabnikovem virtualnem okolju (ang. *environment variables*): njihove vrednosti se pošiljajo upraviteljem spletnih strani, vsebujejo pa podatke, npr. o tipu uporabnikovega spletnega brskalnika, operacijskem sistemu, ki teče na njegovem računalniku, s katere spletne strani je uporabnik prišel do njihove spletne strani itd.

Statistika o odzivnosti (ang. responsegraphic): statistika o odzivnosti, npr. potrošnikov, na reklamno sporočilo.

Stranska vrata (ang. *back door*): obhod, skozi katerega sta napadalcu omogočeni oddaljeno nadzorovanje in upravljanje z računalnikom prek interneta, ne da bi lastnik tega računalnika to opazil.

SSL (*Secure Sockets Layer*): protokol, ki omogoča šifrirano povezavo med odjemalcem in strežnikom. Uporablja se v spletnem bančništvu ali v spletnih trgovinah.

Steganografija (ang. *steganography*): tehnike skrivanja sporočila (npr. v slikovne, zvočne ali tekstovne datoteke). Te tehnike so uporabne za implementacijo t.i. digitalnega vodnega tiska (ang. *digital watermark*) ali označevanje datotek z digitalnimi serijskimi številkami (ang. *digital serial numbers*).

Šifropis ali tajnopis (*kriptogram, ciphertext*): zašifrirano sporočilo, ki ga s pomočjo šifrirnega postopka in ključa dobimo iz čistopisa.

TEMPEST (*Transient Electromagnetic Pulse Emanation Surveillance Technology*): tehnika prestrezanja oddanih začasnih elektromagnetnih signalov (tempest v angleškem prevodu pomeni vihar), kar med drugim omogoča obnovitev slike z zaslona v odaljenosti več sto metrov.

Tempest pisave (ang. *tempest prevention font*): posebne pisave, s katerimi preprečimo da bi prisluškovalcu uspelo rekonstruirati dovolj jasno sliko z nadzorovanega zaslona. To je ena redkih znanih metod za preprečevanje *tempest napada*.

Trajno brisanje (ang. *wiping*) *vsebine datotek:* običajno brisanje datotek ne izbriše popolnoma, saj je mogoča obnovitev podatkov. Trajno brisanje pa stare podatke prepiše z novimi (navadno naključnimi) in s tem onemogoči njihovo obnovitev. Navadno se podatke prepisuje večkrat.

Trojanski konj: zlonamerni program, ki se navadno pretvarja, da je povsem običajen program, njegove skrite funkcije pa omogočajo zlorabo sistema. Za razliko od virusov se ne širi samodejno.

Varnostna pomanjkljivost (ang. *vulnerability*): namerna ali nenamerna pomanjkljivost v sistemu, ki omogoča napad na sistem.

Vohunski programi (ang. *spyware, E. T. application*): programi, namenjeni zbiranju podatkov o uporabniku. Največkrat gre za zbiranje marketinških podatkov.

WEP (*Wired Equivalent Privacy*): šifrirni algoritem ki ga uporabljajo brezžična omrežja, za šifriranje in nadzor dostopa. Algoritem so že uspeli razbiti.

»*Warchalking*«*:* poseben sistem oznak, ki v fizičnem svetu označujejo točke, kjer je mogoč dostop do brezžičnih omrežij.

Zastopniški program (ang. *proxy*): vmesnik med lokalnim računalnikom in internetom, ki v uporabnikovem imenu pošilja zahtevke za dostop do spletnih strani, prejete podatke pa nato posreduje uporabniku. *Anonimni zastopniški program* (ang. *anonymous*

proxy): zastopniški program, ki podatkov o svojih uporabnikih ne shranjuje (ali vsaj ne posreduje naprej) in jim s tem omogoča anonimno brskanje po internetu. V grobem ločimo navadne anonimne zastopniške programe (ang. *standalone anonymous proxy*) ter njihove spletne različice (ang. *web-based anonymous proxy*).

Zmožnosti za oddaljeno prisluškovanje (ang. *remote wiretapping port*): prisluškovanje po telekomunikacijskem omrežju, torej zunaj samega prostora, kjer je nameščena telefonska centrala.