KRIPTOGRAFIJA, ANONIMIZACIJA IN ODPRTA KODA KOT BOJI ZA SVOBODO NA INTERNETU

MATEJ KOVAČIČ

Povzetek

Ko je kriptografija v 60-tih letih pričela postajati javno dostopna so njeno javno uporabo državni organi v ZDA poiskušali omejiti, posledično pa je kriptografija pričela postajati politična tehnologija. Boj za javno dostopno kriptografijo je tako postal boj za zasebnost in svobodo posameznikov. Poiskusi (ameriških) državnih organov omejiti uporabo močne kriptografije sobili sicer neuspešni, vendar pa se je uporaba kriptografije razširila predvsem zaradi razlogov spodbujanja elektronskih transakcij in elektronskega poslovanja, ne pa kot tehnologija varovanja človekovih pravic in svobode posameznikov. Danes kaže, da uporaba kriptografije sama po sebi ne zagotavlja ustrezne stopnje zasebnosti posameznikov, hkrati pa se boj za zasebnost in svobodo nadaljuje še na dveh področjih. Eno je področje zagotavljanja transparentnosti informacijsko komunikacijskih sistemov z možnostjo vpogleda v programsko kodo, kar zagovarjata gibanji za odprto kodo in prosto programje. Drugo področje predstavlja razvoj anonimizacijskih sistemov. Del civilne družbe na internetu namreč anonimizacijske sisteme vidi kot mehanizem ohranjanja civilnih svoboščin na internetu, saj je množičen nadzor mogoče izvajati tudi z analizo prometnih podatkov, spremembe zakonodaje, ki zahtevajo hrambo prometnih podatkov pa nevarnosti sodobnih tehnologij nadzora še povečujejo. Kljub razvoju številnih tehnologij za zaščito zasebnosti pa se večina posameznikov svoji zasebnosti in svoji svobodi odpoveduje prostovoljno - zaradi udobja in brezbrižnosti.

Matej Kovačič je asistent na Fakulteti za družbene vede, Univerza v Ljubljani, e-naslov: matej.kovacic@fdv.uni-lj.si.

Kriptografija: od matematičnega problema do politične tehnologije

Nastanek sodobne kriptografije je povezan s pojavom telegrafa, ki je omogočal hiter in razmeroma preprost prenos sporočil na daljavo, s tem pa tudi možnosti razmeroma enostavnega centralnega prestrezanja. Pravi zagon razvoju kriptografije in kriptoanalize pa sta povzročila izum radia in njegova uporaba za komuniciranje v času prve svetovne vojne, ki je prestrezanje sporočil še olajšal (Kahn 1973, 154–155). Kljub vsemu je bila kriptografija do druge polovice 20. stoletja skoraj izključno v domeni vojske in tajnih služb, potrebe po njeni širši uporabi pa praktično ni bilo videti. S popularizacijo komunikacijske tehnologije se je to začelo spreminjati. Po eni strani se pojavi nevarnost zlorab s strani kriminala, s čimer se je začel vzpostavljati trg za kriptografske izdelke, po drugi strani pa so se s kriptografijo začeli čedalje bolj ukvarjati tudi neodvisni akademski raziskovalci, kar je v končni fazi povzročilo nastanek javno dostopne kriptografije.

Začetek komercializacije razvoja kriptografskih proizvodov predstavlja projekt Lucifer, v okviru katerega so v podjetju IBM konec 60. let osnovali skupino za kriptografske raziskave. Glavni razlog za začetek projekta je bila nevarnost računalniškega kriminala, v čemer je IBM prepoznal velik tržni potencial za prodajo šifrirnih naprav (Bamford 1983, 434). Projekt Lucifer je v ZDA pomenil prvo resno konkurenco šifrirnim algoritmom in napravam, ki jih je razvijala ameriška Agencija za nacionalno varnost (National Security Agency; NSA), saj se je: "prvič v zgodovini NSA soočila s konkurenco na lastnem ozemlju. Zunanji konkurenti pa niso bili ljubitelji, temveč visoko izobraženi profesionalci z neomejenimi sredstvi" (Bamford 1983, 435).

Hkrati so se s kriptografijo začeli ukvarjati tudi neodvisni akademski raziskovalci ameriških univerz. Na nek način je ironično, da je za popularizacijo kriptografije v akademski sferi delno zaslužna ravno ameriška Agencija za nacionalno varnost, ki se je kasneje profilirala kot izrazita nasprotnica javno dostopne kriptografije. NSA je namreč kmalu po ustanovitvi oblikovala desetčlanski znanstveno-svetovalni odbor, v okviru katerega je leta 1957 nastalo posebno poročilo; v njem je bilo predlagano, da si mora NSA zagotoviti dotok znanja in znanstvenikov iz akademskih krogov, če ZDA hočejo ostati vodilne na področju kriptografije (Bamford 1983, 429). Po eni strani si je NSA sicer želela sodelovanje z akademsko sfero, po drugi strani pa je plodove tega sodelovanja hotela obdržati samo zase. S tem namenom je med letoma 1956 in 1962 potekal projekt Lightening, ki je služil za zagon raziskav na področju kriptografije (Bamford 1983, 430). V okviru projekta sta potekali dve poletni šoli, Summer Campus Advanced Mathematics Program ter Advanced Language Program; udeležili so se ju številni znanstveniki in nastali so številni znanstveni članki, doktorske naloge in patentne prijave s področja kriptografije, ki so jih pripravili slušatelji iz akademske sfere. Projekt Lightning je tako rabil za zagon raziskav na področju kriptografije (Bamford 1983, 430), leta 1965 pa so v NSA odprli tudi National Cryptologic School (Bamford 1983, 153).

S tem so se teme, povezane s kriptografijo, usidrale tudi v akademski sferi; leta 1976 sta matematika Whitfield Diffie in Martin E. Hellman v reviji IEEE Transactions on Information Theory objavila članek z naslovom New Directions In Cryptography, kjer sta opisala protokol za varno izmenjavo šifrirnih ključev prek nezaščitenega medija, znan tudi kot sistem šifriranja z javnimi ključi. Leto pozneje

se je Ronald L. Rivest domislil novega šifrirnega algoritma, ki bi temeljil na sistemu javnih ključev, omogočal pa bi tudi digitalno podpisovanje. Algoritem je skupaj z Adijem Shamirjem in Leonardom M. Adlemanom opisal v članku, ki ga je septembra 1977 objavila revija Scientific American. Tehnične podrobnosti algoritma so objavili leto kasneje v reviji Communications of the ACM (RSA Laboratories 2000, 12). Algoritem, ki so ga po začetnicah avtorjev poimenovali RSA, je začrtal nove meje pri razvoju kriptografskih algoritmov. Močna kriptografija je začela postajati javno dostopna. Dokončen mejnik pri razvoju močne javno dostopne kriptografije pa predstavlja računalniški program PGP (Pretty Good Privacy), ki ga je leta 1991 napisal računalniški programer Philip R. Zimmermann in ki je za šifriranje elektronskih sporočil in računalniških datotek na običajnih osebnih računalnikih uporabljal algoritem RSA.

Seveda je pojav praktično nezlomljive javno dostopne kriptografije med ameriškimi državnimi organi sprožil strah, da država ne bi mogla več nadzorovati kriminala oziroma sovražnih dejavnosti proti njej sami, saj bi široka uporaba šifriranja onemogočila tako nezakonito kot tudi zakonito prestrezanje komunikacij. Da ta strah ni bil povsem neupravičen, dokazuje dejstvo, da so kriminalci v ZDA že konec 20. let (v obdobju prohibicije) pri medsebojnem komuniciranju uporabljali kriptografijo (Dupuis 1999), zaradi česar je ameriški FBI celo ustanovil posebni oddelek Cryptanalytical and Translation Section, ki se je ukvarjal z dešifriranjem sporočil tihotapcev alkohola (Shireen 1998; Bamford 1983, 471)

Po drugi strani pa se je za uporabo kriptografije, tokrat kot sredstva zaščite pred preveč radovedno državo, začela zavzemati tudi civilna družba. Avtor šifrirnega programa PGP, Zimmermann, je v nekem pogovoru tako izjavil, da "skuša kriptografija izenačiti odnose moči med vlado in njenimi državljani", zaradi česar je "kriptografija zelo politična tehnologija" (Hoffman 1996).

Takšno gledanje na kriptografijo je bilo značilno predvsem za v 90. letih nastajajočo civilno družbo na internetu, katerega avantgardo so na nek način predstavljali t. i. cypherpunkerji. Gibanje je bilo ustanovljeno leta 1992 na univerzi v Berkleyju, izviralo pa je iz hekerske subkulture že iz konca 80. let. Cypherpunkerji, katerih namen je bil razvoj anonimizacijskih programov ter programske opreme za šifriranje podatkov in sporočil, elektronsko podpisovanje ter anonimni digitalni denar, so zagovarjali predvsem individualne svoboščine posameznika nasproti državi v virtualnem svetu ter odsotnost državne prisile na posameznika (May 1995). Vprašanje kriptografije so postavili predvsem v kontekst varstva zasebnosti oziroma še konkretneje: varstva posameznikove svobode pred državo. Eden izmed ustanoviteljev gibanja, Timothy C. May, je zapisal: "Kriptoanarhija osvobaja posameznike pred ... vlado. Za libertarce močna kriptografija zagotavlja sredstva za izogibanje vladi" (May 1995). In ko je ameriški FBI proti Zimmermannu, avtorju šifrirnega programa PGP, začel preiskavo zaradi suma, da je z objavo programa na internetu omogočil nezakonit izvoz vojaške tehnologije (Gimon 1995), je bil eden izmed najglasnejših očitkov civilne družbe, da "to, česar se, kot kaže, vlada resnično boji pri Zimmermanovem programu, ni precej dobra zasebnost (Pretty Good Privacy – ime Zimmermanovega programa, op. p.), temveč zasebnost kot taka" (The Ethical Spectacle 1995).

Del civilne družbe je kriptografijo dojemal kot tehnologijo, ki bo v razmerju med posameznikom in državo oslabila slednjo. Timothy C. May je na USENET-u tako zapisal: "... Virtualne skupnosti zunaj dosega vladnega nadzora bodo lahko

povzročile probleme pri zagotavljanju zakonitosti (ang. law enforcement) in pobiranju davkov. (Nekaterim od nas je ta vidik všeč.)" in "... moč nacionalnih držav bo zmanjšana ... Je to dobro? Večinoma je" (May 1995).

Po drugi strani pa del borcev za elektronsko zasebnost kriptografije ni videl kot orodja, ki bi oslabilo moč države, pač pa kot tehnologijo, ki bo zgolj znova vzpostavila porušeno ravnotežje med močjo posameznika in močjo države. Zimmermann je tako izjavil, da "če ne bomo storili nič, bodo nove tehnologije dale državi moč nadzora, o kakršni je Stalin lahko samo sanjal" (Zimmermann 1993). Pojav interneta in nove možnosti za nadzor komunikacij so namreč sprožile strah pred možnimi zlorabami s strani države. Ta strah je Zimmermann v nekem intervjuju izrazil takole: "Če bo slaba vlada nekoč prišla na oblast, bo to morda zadnja vlada, ki jo bomo izvolili" (Hoffman 1996). Podobnega mnenja kot Zimmermann je bil tudi Ronald Rivest, ki je v polemiki okrog uvedbe čipa Clipper, pri katerem so ZDA hotele uzakoniti tako kriptografijo, ki bi državnim organom omogočila dostop do nešifriranega besedila, zagovornici Clipperja Dorothy E. Denning zapisal:

> *Samo zato, ker si spoznala trenutne predstavnike različnih državnih agencij in čutiš, da jim lahko zaupaš, to še ne pomeni, da takšno zaupanje lahko prenesemo na njihove naslednike. Treba je vzpostavljati institucionalne varovalke zavor in ravnotežij (ang. checks and balances), ki premagajo občasne moralne spodrsljaje enega ali več trenutnih imetnikov oblasti ... Korumpirani predsednik lahko (za kopije šifrirnih ključev) ukaže, da se uporabijo za neustrezne namene* (Rivest 1994).

Tako je vprašanje kriptografije prenehalo biti zgolj matematičen problem, pač pa je to postala izrazito politična, celo aktivistična tehnologija, kar se je odrazilo tudi tako, da je vprašanje splošne uporabe kriptografije postalo eno pomembnejših vprašanj civilne družbe na internetu.

Boj za javno dostopnost kriptografije

Odkritje močne kriptografije v akademskih krogih in začetek pronicanja te tehnologije v javnost sta v ameriški državni administraciji sprožila preplah. Do odkritja algoritma RSA so ameriške vladne službe večino javnosti (in tujim državam) dostopnih kriptografskih metod znale razbiti, s pojavom računalniškega programa PGP pa je močna kriptografija postala dostopna splošni javnosti. Če so do začetka 70. let v ZDA imeli nad kriptografijo praktično popoln monopol vojska in tajne službe, pa se je z razvojem informacijsko-komunikacijske tehnologije, predvsem interneta, to začelo hitro spreminjati.

Ameriški državni organi so zato na različne načine skušali preprečiti javno dostopnost močne kriptografije. Prvi poskusi so bili celo deloma uspešni. James Bamford navaja, da je IBM-ov projekt razvoja komercialne šifrirne naprave Lucifer v NSA požel veliko pozornosti. Uslužbenci NSA naj bi redno obiskovali IBM in spremljali njihov napredek pri razvoju (Bamford 1983, 435), IBM pa naj bi tudi prepričali, da je šifrirni algoritem za civilno rabo priredila. Leta 1973 je namreč ameriški nacionalni urad za standarde (National Bureau of Standards) začel pripravljati standard za šifriranje civilnih komunikacij. IBM je v tem zaslutil poslovno priložnost in hotel svoj proizvod certificirati kot standard. Prvotna različica šifrirnega algoritma, ki ga je uporabljala tudi vojska, je uporabljala 128-bitni šifrirni ključ. IBM pa je na pobudo NSA šifrirni ključ skrajšal na 56 bitov, poleg tega pa so priredili še nekatere

matematične postopke v samem algoritmu. Po teh spremembah je NSA na spremenjenem algoritmu izvedla analizo in ugotovila, da naj bi v njem ne bilo nobenih statističnih ali matematičnih slabosti (Bamford 1983, 436). Modificirani algoritem je NBS januarja 1977 potrdil kot standard Data Encription Standard (DES).

Zaradi sprememb je DES požel številne kritike. Najglasnejša kritika, akademska kriptologa Martin E. Hellman in Whitfield Diffie, sta bila prepričana, da je bil DES oslabljen, in to namenoma. NBS je v odgovor kritikam leta 1976 pripravil dve delavnici s temo DES, na katerih so ugotovili, da bi razbijanje DES-a trajalo 17.000 let (Bamford 1983, 438), a kasnejši dogodki so pokazali, da ta ocena ni bila upravičena.

V letih 1990 in 1991 sta namreč izraelska kriptografa Eli Biham in Adi Shamir predstavila novo vrsto kriptoanalize, ki sta jo poimenovala diferencialna kriptoanaliza (ang. differential cryptanalysis), kasnejša analiza civilne različice DES-a pa je sprožila sum, da je bila le-ta namerno prirejena tako, da je bila učinkovitost tega dotlej neznanega napada nanj povečana (sci.crypt 1994). Hkrati so kritiki DES-a skušali razviti namensko napravo za razvijanje z DES-om ustvarjenih kriptogramov in s tem dokazati, da s tako opremo po vsej verjetnosti že razpolaga tudi NSA. Leta 1993 je Michael Wiener na konferenci o kriptografiji predstavil načrt za napravo za razbijanje 56-bitne različice DES-a po metodi grobe sile, ki bi stala okrog milijon dolarjev in bi DES lahko razbila povprečno v treh urah in pol. Julija 1998 pa je John Gillmore iz organizacije Electronic Frontier Foundation predstavil napravo DES Cracker, ki je z metodo grobe sile (ang. brute-force) in ob pomoči porazdeljene obdelave podatkov prek interneta DES razbila v 22 urah (RSA Laboratories 2000 63). Istega leta je skupina kriptografov predstavila tudi DES Cracker za 250.000 dolarjev, ki je DES razbil v manj kot treh dneh (Sykes 1999, 173). V dvaindvajsetih letih se je tako čas uspešnega napada na DES skrajšal z domnevnih 17.000 let na manj kot en dan.

Kljub delnemu uspehu, ki ga je NSA imela s civilno različico DES-a, pa je kmalu postalo jasno, da se zanimanje za kriptografijo povečuje in da obstaja verjetnost, da bodo kriptografske metode v prihodnosti razvijali povsem neodvisni raziskovalci. Zato je NSA skušala omejevati znanstveno raziskovanje in izvoz kriptografskih izdelkov onkraj meja ZDA ter vsiljevati svoje kriptografske standarde.

Sprva je NSA želela preprečiti vsakršno javno razpravo o kriptografiji. Direktor NSA Bobby Ray Inman je v javnem govoru marca 1979 dejal, da "je zelo realna in kritična nevarnost, da bo neomejena javna razprava o kriptoloških zadevah resno ogrozila zmožnost vlade, da opravlja obveščevalne dejavnosti (ang. signals intelligence), in zmožnost vlade, da zaščiti informacije v zvezi z nacionalno varnostjo pred tujimi sovražnimi izrabami" (EFF 2001). Hkrati je tudi zagrozil, da bo zahteval sprejem zakonov o omejevanju objave kriptografskih raziskav (Diffie in Landau 1999, 63). Kljub temu da je v demokratični družbi zaradi svobode govora raziskovalcem nemogoče preprečiti javno objavo svojih odkritij, je Inman leta 1983 naročil študijo o omejitvi akademskega raziskovanja na tem področju (Sykes 1999, 174). Ko so v NSA ugotovili, da pravnih možnosti za tovrstno omejevanje ni, so se odločili na raziskovalce pritisniti s finančnimi ukrepi.

Leta 1977 sta tako dva uslužbenca NSA (Bamford 1983, 441–442) obiskala direktorja sklada National Science Foundation Fredericka Weingartna in ga obvestila, da verjetno krši zakon, ker financira kriptografske raziskave Inštituta za tehnologijo v Massachusetsu (Massachusets Institute of Technology, MIT) (Diffie in Landau

1999, 62). Pri tem sta se sklicevala na predsedniško direktivo, ki naj bi dajala NSA pooblastilo, da se edina ukvarja s kriptografijo. NSA je pri tem računala, da bodo v primeru, da se sklad National Science Foundation pritiskom ukloni, postali edina ustanova, ki bi financirala tovrstne raziskave, ter tako dobili neposreden nadzor nad večino raziskovalcev s področja kriptografije.

A pri skladu National Science Foundation so podobne pritiske doživeli že dve leti prej in ugotovili, da omenjena predsedniška direktiva ne obstaja. NSA je zato predlagala sodelovanje, in sicer pri recenziranju predlaganih projektov ter pri financiranju. Leta 1980 je Leonard Adleman (MIT) hotel prijaviti projekt s področja kriptografije, a ga je NSF obvestila, da njegovega projekta ne more financirati, istega dne pa ga je poklical direktor NSA in mu sporočil, da bi si njegov projekt želela financirati NSA. Ker se je Adleman bal, da mu bo NSA postavila pogoje glede objave njegovih odkritij, je financiranje s strani NSA zavrnil (Bamford 1983, 455). Zaradi strahu raziskovalcev, da bodo v primeru financiranja s strani NSA podvrženi pritiskom, je bila kasneje sprejeta odločitev, da bo kriptografske raziskave NSF še naprej financirala neodvisno in da se smejo raziskovalci sami odločiti, čigavo finančno pomoč bodo sprejeli (Diffie in Landau 1999, 63).

Poskus uveljavitve finančnih pritiskov na raziskovalce ni uspel, NSA pa je omejitve skušala doseči še na druge načine. Na podlagi Invention Secrecy Act, sprejetega leta 1951, je NSA leta 1977 samostojnemu raziskovalcu Carlu Nikolaiju in profesorju z Univerze v Wisconsinu Georgeu Davidi, ki sta neodvisno hotela prijaviti vsak svoj patent s področja kriptografije, po prijavi na patentni urad izdala ukaz, da je njun izum postal tajen in da o njem ne smeta govoriti (Bamford 1983, 449). Prepoved je vključevala tudi predstavitve na znanstvenih konferencah. Zadeva je v javnosti sprožila precejšnje razburjenje, zato je NSA zaradi domnevne napake ukaza umaknila (Bamford 1983, 450–451, ter Sykes 1999, 173), kasneje pa je ameriško pravosodno ministrstvo presodilo, da so takšne omejitve neustavne (Phillips 2001, 256–257).

Ker tudi takšne omejitve niso uspele, so pri NSA skušali doseči vsaj prepoved izvoza močnih kriptografskih izdelkov brez ustreznih izvoznih dovoljenj, pri čemer so se oprli na International Traffic in Arms Regulations ter US Export Regulations. Izvozni predpisi so bili deležni številnih kritik zaradi poslovne škode, ki so jo povzročali ameriškim podjetjem, saj so bila podjetja prisiljena svoje izdelke za tuji trg prisiljena kriptografsko oslabiti, hkrati pa je pridobitev izvoznega dovoljenja za podjetje skoraj samodejno pomenila priznanje, da njihovi izdelki niso dovolj varni. Znan je primer, ko je podjetje DEC zaradi izvoznih omejitev in očitkov, da prodaja varnostno nezanesljive izdelke, opustilo vsaj eno računalniško rešitev za varno izmenjavo podatkov med računalniki (Phillips 2001, 257). Kot je pokazal primer šifrirnega programa PGP, ki se je, potem ko ga je ga je njegov avtor Zimmermann objavil na internetu, bliskovito razširil po vsem svetu, pa je bilo omejevanje digitalnih kriptografskih proizvodov z izvoznimi dovoljenji v obdobju interneta povsem neučinkovito. Povrh vsega je maja 1999 zvezno pritožbeno sodišče iz Kalifornije v primeru Bernstein proti Department of Justice razsodilo, da so izvozne omejitve v Export Administration Regulations, ki omejujejo distribucijo kriptografije, neustavne, ker omejujejo znanstveno izražanje (sodišče je zavzelo stališče, da je računalniški program, zapisan v programskem jeziku, oblika govora) in ker vladnim uradnikom podeljujejo neomejeno diskrecijsko pravico, s čimer je kršen prvi amandma ameriške ustave, ki zagotavlja svobodo govora. Zaradi vseh

teh razlogov so ZDA leta 2000 skoraj popolnoma sprostile izvozna dovoljenja za kriptografske izdelke (Madsen in Banisar 2000, 118).

NSA pa se je omejevanja javno dostopne kriptografije lotila še na en način – s poskusom vsiljevanja kriptografskih standardov. NSA je namreč skupaj z National Bureau of Standards (ki se je kasneje preimenoval v National Institute of Standards and Technology, NIST) hotela pripraviti državne kriptografske standarde za civilno sfero. Le-teh bi se obvezno morale držati vse državne agencije in podjetja, ki bi hotela sodelovati z njimi. V praksi pa so te standarde spoštovala tudi preostala podjetja, saj jim je spoštovanje standardov zagotavljalo združljivost in povezljivost z drugimi. Konec 80. let, v času priprave zakona Computer Security Act, je National Bureau of Standards skupaj z NSA v okviru projekta Capstone začel razvijati standarde za javno dostopno kriptografijo. Pred sprejetjem zakona je bil Kongres postavljen pred vprašanje, katera agencija naj skrbi za razvoj civilne kriptografije. NSA si je kongresnike prizadevala prepričati, da bi morali to vlogo prevzeti njeni uslužbenci, saj imajo že dolgoletne izkušnje s kriptografijo, poleg tega pa naj bi se s centraliziranim razvojem kriptografskih rešitev izognili dvojni birokraciji. Kongresnikov argumenti NSA sicer niso prepričali, je pa zakon določil, da se mora NIST pri pripravi kriptografskih standardov posvetovati z NSA (Diffie in Landau 1999, 68). Ker pa NIST za pripravo kriptografskih standardov ni dobil ustreznega financiranja in se je zavezal, da se bo o vseh vprašanjih, povezanih s kriptografijo, posvetoval z NSA (Diffie in Landau 1999, 70), si je NSA zagotovila, da bo na tem področju še naprej igrala pomembno vlogo.

Aprila 1993 so tako objavili predlog novega standarda za obdelavo podatkov (Federal Information Processing Standard), ki je predvideval uporabo standarda Escrowed Encrypted – depozita šifrirnih ključev. Standard je dopuščal uporabo močnih kriptografskih algoritmov, vendar pa bi morali uporabniki svoje ključe deponirati pri pooblaščeni agenciji, kar bi državnim organom omogočilo dostop do teh ključev (EPIC 1998a, in EPIC 1998b). Kmalu se je pojavila še različica za uporabo v telefonskih komunikacijah t. i. čip Clipper, NSA pa je začela kampanjo celo pri tujih državah, da bi sprejele standard (Sykes 1999, 176). ZDA so začele pritiskati tudi na OECD, naj sprejme kriptografske smernice, po katerih bi sistem depozita šifrirnih ključev postal mednarodni standard. Vendar pa sta bila oba predloga deležna številnih kritik. Med drugim so kritiki sredi leta 1994 uspeli dokazati, da se je zaradi napake v šifrirnem sistemu mogoče izogniti hrambi sejnih šifrirnih ključev, kar je celotno zamisel depozita povsem izničilo in zaradi česar je bil predlog še istega leta umaknjen (Phillips 2001, 264).

Je kriptografija prinesla osvoboditev od nadzora?

Tako so se praktično vsi poskusi omejevanja kriptografije v ZDA izkazali za neuspešne, saj so ali omejevali svobodo govora ali pa so s strani vlade predstavljene kriptografske rešitve vsebovale resne varnostne pomanjkljivosti. A če so bili cypherpunkerji, ki so skušali razširiti uporabo šifrirnih programov po vsem svetu, prepričani, da bo kriptografija temeljno spremenila naravo korporacij in vlade (May 1988), se dandanes – ko omejitev pri uporabi kriptografije praktično ni – zdi, da kriptografija ni prinesla želene osvoboditve.

Razlogi za to so večplastni. Po eni strani se kriptografija danes uporablja večinoma v sferi ekonomije. Tudi glavni razlogi zaradi katerih so države podprle neomejen razvoj in rabo kriptografskih izdelkov so bili ekonomski (predvsem

pospeševanje elektronskega poslovanja) in ne človekove pravice. To dokazujejo tudi 1997 sprejete Smernice OECD o kriptografski politiki, ki so med drugim izpostavile načelo, da: "za zaščito priznanega javnega interesa, npr. zaščito osebnih podatkov ali elektronskega poslovanja, lahko države sprejmejo kriptografske politike, s katerimi zahtevajo uporabo takih kriptografskih metod, ki bodo zagotavljale zadostno stopnjo zaščite" (OECD 1997) Kriptografija se tako dandanes že skoraj rutinsko uporablja za varovanje finančnih transakcij na internetu (npr. v elektronskem bančništvu) ter za zaščito avtorskih pravic (regijska zaščita vsebin na DVD ter različne rešitve za upravljanje digitalnih pravic (ang. Digital Rights Management) – DRM), ne pa tudi za zaščito medosebnih komunikacij. Če je uporaba šifriranja pri npr. elektronskem bančništvu razmeroma enostavna in globoko integrirana v sam sistem bančnega poslovanja, pa je šifriranje elektronske pošte ali neposrednih sporočil prek sistemov neposrednega sporočanja in IRC-a še vedno razmeroma zapleteno opravilo, saj v programske odjemalce praviloma niso privzeto vgrajeni standardizirani in enostavni šifrirni vmesniki.

Poleg tega se kriptografija uporablja predvsem za šifriranje podatkov med prenosom po nezaščitenih komunikacijskih omrežjih, npr. od uporabnika do ponudnika storitve, pri ponudniku storitve pa se podatki hranijo v nešifrirani obliki ali pa so šifrirani na tak način, da do njih poleg uporabnika lahko dostopa še ponudnik storitve. Tipičen primer so spletne storitve, kjer so podatki s pomočjo protokola SSL šifrirani le med uporabnikovim spletnim brskalnikom in spletnim strežnikom ponudnika storitve. Uporaba takšnega načina zaščite podatkov tako otežuje zgolj nepooblaščen dostop (npr. s strani kiberkriminala), ne pa dostopa do vsebine podatkov na splošno, s čimer ta tehnologija nastopa predvsem v vlogi zagotavljanja tajnosti transakcij oz. pospeševalca elektronskega poslovanja.

Odprta koda in zasebnost

Dejstvo, da se šifriranje uporablja le znotraj najbolj tveganih sistemov, na izhodu le-teh pa so podatki nešifrirani in s tem dostopni, pa je še posebej problematično zato, ker se osebni podatki posameznikov, elektronska in glasovna pošta itd. čedalje pogosteje hranijo pri ponudnikih storitev.

Tipičen primer je uporaba sistema brezplačne elektronske pošte GMail, ki ga od aprila 2004 ponuja Google. GMail je s svojo storitvijo postavil nove standarde ponujanja brezplačnih elektronskih predalov, saj je uporabnikom v poštnih predalih ponudil bistveno več prostora, kot so ga ponudniki brezplačne elektronske pošte ponujali do tedaj, kakovostne protismetne filtre ter možnost naprednega iskanja po arhivu sporočil. Google je ob promociji svoje storitve izrecno poudarjal, da sporočil ni več treba brisati, pač pa jih uporabniki lahko le arhivirajo. Kritiki so sicer začeli opozarjati, da bo Google nekoč v prihodnosti imel arhiv praktično vseh elektronskih sporočil na svetu (Privacy International 2004, 2), vendar uporabnikov to ni odvrnilo od uporabe nove brezplačne storitve. Dejstva, da se z uporabo različnih spletnih storitev zbirajo številni podatki o uporabnikih, se je javnost začela zavedati šele v zadnjem času. V začetku avgusta 2006 je ameriški ponudnik dostopa do interneta AOL na posebni spletni strani objavil iskalne nize (iskalne pojme, ki jih uporabniki vpisujejo v iskalnike) več kot 650.000 svojih uporabnikov interneta, ki so jih ti vpisovali v spletne iskalnike od marca do maja 2006. Šlo je za več kot 20 milijonov vpisov (1 % AOL-ovih podatkov za to obdobje), ki so bili sicer anonimizirani, kljub

temu pa so nekateri kmalu začeli odkrivati prave identitete posameznih uporabnikov (Schneier 2006a). Med drugim so odkrili tudi uporabnika, katerega iskalni nizi so kazali na to, da načrtuje umor svoje žene (Frind 2006). AOL je sicer objavil le iskalne nize svojih uporabnikov, predstavnik podjetja Google pa je leta 2006 potrdil, da lahko na podlagi IP-naslova ali vrednosti spletnega piškotka prikličejo arhiv seznama vseh iskalnih nizov, ki jih je v iskalnik vpisal določeni uporabnik (Kawamoto in Mills 2006); leta 2006 so Googlove iskalne nize tudi dejansko uporabili tudi kot dokaz proti osebi, obtoženi nezakonitega dostopa do brezžičnega omrežja (McCullagh 2006).

Vse to kaže, da uporabniki izgubljajo nadzor nad svojimi podatki. Bruce Schneier ugotavlja:

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

A ne samo to. V okolju, kjer prevladuje zaprtokodna in lastniška programska oprema, uporabniki tudi nimajo več kontrole in pregleda nad delovanjem sistemov. Privrženci gibanja za odprto kodo in svobodnega programja tako opozarjajo, da so zaprti sistemi netransparentni in da imajo lahko vgrajene skrite nadzorne mehanizme ali varnostne ranljivosti, ki omogočajo zlorabo.

Začetki gibanja odprte kode segajo v sredo 80. let, ko je bila ustanovljena organizacija Free Software Foundation, ki si prizadeva za širjenje ideje o svobodnem programju. Svobodno programje uporabniku omogoča, da programsko opremo prosto "poganja, kopira, distribuira, preučuje, spreminja in izboljšuje" (Free Software Foundation 2005a). Bistveni predpogoj za to je prost dostop do kode programa. Iz gibanja za svobodno programje je leta 1998 vzniknilo odprtokodno gibanje, ki zagovarja podobna stališča, vendar pa vprašanja licenciranja programske opreme ne vidi predvsem kot etičnega vprašanja, pač pa je bolj praktično usmerjeno (Free Software Foundation 2005b). Čeprav je svobodno programje oz. odprta koda pogosto brezplačno dostopna, gre pri tem predvsem za vprašanje svobode in ne za vprašanje cene: "'Svobodno programje' je vprašanje svobode, ne cene. Da bi razumeli ta koncept, je besedico 'svoboden' (ang. free) treba razumeti v kontekstu 'svobode govora' (ang. free speech), ne 'brezplačnega piva' (ang. free beer)" (Free Software Foundation 2005a). Čeprav so zahteve po odprti kodi pogosto prikazane kot nasprotovanje obstoječemu sistemu omejujočega avtorskega prava in celo kot napad na intelektualno lastnino, pa je boj za odprto kodo mogoče razumeti tudi na drugačen način.

Leta 1883 je flamski lingvist in kriptolog Auguste Kerchoffs objavil članek La cryptographie militaire, v katerem je izpostavil šest načel, ki jih morajo upoštevati dobri šifrirni sistemi. Eno izmed teh se imenuje Kerchoffsov zakon, ki pravi, da je dober šifrirni sistem varen, tudi če je o njem znano vse, razen šifrirnega ključa (Schneier 2002 ter Wikipedia – geslo 'Kerchoffs law').[1] Kerchoffsov zakon tako zavrača načelo, da je mogoče varnost zagotoviti s skrivanjem (t. i. 'security through obscurity'), ter poudarja načelo varnosti skozi transparentnost (ang. security through transparency). Kerchoffsov zakon opozarja na dejstvo, da skrivnost ne zagotavlja varnosti, pač pa da vsaka skrivnost celo predstavlja možno točko zloma

varnosti, saj je pri sistemih, ki niso odprti, veliko večja verjetnost, da je v njih kakšna napaka, ki bi jo javni pregled verjetno odkril, avtorji pa bi s tem dobili možnost, da jo odpravijo. Znani ameriški kriptolog Bruce Schneier pravi: "Ne spominjam se nobenega kriptografskega sistema, razvitega na skrivaj, v katerem ne bi, potem ko je bil razkrit javnosti, kriptografska skupnost našla napake" (Schneier 2002).

Kerchoffsovo načelo je mogoče prenesti tudi na programsko opremo. Eric S. Raymond tako pravi: "Vsaka varnostna programska oprema, ki ne predpostavlja, da sovražnik poseduje izvorno kodo, je nevredna zaupanja; zatorej: nikoli ne zaupaj zaprti kodi" (Raymond 2004). Če odprtost zagotavlja transparentnost in nadzor nad delovanjem informacijsko-komunikacijskih sistemov in s tem njihovo varnost za uporabnika, je boj za odprto kodo mogoče razumeti tudi v kontekstu boja za zasebnost.

Da onemogočen dostop do programske kode in posledična netransparentnost delovanja pred uporabnikom lahko skrivata prikrite nadzorne mehanizme, dokazuje tudi primer hitre izsleditve avtorja makrovirusa Melissa. Na začetku leta 1999 se je po internetu razširil makrovirus Melissa, FBI pa je avtorja uspelo izslediti v presenetljivo kratkem času. Ker je bil virus napisan v skriptnem jeziku, ki je del okolja MS Office, se je seveda pojavilo vprašanje, kako je FBI med številnimi uporabniki programskega paketa MS Office uspelo odkriti pravega avtorja. Izkazalo se je, da je Microsoft v Office 97 vgradil t. i. globalni univerzalni identifikator (ang. Global Unique Identifier), ki se je zapisal v vsak dokument MS Office in seveda tudi v kodo virusa Melissa. Del tega identifikatorja je bila tudi serijska številka omrežnega vmesnika, na podlagi česar je bilo mogoče ugotoviti, v katerem računalniku je nastal virus (Lemos 1999). Odkritje prikritega nadzornega mehanizma je poleg ostalih vprašanj odprlo tudi vprašanje, ali ni mogoče take tehnologije zlorabiti tudi za odkrivanje avtorjev ostalih vrst dokumentov ter s tem tudi preganjanja političnih oporečnikov.

Vsekakor so sodobni informacijsko-komunikacijski sistemi kompleksne naprave in že samo to dejstvo uporabnikom onemogoča vpogled v njihovo delovanje. Onemogočen dostop do programske kode transparentnost delovanja le še zmanjšuje, pogosto pa uporabniki niso niti formalni lastniki sistemov, ki jih uporabljajo, saj se čedalje bolj uveljavlja uporaba storitev (in celo programske opreme), s katerimi v resnici upravlja ponudnik storitve in ne uporabnik. V kontekstu množičnega nadzorovanja sta tako boj za transparentnost delovanja ter boj za odsotnost skritih nadzornih mehanizmov oziroma boj za vpogled v programsko kodo v svojem bistvu pravzaprav nadaljevanje boja za zasebnost in svobodo posameznikov. Boja, ki se je začel z zahtevo za prosto uporabo kriptografije.

Boj za anonimizacijo kot nadaljevanje boja za kriptografijo

Sodobni informacijski sistemi pa so zasnovani tudi tako, da čim bolj zmanjšujejo anonimnost posameznika, s čimer zagotavljajo varnost transakcij. Del teh prizadevanj je tudi hramba prometnih podatkov, ki za zasebnost posameznikov prinaša nove nevarnosti. Na podlagi analize prometnih podatkov je namreč mogoče ugotoviti vzorce komuniciranja in socialno omrežje akterjev kljub uporabi šifriranja. Eden bolj nazornih primerov možnosti, ki jih prinaša analiza prometnih podatkov, predstavlja primer analize tokov komuniciranja v ameriškem podjetju Enron.

V okviru preiskave proti Enronu (šlo je za enega večjih finančnih škandalov v ameriški zgodovini) je ameriška Zvezna komisija za regulacijo energetike (ang. Federal Energy Regulatory Commission) na svoji spletni strani objavila elektronsko pošto vseh uslužbencev Enrona. Na podlagi prometnih podatkov – kdo izmed uslužbencev je komu pošiljal elektronska sporočila – so raziskovalci MIT izvedli analizo in prikaz socialnega omrežja. Eden izmed raziskovalcev, William W. Cohen, je na spletni strani projekta Cognitive Assistant that Learns and Organizes zapisal: "Ti podatki so dragoceni; po mojem vedenju gre za edino obsežno zbirko 'pravih' elektronskih sporočil, ki je javna. Druge niso javne zaradi zadržkov glede zasebnosti" (Cohen 2004). Podoben poskus so na MIT izvedli tudi v akademskem letu 2004/2005. V okviru projekta Reality Mining so s pomočjo posebnega programa, ki so ga namestili na mobilni telefon, devet mesecev zajemali podatke o uporabi mobilnih telefonov stotih prostovoljcev. Beležili so podatke o lokaciji mobilnega telefona, komunikaciji (kdo in kako pogosto komunicira s kom) ter bližini ostalih (s pomočjo skeniranja prek povezave Bluetooth). S pridobljenimi podatki so uspeli razkriti vzorce vsakodnevnega vedenja uporabnikov, analiza pa je raziskovalcem celo omogočila, da s 85-odstotno natančnostjo predvidijo, kaj bodo uporabniki storili v naslednjem trenutku (MIT 2005, ter Singel 2005).

Zasebnost posameznikom omogoča, da avtonomno in neodvisno od okolice vzpostavljajo odnose z drugimi. Zasebnost zato ni samo osebnostna pravica, pač pa tudi družbena pravica (Šelih 1979, 151), ki ima tudi politični pomen, saj omogoča svobodo združevanja in svobodo političnega delovanja. DeCewova tako zasebnost povezuje s svobodo povezovanja z drugimi (Wagner DeCew 1997, 71). Pomemben del te razsežnosti zasebnosti je anonimnost. Leta 1958 je Vrhovno sodišče ZDA v primeru National Association for the Advancement of Colored People proti Alabami zavrnilo poizkus države Alabama, da bi združenje NAACP prisilila, naj razkrije seznam svojih članov. V odločitvi so izrecno poudarili, da prek ‚zasebnosti združevanja' (ang. privacy in one's associations) ščitijo svobodo združevanja (Sykes 1999, 85), s čimer so pravzaprav poudarili pomen pravice do anonimnosti. Podobno je Vrhovno sodišče ZDA leta 1960 v primeru Talley proti Kaliforniji odpravilo prepoved objave anonimnih pamfletov, in s tem še enkrat poudarilo pomen anonimnosti in zasebnosti kot pomembnih elementov pri ohranjanju politične svobode. Podobne ideale imajo tudi razvijalci anonimizacijskih sistemov na internetu. Organizacija Electronic Frontier Foundation, ki anonimizacijske sisteme vidi kot mehanizem ohranjanja civilnih svoboščin na internetu (EFF 2006), na spletni strani z opisom anonimizacijskega sistema Tor pravi: "Trenutni trendi v zakonodaji, politiki in tehnologiji ogrožajo anonimnost kot še nikoli prej ter spodkopavajo našo zmožnost svobodno govoriti in brati na internetu" (EFF 2006).

Ideje o razvoju anonimizacijskih sistemov so se pojavile že v zgodnjih 90. letih, vendar takrat problem anonimizacije ni bil navzoč v širšem obsegu, saj v tem času še ni bilo hrambe prometnih podatkov v takem obsegu, kot do tega prihaja danes, poleg tega pa je bilo v tem času v ospredju predvsem vprašanje svobodne rabe kriptografije. Zagotavljanje anonimnosti na internetu pa je bil že takrat eden izmed pomembnih ciljev gibanja cypherpunkerjev in ostale civilne družbe na internetu. Eric Hughes je v Cypherpunks manifestu tako zapisal: "Ko v trgovini kupim časopis in plačam z denarjem, ni treba vedeti, kdo sem" (Hughes 1993). Hkrati pa tudi ideje o obvezni hrambi prometnih podatkov niso nove. Prvi tovrstni poskusi

v Evropi segajo v leto 1996, ko je bila v evropskem uradnem listu objavljena Resolucija o zakonitem prestrezanju telekomunikacij (ang. Resolution on the Lawful Interception of Communications), ki je določila širok nabor prometnih podatkov, ki jih morajo v primeru sodne odredbe beležiti operaterji telefonskih komunikacij. Leta 2002 sprejeta Direktiva o zasebnosti in elektronskih komunikacijah pa je v 15. členu državam članicam že omogočila hranjenje prometnih podatkov za določeni čas tudi brez sodne odredbe, saj so z njo članice EU dobile možnost, da operaterjem telefonije lahko predpišejo rok obveznega hranjenja prometnih podatkov.

Kmalu po njenem sprejemu pa so se pojavile ideje o splošni obvezni hrambi prometnih podatkov. EU je pri tem izhajala iz bojazni, da se:

> *zaradi spremembe tehnologije, poslovnih modelov in ponujenih storitev (npr. enotne tarife za uporabo storitev (ang. flat rate), predplačniške in brezplačne elektronsko komunikacijske, storitve elektronska pošta, SMS in MMS sporočila) ... nekateri prometni podatki ne shranjujejo v takem obsegu kot v preteklih letih. Ti prometni podatki zato niso dostopni oblastem, kadar jih potrebuje* (DG Information Society and DG Justice and Home Affairs 2004).

Sprejemanje Direktive o obvezni hrambi prometnih podatkov so spremljali številni protesti, saj je do tedaj v Evropi veljalo, da so prometni podatki integralni elementi telefonskih komunikacij. Leta 1984 je namreč Evropsko sodišče za človekove pravice v primeru Malone proti Veliki Britaniji presodilo, da morajo prometni podatki uživati enako stopnjo varstva kot sama vsebina komunikacije oz. da naj bi za njihovo beleženje obstajal enak dokazni standard kot za prisluškovanje, z obvezno hrambo prometnih podatkov pa se postavlja načelno vprašanje beleženja osebnih podatkov oseb, ki niso ničesar osumljene ob dejstvu, da je mogoče te podatke kdaj kasneje uporabiti v postopku proti njim.

Direktivi sta nasprotovala tako posebna komisija Evropskega parlamenta, ki sta jo vodila evropski poslanec in poročevalec Komiteja Evropskega parlamenta za civilne svoboščine, pravosodje in notranje zadeve Alexander Alvaro (Alvaro 2005) ter Evropski parlament. Kljub nasprotovanju je bila direktiva decembra 2005 sprejeta. Sprejeta direktiva zahteva obvezno hrambo prometnih podatkov telefonskih in internetnih komunikacij (vključno z naslovi elektronske pošte) ter podatkov o lokacijah mobilnih telefonov, čas hrambe znaša od 6 do 24 mesecev, v nekaterih primerih pa tudi več, poleg tega pa direktiva ne omejuje, za katera kazniva dejanja je mogoče shranjene podatke uporabiti.

Če je bila s tem dana pravna podlaga za izvajanje nadzora prometnih podatkov, pa nekatera razkritja o dejavnosti NSA po terorističnih napadih 11. septembra 2001 kažejo, da imajo državni organi na voljo že tudi ustrezno tehnologijo za tovrsten množični nadzor. Konec leta 2005 je v javnosti prišlo do razkritja, da je NSA na podlagi ukaza predsednika ZDA brez sodnih odredb ter brez vednosti Kongresa prisluškovala Američanom (Schneier 2006b), sredi leta 2006 pa, da je ista služba zbirala tudi prometne podatke o telefonskih klicih več deset milijonov Američanov ter na zbranih podatkih izvajala statistične analize izkopavanja podatkov (t. i. data mining) (Page 2006). Zaradi teh razkritij je ameriška nevladna organizacija Electronic Frontier Foundation s skupino potrošnikov proti telekomunikacijskemu podjetju AT & T januarja 2006 vložila tožbo zaradi domnevno nezakonitega omogočanja dostopa do telefonskih klicev in elektronske pošte tajni službi NSA. V okviru sodnega postopka in nekaterih pričanj je prišlo na dan, da je imela NSA v dogovoru s podjetjem AT & T (ki ima okrog tretjinski tržni delež na področju širokopasovnega dostopa do interneta v ZDA) v mestu Bridgeton, kjer ima AT & T glavno vozlišče za lokalni in mednarodni

promet, ter v AT & T-jevem vozlišču v San Franciscu posebne nadzorne centre, od koder lahko nadzoruje omrežni promet (Harris 2006). Po nekaterih podatkih naj bi množično tajno nadzorovanje Američanov potekalo že sedem mesecev pred terorističnimi napadi 11. septembra 2001 (Harris 2006). Vsekakor tak projekt ne predstavlja nič novega, saj je med letoma 1945 in 1975 NSA oziroma njen predhodnik Black Chamber v okviru projekta Shamrock[2] v ustnem dogovoru z nekaterimi telekomunikacijskimi podjetji prestrezala vsa teleprinterska sporočila (posledica senatne preiskave je bil tudi sprejem Foreign Intelligence Surveillance Act, ki naj bi omejil poseganje NSA v zasebnost Američanov (Schneier 2006c). Vsi ti podatki kažejo, da ima NSA verjetno nadzor nad vsemi poglavitnimi telekomunikacijskimi vozlišči v ZDA.

Kljub temu da se dandanes zdi, da je tovrsten nadzor že vgrajen v informacijsko-komunikacijske sisteme, pa ideje o anonimizaciji še niso povsem zamrle, in to kljub temu da so tovrstni sistemi zaradi zlorab kiberkriminala (predvsem zaradi pošiljanja odpadne elektronske pošte) ter obtožb, da pomagajo pri distribuciji pedofilskih vsebin, sredi 90. let doživeli krizo in delni zaton.

Leta 2002 je nekaj posameznikov v enem izmed laboratorijev ameriške vojne mornarice začelo razvijati anonimizacijsko omrežje, ki bi temeljilo na posebnih preusmerjevalnih točkah, t. i. Onion routers. Razvoj omrežja je konec leta 2004 prevzela ameriška nevladna organizacija Electronic Frontier Foundation in ga poimenovala Tor. Za razliko od klasičnih anonimnih zastopniških programov (ang. anonymous proxy), ki so le enostavni vmesniki med uporabnikovim računalnikom in internetom, je Tor porazdeljeno omrežje anonimizacijskih strežnikov, med katerimi se preusmerja (šifriran) promet posameznega uporabnika, dokler ga na enem izmed izhodnih točk omrežja ne zapusti (EFF 2005). Sistem sicer deluje podobno kot klasični anonimni zastopniški vmesniki, vendar so vhodi v omrežje in izhodi iz njega izbrani naključno, zaradi česar je nadzor omrežja težji, zagotavljanje anonimizacije pa večje.

Če bitko za neomejeno uporabo močne kriptografije v 90. letih civilna družba vsaj formalno dobila, pa se zdi, da se zdaj začenja podobna bitka na področju zagotavljanja anonimizacije. Z največ težavami se trenutno soočajo operaterji omrežja Tor, ki še vedno deluje v razvojni fazi. Omrežje, ki ga sicer uporabljajo tudi številni politični oporečniki iz nedemokratičnih držav in katerega namen je poleg zagotavljanja anonimizacije tudi izogibanje cenzuri, je občasno zlorabljeno s strani kibekriminala. Operaterji izhodnih točk Tora se tako soočajo s preiskavami zaradi distribucije pedofilije, hekerskih vdorov in drugih oblik kibekriminala ter z obtožbami, da pomagajo ščititi kriminalce (Barbut 2006 in drugi). Poleg tega so se v Nemčiji pojavili celo predlogi za sprejem zakonodaje, ki bi od operaterjev anonimizacijskih sistemov zahtevala obvezno beleženje in hrambo prometnih podatkov o uporabi njihovih anonimizacijskih sistemov. Nemško pravosodno ministrstvo je namreč zavzelo stališče, da operaterji anonimizacijskih sistemov opravljajo javne telekomunikacijske storitve, zaradi česar bi morali šest mesecev hraniti prometne podatke (mk 2006).

Boj proti anonimizaciji poteka tudi na bolj prefinjenih ravneh. Operater neke izhodne točke anonimizacijskega omrežja Tor je namreč sredi leta 2005 začel javno objavljati sezname prestreženih uporabniških imen in gesel uporabnikov, ki so prek omrežja Tor uporabljali nešifrirane protokole za dostop do storitev interneta. Seznami so sicer objavljeni v obliki, ki ne omogoča neposredne zlorabe. Avtor

trdi, da sezname objavlja v opomin, da je potrebno pri uporabi anonimizacijskih sistemov uporabljati tudi druge varnostne mehanizme (Schmieder 2005), a primer je kljub temu pokazal, da anonimizacijske sisteme lahko zlorabijo državni organi. Povsem verjetno namreč je, da skušajo anonimizacijske sisteme vzdrževati ali vsaj nadzorovati različne tajne službe in s tem nadzorovati prav komunikacije tistih, ki se želijo izogniti nadzoru. Znani hardvardski profesor in strokovnjak za vprašanja zasebnosti Viktor Mayer Schönberger je na vprašanje o tem odgovoril:

> *Leta 1996 sta na konferenci na Harvardu dva govornika, ki sta delala za oz. tesno sodelovala z ameriško vlado, javno izjavila, da vladne službe ne samo v ZDA, pač pa tudi drugod vzdržujejo večje anonimne strežnike za pošiljanje elektronske pošte oz. anonimizacijske sisteme po vsem svetu. Izrecno sta omenila anonimizacijske poštne sisteme ... Izjava je bila javno izrečena in na moje izrecno vprašanje, ali je izjava za javnost, sta odgovorila 'da'. Kasneje sta izjavo javno zanikala, vendar pa uradni prepis konference potrjuje mojo različico zgodbe* (Mayer-Schoenberger 2006).

Čeprav je bitka za anonimnost na internetu s sprejemom Direktive o obvezni hrambi prometnih podatkov začela postajati izgubljena, pa ideje o anonimizaciji nikakor niso zamrle. Zdi se celo nasprotno, saj tehnologija anonimizacije znova nastopa kot branik svobode, s čimer se tehnologija spet politizira. S tem tehnologija anonimizacije nadaljuje boj za zasebnost in svobodo posameznikov, ki ga je ob začetkih interneta začela kriptografija.

Sklep

Civilna družba je kriptografijo v 90. letih videla predvsem kot orodje zagotavljanja varstva posameznikove zasebnosti in svobode, a njena splošna uporaba se je na koncu razširila predvsem zaradi razlogov spodbujanja elektronskih transakcij in elektronskega poslovanja. Kriptografija je namesto vloge varovanja človekovih pravic dobila predvsem vlogo varovanja ekonomskih interesov korporacij. Hkrati so spremembe modela od trženja programske opreme do trženja storitev povzročile, da imajo posamezniki nad svojimi podatki čedalje manj nadzora, saj z njimi čedalje bolj upravljajo ponudniki storitev. S tem posamezniki izgubljajo neposredni nadzor nad svojimi podatki in to tudi v primeru transparentnosti tehnologije in uporabe odprtokodnih programskih rešitev. V bodoče sicer lahko pričakujemo povečano uporabo odprtokodnih programskih rešitev, vendar to pri varstvu zasebnosti ne bo prineslo bistvenega napredka, saj se bodo trendi ponujanja informacijskih storitev z oddaljeno hrambo uporabniških podatkov le še nadaljevali. Glavni boji za svobodo in zasebnost bodo verjetno v prihodnosti potekali na področju anonimizacije. Sodobne tehnologije za upravljanje digitalnih pravic (DRM) namreč poleg preprečevanja nezakonite rabe avtorsko zaščitenih digitalnih vsebin preprečujejo tudi anonimno potrošnjo le-teh. Hkrati DRM tehnologije omogočajo uveljavitev poslovnega modelova obračunavanja glede na dejansko uporabo digitalnih vsebin ter povezovanje podatkov o potrošnji konkretnih multimedijskih vsebin z identiteto konkretnega potrošnika. To omogoča številne tržne analize in večanje zaslužkov, čemur se lastniki avtorsko zaščitenih digitalnih vsebin verjetno ne bodo želeli odreči. Po mnenju članov Electronic Privacy Information Centra tako DRM tehnologije "označujejo pomemben razvojni mejnik v uporabi avtorskega prava... Avtorske pravice se uporabljajo kot opravičilo tako za zaščito vsebine kot tudi

za profiliranje potrošnikov vsebine" (EPIC, 2004). S tem vprašanjem se bodo slej ko prej morali soočiti tudi razvijalci in podporniki anonimizacijskih sistemov, ki le-te razvijajo zaradi ohranjanja splošne svobode brati in pisati na internetu. Zna se namreč zgoditi, da bodo v prihodnosti anonimizacijski sistemi zaradi visoke stopnje nadzora neuporabni oz. se jih bo uporabljalo le v omejenem in strogo nadzorovanem obsegu, na primer pri zagotavljanju tajnosti elektronskih volitev, hkrati pa njihovi uporabniki ne bodo mogli uporabljati internetnih storitev, ki bodo zahtevale identifikacijo potrošnika.

Ob vsem tem pa je morda glavni problem svobode na internetu dejstvo, da se posamezniki svoji zasebnosti in svoji svobodi odpovedujejo zaradi funkcionalnosti in udobja, in to celo prostovoljno. Boyle ob tem upravičeno opozarja na šibko točko internetne civilne družbe, ki pogosto pretirano poudarja zgolj državni nadzor, ko pravi, da je "digitalni libertanizem neustrezen zaradi svoje slepote do učinkov zasebne moči" (Boyle 1997). Kot ugotavlja Arendtova "ogrožanje svobode v moderni družbi ne prihaja od države, kot domneva liberalizem, temveč od družbe" (Arendt 1958/1995, 69).

Ali, kot je zapisal Bruce Schneier: "Pomnite, grožnje zasebnosti v informacijski družbi ne prihajajo samo od vlade, pač pa tudi od zasebne industrije. In prava grožnja je zavezništvo med njima" (Schneier 2006d). Svobode si torej samo s tehnologijo ne bo mogoče izboriti.

Opombe:

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

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

Viri in literatura:

Agre E. Philip in Rotenberg Marc, ur. 2001. *Technology and Privacy: The New Landscape*. Cambridge, MA: MIT Press.

Alvaro, Alexander Nuno. 2005. Draft report on the initiative by the French Republic, Ireland, the Kingdom of Sweden and the United Kingdom for a Draft Framework Decision on the retention of data processed and stored in connection with the provision of publicly available electronic communications services or data on public communications networks for the purpose of prevention, investigation, detection and prosecution of crime and criminal offences including terrorism (8958/2004 – C6-0198/2004 – 2004/0813(CNS)). Committee on Civil Liberties, Justice and Home Affairs, 18. 4. 2005. <http://www.statewatch.org/news/2005/may/ep-data-ret-alvaro-report.pdf>. Datum dostopa: 24. oktober 2005.

Arendt, Hannah. 1958/1995. *Vita Activa*. Ljubljana: Krtina.

Bamford, James. 1983. *The Puzzle Palace*. Baskerville: Penguin Books.

Barbut, Olivier. 2006. Some Legal Trouble with TOR in France – elektronsko sporočilo Olivierja Barbuta, poslano na poštni seznam uporabnikov orodja za anonimizacijo Tor <or-talk@seul.org>, dne 13. maja 2006. <http://archives.seul.org/or/talk/May-2006/msg00074.html>. Datum dostopa: 14. maj 2005.

Boyle, James. 1997. Foucault in Cyberspace: Surveillance, Sovereignity, and Hardwired Censors. *University of Cincinnati Law Review* 66, 1, 177–205. [Dostopno tudi na: <http://www.law.duke.edu/boylesite/foucault.htm>. Datum dostopa: 30. maj 2004].

Cohen, W. William. 2004. Enron Email Dataset. <http://www-2.cs.cmu.edu/~enron/>. Datum dostopa: 7. december 2004.

DG Information Society and DG Justice and Home Affairs. 2004. DG INFSO – DG JAI consultation document on traffic data retention. Delovni dokument, 30. julij 2004. [Dostopno na: http://

europa.eu.int/information_society/topics/ecomm/doc/useful_information/library/public_consult/data_retention/consultation_data_retention_30_7_04.pdf. Datum dostopa: 26. maj 2004.]

Diffie, Whitfield in Landau, Susan. 1999. *Privacy On the Line: The Politics of Wiretapping and Encryption*. Cambridge, MA: MIT Press.

Dupuis, Clement. 1999. CISSP Study Booklet on Cryptography. <http://comsec.theclerk.com/CISSP/Domain_5.html>. Datum dostopa: 21. april 2005.

EFF. 2001. EFF Quotes Collection 19.6. <http://www.eff.org/Misc/EFF/?f=quotes.eff.txt>. Datum dostopa: 22. april 2005.

EFF. 2006. Tor: An Anonymous Internet Communication System. <http://tor.eff.org/>. Datum dostopa: 25. december 2006.

EPIC. 1998a. Key Escrow. <http://www.epic.org/crypto/key_escrow/>. Datum dostopa: 19. april 2004.

EPIC. 1998b. The Clipper Chip. <http://www.epic.org/crypto/clipper/>. Datum dostopa: 19. april 2004.

Free Software Foundation. 2005a. The Free Software Definition. <http://www.fsf.org/licensing/essays/free-sw.html>. Datum dostopa: 20. december 2006.

EPIC. 2004. Digital Rights Management and Privacy. <http://www.epic.org/privacy/drm/>. Datum dostopa: 3. 6. 2004.

Free Software Foundation. 2005b. Why "Free Software" is better than "Open Source". <http://www.fsf.org/licensing/essays/free-software-for-freedom.html>. Datum dostopa: 20. december 2006.

Frind, Markus. 2006. AOL Search Data Shows Users Planning to commit Murder. *The Paradigm Shift blog*, 7. avgust 2006. <http://plentyoffish.wordpress.com/2006/08/07/aol-search-data-shows-users-planning-to-commit-murder/>. Datum dostopa: 8. avgust 2006.

Gimon, A. Charles. 1995. The Phil Zimmermann Case. *Info Nation*. <http://www.skypoint.com/members/gimonca/philzima.html>. Datum dostopa: 19. januar 2005.

Harris, Andrew. 2006. Spy Agency Sought U.S. Call Records Before 9/11, Lawyers Say. *Bloomberg.com*, 30. junij 2006. <http://www.bloomberg.com/apps/news?pid=20601087&sid=ablV0cO64zJE&refer=#>. (Datum dostopa: 3. julij 2006.

Hoffman, D. Russell. 1996. Interview with author of PGP. <http://www.animatedsoftware.com/hightech/philspgp.htm>. Datum dostopa: 26. maj 2005.

Hughes, Eric. 1993. A Cypherpunk's Manifesto. <http://www.activism.net/cypherpunk/manifesto.html>. Datum dostopa: 5. marec. 2004.

Kahn, David. 1973. *The Codebreakers*. New York: The New American Library.

Kawamoto, Dawn in Mills, Elinor. 2006. AOL Apologizes for Release of User Search Data. *CNET News.com*, 7. avgust 2006. <http://news.com.com/2100-1030_3-6102793.html?tag=nefd.top>. Datum dostopa: 8. avgust 2006.

Lemos, Rob. 1999. How GUID Tracking Technology Works. *ZDNet News*. <http://www.zdnet.com/zdnn/stories/news/0,4586,2234550,00.html>. Datum dostopa: 23. april 2005.

Madsen, Wayne in Banisar, David. 2000. *Cryptography & Liberty 200*0. Washington: EPIC.

May, C. Timothy. 1988. The Crypto Anarchist Manifesto. <http://www.activism.net/cypherpunk/crypto-anarchy.html>. Datum dostopa: 28. maj 2004.

May, C. Timothy. 1995. Crypto Anarchy and Virtual Communities. USENET, oddelki: talk.politics.crypto, alt.politics.datahighway in alt.cyberpunk. <http://www.idiom.com/~arkuat/consent/Anarchy.html#cryptoanarchy>. Datum dostopa: 28. maj 2004.

Mayer-Schoenberger, Viktor. 2006. A Question About Anonymous Remailers – elektronsko sporočilo Viktorja Mayerja-Schoenbergerja avtorju, 23. oktober 2006.

McCullagh, Declan. 2006. Police Blotter: Google Searches Nab Wireless Hacker. *CNet News.com*, 20. december 2006. <http://news.com.com/Police+blotter+Google+searches+nab+wireless+hacker/2100-1030_3-6144962.html?tag=cd.top>. Datum dostopa: 9. januar 2007.

MIT. 2005. Reality Mining Project. <http://reality.media.mit.edu/>. Datum dostopa: 8. maj 2006.

mk. 2006. Obligation of Data Connection Storage for German Anonymizers. *Anti1984.com*, 15. november 2006, <http://www.anti1984.com/en/articles/7.html>. Datum dostopa: 20. december 2006.

Page, Susan. 2006. NSA Secret Database Report Triggers Fierce Debate in Washington. *USA Today*, 11. maj 2006. <http://www.usatoday.com/news/washington/2006-05-11-nsa-reax_x.htm>. Datum dostopa: 3. julij 2006.

Perenič, Anton, ur. 1979. *Zbornik znanstvenih razprav*. Ljubljana: Univerza v Ljubljani, Pravna fakulteta.

Phillips, J. David. 2001. Cryptography, Secrets, and the Structuring of Trust. V: P. E. Agre in M. Rotenberg (ur.), *Technology and Privacy: The New Landscape,* 243–276. Cambridge, MA: MIT Press.

Privacy International. 2004. Complaint: Google Inc - Gmail email service, 19. april 2004. <http://www.privacyinternational.org/issues/internet/gmail-complaint.pdf>. Datum dostopa: 19. junij 2004.

Raymond, S. Eric. 2004. If Cisco Ignored Kerchoffs's Law, Users Will Pay the Price – elektronsko pismo Erica S. Raymonda, poslano 17. maja 2004. *Lwn.net*, <http://lwn.net/Articles/85958/>. Datum dostopa: 20. december 2006.

Rivest, Ronald. 1994. Clipper Chip Will Block Crime – elektronsko pismo Ronalda Rivesta, poslano 25. februarja 1994. V *Computer underground Digest*, 27. februar 1994, Vol. 6, Issue 19. <http://www.totse.com/en/zines/cud_a/cud619.html>. Datum dostopa: 26. maj 2004.

RSA Laboratories. 2000. *RSA Laboratories' Frequently Asked Questions About Today's Cryptography, Version 4.1*. RSA Security Inc.. <http://www.rsasecurity.com>. Datum dostopa: 1. april 2004.

Schmieder, Stephan. 2005. tor.unixgu.ru. <http://tor.unixgu.ru/>. Datum dostopa: 18. avgust 2006.

Schneier, Bruce. 2002. Secrecy, Security, and Obscurity. *Crypto-Gram*, 15. maj 2002. <http://www.schneier.com/crypto-gram-0205.html>. Datum dostopa: 3. maj 2005.

Schneier, Bruce. 2005. T-Mobile Hack. V *Crypto-Gram*, 15. februar 2005. <http://www.schneier.com/crypto-gram-0502.html>. Datum dostopa: 15. februar 2005.

Schneier, Bruce. 2006a. AOL Releases Massive Amount of Search Data. *Schneier.com*, 8. avgust 2006. <http://www.schneier.com/blog/archives/2006/08/aol_releases_ma.html>. Datum dostopa: 8. avgust 2006.

Schneier, Bruce. 2006b. NSA and Bush's Illegal Eavesdropping. V *Crypto-Gram*, 15. januar 2006. <http://www.schneier.com/crypto-gram-0601.html#12>. Datum dostopa: 15. februar 2006.

Schneier, Bruce. 2006c. Project Shamrock. *Crypto-Gram*, 15. januar 2006. <http://www.schneier.com/crypto-gram-0601.html#14>. Datum dostopa: 15. februar 2006.

Schneier, Bruce. 2006d. Auditory Eavesdropping. *Schneier.com*, 19. december 2006. <http://www.schneier.com/blog/archives/2006/12/auditory_eavesd.html>. Datum dostopa: 19. december 2006.

sci.crypt. 1994. The Cryptography FAQ (05/10: Product Ciphers). USENET, oddelek: sci.crypt, 4. oktober 1993 ob 5:00. Datum dostopa: 19. april 2004.

Shireen, J. Herbert. 1998. A Brief History of Cryptography. *Cybercrimes*. <http://cybercrimes.net/Cryptography/Articles/Hebert.html>. Datum dostopa: 22. april 2005.

Singel, Ryan. 2005. When Cell Phones Become Oracles. *Wired*, 25. julij 2005. <http://www.wired.com/news/wireless/0,1382,68263,00.html>. Datum dostopa: 8. maj 2006.

Sykes, J. Charles. 1999. *The End of Privacy.* New York: St. Martin's Press.

Šelih, Alenka. 1979. Zasebnost in nove oblike njenega kazenskopravnega varstva. V: A. Perenič (ur.), *Zbornik znanstvenih razprav*, 149–181. Ljubljana: Univerza v Ljubljani, Pravna fakulteta.

The Ethical Spectacle. 1995. The Zimmermann Case. <http://www.spectacle.org/795/zimm.html>. Datum dostopa: 22. april 2005.

Wagner DeCew, Judith. 1997. *In Pursuit of Privacy*. Ithaca, Cornell University Press.

Wikipedia, geslo: Kerchoffs' law. <http://en.wikipedia.org/wiki/Kerchoffs%27_Law>. Datum dostopa: 24. april 2005.

Zimmermann, Phil. 1993. Testimony of Philip Zimmermann to the Subcommittee on Science, Technology, and Space of the US Senate Committee on Commerce, Science, and Transportation, 12. oktober 1993. <http://www.pgp.com/phil/phil-quotes.cgi> ter <http://www.interesting-people.org/archives/interesting-people/199310/msg00026.html>. Datum dostopa: 9. junij 2004.

Pravni viri

Zakonodaja ZDA

Ustava Združenih držav Amerike (Constitution of the United States of America), 1787.

Listina svoboščin (Bill of Rights), 1791.

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

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

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

Odločitve sodišč ZDA

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

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

Bernstein v. United States Department of Justice, 176 F.3d 1132 (1999).

Dokumenti OECD

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

Dokumenti EU

Resolucija o zakonitem prestrezanju telekomunikacij (Council Resolution of 17 January 1995 on the Lawful Interception of Telecommunications), sprejeta 17. januarja 1995. Official Journal, C 329, 04.11.1996, p. 1–6.

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

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

Odločitev Evropskega sodišča za človekove pravice

Malone v. Velika Britanija, odločba z dne 2. 8. 1984.