Revija za kriminalistiko in kriminologijo / Ljubljana 59 / 2008 / 4, s. 321-338

Boj za prevlado nad internetom - internetno upravljanje in nadzorovanje*

Aleš Završnik[1]

Internet nima centralnega, hierarhično postavljenega koordinatorja, ki bi od zgoraj navzdol določal pravila igre. Tehnični dizajn interneta je vedno deloval kot tehnološko odporen proti poskusom nadzora. Razširjeno je bilo prepričanje, da državna suverenost, ki sloni na teritorialnem načelu, na internetu ne more biti zares učinkovita. A vendar internet kljub spremenjenim načinom upravljanja nikoli ni bil prostor brez pravil ali virtualni »Divji zahod«. Številni trki med interesi uporabnikov, držav, industrije in akademije ob ustvarjanju kode/pravil kažejo, da smo danes priča bojem za nadzor *nad* internetom – bojem za upravljavsko moč nad internetno infrastrukturo (oziroma »arhitekturo«), in bojem za nadzor *na* internetu – za uveljavljanje moralnega in pravnega reda na ravni vsebine.

Prispevek prikaže boj za nadzor *nad* internetom na primeru distribucije IP-naslovov in domenskih imen. Določena mera samoupravljanja internetne infrastrukture je namreč z »webifikacijo« privedla do režima internetnega samoupravljanja, pozneje do režima javno-zasebnega partnerstva, nato pa se je upravljanje razvilo v koncept večpartnerstva (angl. *multistakeholderism*), ki ga uteleša Forum za internetno upravljanje (IGF). IGF pa ne predstavlja le novega pristopa pri urejanju interneta, temveč kar novo paradigmo upravljanja globalnih zadev, ki transcendirajo državne, nacionalne meje in oblike medvladnega sodelovanja, ki kulminirajo v OZN. Predstavlja revolucijo v osmišljanju urejanja skupnih zadev na svetovni ravni, saj v proces odločanja vključuje številne naslovnike in zainteresirane stranke (poleg držav tudi gospodarske, znanstvene in državljanske akterje), s tem pa predstavlja možnost »svetovne demokracije« (Lamy), »hipersestavljenega modela« oziroma postmoderne »nevladne vladavine«. A paradigma večpartnerstva lahko ob ohranjeni centralizaciji dejanskega nadzora nad internetno infrastrukturo postane zgolj maska, ki služi perpetuaciji nasilja, ki ga »prvi« svet izvaja nad preostalim svetom tudi v novem (kiber-) prostoru. Boj za nadzor *na* internetu pa prispevek ponazori z analizo obvezne hrambe prometnih podatkov in strategij ter točk internetnega filtriranja. Obe praksi namreč uresničujeta scenarij »sekuratizacije« na internetu, po katerem rešitve ne odpravljajo problemov, temveč uničujejo to, kar naj bi rešile, in povečujejo nadzor.

Ključne besede: internet, internetno upravljanje, multipartnerstvo, nadzor nad internetom, Forum za internetno upravljanje, internetno filtriranje, hramba podatkov

UDK: 004.738.5 + 004.451.5

1 Ali je internet res dereguliran prostor?

Mit o internetu kot o prostoru brez pravil ali vsaj brez pravil, ki jih je postavila oblast, kjer uporabniki lahko oblikujejo samo svoja pravila (*netiquette*), predstava, da gre pri internetu za nekakšen virtualni ekvivalent »Divjemu zahodu«, je bil dolgo motor za razširjanje interneta. Če je mit resničen, potem obstaja prostor, kamor se lahko umaknemo, da bi bili »pri sebi«, obstaja možnost za novo raven posameznikove svobode in nastanek skupnosti, ki transcendira odtujeno birokratsko in na teritorij vezano državno oblast. Ta mit nazorno ponazarja Deklaracija o neodvisnosti kibernetičnega prostora J. P. Barlowa:

»Vlade Industrijskega sveta, vi nadležni giganti iz mesa in jekla, prihajam iz Kibernetičnega sveta ... V imenu prihodnosti vas, poosebljeno preteklost, pozivam, da nas pustite pri miru. Niste več dobrodošle med nami. Nobene suverenosti nimate tam, kjer se zbiramo mi.«[2]

Internet je kot mreža mrež podvržen pravilom in nikoli ni bil prostor brez regulacije. Za dobro funkcioniranje inter-

* Prispevek je nastal s pomočjo štipendije nacionalnega štipendijskega sklada Svetovne federacije znanstvenikov (*World Federation of Scientists*) za raziskovanje kibernetične kriminalitete v letu 2008. Ob tej priložnosti se Slovenski znanstveni fundaciji zahvaljujem za pomoč.

[1] dr. Aleš Završnik, raziskovalec na Inštitutu za kriminologijo pri Pravni fakulteti v Ljubljani, Poljanski nasip 2, Ljubljana; e-pošta: ales.zavrsnik@pf.uni-lj.si.

[2] Barlow, 1996.

neta je potrebna dobra koda ali, kakor meni Lessig,[3] koda je pravo (*Code is Law*), ki določa meje mogočega in dovoljenega. Svoboda internetnega upravljanja je zato zgolj pogojna. Ne gre za dereguliran prostor, ki ga ni mogoče upravljati (angl. »*ungovernability of cyberspace*«), obstaja pa določena mera samoupravljanja internetne infrastrukture, ki je veljala v prvi fazi internetnega upravljanja do začetka devetdesetih let prejšnjega stoletja. V tistem obdobju so imeli glavno vlogo inženirji. Vlade so bile po eni strani nezainteresirane za internet, ki je bil bolj kot polje za uveljavljanje nacionalnih interesov – kibernetični terorizem in kibernetično vojskovanje sta bila takrat še znanstvena fantastika – percipiran kot projekt »getoiziranih« akademikov, ki so jih na ta način držali na »varni razdalji«.[4] Po drugi strani pa je internet tudi liberalna tržna politika v ZDA – internet je bil projekt, ki ga je financirala ameriška vojska in pozneje ameriška nacionalna znanstvena fundacija – prepustila inženirjem. Ti naj razvijajo ta »produkt« svobodno in ga plasirajo na svoboden trg, ki bo o njem podal (povsem svobodno in racionalno) sodbo.

Neformalna skupina inženirjev je tehnično infrastrukturo upravljala relativno samostojno in v osemdesetih letih je ta skupina zrasla v pomembno organizacijo IETF (*Internet Engineering Task Force*). Njena glavna značilnost je bila visoka tehnična strokovnost, odprtost za vložke številnih posameznikov, vse s ciljem skrbeti za arhitekturo interneta in jo razvijati. Upravljanje internetne infrastrukture, na primer oblikovanja protokolov (pravil »lepega vedenja«) za medsebojno komunikacijo računalnikov, razdeljevanja IP-naslovov,[5] domenskih imen itn., je bilo prilagojeno akademski strukturi: iskanje najboljših rešitev, revizija medsebojnega dela (*peer-to-peer review*), graditev novih rešitev na podlagi izboljšave prejšnjih, vse to pa je potekalo brez spremljajočih lastninskih zahtev po nadomestilih – cilj je bil izdelati dobro delujočo mrežo računalnikov.[6]

Z rastjo interneta je del aktivnosti IETF prevzela IANA (*Internet Assigned Numbers Authority*), ki jo je ustanovil in vodil zgolj en človek – Jon Postel, in sicer vse do svoje smrti leta 1998. Danes IANA skrbi za (1) alokacijo IP-naslovov do šestih regionalnih registrov (*RIRs*),[7] ki skrbijo za nadaljnje razpečevanje IP-naslovov v svoji regiji, (2) za razdeljevanje vrhnjih domenskih imen (*DNS Root Zone Management*) in (3) upravlja nekatere parametre protokolov. Pomen vseh treh nalog je velik in zato neizogibno podvržen natančni regulaciji. Ker mora na primer IP-naslov imeti vsaka terminalska naprava, ki je povezana na mrežo, da se paketki podatkov ne izgubijo, ob tem pa je število IP-naslovov omejeno, je zelo pomembno, da je njihova distribucija dobro koordinirana, in ne prosta. Po četrti verziji internetnega protokola (IPv4) obstaja zgornja meja dobrih 4 milijard (2^{32}) edinstvenih IP-naslovov. Številka je na prvi pogled dovolj velika, da bi zadostila svetovnemu povpraševanju po IP-naslovih, a tehnološki napredek, ki generira stalno priključene naprave na mrežo in s tem možnost oddaljenega upravljanja (na primer od dlančnikov, mobilnih telefonov do peči za ogrevanje prostora, ki jo lahko nastavimo že pred prihodom v prostor), resno grozi, da bo IP-naslovov zmanjkalo. Ob paniki bi se tako lahko začelo kopičenje IP-naslovov na zalogo in oblikoval nekakšen »mimobežen« trg za preprodajo.[8]

Internetna infrastruktura obsega tudi sistem relativno razpršenih korenskih strežnikov (*root server*), ki sicer niso nadzorovani iz nekega središča, a vendarle delovanje sistema ni deregulirano. Vsaj na začetku je bilo teh strežnikov, ki imajo enako vsebino, zgolj 13 in le delno razpršenih po svetu (10 v ZDA, preostali v Amsterdamu, Stockholmu in Tokiu), danes pa korenske strežnike upravlja 12 organizacij (t. i. *root server operators*), s strojno opremo na več kot 130 lokacijah po svetu in v 53 državah.[9] Ta razpršena struktura tako omogoča relativno nemoteno delovanje sistema: če bi na primer ena država onemogočila delovanje enega ali nekaj strežnikov, bi drugi delovali neodvisno, saj ti strežniki nimajo med seboj nobenih obveznosti.

---

[3] Lessig 1999: *passim*.

[4] Evropske vlade so še v zgodnjih 90. letih prejšnjega stoletja dojemale internet kot »igračo akademikov«. Več o tem v Abbate, 1999.

[5] IP-naslov (angl. *IP address*) je logični naslov omrežnega vmesnika računalnika, pri katerem poteka komunikacija prek TCP/IP-ja. (Po iSlovarju, dostopnem na URL: http://www.islovar.org/.)

[6] Velik pomen IETF in njegova formalno zelo ohlapna institucionalna oblika sta leta 1992 privedla do nastanka neodvisne mednarodne organizacije Internetna družba (*Internet Society*), ki ima 150 organizacijskih in 6000 samostojnih članov v nekaj več kot 100 državah. Pod njenim okriljem deluje tudi Slovensko združenje Internet ISOC-SI. Več o ISOC-SI na URL: http://www.isoc-drustvo.si/, 9. 11. 2008.

[7] Na svetu obstaja 5 internetnih regionalnih registrov (*Regional Internet Registries* – RIRs): (1) ARIN (*American Registry for Internet Numbers*) skrbi za distribucijo IP-številk za Severno Ameriko in del karibskega območja, (2) RIPE NCC (*Réseaux IP Européens Network Coordination Centre*) za Evropo, Bližnji vzhod in dele centralne Azije, (3) APNIC (*Asia Pacific Network Information Centre*) za Azijo in Pacifik, (4) LACNIC (*Latin American and Caribbean Internet Addresses Registry*) za Latinsko Ameriko in drug del karibskega območja, ter (5) AfriNIC (*African Network Information Center*) za Afriko.

[8] Več o uvedbi in prehodu z internetnega protokola verzije 4 (IPv4) na IPv6 v Furht 2008. Glej še URL: http://www.ipv6.org/ in http://www.ipv6.com/, dostop 17. 11. 2008.

[9] Podatki iz septembra 2007. Po Karrenberg, 2007. Zemljevid z lokacijami korenskih strežnikov DNS je dostopen na URL: http://www.root-servers.org/, 10. 11. 2008.

Drug del nalog, ki jih opravlja IANA, je upravljanje vrhnjih domenskih imen, ki jih je trenutno pet vrst: generična (na primer .org., .net, .com, .info, imenovana gTLD – *generic top-level domain*), deželna (na primer .si za Slovenijo, imenovana ccTLD – *country code top-level domain*), sponzorska (na primer .edu, .gov, imenovana sTLD – *sponsored top-level domain*), infrastrukturna (.arpa) in omejena generična (na primer .biz, .pro; *generic-restricted top-level domain*). Sistem vrhnjih domenskih imen je bil do nedavnega izredno zaprt in upravljanje precej konservativno. Omejenost števila črk in njihovih kombinacij je namreč pomenilo, da gre za omejeno dobrino, ki jo kaže deliti preudarno. Šele pred kratkim (junija 2008) je bila dovoljena večja liberalizacija gTLD, ko je ICANN[10] potrdil predlog novega gTLD-programa, ki bo dopuščal podjetjem registracijo dodatnih gTLD (na primer .cocacola, .ljubljana).[11] Področje domenskih imen je bilo kljub konservativni ureditvi vedno kontroverzno in je sprožalo številne spore: podobnost domenskih imen je predstavljala možnost za zavajanje uporabnikov, podobna imena so odpirala konkurenčno pravne dileme, določena imena so pravno že zaščitena (na primer kot blagovne znamke) itn.

Ureditev delovanja interneta prek domenskih imen ima danes velik pomen, saj so postavila svojevrsten zemljevid interneta, ki nam omogoča relativno enostavno »potovanje« po kiberuniverzumu. Glavna ideja pri uvedbi domenskih imen pa je bila »zgolj« to, da si lažje zapomnimo ime, na primer »www.inst-krim.si«, kot pa IP-naslov strežnika, na katerem spletna stran gostuje – v tem primeru »91.185.203.171«. Domenska imena so zagotovila večje in lažje uporabljanje prek lažjih simbolnih reprezentacij večinoma številčnih naslovov internetnih virov (od dostopa do spletnih strani do vseh drugih komunikacijskih storitev, osnovanih na IP). A ta konverzija je hkrati pomenila enega poglavitnih epistemoloških rezov, po katerem danes internet razumemo. Teza o nereguliranosti interneta je zato veljavna le v toliko, kolikor v nekem obdobju regulacijske oblasti niso imele države. Vsaj na primer alokacija domenskih imen je bila oblikovana povsem neodvisno od državnih oblasti. Znana je anekdota, da je razdeljevanje vrhnjih domenskih imen potekalo tako, da je Postel po svetu pozival znance, ki bi bili pripravljeni prevzeti njihovo upravljanje. V različnih državah so skrb za njihovo razdeljevanje zato prevzeli različni subjekti: podjetja, posamezniki ali tako kot na primer v Sloveniji za ccTLD .si skrbi javni zavod ARNES (Akademska in raziskovalna mreža Slovenije). Za ccTLD je Postel za podlago vzel standard ISO 3166, ki je takrat obsegal 243 držav, in tako so bile oblikovane domene z dvema črkama za vsako državo (na primer .si za Slovenijo). Šele pozneje, ko je internet rasel, so države želele uveljaviti svojo suverenost tudi na internetu. Nove države so zahtevale nova pokrajinska vrhnja domenska imena, ki naj bi odražala njihovo suverenost tudi na internetu (na primer Republika Črna gora danes uporablja internetno vrhnje domensko ime ».me«).

Primera IP-naslovov in domenskih imen jasno ponazarjata, kako pomembno je upravljanje internetnega prostora. Regulacija interneta torej obstaja. Kar je vodilo k ocenam, da je ni, je dejstvo, da je kakovost te regulacije drugačna. Primarni igralci v upravljanju interneta namreč niso bile toliko nacionalne države, temveč je bilo upravljanje razpršeno in dodeljeno organizacijam, kot sta IETF in IANA. Decentralizirano in razpršeno upravljanje interneta je zato morda omogočalo prehitro sklepanje, da se nam obeta »dežela« svobodnega prostora. Tehnični dizajn interneta je deloval kot tehnološko odporen proti poskusom nadzora.[12] Razširjeno je bilo prepričanje, da državna suverenost, ki sloni na teritorialnem načelu, na internetu ne more biti zares učinkovita, in to je porajalo vznesene deklaracije in mit o novi emancipirajoči realnosti kibernetičnega prostora.

2 Internetno upravljanje in nadzor *nad* internetom

Nadzorovanje interneta poteka danes na vseh njegovih plasteh, na ravni infrastrukture, kode, prava in idej.[13] Splošneje boj za internet poteka na dveh »bojiščih«: (1) boj za nadzor *nad* internetom, kjer gre za poskuse nadzora infrastrukture, ki internet sploh omogoča (na primer za lastništvo nad telekomunikacijskimi omrežji, za moč nad določanjem »politike« protokolov), in (2) boj za nadzor *na* internetu, kjer gre za vpliv na vsebino, ki je na internetu dostopna in se nanaša na uporabniško raven; tu gre za vprašanja svobode izražanja, sprejemanja, mnenj in iskanja informacij ter pravico do informacijske zasebnosti.

Če na internet gledamo kot na peščeno uro, sestavljeno iz več ravni, je nujno pred analizo »internetnega nadzorovanja«,

[10] ICANN (*Internet Corporation for Assigned Names and Numbers*) je neprofitna organizacija ustanovljena »za dobrodelne in javne namene«, ki deluje pod Kalifornijskim pravom in na svetovni ravni nadzira sisteme internetnih edinstvenih označevalcev. Bolj konkretno: če želimo na internetu doseči drugo osebo, moramo v računalnik vpisati naslov, tj. ime ali številko. Ta naslov mora biti edinstven, tako da računalniki lahko najdejo naslovnika, da podatki prispejo do cilja. ICANN pa koordinira te edinstvene označevalce po celem svetu. Več o ICANN v nadaljevanju. Glej tudi URL: http://www.icann.org/, 1.12.2008.

[11] Liberalizacija se kaže tudi v Sloveniji z odločitvijo ARNES-a, da lahko od novembra 2008 domeno pod vrhnjo domeno ».si« registrira vsakdo, torej po novem tudi fizične osebe, od koder koli, ne le iz Slovenije.

[12] Walker, 2003.

[13] Podobna ocena v Zittrain, Palfrey 2007: 3.

»informacijske varnosti« ali »kibernetične varnosti« določiti raven, o kateri teče beseda: ali gre za tehnično raven, na katero najprej pomislijo tehnični eksperti, ali morebiti vsebino, na katero pomislimo pravniki ali sociologi (na primer za »sovražni govor« na internetu ali razmisleke o tem, kako inkriminirati otroško pornografijo). Družboslovci ob kibernetični varnosti razmišljamo o drugih objektih varstva kot varnostni sistemski inženirji, zato je brez opredelitve internetne plasti uporaba pojmov, kot sta »kibernetična« ali »informacijska varnost« (angl. *cybersecurity*), nejasna, če že ne zavajajoča. Doria[14] na primer navaja več možnosti razumevanja koncepta »kibernetične varnosti«, ki jo lahko razumemo kot varnost (1) internetnih protokolov, kar pomeni, da gre za objekte varstva, za katere skrbi IETF, (2) mrež, tj. za objekte varstva, na katere se osredotočajo CERT-i (*Computer Emergency Response Team*), (3) poslovanja na internetu, ki ščiti interese podjetij (na primer varnost e-bančnega poslovanja), (4) državne suverenosti in nacionalnih interesov (na kar merita koncepta kibernetičnega vojskovanja in kibernetičnega terorizma) ali (5) posameznika, njegovih temeljnih človekovih pravic in svoboščin (na primer varstvo informacijske zasebnosti). V nadaljevanju poglejmo, kako je potekal boj za nadzor *nad* internetom.

Zgodovina interneta se začenja v ZDA in od tod tudi mit, da internet (še vedno) nadzorujejo ZDA bodisi prek IETF bodisi (in še posebej) prek leta 1998 ustanovljene organizacije ICANN. Če je mit resničen, je treba za nadzor nad internetom ukiniti ali pridobiti vzvode moči nad temi organizacijami. Druga različica mita nadzor nad internetom locira v OZN. Ta se opira zlasti na dejstvo, da je vodilna agencija OZN za informacijsko-komunikacijske tehnologije – Mednarodna telekomunikacijska zveza (*International Telecommunications Union* – ITU) leta 2003 in 2005 organizirala Svetovni vrh o informacijski družbi (*UN World Summit on the Information Society* – WSIS-I in WSIS-II), s čimer naj bi OZN, ki je že dalj časa v krizi, pridobila vodilno svetovno nadzorstveno vlogo pri upravljanju internetne infrastrukture, transakcij in vsebine na internetu. Bistvena zgrešenost obeh mitov je v tem, da spregledujeta večplastno naravo interneta in boje za njegovo upravljanje, ki smo jim priča vse od komercializacije interneta.

Internet ni le prostor, ki je reguliran, temveč hkrati tudi prostor, kot smo že ugotovili, ki ni reguliran na načine, kakršne smo poznali doslej. Splošneje velja, da je zanj ključno, da nima centralnega, hierarhično postavljenega upravljavca, ki bi po piramidalni strukturi od zgoraj navzdol določal pravila za vse internetne plasti. Če ga primerjamo s sistemom klasične telefonije, ki je tudi svetovni komunikacijski sistem, se internet od njega bistveno razlikuje. OZN oziroma njena agencija ITU je pri telefoniji na vrhu piramide odločanja (v začetku internetnega razvoja s *klicnimi* povezavami je bil internet tudi vezan nanjo, a se je z novimi povezavami to spremenilo), skrbi za porazdelitev telefonskih številk po državah, te naprej regijah itn. Kot hierarhično najvišja institucija nadzoruje, koordinira in podpira tehnologije in storitve, ki tvorijo hrbtenico enega največjih in najbolj povezanih človeških sistemov na svetu. Pri internetu pa je ta shema sprejemanja odločitev bistveno drugačna. Če na internet gledamo kot na peščeno uro, ki obsega številne plasti, to pomeni od fizične infrastrukture (na primer optičnih kablov, žičnega omrežja, satelitov itn.) prav na dnu, prek komunikacijskega protokola, ki omogoča komunikacijo med usmerjevalniki različnih proizvajalcev (PPP), do sloja internetnega protokola (IP), ki je ozko grlo peščene ure, ter vse do višje ležečih plasti, na primer TCP-ja,[15] HTTP-ja[16] in nazadnje do storitev, znanih vsakemu povprečnemu uporabniku (kot so spletne strani in e-pošta), prav na vrhu peščene ure, se pokaže, da je regulatorjev (upravljavcev) interneta cela množica. Vloga regulatorja posameznega internetnega sloja (če ta sploh obstaja) ni v nobenem primeru središčna ali primerljiva z vlogo ITU pri klasični telefoniji. Upravljanje interneta je zato v primerjavi z modernimi birokratskimi oblikami odločanja, ki so pogosto vezane na odločitev vlad ali medvladnih forumov, razpršeno, njegova upravljavska struktura decentralizirana.

Že organizacije, kot sta IETF in IANA, so vzpostavile nove, mrežne, »postmoderne« oblike vodenja. Ob današnjem stanju, ko je internetu uspelo penetrirati v vse predele sveta, je zato toliko neverjetnejše, da je lahko en sam človek mimo vlad oblikoval mrežo razdeljevanja številk (IP) in vrhnjih domenskih imen, ki so oblikovale zemljevid interneta. Ta »nevladna vladavina« je delovala mimo obstoječih družbenih hierarhij in (nad)državnih institucij. IETF je zato še danes nenavaden v tem, da obstaja kot kolekcija dogodkov, a vendar ni korporacija in nima izvršnega odbora, nima članov in ne članarin.[17] Sestanki IETF-a obstajajo, a niso konference, čeprav se na njih prikazujejo tehnične predstavitve. Sestavljajo ga prostovoljci in nekateri se srečajo tudi trikrat letno, da bi izpolnili poslanstvo IETF-a. Vanj niso združeni člani, saj se vsakdo lahko registrira in udeleži srečanj, še najbližje članstvu pa predstavlja dejstvo, da se lahko vsak vključi na njihov poštni seznam. Njegovo delovanje vodita dve načeli: (1) »Ne priznavamo kraljev, predsednikov in glasovanja. Verjamemo v »*rough consensus*«[18] in

[14] Doria, 2007.

[15] TCP – *Transmission Control Protocol.*

[16] HTTP – *HyperText Transfer Protocol* je glavna metoda za prenos informacij na spletu.

[17] Po IETF Trust, 2008.

[18] Definicija *rough consensus*: »Soglasje ne zahteva, da se vsi udeleženci strinjajo, čeprav je to, seveda, zaželeno. Na splošno velja, naj prevladujoči pogled delovne skupine prevlada. (Vendar mora biti znano, da »prevladujoč« pogled ne bo določen na podlagi obsega podpore ali trdoživosti pogleda, temveč na podlagi bolj splošnega soglasja.)

poganjanje kode« (David Clark). (2) Drugo pa je izrekel Jon Postel: »Bodi konservativen pri tem, kar pošiljaš, in liberalen v tem, kar sprejemaš.« IETF je zato pomemben regulator interneta, a to še ne pomeni, da vodi, nadzoruje internet ali celo patruljira po njem.[19]

Pripoved o tem, da je internet revolucioniral komunikacije in spremenil percepcijo časa in prostora, je zato nezadostna. Internet ne predstavlja revolucije zgolj v tehnološkem smislu, temveč je tudi nova paradigma vodenja v zadevah, ki vključujejo množico zainteresiranih strani/strank, kjer gre za vključevanje palete interesov industrije, uporabnikov, mednarodnih organizacij, nacionalnih interesov in številnih drugih interesov centrov politične, gospodarske, moralne, ideološke idr. moči. V bistvu je danes že jasno, da smo vstopili v »kozmopolitsko dobo« (Kirsch), ko se na svetovni ravni organizacija oblasti oddaljuje od modela nacionalne države.[20] Upravljanje internetnega režima je v tej optiki »poskusni zajec« pri konceptualiziranju novih oblik svetovnega vladanja. Doslejšnji forumi odločanja, ki se na številnih področjih vedno bolj kažejo kot impotentni, rigidni, neučinkoviti in preobremenjeni s preteklimi medsebojnimi koncesijami, njihovo delovanje pa oteženo zaradi »birokratskih ovir« in inercij lastnim okornim mastodontskim organizacijam, onemogočajo spopad z resnimi problemi, ki nas zadevajo vse. Na primer vprašljiva je učinkovitost Kjotskega protokola, ki skuša zmanjšati emisije ogljikovega dioksida in toplogrednih plinov, ali na primer legitimnost Rimskega statuta Mednarodnega kazenskega sodišča, saj sodišče neposredno ignorirajo velike države, posredneje – z nedoslednostjo podvreči njegovi adjudikaciji lastne voditelje – pa tudi na videz njegove goreče podpornice.[21] Ali na primer upravljanje finančnega sistema na svetovni ravni, o čemer se strinjajo malodane vsi ekonomisti od finančne krize septembra 2008 dalje. Doslejšnji koncept upravljanja (angl. *governance*, fr. *gouvernance*) zadev na svetovni ravni, po katerem so glavni subjekti države in/ali medvladne mednarodne organizacije, se kaže kot problematičen in internet odpira nov koncept upravljanja, ki ga danes uteleša koncept Foruma za internetno upravljanje (*Internet Governance Forum* – IGF).

2.1 Tehnični režim

Koncept IGF na laž postavlja tezo, da imata ZDA ali OZN središčno vlogo pri upravljanju interneta. Morda v nekaterih zgodovinskih fazah ali glede nekaterih vprašanj, nikakor pa ne v celoti in vedno. Pot do IGF je bila vijugasta, primarno vlogo pri njegovem nastanku pa je igrala tehnološka plat. Ključna je bila, kot sugerira že ime »medmrežje«, mrežna oblika, saj se je tehnološka narava zrcalila tudi v družbenem segmentu – v upravljanju. A vendar, kako se je skozi razmeroma kratko zgodovino in burne boje za nadzor nad internetom razvila današnja »postvladna« oblika upravljanja, ki po mnenju nekaterih udeležencev tega procesa predstavlja novo paradigmo?[22]

V prvi fazi internetnega razvoja je bilo upravljanje interneta izenačeno s tehničnim režimom.[23] Obsegalo je razvijanje internetnih standardov, kakor jih je ustvarjala osrednja institucija IETF (*Internet Engineering Task Force*). Arhitektura interneta je že v začetku pomenila prelom z doslejšnjim komunikacijskim omrežjem, saj so bile komunikacijske mreže v večini držav pod državnim monopolom, ki so ga imele trdno v rokah nacionalne poštne in telefonske uprave. Te telefonske mreže so bile nacionalno in hierarhično strukturirane tako kot njihova nacionalna monopolna podjetja, ki so se »srečala« v ITU. IETF je bil v nasprotju z ITU ohlapna neformalna institucija inženirjev, primer »nevladne vladavine«,[24] ki je bila oblikovana kot alternativen model državnim in medvladnim institucijam, ki so določale standarde (protokole) za komunikacijo. V takšni obliki je v bistvu IETF ostal vse do danes.

2.2 Režim internetnega samoupravljanja

A vendarle ta oblika internetnega upravljanja po eni strani ni trajala dolgo, po drugi strani pa zaradi »getoizacije« interneta v akademskem svetu in zato relativno majhnega števila interesov pri njegovem upravljanju niti ni bila zanimiva kot upravljalski model za druga področja. Šele razvoj nove komunikacijske storitve, ki je poenostavila internet in omogočila njegovo komercializacijo – tj. razvoj www (*World Wide Web*),

Soglasje je lahko ugotovljeno z dvigom rok, »brenčečim odzivom« (angl. *humming*) ali katerim koli drugim sredstvom, o katerem se delovna skupina sporazume (seveda z »*rough consensus*«). Upoštevati je treba, da 51 odstotkov članov delovne skupine ne predstavlja »*rough consensus*« in da je 99 odstotkov bolje kot *rough*«. (*IETF Working Group Guidelines and Procedures*.)

[19] Po IETF Trust, 2008.

[20] Pravzaprav je dejstvo, da nacionalni državi uhaja (prava) oblast (konceptualnim mrežam »njenega« kazenskopravnega sistema pa tudi ključni zločini) lažje razumeti ob podatku, ki ga navaja Delmas-Marty, da je med stotimi najmočnejšimi gospodarskimi entitetami več kot dve tretjini podjetij, ne pa držav. Povzemam po Delmas-Marty 2008: 53, 134.

[21] Na primer Žižek opozarja na sporno vlogo francoskega predsednika Mitteranda pri podpori profrankofonske skupine Hutujev v Ruandi, ki so pozneje izvedli genocid nad Tutsiji. V Žižek 2008: 21.

[22] Na primer Bertrand de la Chapelle, direktor multipartnerske platforme *WSIS-online.net* v letih 2004–2005.

[23] Analizo zgodovinskih faz internetnega upravljanja povzemam po Drake, 2004; Hofmann, 2005; Kleinwœchter, 2003; Kleinwœchter, 2007.

[24] Po Bear 1996: 542.

je povečal vložke posameznih strani in apetite po polaščanju njegovega upravljanja. Sredi 90. let prejšnjega stoletja se je tako oblikoval nov koncept – režim internetnega samoupravljanja (angl. *internet self-governance*). WWW je namreč v ospredje postavil nekaj, kar je bilo inženirjem dotlej zgolj »postranskega« pomena: sistem domenskih imen je postal naenkrat ključen. S komercializacijo (oziroma »webifikacijo«)[25] interneta se je pomen domenskih imen močno povečal, ker so podjetja, države in posamezniki želeli pridobiti točno določena imena, smiselnih kombinacij (relativno majhnega števila) črk pa je relativno malo, in področje domenskih imen je postalo veliko interesno bojišče in/ali posel.[26] V tej drugi fazi internetnega razvoja, katere cilj je bil vzpostavitev samoregulacije, v bistvu pa zagotoviti večjo regulativno moč uporabnikov in zasebnega sektorja, je nastal ICANN (leta 1998). Široko sprejeto soglasje za tovrstno ureditev upravljanja, ki je bila zaradi močnih in nasprotujočih si interesov nujna, je bilo, da je treba držati vlade in medvladne organizacije (tipa ITU) kolikor je le mogoče na varni razdalji. Znanstveniki (inženirji), poslovna skupnost in civilna družba so vladam zanikali pravico in še posebej zmožnost razvijati primerne in legitimne strukture za internet. *Modus operandi*, ki so ga pripisovali vladam in njihovim organizacijam, so enačili s hierarhijami, birokratsko počasnostjo, konceptualiziranjem problemov (in njihovih rešitev) v smislu nacionalnih interesov ipd. V nasprotju s tovrstnimi portreti upravljanja je bila ideja internetnega samoupravljanja dojeta kot vključevalna in odprta za različne interese, orientirana od spodaj navzgor (in ne obratno), osnovana na soglasju (in ne preglasovanju), še posebej privlačna pa je bila zaradi decentralizacije avtoritete.

ICANN žal ni izpolnil teh pričakovanj. Omogočil je sicer sodelovanje široke množice zainteresiranih strank, od podjetij, željnih dobička, tehnologov do civilne družbe (uporabnikov) in (nevladnih) mednarodnih organizacij, prvotno tudi brez držav in medvladnih mednarodnih organizacij. Glavna sporna točka je bila že od vsega začetka ICANN-ova vključitev uporabnikov in vlad.[27] Težava v zvezi s prvimi je bila, kako zagotoviti njihovo reprezentativnost, saj na svetovni ravni ni obstajala nobena institucionalizirana organizacija uporabnikov. Vključitev uporabnikov je zato leta 2000 nujno privedla do oblikovanja globalnih volitev. Ocene teh volitev so številne in kontradiktorne, a ne glede na vse pomanjkljivosti so bile to prve svetovne volitve – za nadnacionalno uporabniško organizacijo »*At Large Membership*« je glasovalo 170.000 uporabnikov. Kljub vsem inspiracijam o »transcendenci« teritorialnih meja, ki so jih sprožale volitve, pa prevladuje enotno mnenje v teoriji, da so prevladali nacionalni volilni interesi.[28] Uporabniki še zdaleč niso »transcendirali« svojih nacionalnih identitet v domnevno apolitičnem kibernetičnem univerzumu, ki bi »lebdelo« nad lokalnimi nacionalnimi partikularizmi.

Režim internetnega samoupravljanja, ki naj bi ga poosebljal ICANN, pa je trpel še zaradi dveh slabosti. Po eni strani se je kombinacija zasebne vladavine in prostovoljnosti izkazala za neučinkovito. Konflikti, povezani z domenskimi imeni, so se nadaljevali, sodelovanje z nekaterimi ponudniki infrastrukture je bilo težko, številni registrarji imen in številk pa niso podvrgli svojega poslovanja pogodbenemu nadzoru ICANN-a. Po drugi strani pa je neuspeh ICANN-a posledica njegovega razmerja do vlade ZDA, ki je sprožil enega najtežjih bojev za oblast nad internetno infrastrukturo. Ta korporacija ima sedež v Kaliforniji in jo zavezuje pravo sedeža, pogodbeno pa je vezana na Ministrstvo za trgovino (*Department of Commerce*) ameriške zvezne vlade. Kompleksna organizacijska struktura omogoča vključevanje različnih interesnih skupin (različnih nacionalnih vlad, industrije, uporabnikov), a vendarle teze o neodvisnosti te organizacije močno bledijo ob posamičnih primerih, ki tudi bolj oddaljenim opazovalcem razkrijejo vene internetne infrastrukture. Takšen je bil primer poskusa uvedbe nove sponzorske vrhnje domene .xxx (sTLD), ki bi bila rezer-

---

[25] Tako Mueller 2002: *passim*.

[26] Na primer pokrajinsko vrhnjo domeno (ccTLD) *.eu* upravlja zasebna, neprofitna (!) organizacija EURid, ki deluje pod belgijskim pravom in ima 51 zaposlenih. »Trgovanje« s to domeno poteka po tripartitni shemi: EURid je register (angl. *registry*) za domeno, ki jo »proda« registru (angl. *registrar*), ta pa omogoči registracijo končnim uporabnikom (angl. *registrant*). Posameznik ali podjetje, ki na primer želi svojo spletno stran z domeno .eu, te ne more registrirati neposredno pri EURid, temveč pri enem izmed več kot 1000 registrov te domene po svetu. Cene: EURid zahteva pred začetkom postopka od registra 10.000 EUR depozita, posredniki pa omogočajo registracijo domene končnemu uporabniku po (različnih) tržnih cenah; na primer pri slovenskih registrih jo je mogoče registrirati za (okrog) 15 EUR letno. Od decembra 2005, odkar je mogoče registrirati domeno .eu, jih je bilo registriranih skoraj 3 milijone (»prirastek« znaša okrog 1000 registracij dnevno), kar skupno znese (približno) pol milijarde EUR. Podatki po URL: http://www.eurid.eu/, s 13. 11. 2008.

Če upoštevamo še druge vrhnje domene ccTLD, gTLD, sTLD, skripte, ki niso zgolj v latinici (kot je domena .eu), dejstvo, da domeno zgolj registriramo, in ne morda kupimo, dobimo približno ilustracijo boja za prevlado nad internetom, ki poteka na tem segmentu internetne infrastrukture. Žal je v običajni percepciji v zvezi s »trgovanjem« domen kot problematičen razumljen zlasti pojav »*cybersquatting*« – registracije znanih domen za poznejšo preprodajo, kar naj bi domnevno kršilo pravice imetnikov blagovnih znamk. Ne tako dolgo v preteklosti je veljalo pravilo Postela, »očeta« interneta, da se pri domenah ne upoštevajo lastninske zahteve: dodeljene so bile po načelu »prvi pride, prvi melje«. Ta pristop je omogočil razširjenje interneta in onemogočil čezmerne lastninske zahteve vplivnih in mogočnih imetnikov pravic intelektualne lastnine.

[27] Po Mueller 2002: 166 in nasl.

[28] Po Hofmann, 2002.

virana za pornografske vsebine. Ameriška konservativna desnica je takrat prek Busheve administracije vplivala na ICANN, ki je nazadnje zavrnil uvedbo nove vrhnje domene.[29] V bistvu je zagrozila, da bo zavrnila odločitev domnevno neodvisnega nadzornega organa ICANN-a, kljub temu da je Ministrstvo za trgovino ves čas zatrjevalo, da »ne igra nobene vloge« pri vsakodnevnem delovanju interneta. Glavni argument proti uvedbi pa je bil, da bi ta nova domena sprožila več težav, kot bi jih rešila. Nadzorovanje vsebine ni delo ICANN-a, je zatrjevalo njegovo vodstvo, in na primer nosilci znamk ali institucije bi bili zaradi kršitev dobrega imena in časti prisiljeni v nakupe teh domenskih imen, da bi preprečili blatenje svojega imena (lokalna Katoliška dekliška šola, so navajali nasprotniki .xxx, naj bi bila prisiljena v nakup svoje domene .xxx, da bi preprečila, da »se njihovo dobro ime povezuje s pornografijo v obliki pornografske spletne strani, kot je na primer www.katoliškadekleta.xxx«).[30] Podjetju *Internet Content Management Registry,* ki je želelo uvesti novo domeno, ni uspelo priti do vseh dokumentov ICAAN-a, ker je prevladalo stališče, da gre za privilegirane podatke – to pa je implicitno pomenilo, da je ICANN administrativna agencija federalne vlade in/ali pod nadzorom Ministrstva za trgovino.[31]

Da ZDA obvladujejo ICANN, ostaja v veliki meri prikrito, čeprav se vpliv razkriva ob posamičnih ideološko in/ali moralno kontroverznejših primerih. Za vse afriške in arabske države in Kitajsko pa ostaja primer vmešavanja ameriške zvezne administracije v postopek oblikovanja nove domene .xxx neizpodbiten dokaz, da na razvoj interneta ne morejo vplivati. Internet je zgolj nova oblika izkoriščanja, ki ga izvajajo države »prvega« sveta nad preostalim svetom. Bolj konspirativne teorije pa so v tem boju prepoznavale boj za oblast med ZDA in EU. Slednja naj bi poskusila pridobiti večjo moč pri reguliranju in vpliv na bodoči razvoj interneta z očrnitvijo ameriške vlade, češ da pod vplivom konservativne desnice obvladuje smer razvoja domnevno neodvisnih regulatornih institucij interneta.

Položaj, ko so vlade izločene iz upravljanja interneta (oziroma imajo zgolj posvetovalno vlogo v eni izmed notranjih organizacijskih enot, tj. v ICANN *Governmental Advisory Committee* – GAC), kar je podprto z močno in prepričljivo retoriko o zbirokratiziranosti in rigidnosti vlad, ki jih je treba držati proč od upravljanja, a je hkrati ena izmed vlad (ZDA) nadzorno telo nad glavnimi nadzornikom in hkrati njegova pogodbena stranka, je bil za veliko večino držav upravičeno nevzdržen. Internet je v tistem času že dosegel vse dele sveta in se infiltriral v malodane vse družbene podsisteme, zato se je interes nacionalnih vlad, ki so se začele sklicevati na javni interes pri upravljanju interneta, občutno povečal. ICANN je legitimnost črpal na postvladnih vrednotah, ki so izvirale še iz časov tehničnega režima in vrednot akademije zgodnjega interneta, a je to legitimnost zapravil s kontrahiranjem s »hudičem« – vlado ZDA. Predstavniki kitajskega Ministrstva za informacijsko industrijo so bili, kot navaja Zicai,[32] precej nazorni: »Danes upravljavec interneta ni ICANN, niti zasebni sektor, niti posamezniki (*netizens*), niti vlade. Upravljavec je zgolj in samo vlada ZDA.«

2.3 Javno-zasebno partnerstvo in proces WSIS/WGIG

Vlade so po neuspehu paradigme internetnega samoupravljanja odločno stopile v upravljavske mreže interneta. Neuspeh ICANN-a, ki ga je njegov predsednik razglasil za nefunkcionalnega že leta 2002, je rodil zamisli o novi ureditvi, o režimu »resničnega« oziroma »dobro uravnoteženega javnozasebnega partnerstva«. Da je bil ICANN obsojen na neuspeh že ob svojem »rojstvu« leta 1999, pa je pripisati še nadaljnjemu razlogu. Ne le da ZDA z ICANN-om niso bile pretirano resne, saj jim je ta organizacija omogočala pogodbeno in nadzorno pozicijo. Že »ob rojstvu«, leta 1999, je namreč Mednarodna telekomunikacijska zveza (ITU) začela prizadevanja, da bi preselila delikatno področje razdeljevanja domenskih imen na medvladno raven. Formalno pa je Generalna skupščina OZN decembra 2001 sprejela resolucijo[33] o Svetovnem vrhu o informacijski družbi (*UN World Summit on the Information Society* – WSIS), ki se je odvila v dveh fazah: WSIS-I je potekal v Ženevi (19.–12. december 2003), druga faza WSIS-II pa v Tunisu (16.–18. novembra 2005). Kljub temu da je ICANN poudaril večjo vlogo vlad, zmanjšal vlogo uporabnikov, standardne organizacije pa niso želele več sodelovati, se je vloga vlad okrepila do te mere, da so ICANN pustile zadaj. Forum, kjer potekajo boji za nadzor nad internetnim upravljanjem, se je spremenil in se znašel v domeni meddržavnega dogovarjanja.

Proces WSIS-I je zaznamoval organizacijski in regulativni okvir OZN: primarno vlogo so imeli predstavniki držav, ti so bili glavni govorniki in pogajalci, predstavniki »civilne družbe« pa so imeli priložnost izraziti svoje mnenje zgolj v primerih, predvidenih vnaprej s postopkovnimi pravili. Že v prvi fazi je postalo popolnoma jasno, da je boj za nadzor nad internetom dobil meddržavne dimenzije. Glavna sporna točka, ki se je pokazala na WSIS-I, je bilo vprašanje državnega nadzora

[29] Glej še McCarthy, 2005.

[30] Glej še Morphy, 2007.

[31] ICANN je zavrnil vlogo za uvedbo domene .xxx 30. marca 2007. Več o tej (tretji) odločitvi na URL: http://www.icann.org/en/announcements/announcement-30mar07.htm, 8. 11. 2008.

[32] Zicai, T. (2004). Core Issues for the UN Working Group on Internet Governance. Po Hofmann 2005: 15.

[33] The UN General Assembly Resolution 56/183 (21 December 2001).

nad infrastrukturo. Vzpostavila sta se dva tabora, ki sta vsak po svoje razumela probleme in njihove rešitve internetnega upravljanja: (1) *države v razvoju* so zagovarjale stališče, da se mora regulacija internetnih kritičnih resursov »dvigniti« na raven medvladnega sodelovanja. To je bil za njih edini način, ki omogoča spoštovanje nacionalne suverenosti in državam v razvoju ponuja možnosti za sodelovanje pri nadaljnjem razvoju interneta. Dotlejšnje reguliranje interneta so doživljale kot kršitev nacionalne suverenosti. Pri tem pa ni šlo zgolj za vprašanja »načelne« narave. Na primer Hofmann[34] navaja, kako internetna telefonija (*VoIP*) državam, ki imajo v lasti monopolna telekomunikacijska podjetja, odžira pomemben vir dohodka, kar vodi te države tudi do inkriminiranja uporabe internetnega telefona. To jasno kaže, kako je internet spreminjal moč držav ne le navzven, temveč tudi navznoter, s povsem konkretnimi učinki na nacionalno ekonomijo. Naslednji razlog, ki je vodil države v razvoju, da so se zavzemale za medvladno regulacijo interneta (na primer z vodilno vlogo ITU), je tudi ta, da imajo v OZN te države relativno veliko moč. ICANN je bil za njih ekskluzivni klub (belih) bogatih držav, ki omogoča njihovo nadaljnje izkoriščanje še v novem (kiber-) svetu. Posledično so te države internetno upravljanje razumele širše. Ta za njih ne pomeni zgolj razdeljevanja in upravljanja domenskega prostora in razdeljevanja IP-naslovov, temveč mora vključevati tudi teme, kot so dostop do interneta, kulturna raznolikost (na primer uporaba arabskih, kitajskih, ciriličnih, in ne le latiničnih skript), digitalni razkorak,[35] plačevanje stroškov medsebojne povezave,[36] mrežna varnost, pravice intelektualne lastnine, varstvo potrošnikov in varstvo podatkov. Kolektivno in koordinirano upravljanje interneta na medvladni ravni se jim je zdelo nujno za pravično delitev stroškov in koristi.

Na drugi strani (2) so *razvite države* začele razvijati nov koncept večpartnerskega urejanja zadev (angl. *multistakeholderism*): poleg vlad in mednarodnih vladnih organizacij to pomeni vključevanje zasebnega sektorja (industrije) in civilne družbe. Ta koncept so seveda podpirali tudi zagovorniki ICANN-a, ker tako sodelovanje nadaljuje internetno tradicijo in njegovo organizacijsko strukturo.

WSIS-I je v sklepni Deklaraciji o načelih internetno upravljanje definiral kot »multilateralno, transparentno in demokratično mednarodno upravljanje, ki polno vključuje vlade, zasebni sektor, civilno družbo in mednarodne organizacije. Zagotovi naj enakopravno razporeditev virov, pospešuje dostop za vse in upoštevajoč večjezičnost zagotovi stabilno in varno delovanje interneta«.[37] Za glavne zainteresirane stranke (angl. *stakeholders*)[38] so bili prepoznani (49. člen Deklaracije o načelih):[39] (1) države, (2) zasebni sektor, (3) civilna družba, (4) medvladne organizacije in (5) mednarodne organizacije. Vloga držav je bila opredeljena tako, da se države štejejo kot »politična avtoriteta za zadeve javnega pomena, povezanega z internetom (*internet-related public policy issues*), vloga zasebnega sektorja je bila »razvoj interneta kot tehničnega in ekonomskega področja«, vloga civilne družbe je bila opredeljena kot »pomembna vloga o zadevah interneta, še posebej na ravni skupnosti«, vloga medvladnih organizacij pa kot »koordinacija zadev javnega pomena, povezanega z internetom«.Vloga mednarodnih organizacij je bila skrb za »razvoj z internetom povezanih tehničnih standardov in s tem v zvezi relevantnih politik«.

Soglasje o drugih materialnih vprašanjih na WSIS-I v Ženevi ni bilo doseženo. Dosežen pa je bil sporazum o postopku obravnavanja teh vprašanj. Ustanovljena je bila 40-članska Delovna skupina o internetnem upravljanju (*Working Group on Internet Governance* – WGIG), ki je izdala 20 obsežnih tematskih študij (»*issue papers*«).[40] Njen mandat je bil v vmesnem času, med WSIS-I (2003) in WSIS-II (2005), (1) opredeliti delovno definicijo internetnega upravljanja, (2) identificirati področja javnega pomena (*public policy issues*), ki ostajajo v domeni suverene pravice držav, in (3) definirati vloge in odgovornosti vseh zainteresiranih skupin (vlad, civilne družbe in zasebnega sektorja) razvitih držav in držav v razvoju. Rezultate je Delovna skupina predstavila v končnem poročilu, kjer je podala predloge, kako izboljšati obstoječo ureditev internetnega upravljanja, in določila priorite za prihodnost. Zavzela se je za krepitev koncepta večpartnerskega urejanja zadev in sodelovanje med vladami, zasebnim sektorjem in civilno družbo. V poročilu je posebej predlagala poglobljeno internacionalizacijo obstoječih aranžmajev internetnega upravljanja in »globalnega prostora za dialog vseh zainteresiranih

---

[34] Po Hofmann 2005: 17.

[35] Digitalni razkorak (angl. *digital divide*) je razkorak v dostopnosti do interneta.

[36] Stroški medsebojne povezave (angl. *interconnection costs*) so stroški, ki ji je treba plačevati za povezanost v omrežje. Povezanost dveh enakovrednih sistemov pomeni, da vsak izmed njiju pridobi lastnosti drugega, in zato naj bi ob pravični delitvi ti stroški bremenili obe strani enako. Veliko krivica se pri tem godi zlasti afriškim državam, ki morajo nositi polne stroške povezanosti na internet, ne glede na to, da tudi iz drugih delov sveta lahko dostopamo do njihovih vsebin. A ker naj bi bile njihove vsebine »revne« (in takšne bodo zaradi visokih stroškov tudi ostale), naj bi več prejemale kot dajale, zato morajo nositi breme stroškov medsebojne povezave.

[37] WSIS 2003: *Geneva Declaration of Principles. Building the Information Society: A Global Challenge in the New Millenium.*

[38] Prevod angl. *stakeholder* je »vplivnik«. Opisen prevod je manj okoren: posameznik ali organizacija, ki sta vključena v projekt, ali bo izvedba projekta kakor koli vplivala na njune koristi. (Vir: iSlovar.)

[39] WSIS 2003: *Geneva Declaration of Principles. Building the Information Society: A Global Challenge in the New Millenium.*

[40] Sumarno o WGIG v Drake, 2005.

strank«. Glede vlog in odgovornosti zainteresiranih skupin je dopustila raznolike relativne prispevke posameznih strank glede na predmet zadeve. Poleg ključnih področij javnega pomena, ki so bila ves čas nejasna in ključni »kamen spotike«, je WGIG identificirala in določila prioritete in priporočila še za upravljanje korenskega datotečnega sistema (t. i. *root zone files* in *root zone system*), alokacijo domenskih imen in IP-naslovov, stroške medsebojne povezave (*interconnection costs*), internetno stabilnost, varnost in kibernetično kriminaliteto, neželeno pošto, varstvo podatkov in pravico do zasebnosti, pravice potrošnikov, pravice intelektualne lastnine, svobodo izražanja in uresničevanja načela večjezičnosti interneta.

Splošna ocena je, da je prišlo do občutne širitve koncepta internetnega upravljanja. Aktivnosti držav pri upravljanju interneta se ne enači več z zatiranjem svobode in neučinkovitostjo. Trend je celoviteje urejati internet zaradi različnih zlorab, ki utegnejo blokirati njegovo delovanje (od neželene pošte, zlonamerne kode in okuženih mrež računalnikov – *botnets*). Diskurz o varnosti interneta je potegnil vlade v ospredje, strah je postal novo gonilo interneta in liberalna retorika o svobodi in omejevanju države je izgubila moč. Urejanje interneta je v tej fazi tako spremenilo smer in postalo vedno bolj podobno urejanju drugih komunikacijskih infrastruktur – mednarodna koordinacija, za katero skrbijo države.

Boj za primerno regulatorno oblast in nadzor pa se s temi premiki ni končal. Delovna skupina WGIG je sama po sebi že predstavljala nove institucionalne dimenzije urejanja interneta. Sestavljala jo je heterogena množica 40 članov, ki so sicer nastopali kot posamezniki, in ne predstavniki posameznih interesnih skupin, a so bili izbrani tako, da bi bila zagotovljena reprezentativnost po regijah in interesnih skupinah. Kot navaja njen vodja,[41] so poseben pečat na delovanju skupine pustili predstavniki akademske skupnosti, kar je pogosto pomenilo daljše razprave, kot bi jih vodili predstavniki poslovne skupnosti, a narava teh razprav je članom zagotavljala spoštovanje, vsak izmed članov delovne skupine je dobil možnost za predstavitev svojih pogledov in prejel tudi refleksije drugih. Poleg sestave WGIG pa je v končnem poročilu skupina podala pomemben predlog – ustanovitev globalnega, večpartnerskega foruma (*multistakeholder forum*) za pospeševanje inkluzivnega dialoga o internetnem upravljanju.

2.4 Multipartnerstvo in IGF

Najrazličnejše institucionalne oblike upravljanja interneta so danes kulminirale v koncept večpartnerstva (angl. *multi-stakeholdersim*, fr. *multipartneriat*). Druga faza Svetovnega vrha o informacijski družbi OZN (WSIS-II) v Tunisu 2005 ponovno ni dosegla ključnih dogovorov o materialnih vprašanjih, a je podelila generalnemu sekretarju OZN mandat, da skliče nov večpartnerski forum za internetni politični dialog – Forum za upravljanje interneta (*Internet Governance Forum* – IGF).[42] IGF je postal forum za dialog med vsemi zainteresiranimi strankami za upravljanje interneta in zadeva vprašanja javnega pomena (angl. *multi-stakeholder policy dialogue*). Glavne teme IGF-agende so dostop do interneta, njegova odprtost, raznolikost, varnost in kritični internetni viri.[43] Ta model internetnega upravljanja pa je nekaj novega v tem, da se ponuja kot alternativni model državnemu in medvladnemu sodelovanju. Na svetovni ravni naj bi združil prizadevanja vseh »zainteresiranih strank«, ne le vlad, temveč tudi industrije in civilne družbe. Boj za prevlado nad upravljanjem interneta se tako danes odvija v trku med suverenimi pravicami držav in vizijo, ki jo ponuja koncept internetnega upravljanja, ki uresničuje vizijo transnacionalne globalne demokracije. Vpliv IGF-a je tako velik, ne le morda zaradi »mogočnega« pomena interneta, kot bi trdili kiberoptimisti, temveč zato, ker presega razprave o internetu in režimu upravljanja telekomunikacij. Navdihuje pravnopolitične razmisleke, ki zastavljajo vprašanje, kot je: kako reševati globalne mednarodne zadeve (na primer ekološka, biotehnološka ali jedrska tveganja, finančne trge itn.), ne da bi bilo upravljanje teh zadev hierarhično in podrejeno centrom obstoječe svetovne porazdelitve moči, temveč bi bilo horizontalno, večcentrično oziroma večpartnersko (»*multi-stakeholdership*«), kjer ima vsak naslovnik svoj »glas«, ki dejansko šteje?[44] Model internetnega upravljanja danes ponuja revolucionaren pogled na upravljanje skupnih zadev, ki ga na primer de la Chappelle opredeljuje kot novo pravnopolitično paradigmo. IGF je na-

[41] V Drake 2005: viii.

[42] Prvo srečanje IGF je bilo v Atenah (november 2006), drugo srečanje IGF je bilo v Riu de Janeiru (november 2007), tretje pa bo v Hyderabadu (Indija) 3.–6. decembra 2008. V pripravo na tretji IGF-forum je bil oktobra 2008 v Strasbourgu sklican *European Dialogue on Internet Governance (EuroDIG),* kjer so nastopile številne evropske »zainteresirane stranke« *(t. i.* »*European stakeholders*«*):* predstavniki civilne družbe, vlad, industrije, tehnične in akademske skupnosti. Kdo je sklical EuroDIG? Uradni koordinator EuroDIG je bil Svet Evrope, s podporo številnih »zainteresiranih«, a v bistvu gre za zelo ozko jedro skupine: t. i. programska mreža (EuroDIG PN) se predstavlja kot »odprta skupina angažiranih posameznikov, ki pospešujejo razvoj programa EuroDIG« (med njimi pa lahko najdemo predstavnika francoske vlade, Mednarodne trgovinske zbornice (ICC), Sveta Evrope, akademske skupnosti, nacionalnega telekomunikacijskega regulatorja in predstavnika evropskega registra ccTLD). Več o EuroDIG na URL: http://www.eurodig.org/, 15. 11. 2008.

[43] Namen tretjega srečanja IGF v Hyderabadu (Indija) decembra 2008 je soočiti poglede zainteresiranih strank o varnosti, zasebnosti, odprtosti interneta, dostopu do interenta in upravljanja internetnih kritičnih virov (domene, IP, korenski strežniki).

[44] Glej na primer Delmas-Marty, 2008.

mreč vezan na generalnega sekretarja OZN, a ni vezan na postopkovna pravila OZN. Omogoča enakopraven položaj vsem »zainteresiranim strankam«, saj pravice do sodelovanja nimajo zgolj predstavniki držav in mednarodnih organizacij, temveč neposredno tudi posamezniki. Zainteresirane stranke se povezujejo v »tematske mreže«, ki tvorijo »dinamične koalicije«, kar omogoča oblikovanje tematsko osredotočenih formacij, ki transcendirajo »klasične« geografske usmerjenosti. Namesto suverenosti so v IGF ključni odgovornost, prispevanje, in ne reprezentativnost, predstavljanje različnih pogledov in zornih kotov, in ne ljudi, oblikovanje odločitev (*decision-shaping*), in ne sprejemanje odločitev (*decision-making*). Model odločanja ne temelji več na hierarhični delegaciji, temveč na oblikovanju tematskih »grozdov« (vsebinskih sklopov), ki se delno prekrivajo. Bistveno načelo pri sprejemanju odločitev je izhajati »od spodaj navzgor« (od delavnic k panelom in nato k plenarnim zasedanjem), in ne od »zgoraj navzdol«. Vsaj takšna je ideološko obarvana retorika.

Boj za prevlado na internetu je tako prejel nove dimenzije z idejami o možnosti transnacionalne demokracije. Vključitev demokratičnosti v koncept internetnega upravljanja v procesu WSIS-a ima pomembne posledice, kot je opozarjala Hofmannova. Če demokracijo jemljemo resno, to pomeni, da obstoječi regulativni modeli in organizacijske strukture, kot jih predstavljajo agencije OZN (kot je ITU) ali javna-zasebna partnerstva (kot je ICANN), ne zadostujejo (več).

Regulatorni okvir interneta se je torej tekom časa spreminjal: na primer diskusije WSIS/WGIG o upravljanju interneta so poudarile, da je treba uporabiti obstoječe nacionalne in mednarodne pravne mehanizme za regulacijo interneta. Držav, ki so v času komercializacije interneta pomenile za uporabnike in zasebni sektor sovražnika, pozneje niso več dojemali kot »naravnih sovražnikov«. A s komercializacijo interneta so prvotne akademske vrednote, na katerih je temeljil zgodnji internet, prejele paleto drugih njim antagonističnih vrednot, ki so privedle do številnih zlorab nevtralne in odprte narave interneta. To je tudi razlog, da je treba nekaj storiti. Vprašanje pa je, ali bo povečana vloga držav to spremenila, zlasti v dobi poudarjene »sekuratizacije« v kriminalitetni politiki. Bolj kot krepitev večpartnerskega modela je zato zaznati moč kapitala, ki tudi prek sklepanj koalicij z državo nadaljujejo svoj pohod na še neosvojene teritorije.

Teza o tem, da ZDA nadzira internet prek institucije, kot je ICANN, ali da ga nadzira OZN prek svoje agencije ITU, je zato zgrešena, ker spregleduje številne zgodovinske faze v iskanju »pravilnega« ravnotežja med številnimi zainteresiranimi strankami. Spregleduje tudi moč, ki jo prinaša internet.[45] Komunikacija je vir moči, dominacije in družbenih sprememb. Zgodovina internetnega upravljanja to moč komunikacije nazorno odraža. Internet so nadzorovale zdaj ene in zdaj druge »zainteresirane stranke«, njihov vpliv je bil odvisen od predmetne internetne plasti. Morda je danes najpomembneje prav to, da ga diskurz o (ne)varnosti vrača v objem držav. Analiza moči nad internetno infrastrukturo in vsebino danes kaže, da je internet presegel prvotne akademske koordinate, prišel med uporabnike, zasebno industrijo in kapital. Kar pa danes navdihuje, je njegov primer, kako si zamisliti svetovno regulacijo onkraj obstoječih družbenopolitični aranžmajev, onkraj medvladnega dogovarjanja, ki izpušča dejanske centre moči in pomembne akterje (bodisi gospodarske bodisi državljanske – civilno družbene bodisi znanstvene akterje) in ne nazadnje s tem tudi onkraj OZN.

3 Nadzorovanje *na* internetu in anonimnost kibernetičnega prostora

Ob zgodnji komercializaciji interneta je Peter Steiner v New Yorkerju objavil karikaturo, ki je ujela takratno razumevanje kibernetičnega prostora.[46] Karikatura je prikazovala psa, ki sedi za računalnikom in razlaga drugemu psu, da »na internetu nihče ne ve, da si pes«! Karikatura je tako sporočala, da uporabniki na internetu uživamo veliko anonimnosti oziroma da kibernetični prostor ponuja neslutene možnosti »transcendence« spola, rase in celo »pasjosti«.

Mit o anonimnosti na internetu je danes preteklost. Nadzorovanje izvajajo različni akterji, od podjetij za »potrebe trženja« (na primer prek »piškotkov« (*cookies*), ki javljajo naše obiske spletnih strani) do vedno bolj angažirane države, ki nadzorstvo izvaja na več načinov, ne le s kazenskim pravom. Nadzorstvo izvaja prek zasebnih entitet, na primer ponudnikov storitev informacijske družbe, da sodelujejo pri cenzuri in nadzorovanju (na primer z obveznim shranjevanjem podatkov o prometu, lokacijskih podatkov),[47] ali z vzpostavitvijo tehničnih preprek, ki preprečujejo tok bitov od enega do drugega uporabnika. Poleg »klasične« (javne) policije, ki je bila primarno zadolžena za zagotavljanje javnega reda in miru v preteklosti, v kibernetičnem svetu zanj skrbi v veliki meri neformalna arhitektura akterjev oziroma »javno-zasebne koalicije mrežno povezanih akterjev«:[48]

– uporabniki in njihove skupine (na primer *Cyberangels* za varstvo otrok),

[45] Glej Castells, 2005.

[46] Steiner 1993: 61.

[47] Več v Zittrain 2007: 4 in nasl.

[48] Po Wall 2007:167–177.

– upravljavci virtualnih skupnosti (na primer v klepetalnicah),

– ponudniki infrastrukture (na primer ISP-ji, registrarji domenskih imen),

– zasebni informacijski varnostniki (na primer banke imajo svoje varnostne sistemske inženirje),

– nevladna nepolicijska hibridna telesa (na primer CERT-i),

– vladna nepolicijska telesa (na primer carina, obveščevalne enote) in šele na koncu

– vladna (javna) policija.

V skladu z načelom, da je (programska) koda pravo (*Code is Law*)[49] in da tehnično in politično nikakor nista dve ločeni ravni,[50] manipuliranje s tehnologijo omogoča v kiberprostoru še učinkovitejši nadzor, kot na primer kazensko pravo, celo absoluten nadzor. Na primer Wall[51] v tej zvezi omenja možnosti »razinženirjenja« (»*engineering-out*«) kibernetične kriminalitete, ki jo omogoča tehnološka »infrastruktura« oziroma »arhitektura interneta«. Osnovna ideja tovrstnega »boja« zoper kibernetično kriminaliteto izhaja iz uvida, da v enaki meri kot neka tehnologija povzroča ali generira odklonsko vedenje, ta ista tehnologija omogoča in vsebuje možnosti za preprečitev oziroma popolno odstranitev možnosti za takšno vedenje. Tovrstni ukrepi popolnoma odpravljajo polje svobode: manevrski prostor posameznika se zoži do te mere, da kršitve niti niso več mogoče.[52]

Na tem mestu zato ne želim analizirati materialnih kazenskih določb (kibernetičnih kaznivih dejanj), temveč prikazati, kako potekajo druge (morda) manj opazne nadzorstvene prakse (nekatere od njih, v nasprotju s kazenskopravnimi prepovedmi in zapovedmi, niso prav nikjer objavljene in razglašene). V naslednjem podpoglavju si zato poglejmo obseg digitalnih sledi, ki jih puščamo za seboj v kibernetičnem svetu in ki jih morajo ponudniki informacijskih storitev hraniti, in nato še metode internetnega filtriranja prepovedanih ali neželenih vsebin.

3.1 Anonimnost in hramba podatkov

Z vsakim klikom miške za seboj puščamo digitalne »prstne odtise«. Kibernetični svet je tehnološko generiran na način, ki v njem omogoča absolutno sledljivost. Ali drugače, sama arhitektura interneta vsebuje parametre o tem, kaj je tam sploh mogoče početi, in s tem vsebuje tudi možnost za nadzor nad kršitvami pravnih pravil.[53] Težave preiskovalcem zato v enaki meri povzročajo tudi prevelike, ne le premajhne količine digitalnih sledi. Digitalna forenzična ekspertiza, katere smiselni začetni del predstavlja hramba podatkov, se osredotoča na naslednje tri korake: (1) poleg zbiranja netelesnih podatkov obsega še (2) njihovo osmišljanje ter (3) ohranjanje v (nekompromitirani) obliki, ki bo služila kot pravno veljaven dokaz (to pomeni na način, ki bo omogočil sledljivost forenzične analize, ohranjena integriteta podatkov itn.).

Pomemben del nadzora internetne vsebine so predpisi o zasebnosti, elektronskih komunikacijah in hrambi podatkov, ki se prenašajo po javnih komunikacijskih mrežah. V EU so za zasebnost na internetu in hrambo podatkov, povezanih z internetom, ključne naslednje direktive:

1. Direktiva 95/46/ES o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov s 24. oktobra 1995 (*Data Protection Directive*),[54]

2. Direktiva 2002/58/ES o obdelavi osebnih podatkov in varstvu zasebnosti na področju elektronskih komunikacij z 12. julija 2002 (Direktiva o zasebnosti in elektronskih komunikacijah) (*ePrivacy Directive*)[55] in

3. Direktiva 2006/24/ES 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 s 15. marca 2006 (*Data Retention Directive*; v nadaljevanju Direktiva o hrambi podatkov).[56]

Sprejem Direktive o hrambi podatkov[57] so spremljale različne legitimacije. Njeno sprejetje naj bi bilo nujno zaradi boja zoper terorizem. Pozneje se so njeni zagovorniki sklicevali na boj zoper pedofile in nazadnje tudi na potrebe boja zoper piratstvo,

---

[49] Lessig, 1999.

[50] Drake 2004: 5.

[51] Wall, 2007.

[52] Na primer kršitve cestnoprometnih predpisov o dovoljeni hitrosti vozil – kršitve avtomobilske tehnologije lahko absolutno sankcioniramo s spremembo te tehnologije: avtomobil z blokado motorja ne bi več mogel preseči meje dovoljene hitrosti. A vsaj pri avtomobilih si te svobode še ne želimo odvzeti, ne glede na »davek, ki ga terjajo ceste«.

[53] Glej Lessig 2004: 147–161.

[54] Implementacija v slovenski pravni red je bila izpeljana z *Zakonom o varstvu osebnih podatkov* (ZVOP-1), ki velja od 1. 1. 2005, in *Zakonom o Informacijskem pooblaščencu* (ZInfP), ki velja od 31. 12. 2005.

[55] Implementacija v slovenski pravni red je bila izpeljana z *Zakonom o elektronskih komunikacijah* (ZEKom), ki velja od 1. 5. 2004 (10. poglavje).

[56] Implementacija v slovenski pravni red je bila izpeljana z *Zakonom o spremembah in dopolnitvah Zakona o elektronskih komunikacijah* (ZEKom-A), ki je stopil v veljavo 27. 12. 2006. Ta zakon je odložil uporabo določb, ki se nanašajo na hrambo podatkov pri *telefonskih storitvah* – te so se začele uporabljati 15. 9. 2007, in določb, ki se nanašajo na hrambo podatkov o dostopu do *interneta*, *elektronski pošti* in *internetni telefoniji* (*VoIP*), ki se bodo začele uporabljati 15. 3. 2009.

[57] Uradni list Evropske unije L 105, 13. 4. 2006, str. 54.

povezano z izmenjavo datotek v P2P-omrežjih. Mešani in mestoma nejasni razlogi hrambe podatkov so ostali in jih vsebuje tudi preambula direktive. Sprejetje te direktive naj bi bilo tako nujno, ker »(p)ravne in tehnične razlike med nacionalnimi določbami glede hrambe podatkov za namen preprečevanja, preiskovanja, odkrivanja in pregona kaznivih dejanj predstavljajo *ovire za notranji trg elektronskih komunikacij*« (6. točka preambule). Po drugi strani naj bi bila direktiva »dragoceno sredstvo za preprečevanje, preiskovanje, odkrivanje in pregon kaznivih dejanj, zlasti *organiziranega kriminala*« (7. in 9. točka preambule), po tretji plati naj bi bila nujna za učinkovit boj zoper *terorizem* (8., 9. in 10. točka preambule), nazadnje pa naj bi bila koristna »za namene preiskovanja, odkrivanja in pregona *hudih kaznivih dejanj*, kakor jih države članice opredeljujejo v svojih nacionalnih zakonodajah« (21. točka preambule in 1. člen).

Sporno pri tem opredeljevanju namenov je, da namen shranjevanja podatkov ni jasen. Glede na to, da formalnopravno preambula ni zavezujoč del direktive, pa je namen preiskovanja, odkrivanja in pregona »hudih kaznivih dejanj« (1. člen direktive) premalo določen: katera kazniva dejanja so huda? V naslednjem koraku bi bilo treba določiti tudi, kateri organi imajo pravico do vpogleda v te podatke, našteti pa tudi »organe pregona« v posamični državi.

Slovenski pravni red ščiti več vrst podatkov v zvezi z elektronskimi komunikacijami: (1) vsebino komunikacije (103. člen ZEKom), (2) podatke o prometu (104. člen ZEKom), (3) lokacijske podatke (106. člen ZEKom), (4) dejstva in okoliščine v zvezi s prekinitvijo povezave ali s tem, da povezava ni bila vzpostavljena (103. člen ZEKom), in (5) podatke o naročniku (110. člen ZEKom). Vse oblike nadzora oziroma prestrezanja teh podatkov so prepovedane, razen če je podan kateri izmed naslednjih zakonskih razlogov: (1) če je podano soglasje uporabnika, (2) če se izvaja v okviru zakonite poslovne prakse z namenom, da se zagotovi dokaz o tržni transakciji ali kateri koli drugi poslovni komunikaciji,[58] (3) v okviru organizacij, ki sprejemajo klice v sili, zaradi njihove registracije, identifikacije in reševanja,[59] (4) tehnično shranjevanje podatkov ali dostop do njih izključno za namen opravljanja ali lajšanja prenosa sporočila prek elektronskega komunikacijskega omrežja ali če je nujno potrebno za zagotovitev storitve informacijske družbe.[60] Ti razlogi vsaj načelno niso sporni, ključne in zanimivejše pa so določbe, ki se (5) nanašajo na hrambo podatkov o prometu, ki jih operaterji ustvarijo ali obdelajo pri zagotavljanju javnih komunikacijskih storitev, za namene, kot jih določajo naslednji trije zakoni:[61]

(a) *Zakon o kazenskem postopku* za namene odkrivanja in pregona kaznivih dejanj (149.b člen ZKP),

(b) *Zakon o Slovenski obveščevalno-varnostni agenciji* za namene zagotavljanja nacionalne varnosti in ustavne ureditve ter varnostnih, političnih in gospodarskih interesov države (21.–24c. člen ZSOVA) in

(c) *Zakon o obrambi* za namene obrambe države (32.–34. člen ZObr).

Hramba podatkov, pridobljenih ali obdelanih v zvezi z zagotavljanjem javno dostopnih elektronskih komunikacijskih storitev ali javnih komunikacijskih omrežij, po direktivi in ZEKom, se ne nanaša na vsebino komunikacij in tudi ne na podatke o povezavah, ki niso bile uspešno vzpostavljene. Nanaša pa se na naslednje kategorije podatkov, ki odkrivajo dimenzije vseprisotnih »digitalnih sledi«. Po ZEKom[62] se shranjujejo podatki, potrebni za (1) odkritje in prepoznanje *vira komunikacije*,[63] (2) prepoznanje *cilja komunikacije*,[64] (3) ugotovitev *datuma, časa in trajanja komunikacije*,[65] (4) ugotovitev *vrste komunikacije*,[66] (5) razpoznavo *komunikacijske*

[58] 7. odstavek 103. člena ZEKom.

[59] 7. odstavek 103. člena ZEKom.

[60] 9. odstavek 103. člena ZEKom.

[61] 107.a do 107.e člen ZEKom.

[62] 107.b člen ZEKom, ki v celoti povzema 5. člen Direktive o hrambi podatkov.

[63] Podatki, potrebni za odkritje in prepoznanje *vira komunikacije*, so: (1) pri telefonskih storitvah v fiksnem in mobilnem omrežju: telefonska številka kličočega ter ime in naslov naročnika ali registriranega uporabnika; (2) pri dostopu do interneta, elektronske pošte in uporabi internetne telefonije: uporabniško ime in telefonska številka, dodeljena za vsako komunikacijo, s katero se vstopa v javno telefonsko omrežje, ime in naslov naročnika ali registriranega uporabnika, ki mu je bil v času komunikacije dodeljen naslov internetnega protokola, uporabniško ime ali telefonska številka.

[64] Podatki, potrebni za prepoznanje *cilja komunikacije*, so: (1) pri telefonskih storitvah v fiksnem in mobilnem omrežju: klicana telefonska številka in v primerih, ki vključujejo dodatne storitve, kot je preusmeritev ali predaja klica, številka ali številke, na katere je klic preusmerjen, ime in naslov naročnika ali registriranega uporabnika; (2) pri dostopu do elektronske pošte in uporabi internetne telefonije: uporabniško ime ali telefonska številka prejemnika klica prek internetne telefonije, ime in naslov naročnika ali registriranega uporabnika in uporabniško ime namembnega prejemnika komunikacije.

[65] Podatki, potrebni za ugotovitev *datuma, časa in trajanja komunikacije*, so: (1) pri telefonskih storitvah v fiksnem in mobilnem omrežju: datum ter čas začetka in trajanje ali čas konca komunikacije; (2) pri dostopu do interneta, elektronske pošte in uporabi internetne telefonije: datum in čas prijave na internet in odjave z njega, pri čemer se upošteva določen časovni pas, skupaj z naslovom statičnega ali dinamičnega internetnega protokola, ki ga je ponudnik dostopa do interneta dodelil komunikaciji, in uporabniško ime naročnika ali registriranega uporabnika ter datum in čas prijave in odjave z internetnih storitev elektronske pošte ali internetne telefonije glede na določen časovni pas.

opreme uporabnikov,[67] (6) identifikacijo *lokacije* mobilne komunikacijske opreme[68] in podatki o (7) *neuspešnih* klicih.[69]

Zbiranje podatkov po vseh treh zakonih je urejeno zelo različno, še zdaleč največje varstvo posameznika pred posegi v informacijsko zasebnost pa zagotavljajo določbe ZKP. Po 149.b členu ZKP je mogoče pridobiti podatke o prometu v elektronskem komunikacijskem omrežju za katero koli kaznivo dejanje, ki se preganja po uradni dolžnosti. Edina omejitev je višji dokazni standard – »razlogi za sum«. Ukrep lahko odredi *preiskovalni sodnik* - v tem primeru se lahko nanaša na vse podatke o udeležencih, okoliščinah in dejstvih elektronskega komunikacijskega prometa, ali *policija* (za podatke o lastniku/uporabniku in o času uporabe).

Slabost ureditve po ZKP je, da je ukrep mogoče uporabljati za vsa kazniva dejanja. A v primerjavi z obema drugima zakonoma je ureditev neprimerno bolj določna in varstveno naravnana. Razlogi za pridobivanje podatkov po ZSOVA (21.–24c. člen) so raznovrstni, sem sodijo tudi eklatantno nedoločni »politični« interesi države. Poleg tega je vprašljiv nadzor nad pridobivanjem podatkov: delovanje Slovenske obveščevalno-varnostne agencije zgolj delno nadzoruje predsednik Vrhovnega sodišča RS (24.– 24.c člen ZSOVA),[70] nadzor pa je še neprimerno manj določen po Zakonu o obrambi (32.–34. člen ZObr). Obveščevalne, protiobveščevalne in varnostne naloge po ZObr opravlja obveščevalno varnostna služba Ministrstva za obrambo, delno (protiobveščevalne in varnostne naloge) pa tudi štabni varnostni organi Slovenske vojske. Elektronsko spremljanje mednarodnih sistemov zvez za oboje opravljajo enote za elektronsko bojevanje Slovenske vojske.[71] Pri tem ni, tako kot pri Slovenski obveščevalno-varnostni agenciji, zagotovljene nobene, niti delne, sodne kontrole. Edina kontrola je politične narave, saj obveščevalno-varnostna služba o svojem delu obvešča ministra za obrambo, načelnika generalštaba, predsednika vlade in predsednika republike. Vprašljivo je, ali je takšna notranja in/ali politična kontrola primerna. Sodni organi bi morali za vsak primer posebej dovoliti dostop do podatkov. Enak očitek o nedoločnosti koncepta t. i. »spremljanja mednarodnih sistemov zvez« pa se ne nanaša zgolj na dejavnost, ki jo opravlja SOVA, temveč tudi obveščevalno-varnostna služba Ministrstva za obrambo.

Obdobje hrambe po ZEKom znaša 2 leti, ki pa ga je mogoče podaljšati za omejen čas, če to »opravičujejo posebne okoliščine« po vseh treh zakonih (tj. ZKP, ZSOVA, ZObr).[72] V primeru podaljšanja obstajajo obveznosti nadaljnjega obveščanja (informacijskega pooblaščenca in ministra za javno upravo, slednji pa mora obvestiti Evropsko komisijo in druge države članice Evropske unije). Nekateri podatki se hranijo trajno: to so tisti, do katerih se je dostopalo, se jih shranilo in izročalo.[73]

Nadzor nad izvajanjem ZEKom izvajata dva organa: (1) nadzor o zaščiti tajnosti, zaupnosti in varnosti elektronskih komunikacij izvaja *Agencija za pošto in elektronske komunikacije RS*, (2) nadzor nad hrambo prometnih in lokacijskih podatkov, pridobljenih ali obdelanih v zvezi z zagotavljanjem javnih komunikacijskih omrežij ali storitev v skladu s 107.a do 107.e členom ZEKom, pa izvaja *informacijski pooblaščenec*.[74]

Kdo ima dolžnost hraniti podatke? Vsi operaterji, a zgolj *javno* dostopnih elektronskih komunikacijskih storitev in *javnih* komunikacijskih omrežij (tj. dostopa do interneta, e-pošte, telefona, mobilnih telefonije itn.), to pa so dolžni zagotoviti na

---

66 Podatki, potrebni za ugotovitev *vrste komunikacije*, so: (1) pri telefonskih storitvah v fiksnem in mobilnem omrežju vrsta uporabljene telefonske storitve; (2) pri dostopu do elektronske pošte in uporabi internetne telefonije vrsta uporabljene storitve.

67 Podatki, potrebni za razpoznavo *komunikacijske opreme* uporabnikov, so: (1) pri telefonskih storitvah v fiksnem omrežju: kličoča in klicana telefonska številka; (2) pri telefonskih storitvah v mobilnem omrežju: kličoča in klicana telefonska številka, mednarodna identiteta mobilnega naročnika kličoče in klicane stranke, mednarodna identiteta mobilnega terminala kličoče in klicane stranke, v primeru predplačniških anonimnih storitev pa datum in čas začetka uporabe storitve ter ID celice, kjer je bila storitev izvedena; (3) pri dostopu do interneta, elektronske pošte in uporabi internetne telefonije: kličoča telefonska številka za klicni dostop, digitalni naročniški vod ali druga končna točka začetnika komunikacije, ID celice na začetku komunikacije, oziroma podatki, ki določajo zemljepisno lego med obdobjem, za katerega se hranijo podatki o komunikaciji.

68 Podatki, potrebni za identifikacijo *lokacije* mobilne komunikacijske opreme, so: (1) lokacijska oznaka (ID celice) na začetku komunikacije; (2) podatki, ki določajo zemljepisno lego celic z navedbo njihovih lokacijskih oznak (ID celice) med obdobjem, za katerega se hranijo podatki o komunikaciji.

69 To pomeni, če je zveza vzpostavljena, a ni bilo odgovora.

70 Predsednik Vrhovnega sodišča RS je v tej zvezi že sprožil postopek za presojo ustavnosti 21. člena Zakona o SOVI, ki se nanaša na »spremljanje mednarodnih sistemov zvez«. To se ne sme nanašati na določljiv priključek telekomunikacijskega sredstva ali na določenega uporabnika tega priključka na območju RS (3. odstavek 21. člena). Določba je po njegovem mnenju preširoka in nejasna, naraščajoča baza podatkov pa krši temeljno človekovo pravico do informacijske zasebnosti.

71 4. odstavek 32. člena ZObr.

72 5. odstavek 107.a člena ZEKom.

73 Varovani morajo biti z (najmanj) oznako stopnje tajnosti »zaupno«. Glej še 3. odstavek 13. člena Zakona o tajnih podatkih (ZTP).

74 Po 112. člen ZEKom.

lastne stroške. Težave, ki se pri tem pojavljajo, so večplastne: problematično je, da minimalnih standardov glede tehničnih in organizacijskih varnostnih ukrepov, ki jim morajo zadostiti operaterji, ni. Ti opravljajo storitve informacijske družbe kot poslovno dejavnost, kar pomeni, da te odločitve pretežno vodijo ekonomski razmisleki. Možnosti zlorab predstavlja tudi dejstvo, da ne obstaja obveznost ločevanja podatkov, shranjenih za namene javnega reda in lastnega poslovanja. Poleg mešanja teh dveh vrst podatkov, zbranih za različne namene, pa lahko prihaja tudi do mešanja med »brkljanjem« (rudarjenjem) po podatkih o posameznikih, ki so že osumljeni storitve določenega kaznivega dejanja, in o posameznikih, ki niso še ničesar osumljeni (o na primer njihovih komunikacijskih, potovalnih vzorcih ipd). Operaterji sami tudi opozarjajo, da niso dolžni opravljati nalog države na lastne stroške, pomembnejši pa je njihov očitek, da je določba premalo rafinirana. Operaterjev je v mrežnem sistemu več vrst in vmesni ponudniki tudi tehnično ne morejo zagotoviti enakega nadzora, kot to lahko storijo končni.[75]

V Direktivi o hrambi podatkov je predvidena evalvacija direktive in njenega vpliva na uporabnike in raziskava, ki jo je izvedla FORSA maja 2008,[76] je pokazala, kakšne učinke ima obsežno generiranje baz podatkov: 73 % vprašanih Direktivo o hrambi podatkov pozna, 11 % jih zaradi tovrstne ureditve ni uporabilo telefona ali e-pošte, 6 % jih domneva, da zaradi tovrstne ureditve prejemajo manj informacij, kar 52 % vprašanih pa telekomunikacijskih storitev ne bi uporabilo za razgovore o bolj osebnih zadevah (na primer s farmacevti, psihoterapevti ipd.) To pomeni, da se uresničuje scenarij »sekuratizacije«: naše rešitve (v tem primeru Direktiva o hrambi podatkov) ne odpravljajo problemov (kriminalitete, terorizma, pedofilije itn.), temveč uničujejo to, kar naj bi rešile (povzročajo manjšo uporabo tehnologije, in ne večje, nezaupanje in občutek nadzorovanosti).

3.2 Anonimnost in internetno filtriranje

Obseg, intenzivnost in dodelanost internetnega filtriranja, nadzorovanja in drugih metod internetnega nadzorstva hitro naraščajo in se širijo globalno.[77] Ti ukrepi so sicer primarno naperjeni zoper »necivilno« družbo, »temne mreže« in zoper akterje, ki so dojeti kot grožnja nacionalni varnosti, a sprejeti ukrepi v enaki meri učinkujejo na »običajne« mreže civilne družbe. Notoričnо znani in skozi evropska »vrednostna očala« še posebej obsodbe vredni so poskusi internetnega filtriranja, ki ga izvaja Kitajska. A drugače od nadzora tiska, ki se ga vsakokratna oblast skuša polastiti (od cerkvene oblasti v 15. stoletju, ki je skušala preprečiti širitev Gutenbergovega izuma in ponatise »svete knjige«, ker naj bi to ogrožalo njeno posredniško vlogo), je nadzor digitalnih vsebin v odprtem internetu izjemno težaven. Če je bil v preteklosti glavni strah, da bomo s časom pomembne informacije izgubili, je danes glavni strah, da nekatere informacije ne bodo nikoli zares pozabljene. Material, ki je enkrat objavljen na internetu, je praktično nemogoče izbrisati, saj ga je mogoče neomejeno množiti in prenašati po različnih strežnikih po svetu – grozi nam kar »Černobil zasebnosti« (»*privacy Chernobyl*«), poudarjajo zagovorniki informacijske zasebnosti. Tako je na primer tudi eden izmed glavnih trikov kitajske partije v tem, da dostopanje do »kritičnih« spletnih strani (na primer podatkov o praktikantih meditativnih vaj Falun Gong) otežujejo (na primer s počasnim nalaganjem spletnih strani), ne morejo pa dostopa absolutno preprečiti.

Podatki *OpenNet Initiative*[78] kažejo, da se internetno filtriranje legitimira z močno retoriko boja zoper kršitelje pravic intelektualne lastnine, varovanja nacionalne varnosti, ohranjanja kulturnih norm in verskih vrednot ter varstva otrok pred pornografijo. V boju za nadzor vsebine so uporabljeni tehnološki ukrepi različnih vrst in intenzivnosti. *Strategije* internetnega filtriranja (cenzuriranja in omejevanja dostopanja do) vsebine so:[79]

1. tehnično blokiranje internetnih strani: (a) blokiranje IP-naslovov, (b) manipulacije sistema domenskih imen in (3) blokiranje internetnih naslovov s pomočjo spletnega strežnika, ki ob požarni ogradi omejuje dostop do posamezne spletne strani (*URL blocking using a proxy*). Te metode omogočajo učinkovito blokiranje tudi zunaj jurisdikcijskih meja. Po podatkih *OpenNet Initiative* najbolj narašča uporaba tehnike blokiranja po ključnih besedah, ki blokirajo dostop do določenih spletnih strani (če je ključna beseda del URL-ja) ali pa iskanje (glede na seznam spornih ključnih besed). Zahtevnejša in natančnejša oblika pa je filtriranje z dinamično analizo vsebine (*dynamic content analysis*), ki prebira sámo vsebino spletnih strani, ki pa je redka;

---

[75] Po Einzinger, 2007. Več o ugovorih ISP-jev na spletni strani krovne organizacije ponudnikov internetnih storitev v EU – EuroISPA (*European assocition of European Internet Services Providers Associations*), URL: http://www.euroispa.org/.

[76] Po FORSA, 2008.

[77] Deibert, Rohozinski 2008: 146.

[78] *The OpenNet Initiative* skupno vodijo štiri vrhunske znanstvene inštitucije: *The Citizen Lab* Univerze v Torontu, *Berkman Center for Internet & Society* pri Harvard Law School, *The Advanced Network Research Group* pri Univerzi v Cambridgeu in *The Oxford Internet Institute* Univerze v Oxfordu. Več na URL: http://opennet.net/about-filtering.

[79] Po *The OpenNet Initiative*. (Vir URL: http://opennet.net, 20. 11. 2008.)

2. umik iskalnih zadetkov: ponudniki storitev informacijske družbe lahko s seznama zadetkov v iskalnikih izpustijo nezakonita ali neželena spletna mesta, kar pomeni, da so določene strani še vedno dosegljive, le njihovo iskanje je oteženo;

3. odstranitev: če ima nadzornik neposreden dostop in pravno jurisdikcijo nad gostitelji vsebin, lahko od njih zahteva odstranitev spletišč z neželeno vsebino in spletišče postane nevidno za brskalnike;

4. samocenzura: promocija konformnosti, grožnje s tožbami in podobne metode generirajo samocenzuro. Čeprav je lahko patroliranje in nadzorovanje po internetu izvedeno v izjemno majhnem številu primerov, je občutek nadzorovanja običajno (občutno) disproporcionalen.

Točke kontrole vsebine so lahko na kateri koli točki med številnimi vozlišči mreže: (1) na internetni hrbtenici: takšno filtriranje je najobsežnejše in podvrže cenzuri celotne države; (2) pri ponudnikih internetnih storitev, ki zagotavljajo dostop do interneta; (3) v posameznih institucijah (na primer podjetja, šole, knjižnice imajo svojo politiko, ki jo uresničujejo tudi s filtriranjem); (4) uporabniki sami lahko namestijo opremo (*filtration software*), ki preprečuje dostopanje do določenih strani.

Tako kot »razinženirjenje« kibernetične kriminalitete tudi ta tehnološka rešitev za družbene probleme poraja več težav, kot jih rešuje. Slabost filtriranja je, da je vedno nujno tehnično nesorazmerno in nikoli ne doseže zgolj predvidene tarče: bodisi filtri predstavljajo premajhno (*underblocking*) ali preveliko (*overblocking*) sito. Slabost je tudi, da se pristojnosti odločanja o vprašanjih javnega reda na ta način prenašajo na proizvajalce programske opreme za avtomatizirano identifikacijo vsebin. Dejansko o vprašanjih javnega reda ne odločajo politiki, temveč zasebni subjekti, korporacije, ki ne le da imajo svoje končne cilje, ki jih zasledujejo, temveč niso pod nobeno zunanjo kontrolo. Mit, ki se ustvarja in ki podpira tovrsten premik moči, pa je mit, da sta tehnična in politična raven dve ločeni ravni. A tehnična raven ima nujno družbenoekonomske posledice. Na primer programska koda in standardi vsebujejo implicitne odločitve o tem, kaj naj bo mogoče in kaj naj bo dovoljeno. Lessig[80] na primer prepričljivo opozarja, kako je avtorsko pravico na internetu mogoče precej učinkovito zavarovati, saj sama arhitektura interneta omogoča vzpostavitev takšnega okolja, ki omogoča *absoluten* nadzor nad kršitvami pravnih pravil. Podobno tudi Drake ugotavlja,[81] kako so internetni standardi – tehnološki dizajn – močno prežeti z organizacijami in njihovimi cilji.

[80] Lessig 2004: 147-161.

[81] Drake 2004: 5.

4 Sklep

Internet brez oblastnih posegov je danes spomin na preteklost. Paleta konfliktnih interesov na internetu je postopno privedla do militarizacije kibernetičnega prostora: internet je postal objekt geopolitičnega dokazovanja moči med državami in na vseh plasteh njegove arhitekture lahko opazujemo boj za nadzor. Bolj kot dereguliranemu svobodnemu prostoru smo danes priča vojni za nadzor *nad* internetom – vojni za upravljavsko moč nad internetno infrastrukturo na eni in vojni za nadzor *na* internetu – za uveljavljanje moralnega in pravnega reda na ravni vsebine – na drugi strani. Poleg držav, ki so postale zelo zainteresirane za to, kaj se na internetu in z njim dogaja, so v tej vojni prisotni še interesi proizvajalcev informacijske tehnologije in internetnih vsebin. »Informacijska družba« je družba, ki je odvisna od informacijske tehnologije, in ta je postala donosen posel. Poleg interesov države in podjetij pa so nazadnje na tem prostoru tudi interesi posameznikov, nas uporabnikov, ki zahtevamo na primer to, da nas pustijo pri miru v potovanjih po kibernetičnem prostoru.

Internet spreminja politično ravnovesje sil na globalni ravni.[82] To sproža militarizacijo, ki se kaže v geopolitičnih zaostrovanjih, kjer se v zadnjih letih spopadi med državami prenašajo v kibernetični prostor. Pojavi kibernetičnega terorizma (*cyber terrorism*) in vojn (*cyber war*) so znani: med Indijo in Pakistanom leta 2001, prva evropska kibernetična vojna med Rusijo in Estonijo maja 2007, ko je estonski premier obtožil ruske vojaške sile za DoS-napade in iznakaženja (*defacement*) spletnih strani estonske vlade in *on-line* bančnih sistemov,[83] ali incidenti med Rusijo in Gruzijo v sporih glede pokrajine Južne Osetije avgusta 2008. Ne glede na izjemno težavnost ugotavljanja, kdo je v ozadju teh napadov in še posebej kdo dejansko vodi niti teh napadov, ali so to res države (in katere) ali morda »zgolj« posamezniki – hacktivisti,[84] je danes gotovo vsaj to, da države zahtevajo moč (suverenost) tudi na internetu. Boj se prenaša v domnevno neodvisne, zgolj »tehnične« in domnevno apolitične institucije, kot sta IETF in ICANN, ter se iz internetne infrastrukture širi v višje plasti interneta vse do ravni vsebin.

[82] Po Delmas-Marty 2008: 210.

[83] Glej več o kibervojni med Rusijo in Gruzijo na URL http://www.crime-research.org/articles/Cyberwar-Russia-vs-Estonia/, 8. 11. 2008.

[84] Napadov na gruzijske spletne strani avgusta 2008 naj ne bi sprožile ruske obveščevalne in/ali vojaške sile, temveč naj bi jih sprožili posamezni relativno nepovezani ruski hekerji – aktivisti, ki so želeli pomagati svojim »bratom in sestram«, in so tako rekoč delali »na lastno pest«. Glej na primer poročanje v Wired: http://blog.wired.com/defense/2008/10/government-and.html (dostop 8. 11. 2008), ter ruski časopis *Xakep* (*Heker*), kjer takšen *hektivist* opisuje napad na spletno stran gruzijskega parlamenta *parliament.ge*.

Izvor interneta in zgodovina njegovega upravljanja (angl. *internet governance*) kažeta, da je v njegovem izvoru položena moč neodvisnega kompetitivnega vojnega nasilja. Vojska je internet ustvarila in sorodni impulzi ga tudi uničujejo po metodi »tisočerih rezov«.[85]

Po eni strani je internet na globalni ravni prinesel novo konstelacijo moči, novo centralizacijo moči in kapitala. Forum za internetno upravljanje (IGF) nakazuje nov pristop pri urejanju interneta, pristopu večpartnerstva (angl. *multi-stakeholderism*). Ta paradigma se kaže kot povsem nov način upravljanja globalnih vprašanj, ki transcendirajo državne, nacionalne meje in medvladna sodelovanja, ki kulminirajo v OZN. Zanjo nista več značilna reprezentacija v obliki demokratično izvoljenih predstavništev in hierarhično odločanje, temveč horizontalna porazdelitev moči.

Po drugi strani pa je koncept večpartnerskega upravljanja interneta mit, ki zakriva novo nasilje: revne države ostajajo še bolj podrejene, kar na primer predstavlja ureditev t. i. stroškov povezljivosti, po katerih priključitev afriških držav na skupne mreže vodi v distribucijo stroškov, ki bremeni le njih: če želijo biti v tem elitnem klubu »omreženih«, morajo plačati vse stroške druženja v skupnem klubu. V tej luči se »paradigmatske izboljšave«, ki jih uteleša IGF, kažejo kot maska za pravično upravljanje enega največjih svetovnih infrastrukturnih sistemov. IGF je Potemkinova vas, sredstvo, s katerim okcidentalne družbe ohranjajo vzvode regulatorne in nadzorstvene moči nad internetno infrastrukturo in tudi moralne, ideološke in kulturne moči nad internetno vsebino.

Literatura

1. Abbate, J. (1999). **Inventing the Internet**. Cambridge, MA: MIT Press.
2. Barlow, J. P. (1996). **A Declaration of the Independence of Cyberspace**. Po URL: http://homes.eff.org/~barlow/Declaration-Final.html, 14. 8. 2008.
3. Bear, W. S. (1996). Will the Global Information Infrastructure Need Transnational (or Any Governance)? RAND/RP-603, ponatis iz **National Information Infrastructure Initiatives: Visions and Policy Design**, str. 532–552.
4. Brin, D. (1998). **The Transparent Society: will technology force us to choose between privacy and freedom?** New York: Perseus Books.
5. Castells, M., ed. (2005). **The Network Society: a cross-cultural perspective**. Cheltenham: Edward Elgar.
6. Deibert, R.; Rohozinski, R. (2008). Good for Liberty, Bad for Security? Global Civil Society and the Securitization of the Internet. V: Deibert, R.; Palfrey, J.; Rohozinski, R.; Zittrain, J., eds., **Access Denied: The Practice and Policy of Global Internet Filtering**, Cambridge: MIT Press.
7. Delmas-Marty, M. (2008). **Preureditev oblasti.** Ljubljana: GV založba (Zbirka Pravna obzorja; 36).
8. Doria, A. (2007). What do the Words »Internet Security« Mean? V: Kleinwœchter, **The Power of Ideas: Internet Governance in a Global Multi-Stakeholder Environment**. Berlin: Marketing für Deutschland GmbH, s. 197–207.
9. Drake, W. J. (2004). **Reframing Internet Governance Discourse: Fifteen Baseline Propositions**. Dostopno na URL: http://media-researchhub.ssrc.org/reframing-internet-governance-discourse-fifteen-baseline-propositions/resource_view, 11. 11. 2008.
10. Drake, W. J., ed. (2005). **Reforming Internet Governance: Perspectives from the Working Group on Internet Governance (WGIG)**. New York: The United Nations Information and Communication Technologies Task Force.
11. Einzinger, K. (2007). **Application of the Data Retention Directive to Data Relating to Internet Access, Internet Telephony and Internet E-mail: the view of the providers**. Prispevek na konferenci »Lex Informatica 2007«, Dunaj, 6. –7. julij 2007. Dostopno na URL: http://www2.wu-wien.ac.at/informationsrecht/viennagroup/lexinformatica/Data%20Retention_Einzinger.pdf.
12. FORSA Gesellschaft für Sozialforschung und statistische Analysen. Po URL: http://www.vorratsdatenspeicherung.de/images/forsa_2008-06-03.pdf.
13. Furht, B. (2008). **The Encyclopedia of Multimedia**. New York, London: Springer.
14. Goldsmith, J.L.; Wu, T. (2006). **Who Controls the Internet: Illusions of a Borderless World**. New York: Oxford University Press.
15. Hofmann, J. (2002). **Verfahren der Willensbildung und der Selbstverwaltung im Internet – Das Beispiel ICANN und die At-Large-Membership**. WZB Discusion Paper FS II 02-109.
16. Hofmann, J. (2005). **Internet Governance: A Regulative Idea in Flux**. Dostopno na URL: http://www.internetgovernance.org/people-hofmann.html, 12. 11. 2008.
17. iSlovar, URL: http://www.islovar.org/.
18. IETF Trust (2008).**The Tao of IETF**. Po URL: http://www.ietf.org/tao.html#about.iana, 8. 11. 2008.
19. Karrenberg, D. (2007). **DNS Root Name Servers Explained For Non-Experts**. Dostopno na URL: http://www.isoc.org/briefings/019/, 10. 11. 2008.
20. Klein, N. (2007). **The Shock Doctrine: The Rise of Disaster Capitalism**. London etc.: Penguin Books.
21. Kleinwœchter, W. (2003). **From Self-Governance to Public-Private Partnership: the Changing Role of Govenments in the Management of the Internet's Core Resources**. Loyola of Los Angeles Law Review, let. 36, s. 1104–1126.
22. Kleinwœchter, W., ed. (2007). **The Power of Ideas: Internet Governance in a Global Multi-Stakeholder Environment**. Berlin: Marketing für Deutschland GmbH.
23. Lessig, L. (1999). **Code and Other Laws of Cyberspace**. New York: Basic Books.
24. Lessig, L. (2004). **Free Culture.** New York: Penguin Press.
25. McCarthy, K. (2005). **ICANN kills .xxx porn domain: But where's the pressure come from?** Po: http://www.theregister.co.uk/2005/12/01/icann_kills_xxx/, dostop 8. 11. 2008.

[85] Zittrain, 2008.

26. Morphy, E. (2007). **ICANN Axes .XXX Domain**. Po URL: http://www.technewsworld.com/story/56631.html?wlc= 1226139494, 9. 11. 2008.
27. Mueller, M. (2002). **Ruling the Root: Internet Governance and the Taming of Cyberspace**. Cambridge, MA: MIT Press.
28. Steiner, P. (1993). **On the Internet, nobody knows you're a dog.** The New Yorker, 5. julij 1993, let. 69 (LXIX), št. 20, s. 61.
29. UN General Assembly Resolution 56/183 (21 December 2001), po URL: http://www.itu.int/wsis/docs/background/resolutions/56_183_unga_2002.pdf, 5. 11. 2008.
30. Walker, J. (2003). **The Digital Imprimatur: How Big Brother and Big Media Can Put the Internet Genie Back in the Bottle**. URL: http://www.fourmilab.ch/documents/digital-imprimatur, 14. 8. 2008.
31. Wall, D.S. (2007). **Cybercrime: the transformation of crime in the information age**. Cambridge, UK, Malden, MA: Polity (Crime and society series).
32. Wall, D. S. (2008). Cybercrime and the Culture of Fear: Social Science Fiction(s) and the Production of Knowledge about Cybercrime. **Information, Communication & Society**, let. 11, št. 6, str. 861–884.
33. WSIS 2003: **Geneva Declaration of Principles. Building the Information Society: A Global Challenge in the New Millenium**, WSIS-03/GENEVA/DOC/4-E, 12 December, 2003. Vir: URL: http://www.itu.int/wsis/documents/doc_multi.asp?lang=en&id=1161|1160, dostop 19. 11. 2008.
34. Zittrain, J.L.; Palfrey J.G. Jr. (2007). **Access Denied: The Practice and Policy of Global Internet Filtering**. Oxford Internet Institute, Research Report No. 14.
35. Zittrain, J. (2008). **The Future of the Internet and How to Stop It**. New Haven [Conn.]: Yale University Press.
36. Žižek, S. (2008). Globalni kapitalizem: kje je srce teme Konga?. **Dnevnik**, 8. 11. 2008 (Priloga Objektiv), s. 21.

Internetne institucije

– Internet Assigned Numbers Authority (IANA), URL: http://www.iana.org/
– Internet Corporation for Assigned Names and Numbers (ICANN), URL: http://www.icann.org/
– Internet Engineering Task Force (IETF), URL: http://www.ietf.org/
– Internet Society (ISOC), URL: http://www.isoc.org/
– Number Resource Organization, URL: http://www.nro.net/
– Regional Internet Registries (RIRs)

OZN

– Internet Governance Forum (IGF), URL: http://igf.wgig.org/cms/, http://www.intgovforum.org/
– International Telecommunications Union (ITU), URL: http://www.itu.int/ITU-T/
– Working Group on Internet Governance (WGIG), URL: http://www.wgig.org/
– World Summit on the Information Society (WSIS), URL: http://www.itu.int/wsis/index.html

Drugi viri

– European Dialogue on Internet Governance (EuroDIG), *URL:* http://www.eurodig.org/
– European assocition of European Internet Services Providers Associtions (EuroISPA), URL: http://www.euroispa.org/
– OpenNet Initiative, URL: http://opennet.net
– Slovensko združenje Internet ISOC-SI, URL: http://www.isoc-drustvo.si/

Revija za kriminalistiko in kriminologijo / Ljubljana 59 / 2008 / 4, s. 321-338

The struggle for power over the internet – internet governance and control

Aleš Završnik, LL.D. Institute of Criminology at the Faculty of Law,
Poljanski nasip 2, 1000 Ljubljana, Slovenia

The internet does not have any central, hierarchically established coordinator, able to establish rules of the game from top to bottom. The technical design of the internet has always been technologically resistant to all attempts of control. There was even a widespread belief that the exercise of state sovereignty, resting on the principle of territoriality, cannot be really efficient on the internet. However, in spite of changed means of governance, the internet has never been a forum without rules or a sort of virtual "Wild West". The numerous collisions between the interests of users, states, industry and academia in the creation of codes/rules demonstrate that we are faced today with a struggle for control *over* the internet – a struggle for power and governance over the internet infrastructure, and a struggle for control *on* the internet – namely, for the implementation of a moral and legal order in terms of contents.

The paper presents the struggle for control *over* the internet on the example of the distribution of IP addresses and domain names. A certain extent of self-governance of the internet infrastructure, with "webification", lead at first to a regime of internet self-governance, later to a regime of public-private partnership, and finally, governance has evolved to the concept of multi-stakeholderism, embodied by the Internet Governance Forum (IGF). IGF not only represents a new approach to the regulation of the internet, but rather a new paradigm of governance of global matters which transcend state and national boundaries as well as forms of intergovernmental cooperation, culminating in the UN and its agencies. IGF is a revolution in the regulation of many common matters on the global level by incorporating many subjects and stakeholders in processes of decision making and thus providing the possibility of a "world democracy" (Lamy), a "hyper-complex model" or post-modern "non-governmental governance". By preserving the centralisation of control over the internet infrastructure, a paradigm of multi-stakeholderism can become just a mask, serving the perpetuation of the violence that the "first" world uses against the rest of the world also in the new (cyber) space. The struggle for control *on* the internet is illustrated in this paper by an analysis of the mandatory retention of traffic data and strategies (and spots) of internet filtering. Both of the aforementioned practices realize a scenario of internet security by which solutions do not solve problems, but rather create them, destroy that which they are supposed to save, and increase control.

Key words: internet, internet governance, multistakeholderism, control over the internet, Internet Governance Forum, internet filtering, data retention

UDC: 004.738.5 + 004.451.5