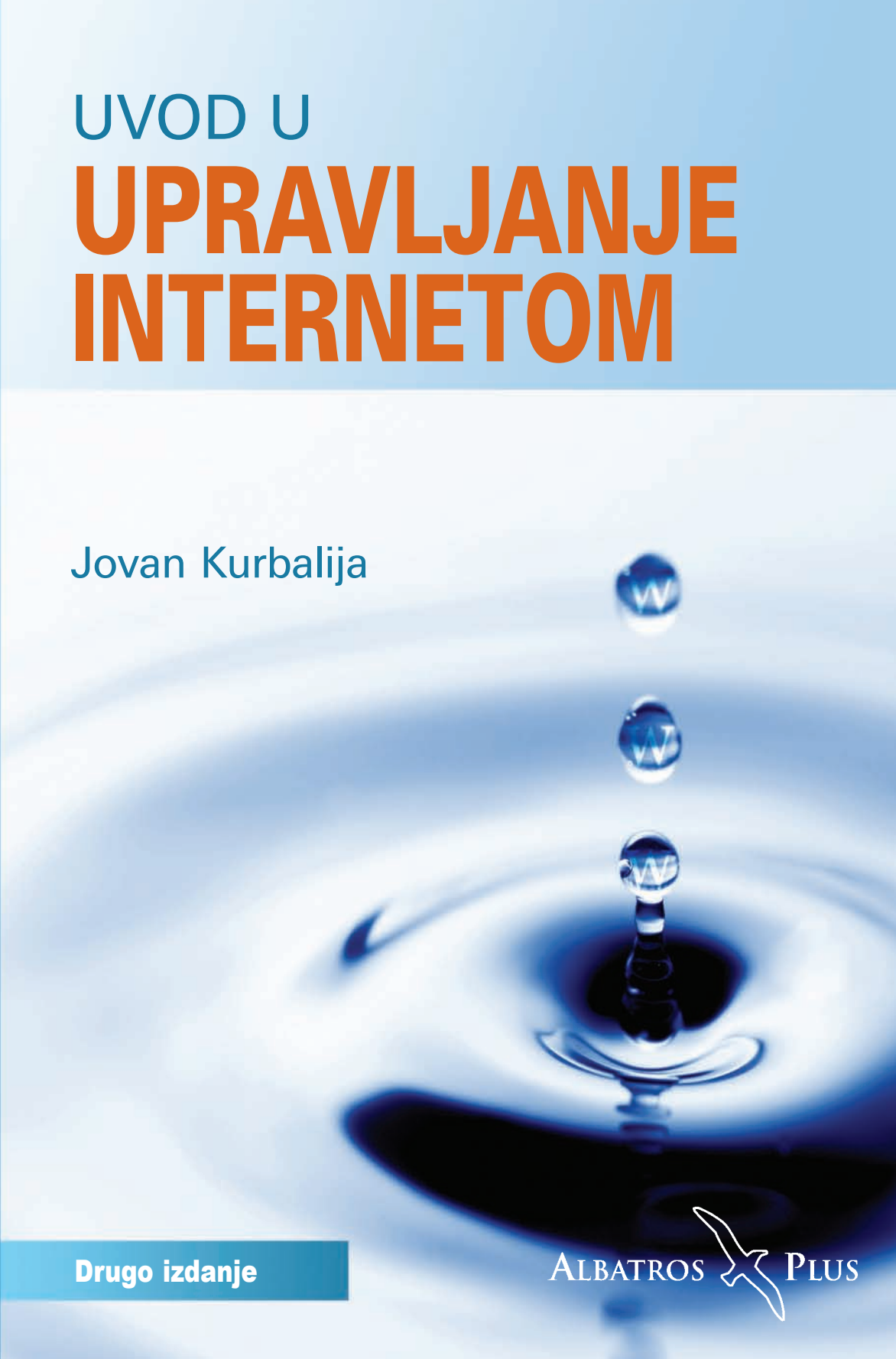
UVOD U
UPRAVLJANJE INTERNETOM

Jovan Kurbalija



Drugo izdanje

ALBATROS PLUS

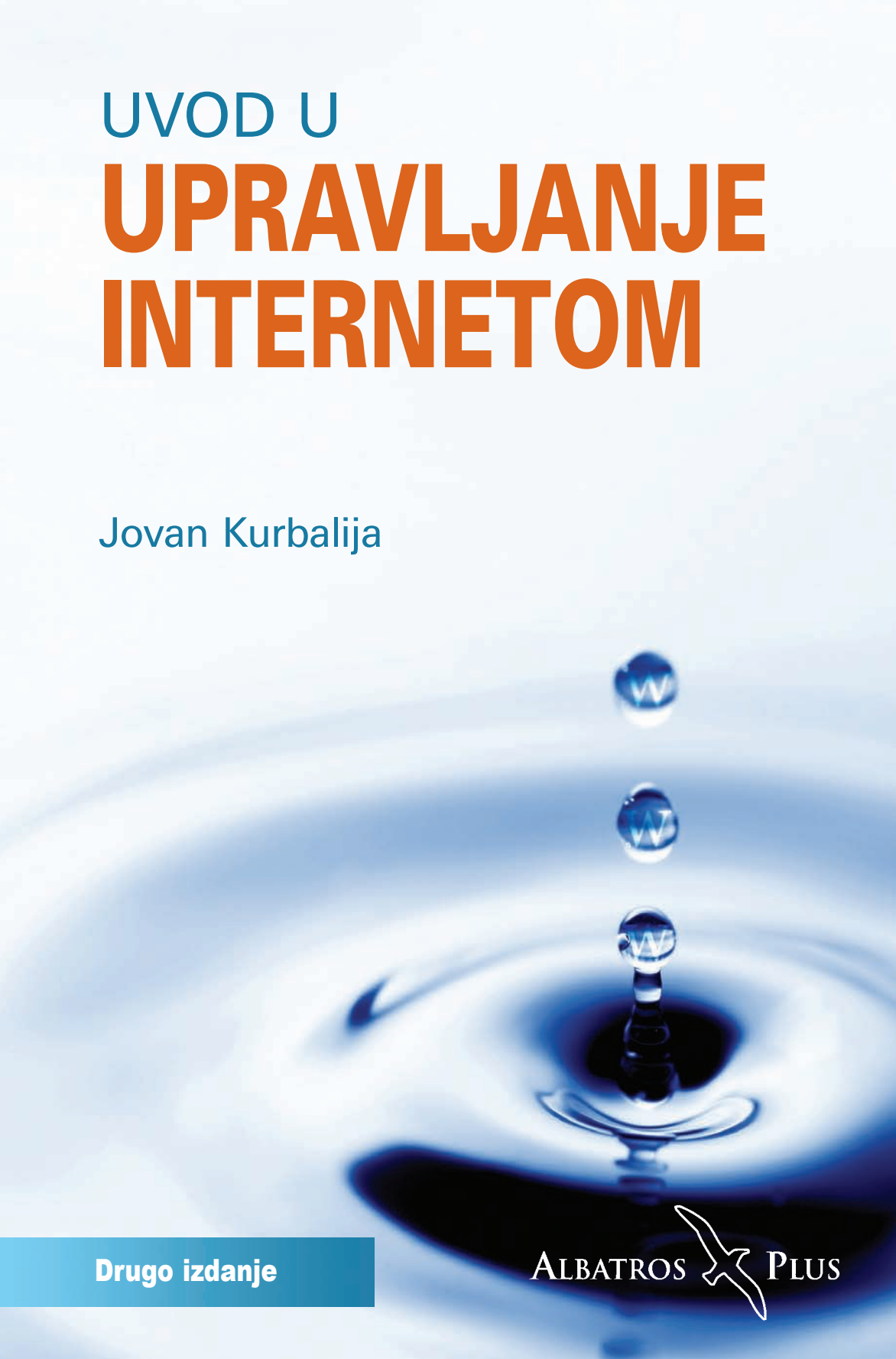
U eri brzog razvoja interneta, računajući internet vreme, istorija ove knjige je duga. Izvorni tekst i ukupan pristup, uključujući metodologiju pet korpi, nastali su 1997. godine kao kurs u vezi sa programom informacionih i komunikacionih tehnologija (IKT) za vladine službenike zemalja Komonvelta.

Godine 2004. DiploFondacija je objavila publikaciju *Upravljanje internetom – pitanja, akteri i jazovi.* Ova knjižica je bila deo *Biblioteke informacionog društva,* koju su pokrenuli Stefano Baldi, Eduardo Gelbstajn i Jovan Kurbalija. Posebna zahvalnost pripada Eduardu Gelbstajnu, koji je dao značajne priloge delovima vezanim za sajber-bezbednost, spem i privatnost, i Vladimiru Radunoviću i Džindžer Pak koji su osavremenili sadržaje kursa. Priznanja komentarima i sugestijama drugih kolega nalaze se u samom tekstu. Stefano Baldi, Eduardo Gelbstajn i Vladimir Radunović dali su značajan doprinos razvijanju koncepata koji stoje iza ilustracija prisutnih u knjizi.

Godine 2008. objavljena je specijalna, revidirana verzija ove knjige, pod jednostavnim naslovom *Uvod u upravljanje internetom,* i to u saradnji sa NIXI-Indija, povodom Foruma o upravljanju internetom održanog iste godine u Hajderabadu, Indija. Tokom 2009. godine objavljeno je revidirano treće izdanje u saradnji sa Ministarstvom za komunikacione i informacione tehnologije Egipta. *Upravljanje internetom* doživljava svoje četvrto izdanje (2010), koje je nastalo uz pomoć Evropske unije.

UVOD U UPRAVLJANJE INTERNETOM

Jovan Kurbalija



Drugo izdanje

ALBATROS PLUS

Izdavač
Albatros Plus

Biblioteka
Posebna izdanja

Glavni i odgovorni urednik
Jagoš Đuretić

Urednik
Jovo Cvjetković

Beograd 2011.

Iza ovog izdanja programski stoji DiploFoundation, a finansijski ga podržavaju Registar nacionalnog internet domena Srbije i Uprava za digitalnu agendu Republike Srbije.

Sadržaj

Predgovor srpskom izdanju 1
Predgovor izvornom engleskom izdanju 5

Prvi deo: Uvod 7
Šta znači upravljanje internetom? 9
Evolucija upravljanja internetom. 11
Kognitivni alati upravljanja internetom. 16
Pristupi i obrasci 18
Vodeći principi 23
Analogije 26
Klasifikacija tema upravljanja internetom 31
Zgrada u izgradnji: Gradimo li Vavilonsku kulu XXI veka? 33

Drugi deo: Infrastrukturna i standardizaciona korpa 37
Telekomunikaciona infrastruktura 40
Protokol kontrole prenosa/Internet protokol (TCP/IP) 42
Sistem imena domena (DNS). 45
Glavni serveri 49
Mrežna neutralnost 51
Provajderi internet usluga (ISP) 59
Provajderi za pružanje širokopojasnih internet usluga (IBP) 61
Ekonomski model povezivanja internetom 62
Veb-standardi 65
Servisi u oblaku (cloud computing) 66
Konvergencija: Internet – telekomunikacije – multimediji 68
Sajber-bezbednost 70
Kodiranje 73
Spem 75

Treći deo: Pravna korpa 83
Pravni instrumenti 85
Sudska nadležnost 90
Arbitraža 93
Autorska prava 95
Zaštitni žigovi 100
Patenti 100
Sajber-kriminal 101
Radni odnosi 102

Četvrti deo: Ekonomska korpa 107
Definicija elektronske trgovine 109
Zaštita potrošača 112
Oporezivanje i takse 114
Digitalni potpisi 115
Elektronska plaćanja: elektronsko bankarstvo i elektronski novac 117

Peti deo: Razvojna korpa 123
Digitalni jaz 127
Opšti pristup 128
Strategije za prevazilaženje digitalnog jaza 128

Šesti deo: Društveno-kulturna korpa 135
Ljudska prava 137
Politike sadržaja 140
Privatnost i zaštita podataka 144
Multijezičnost i kulturna raznolikost 148
Globalno javno dobro 150
Prava osoba sa invaliditetom 151
Obrazovanje 152
Bezbednost dece na internetu 154

Sedmi deo: Akteri upravljanja internetom 161
Vlade 164
Poslovni sektor 169
Civilno društvo 171
Međunarodne organizacije 172
Internetska zajednica 173
Internetska korporacija za dodeljena imena i brojeve (ICANN) 175

Osmi deo: Proces upravljanja internetom 181
Šta tvorci politika mogu da nauče od IGF-a 183
Pristupi za bavljenje pitanjima globalne politike 184
Rukovođenje političkim procesima 186
Bavljenje naučnim i tehničkim aspektima političkih pitanja 189
Povećana uključenost i učestvovanje 191

Deveti deo: Dodatak 197
Putovanje kroz upravljanje internetom 199
Kocka upravljanja internetom 200
Pregled evolucije upravljanja internetom 201
Predlog za standardizaciju stručnih termina 204
O Digitalnoj agendi, RNIDS i Diplo 206
O autoru 208

Predgovor srpskom izdanju

Knjiga «Uvod u upravljanje internetom» trebalo bi da odgovori na sve veće interesovanje domaće javnosti za pravne, političke, kulturne i ostale apsekte korišćenja inerneta. Ona je prevod četvrtog izdanja knjige «Introduction to Internet Governance», koja je prvi put objavljena 2004. godine i od tada odštampana na šest svetskih jezika (arapski, francuski, kineski, portugalski, ruski i španski) u preko 10,000 primeraka. Knjiga se koristi kao nastavna literatura na više od 20 svetskih univerziteta za kurseve upravljanja internetom.

Vreme objavljivanja knjige nije slučajnost. Niz skorašnjih događaja – poput vikiliksa, uloge socijalnih mreža u „arapskom proleću“, sajberupada u naizgled neprobojne sisteme velikih svetskih kompanija poput Sonija ali i kritičnu infrastrukturu poput e-uprave Estonije i nuklearnih postrojenja Natanc u Iranu – učinio je da poraste interesovanje za upravljanje internetom. Upravljanje internetom postaje sve važnija tema mnogh diplomatskih i političkih tela, uključujući i Ujedinjene nacije, G8, OECD, Evropsku komisiju, Savet Evrope, Međunarodnu telekomunikacionu uniju i druge.

Uporedo sa globalnim zbivanjima ali i usred napretka u razvoju telekomunikacione infrastrukture i usluga, u Srbiji i regionu aktuelizovala su se pitanja poput bezbednosti, privatnosti i prava korisnika, regulative sadržaja novih medija i zaštite intelektualne svojine na internetu.

Iako su podstaknuta tehnologijom, pitanja upravljanja internetom, u velikoj meri nisu tehnološka. Ona se često svode na ključne dilema razvoja savremenog drustva. Bez interneta, kao komunikacijske strukture savremenog drustva, teško je zamisliti sveopšti ekonomski i društveni razvoj. Za Srbiji i zemlje regiona, koje prolaze kroz dugu i

tešku tranziciju, internet pruža nove mogućnosti ekonomskog razvoja i opšteg boljitka.

Interes za upravljanje internetom, posebno je podstaknut organizacijom četvrtog pan-evropskog Dijaloga o upravljanju internetom (EuroDIG) u maju 2011. Godine u Beogradu. Na taj način poslat je jasan signal da je Srbija – kao i jugoistočna Evropa – zainteresovana i spremna da zajedno sa evropskim institucijama strateški radi na kompleksinim pitanjima upravljanja internetom.

EuroDIG 2011 je vrlo dobar primer nove diplomatije koja zahteva učešće raznorodnih aktera. Kroz funkcionalnu i kreativnu saradnju spojen je talenat i entuzijazam nekolicine domaćih stručnjaka u ovoj oblasti sa podrškom institucija, pre svega Ministarstva telekomunikacija kao zvaničnog domacina skupa. Medju više od 500 inostranih i domaćih učesnika nalazili su se, izmedju ostalih, predstavnici policije koji se bave sajber-kriminalom i aktivisti piratskih partija u Srbiji.

Tokom pripreme i u vreme EuroDIG-a 2011 domaći akteri – uključujući državne institucije, privatni i nevladin sektor, mediji i akademski sektor – razvili su mnogobrojne sinergije i praktično pokazale sta se sve može postići uz kreativnu saradnju koja prevazilazi tradicionalne institucionalne okvire.

Trebalo bi iskoristiti taj zamajac kako bi se dalje izgradile državne institucije, osnažili pojedinci, organizacije i mediji u Srbiji i regionu na polju pravljanja internetom. Za to je, pre svega, značajno odrzavanje pokrenute saradnje i dijaloga izmedju različithih aktera, ali i intenziviranje profesionalnog treninga i podizanje svesti o pitanjima upravljana internetom.

Srpsko izdanje knjige „Uvod u upravljanje internetom“ je tek prvi naš korak u ovom smeru. Posebno je zadovoljstvo činjenica da su ovaj korak podržali i Uprava za digitalnu agendu Republike Srbije i Registar nacionalnog Internet domena Srbije (RNIDS), koji su prepoznali značaj strateškog planiranja upravljanja internetom u Srbiji kao i pravovremenog i pravilnog pozicioniranja Srbije u međunarodnim pregovorima o budućnosti interneta. Ova knjiga je rezultat inicijative Slobodana Markovića i Vladimira Radunovića, dvojice stručnjaka koji su puno učinili na razvoju upravljanja interneta i pozicioniranju Srbije kao profesionalnog i priznatog aktera u ovoj oblasti na regionalnom i globalnom niovu.

Ova knjiga će neminovno pratiti dinamku razvoja interneta i društveno-političkih promena koje on inicira. Posebno je značajno nastaviti dalju «lokalizaciju» terminologije upravljanja internetom. Interesantno je da je, zapravo, ovo formalno drugo po redu izdanje na srpskom: prvo „specijalno“ izdanje pripremljeno uz EuroDIG skup u Beogradu je, zahvaljujući konstruktivnim predlozima domaće zajednice a pre svih Nikoli Božiću, Iliji Virijeviću i Tanji Milovanović, ubrzo iznedrilo i ovo drugo izdanje u kome je prevod termina koji još nisu standardizovani prilagođen terminima koji su se ustalili u govornoj praksi; za pojmove koji su potpuno novi u srpskom jeziku hrabro su predloženi prevodi.

Neka ovo bude i poziv čitaocima i stručnoj zajednici da predlože korekcije i dopune rečnika termina iz oblasti upravljanja internetom kako bi zajedno pomogli standardizaciju u srpskom jeziku, a time i unapređenju diskusije o upravljanju internetom.

Jovan Kurbalija
DiploFondacija
jul 2011.

Predgovor izvornom engleskom izdanju

Godine 2004, kada sam pokušavao da objasnim prijateljima na pitanje šta radim kao član WGIG-a (Working Group on Internet Governance – Radna grupa za upravljanje internetom), često su me zvali da im priključim štampače ili da instaliram novi softver. Što se njih tiče, ja sam radio nešto što ima veze s kompjuterima. Sećam se da sam proveo blic-anketu među svojim kolegama u WGIG-u, pitajući ih na koji način oni objašnjavaju svojim prijateljima, partnerima i deci šta rade. Kao i ja, imali su puno poteškoća. To je jedan od razloga zbog kojih sam počeo da smišljam i pripremam prvi tekst i ilustracije DiploFondacije u vezi sa upravljanjem internetom.

Danas, šest godina posle, isti oni ljudi koji su me molili da im priključim štampače dolaze mi s pitanjima o tome kako da zaštite svoju privatnost na Fejsbuku ili kako da osiguraju deci da bezbedno surfuju internetom. Sve više se itneresuju za pitanja kao što je pozicija Gugla u Kini ili mogućnosti sajber-rata.

Upravljanje internetom nalazi se sve više u fokusu javnosti. Što savremeno društvo više zavisi od interneta, to je važnije pitanje upravljanja internetom. To nije više pitanje za uske stručne krugove. Upravljanje internetom tiče se, u manjoj ili većoj meri, svih nas.

Upravljanje internetom posebno je značajno za one koji su duboko integrisani u elektronski svet, bilo preko elektronskog poslovanja ili korišćenja Fejsbuka. Šira grupa zainteresovanih za upravljanje internetom obuhvata vladine činovnike, vojne kadrove, advokate, diplomate i ostale koji su uključeni, bilo u obezbeđivanje javnih dobara ili očuvanje javne stabilnosti. Upravljanje internetom, a naročito zaštita privatnosti i ljudskih prava, je/su u fokusu civilnog društva i brojnih nevladinih organizacija. Za naučne krugove i inovatore širom sveta

bitno je da internet ostane otvoren za razvoj i inovacije. Jedan od glavnih ciljeva upravljanja internetom jeste stvaranje razvojnog ambijenta koji treba da omogući dalje korišćenje interneta kao lokomotive ekonomskog i drustvenog razvoja.

Ja se nadam da ova knjiga predstavlja jasan i pristupačan uvod u oblast upravljanja internetom. Za neke od vas, ona će biti prvi susret sa ovom temom. Drugima može poslužiti kao podsetnik da je ono što već rade u svojoj oblasti – bilo da je reč o elektronskom zdravlju, elektronskoj trgovini, ili elektronskom bilo čemu – deo šire porodice pitanja upravljanja internetom.

Glavni cilj ove knjige je da doprinese očuvanju interneta kao integrisanog i moćnog medija za milione ljudi širom sveta. Nadam se da vam otvara apetit i da vas podstiče da dublje zaronite u ovu značajnu i raznoliku oblast. Budite u toku. Pratite dešavanja na **http://www.diplomacy.edu/isl/ig/.**

Jovan Kurbalija
DiploFondacija
avgust 2010.

Prvi deo

Uvod

Iako se upravljanje internetom bavi suštinom **digitalnog** sveta, upravljanje ne može da se vrši digitalno-binarnom logikom (istinito/lažno i dobro/loše). Umesto toga, upravljanje internetom zahteva mnoštvo finesa i nijansi značenja i percepcije; ono tako zahteva **analogan** pristup, koji pokriva neprekidan niz opcija i kompromisa.

Zbog toga ova knjiga ne pokušava da pruži definitivne konstatacije u vezi s pitanjima upravljanja internetom. Njen cilj je pre da ponudi jedan praktičan okvir za analizu, raspravu i razrešenje značajnih pitanja u ovoj oblasti.

Uvod

Kontroverze koje okružuju upravljanje internetom počinju s njegovom definicijom. Nije u pitanju puka jezička pedanterija. Različite perspektive značenja upravljanja internetom pokreću različite praktične pristupe i očekivanja. Na primer, stručnjaci za telekomunikacije sagledavaju upravljanje internetom kroz prizmu razvoja tehničke infrastrukture. Informatičari se fokusiraju na razvoj različitih standarda i primena, kao što je XML (eXtensible Markup Language – jezik sa neograničenim i nepredefinisanim oznakama) ili Java. Stručnjaci za komunikacije ističu olakšanje komunikacije. Borci za ljudska prava posmatraju upravljanje internetom iz perspektive slobode izražavanja, privatnosti i drugih temeljnih ljudskih prava. Advokati se koncentrišu na sudsku nadležnost i rešavanje sporova. Političari širom sveta obično se fokusiraju na pitanja koja imaju odjeka u biračkom telu, kao što su tehno-optimizam (više kompjutera = više obrazovanja) i opasnosti (bezbednost interneta, zaštita dece). Diplomate se prvenstveno interesuju za razvijanje i zaštitu nacionalnih interesa. Spisak potencijalno konfliktnih stručnih perspektiva upravljanja internetom je dug.

Šta znači upravljanje internetom?

Svetski samit o informatičkom društvu (WSIS)[1] izašao je sa sledećom definicijom upravljanja internetom:

> *Upravljanje internetom predstavlja razvoj i primenu od strane vlada, privatnog sektora i civilnog društva, u njihovim specifičnim ulogama, zajedničkih principa, normi, pravila, postupaka pri donošenju odluka i programa koji oblikuju evoluciju i korišćenje interneta.*[2]

Ova, prilično široka, radna definicija ne razrešava pitanje različitih tumačenja dva ključna termina: 'interneta' i 'upravljanja'.

'I'nternet ili 'i'nternet i diplomatsko signaliziranje

Još 2003, časopis *Ekonomist* počeo je da piše internet s malim početnim slovom. Ova promena u uređivačkoj politici bila je inspirisana činjenicom da je internet postao svakodnevni pojam, da nije više bio dovoljno jedinstven i poseban da bi zahtevao veliko početno slovo. Reč 'internet' sledila je jezičku sudbinu (t)elegrafa, (t)elefona, (r)adija i (t)elevizije, kao i drugih takvih izuma.

Pitanje pisanja Interneta/interneta s velikim ili malim 'i' pojavilo se ponovo na konferenciji Međunarodne telekomunikacione unije (ITU) koja je održana novembra 2006. u Antaliji, gde je uvedena politička dimenzija kada se termin 'internet' pojavio u Rezoluciji ITU o upravljanju internetom, s malim umesto sa uobičajenim velikim 'I'. Dejvid Gros, američki ambasador za upravljanje internetom, izrazio je zabrinutost da pisanje malim početnim slovom može da signalizira nameru da se internet tretira kao i drugi međunarodni telekomunikacioni sistemi kojima upravlja ITU. Neki su ovo protumačili kao diplomatski signal namere ITU da igra značajniju ulogu u upravljanju internetom.[3]

Internet

Neki autori tvrde da termin 'internet' ne pokriva sve postojeće aspekte globalnih digitalnih tokova. Dva druga termina – informaciono društvo i informacione i komunikacione tehnologije (IKT) – obično se ističu kao obuhvatniji. Oni podrazumevaju oblasti koje se nalaze van domena interneta, kao što je mobilna telefonija. Međutim, argument za korišćenje termina 'internet' pojačava se brzom tranzicijom globalnih komunikacija prema korišćenju internet protokola (IP) kao glavnog tehničkog standarda komunikacija. Već sveprisutni internet nastavlja da se naglo širi, ne samo u smislu broja korisnika nego i u smislu usluga koje nudi, naročito govorni internetski protokol (VoIP), što može da potisne konvencionalnu telefoniju.

Upravljanje

Prilikom rasprave o upravljanju internetom, naročito u ranoj fazi WSIS-2003, došlo je do polemike u vezi s terminom 'upravljanje' i njegovim različitim tumačenjima. Po jednom tumačenju, upravljanje je sinonim sa drzavnom vlascu. Mnoge nacionalne delegacije su imale ovo početno shvatanje, što je dovelo do tumačenja da upravljanje internetom treba da bude posao države i da se njime treba baviti na međuvladinom nivou, sa ograničenim prisustvom drugih, uglavnom nedržavnih, učesnika.[4] Ovo tumačenje se sudarilo sa širim značenjem termina 'upravljanje', koje podrazumeva upravljanje poslovima bilo koje institucije, uključujući i one nevladine. Ovo je bilo značenje koje

su prihvatile internetske, uglavnom ne-vladine, organizacije, budući da opisuje način na koji se internetom upravlja od njegovih prvih dana.

Terminološka zbrka bila je dodatno iskomplikovana prevodom termina 'upravljanje' na druge jezike. Na španskom, ovaj termin prvenstveno se odnosi na javne aktivnosti ili vladu (*gestión público,* i *función de gobierno*). Asocijacija na javne aktivnosti ili vladu pojavljuje se i na francuskom (*gestion des affaires punliques, efficacité de l'administration, qualité de l'administration,* i mode de gouvernement). Portugalski sledi sličan obrazac kada se misli na javni sektor i vladu (*gestão pública* i *administração pública*).

Evolucija upravljanja internetom

Rano upravljanje internetom (od sedamdesetih godina XX veka do 1994)

Internet je počeo kao vladin projekat. Krajem šezdesetih godina XX veka, Vlada SAD finansirala je Agencijsku mrežu za razvijeni odbrambeni istraživački projekat (DARPA Net), elastično sredstvo komunikacija. Sredinom sedamdesetih godina, izumom TCP/IP (protokola za kontrolu prenosa/internet protokola), ova mreža se razvila u ono što danas poznajemo kao internet. Jedan od ključnih principa interneta predstavlja njegov podeljeni karakter: paketi podataka mogu da krenu mrežom različitim putevima, izbegavajući prepreke i kontrolne mehanizme. Ovom tehnološkom principu približio se sličan pristup regulisanju interneta u njegovim ranim fazama: Radna grupa o upravljanju internetom (WGIG), osnovana 1986, usavršavala je internet kooperativnim procesom donošenja odluka na bazi konsenzusa, što je podrazumevalo veoma širok krug različitih pojedinaca. Nije bilo centralne uprave, nije bilo centralnog planiranja, niti nekog velikog plana.

Ovo je navelo mnoge ljude da pomisle da je internet na neki način jedinstven i da može da ponudi alternativu politici savremenog sveta. U svojoj čuvenoj Deklaraciji o nezavisnosti sajber-prostora, Džon Peri Barlou je rekao:

> *(Internet) je suštinski vannacionalan, suštinski antisuveren i vaša (državna) suverenost ne može se primeniti na nas. Mi sami moramo da razmotrimo stvari.*

DNS rat (1994-1998)

Ovaj decentralizovani pristup upravljanju internetom ubrzo je počeo da se menja budući da su vlade i poslovni sektor shvatili značaj globalne

Prefiksi: e- / virtuelni / sajber / digitalni

Prefiksi **e- / virtuelni / sajber / digitalni** koriste se za opis raznih unapređenja IKT/interneta. Njihova upotreba počinje devedesetih godina i podrazumeva razne društvene, ekonomske i političke uticaje u razvoju interneta. Na primer, prefiks e- obično se povezuje sa elektronskom trgovinom i komercijalizacijom interneta krajem devedesetih godina. Stručnjaci i pioniri interneta koristili su i sajber i virtuelni za isticanje neobičnosti interneta i pojave vrlog novog sveta. Digitalni je počeo da se koristi prvenstveno u tehničkim oblastima, a naročito u kontekstu rasprava o digitalnom jazu.

U međunarodnoj areni, prefiks sajber koristio je Savet Evrope za Konvenciju o sajber-kriminalu (2001). U novije vreme se koristi za opis stvari vezanih za sajber-bezbednost. Svoju inicijativu u ovoj oblasti, Međunarodna unija za telekomunikacije (International Telecommunication Union – ITU) je nazvala Program globalne sajber-bezbednosti. Reč virtuelan retko se pojavljuje u međunarodnim dokumentima. Prefiks e- zadobio je posebnu naklonost u EU, gde opisuje raznovrsne postupke koji se odnose na elektronsku nauku i elektronsko zdravlje. Tokom WSIS-a, e- je uveden u Panevropski bukureštanski regionalni skup i postao je dominantan u svim tekstovima WSIS-a, uključujući završne dokumente. Primena kod WSIS-a koncentriše se na linije delovanja uključujući e-upravu, e-poslovanje, e-učenje, e-zdravlje, e-zapošljavanje, e-poljoprivredu i e-nauku.

mreže. Godine 1994, Nacionalna naučna fondacija SAD, koja je upravljala ključnom infrastrukturom interneta, odlučila je da zaključi podugovor za upravljanje Sistemom imena domena (Domain Name System – DNS) sa privatnom američkom kompanijom Sjedinjena mrežna rešenja (NSI). Ovo nije lepo primljeno u internetskoj zajednici i dovelo je do takozvanog 'DNS rata'.

Ovaj 'rat' doveo je na scenu nove igrače: međunarodne organizacije i države. Završio se 1998. osnivanjem nove organizacije, Internetske korporacije za dodeljena imena i brojeve (ICANN). Od tada, raspravu o upravljanju internetom karakteriše intenzivnije učestvovanje nacionalnih vlada.

Svetski samit o informacionom društvu (2003–2005)

WSIS, održan u Ženevi (2003) i Tunisu (2005), zvanično je postavio na dnevni red diplomatskih sastanaka pitanje upravljanja internetom. Fokus ženevske faze samita, kojoj je prethodio veći broj pripremnih komiteta i regionalnih sastanaka, bio je prilično širok, sa lepezom pitanja u vezi sa infromatikom i komunikacijama koja su iznosili učesnici. U stvari, tokom prvih pripremnih i regionalnih sastanaka, nije se koristio termin 'internet' a kamoli 'upravljanje internetom'.[6]

Upravljanje internetom uvedeno je u proces WSIS-a za vreme regionalnog sastanka za zapadnu Aziju u februaru 2003, pošto je Ženevski samit postao ključno pitanje pregovora WSIS-a.

Posle dugotrajnih pregovora i dogovora u poslednjem času, Ženevski samit WSIS-a saglasio se da osnuje Radnu grupu o upravljanju internetom (WGIG). WGIG je pripremila izveštaj koji je korišćen kao osnov za pregovore na drugom samitu WSIS-a održanom u Tunisu (novembar 2005). Program Tuniskog Samita o informacionom društvu razradio je pitanje upravljanja internetom, uključujući usvajanje definicije, navođenje pitanja u vezi sa upravljanjem internetom i osnivanje Foruma o upravljanju internetom (Internet Governance Forum – IGF), multiakterskog tela koje saziva generalni sekretar UN.

Dešavanja tokom 2006. godine

Posle Tuniskog samita, raspravu o upravljanju internetom obeležila su tri glavna događaja. Prvi je bio prestanak postojanja Memoranduma o razumevanju (MoU) i osnivanje novoga između ICANN-a i Ministarstva trgovine SAD. Neki su se ponadali da će ovaj događaj promeniti odnos između ICANN-a i Vlade SAD i da će ICANN postati nova vrsta međunarodne organizacije. Međutim, iako je MoU stanjio pupčanu vrpcu između ICANN-a i Vlade SAD, zadržao je mogućnost konačne internacionalizacije statusa ICANN-a.

Drugi događaj iz 2006. bio je IGF u Atini. Bio je to prvi takav forum i u mnogočemu je predstavljao eksperiment iz multilateralne diplomatije. Ovaj forum je zaista bio multiakterski. Svi igrači – države, kompanije i civilno društvo – učestvovali su na ravnopravnoj osnovi. Forum je takođe imao zanimljivu organizacionu strukturu za glavne događaje i radionice. U ulozi voditelja rasprava pojavljivali su se novinari i zbog toga se ovaj forum razlikovao od uobičajenog vođenja sastanaka pod okriljem UN. Međutim, neki su kritičari tvrdili da je forum bio samo ‘tok šou’ bez ikakvih opipljivih rezultata u obliku nekog završnog dokumenta ili plana akcije.

Treći glavni događaj tokom 2006. bila je Konferencija opunomoćenika ITU održana u Antaliji, Turska, u mesecu novembru. Izabran je novi generalni sekretar ITU, dr Hamdun Ture. On je najavio snažnije angažovanje na sajber-bezbednost i pomoć u razvoju. Takođe se očekivalo da će on uvesti nove modalitete u pristup ITU upravljanju internetom.

Dešavanja tokom 2007. godine

Tokom 2007, rasprave u ICANN-u bile su usredsređene na .xxx domene (sadržaji za odrasle), na obnavljanje debata o brojnim pitanjima upravljanja, uključujući i to da li ICANN treba da se bavi samo tehničkim problemima ili i pitanjima koja imaju značaj za javnu politiku.[7] Intervencije američke i drugih vlada koje su se odnosile na .xxx domene dodatno su podstakle pitanje na koji način vlade treba da budu uključene u savetovanja ICANN-a. Na drugom IGF-u, održanom novembra meseca u Rio de Žaneiru, glavni događaj bio je dodavanje kritičnih internet resursa (imena i brojeva) programu IGF-a.

Dešavanja tokom 2008. godine

Glavni događaj 2008, koji će nastaviti da utiče na upravljanje internetom, kao i drugim političkim sferama, bio je izbor Baraka Obame za američkog predsednika. Tokom svoje izborne kampanje, on je intenzivno koristio sredstva interneta i Veba 2.0. Neki čak tvrde da je to bio jedan od razloga njegovog uspeha. Među njegovim savetnicima nalaze se mnogi ljudi iz internetske delatnosti, uključujući direktora Gugla. Pored svesti o tehničkim dostignućima, predsednik Barak Obama podržava multilateralizam koji će neminovno uticati na raspravu o internacionalizaciji ICANN-a, i na razvoj režima upravljanja internetom.

Detaljnije o mrežnoj neutralnosti videti u Drugom delu

Tokom 2008. pojavila se mrežna neutralnost[8] kao jedno od najznačajnijih pitanja upravljanja internetom. O njoj se najviše raspravljalo u SAD između dva glavna suprotstavljena bloka. Obeležila je čak predsedničku kampanju u SAD, gde je imala podršku predsednika Obame. Mrežnu neutralnost uglavnom podržava takozvana internetska industrija, uključujući kompanije kao što su Gugl, Jahu i Fejsbuk. Promena u arhitekturi interneta koju je izazvalo narušavanje mrežne neutralnosti mogla bi ugroziti njihovo poslovanje. S druge strane se nalaze telekomunikacione kompanije, kao što su Verizon i AT&T, provajderi internet usluga (ISP-ovi) i multimedijska industrija. Zbog različitih razloga, ove bi industrije želele da vide neku vrstu diferencijacije u paketima koji putuju internetom.

Drugi veliki događaj predstavljao je brz razvoj Fejsbuka i društvenog umrežavanja. Kada je reč o upravljanju internetom, povećano korišćenje sredstava Web 2.0 otvorilo je pitanje privatnosti i zaštite podataka na Fejsbuku i sličnim servisima.

Dešavanja tokom 2009. godine

Prvi deo 2009. obeležen je čekanjem na pristup Obamine administracije pitanjima upravljanja internetom. Obamina imenovanja na ključna mesta na internetu nisu donela nikakvo veliko iznenađenje. Ona su sledila njegovu podršku otvorenom internetu. Njegov tim se takođe zalagao za primenu principa mrežne neutralnosti, u skladu sa obećanjima datim u toku njegove izborne kampanje.

Glavni događaj u 2009. godini bio je Zaključak o potvrdi obaveza između ICANN-a i Ministarstva trgovine SAD, koji bi trebalo da učini ICANN nezavisnijom organizacijom. Iako je ovaj potez rešio jedan problem u upravljanju internetom – nadzornu ulogu SAD u ICANN-u – otvorio je mnoga nova pitanja, kao što je međunarodna pozicija ICANN-a i nadzor aktivnosti ICANN-a. Potvrda obaveza daje osnovne smernice, ali ostavlja mnoga druga pitanja u predstojećim godinama.

U novembru 2009, u Šarm el Šeiku, Egipat, održan je četvrti IGF. Glavna tema bila je budućnost IGF-a obzirom na reviziju njegovog mandata predviđenu za 2010. godinu. U svojim referatima, akteri su izložili širok raspon pogleda o budućnosti IGF-a. Iako je većina podržala njegov nastavak, bilo je velikih razlika u mišljenjima u vezi s njegovom organizacijom. Kina i mnoge zemlje u razvoju zalagale su se za snažnije uklapanje IGF-a u sistem UN-a, što bi podrazumevalo značajniju ulogu vlada. SAD, većina zemalja u razvoju, poslovni sektor i civilno društvo zalagali su se za očuvanje sadašnjeg modela IGF-a.

Dešavanja tokom 2010. godine

Od avgusta 2010, glavna pitanja upravljanja internetom vezana su za sve veći značaj platformi društvenih medija kao što su Fejsbuk i Tviter. Jedno od glavnih pitanja jeste zaštita privatnosti korisnika ovih platformi. U onome što se može nazvati 'internetska geopolitika', glavni događaj bio je govor državne sekretarke Hilari Klinton o slobodi izražavanja na internetu, naročito u vezi sa Kinom.[9] Gugl i kineske vlasti sukobili su se z bog ograničenog pristupa Guglovoj pretrazi u Kini. To je dovelo do zatvaranja pretraživačkih operacija Gugla u ovoj zemlji.

Bila su dva značajna događaja u svetu ICANN-a. Prvi je bio uvođenje prvih ne-ASCII imena domena za arapski i kineski. Rešavanjem problema imena domena na drugim jezicima, ICANN je smanjio opasnost od dezintegracije DNS-a. Drugi događaj bilo je odobrenje koje je dao

ICANN za .xxx (sadržaje za odrasle). Ovom odlukom, ICANN je formalno prešao Rubikon, usvojivši zvanično odluku visoke važnosti za javnu politiku na internetu. Pre toga, ICANN je pokušavao da ostane, barem formalno, u okviru donošenja samo tehničkih odluka.

Proces revizije IGF-a počeo je 2010. godine, kada je Komisija za nauku i razvoj UN usvojila rezoluciju o nastavku IGF-a, što predstavlja nastavak za sledećih pet godina, sa neznatnim promenama u organizaciji i strukturi. Jula meseca 2010, Ekonomski i društveni savet UN podržao je ovu rezoluciju. Konačna odluka o nastavku IGF-a biće doneta tokom zasedanja Generalne skupštine UN u jesen 2010.

Kognitivni alati upravljanja internetom

Za duboke istine i suprotnosti su istinite, nasuprot trivijalnostima gde se suprotnosti isključuju

Nils Bor, atomski fizičar (1885–1962)

Kognitivni alati upravljanja internetom sastoji se od niza sredstava za razvijanje politike i pripremanje argumentacije te politike. On ima brojne praktične funkcije za one koji su uključeni u upravljanje internetom. Doprinosi rukovanju ogromnom količinom informacija, dokumenata i studija o upravljanju internetom, kao i razradi opisa te politike i razumevanju drugih pristupa istoj.

Konačno, ovi alati poboljšavaju kvalitet pregovora povećavanjem mogućnosti za uključnost i rešenja zasnovana na kompromisu. On se bavi sve razvijenijim režimom upravljanja internetom, koji se još nalazi u sasvim početnim fazama razvoja. Iskustvo iz drugih međunarodnih režima (npr. ekologija, vazdušni saobraćaj, kontrola naoružanja) pokazalo je da takvi režimi najpre nastoje da razviju zajednički okvir, uključujući vrednosti, percepciju odnosa uzroka i posledice, načine razmišljanja, terminologiju, rečnik, žargon i skraćenice. Ovaj okvir je veoma značajan u političkom životu. On određuje kakva se naročita pitanja formiraju i kakve se radnje preduzimaju.

U mnogim slučajevima, ovaj zajednički okvir dolazi pod uticaj specifične profesionalne kulture (obrasci znanja i ponašanja koje dele pripadnici iste profesije). Postojanje takvog okvira obično olakšava komunikaciju i razumevanje. On takođe može da se koristi za zaštitu profesionalnog

delokruga i za sprečavanje spoljnih uticaja. Da citiramo američkog lingvistu Džefrija Majrela: “Svaki stručni jezik je zaštitni jezik.”

Režim upravljanja internetom kompleksan je zato što uključuje mnoga pitanja, aktere, mehanizme, postupke i instrumente. Gornja slika, koju je inspirisao holandski slikar M. K. Esher (Escher), pokazuje neke paradoksalne perspektive povezane s internetom.

Ovi alati odražavaju karakter upravljanja internetom, kao takozvano područje ‘pogrešne politike', koju karakteriše veliki broj katalizatora, kao i poteškoća na koju nailazimo prilikom dodeljivanja uzročnosti za razvoj politike jednom specifičnom razlogu. U mnogim slučajevima, svaki problem je simptom nekog drugog, pri čemu se ponekad stvaraju začarani krugovi. Neki kognitivni pristupi, kao što je linearno, jednoznačno i/ili razmišljanje, imaju vrlo ograničenu korisnost u oblasti upravljanja internetom. Upravljanje internetom je odveć kompleksno da bi se steglo steznjakom doslednosti, nekontradikcije i konsekventnosti. Fleksibilnost i otvorenost, i spremnost na neočekivano, mogli bi biti bolji deo vrednosti upravljanja internetom.

Kao i sam proces upravljanja internetom, i alati su raznoliki. Pristupi, obrasci, vodeći principi i analogije pojavljuju se i nestaju u zavisnosti od njihovog aktuelnog značaja u političkom procesu.

Pristupi i obrasci

Upravljanje internetom kao celina, kao i specifična pitanja upravljanja internetom, bili su neko vreme deo političkih rasprava i akademskih razmena mišljenja. Postepeno je dolazilo do pojave nekih pristupa i obrazaca, koji su predstavljali tačke u kojima su se mogle identifikovati razlike u pregovaračkim pozicijama, kao i u profesionalnim i nacionalnim kulturama. Identifikovanje zajedničkih pristupa i obrazaca može da smanji kompleksnost pregovaranja i da doprinese stvaranju zajedničkog okvira.

Uski nasuprot širokom pristupu

Rasprava o uskom nasuprot širokom pristupu upravljanju internetom do sada je zauzimala centralno mesto, odražavajući različite pristupe i interesovanja za ovaj proces.

Uski pristup koncentriše se na infrastrukturu interneta (DNS, IP brojevi i glavni serveri) i na poziciju ICANN-a kao ključnog aktera u ovoj oblasti. Prema širokom pristupu, trebalo bi da pregovori o upravljanju internetom idu van infrastrukturnih tačaka i da se bave drugim pravnim, ekonomskim, razvojnim i društveno-ekonomskim pitanjima. Ovaj potonji pristup usvojen je u Izveštaju WGIG-a i u Završnom dokumentu WSIS-a. On se takođe koristi kao temeljni princip arhitekture IGF-a.

Razlikovanje između ova dva pristupa bilo je naročito značajno tokom pregovora u okviru WSIS-a. Međutim, ono nije potpuno razrešeno do kraja procesa WSIS-a. Rasprave na IGF-u u Rio de Žaneiru (novembra 2007) jasno ističu da široki pristup ne znači da bi trebalo da razgovori budu magloviti. IGF u Riju je odlučio da se vrati na pitanje suštinskih izvora interneta (tzv. ICANN pitanjima) u programu Foruma.

Tehnička i politička doslednost

Značajan izazov s kojim se suočava proces upravljanja internetom jeste integracija tehničkih i političkih aspekata, budući da je teško povući jasnu razliku između ovih elemenata. Tehnička rešenja nisu neutralna. U krajnjem slučaju, svako tehničko rešenje/opcija forsira određene interese, favorizuje neke grupe i u izvesnoj meri, utiče na društveni, politički i ekonomski život.

U slučaju interneta, dugo vremena je i tehničkim i politčkim aspektima vladala samo jedna društvena grupa – prva Internet zajednica. Razvojem

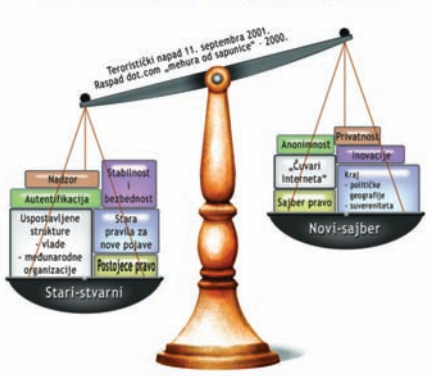
interneta i pojavom novih aktera tokom devedesetih godina – uglavnom poslovnog sektora i vlada – više nije bilo integrisanog pokrivanja tehničkih i političkih pitanja pod jednim krovom od strane internetske zajednice. Potonje reforme, uključujući formiranje ICANN-a, pokušale su da ponovo uspostave čvrstu vezu između tehničkih i političkih aspekata. Ovo pitanje ostaje otvoreno i ispostavilo se, prema očekivanjima, da predstavlja jednu od kontroverznih tema na debati Foruma o upravljanju internetom.

'Stari-realni' nasuprot 'novom-sajber' pristupu

Postoje dva pristupa gotovo svim pitanjima upravljanja internetom. 'Stari-realni' pristup – zamislite 'novo vino u starim flašama' – tvrdi da internet nije uveo ništa novo u oblast upravljanja. On predstavlja samo novo sredstvo, koje se iz perspektive upravljanja ne razlikuje od prethodnih: telegrafa, telefona i radija.

Paradigma upravljanja internetom

Stari-realni vs novi-sajber



Na primer, u pravnim raspravama, ovaj pristup smatra da se postojeći zakoni mogu primeniti na internet sa minimalnim prilagođavanjima. U ekonomskoj oblasti, ovaj pristup smatra da ne postoji nikakva razlika između redovne i elektronske trgovine. Shodno tome, nema nikakve potrebe za posebnim tretmanom elektronske trgovine.

'Novi-sajber' pristup smatra da je internet suštinski različit sistem komunikacije od svih prethodnih. Glavna premisa sajber pristupa glasi da je internet uspeo da odvoji našu društvenu i političku stvarnost od (geografski odvojenog) sveta suverenih država. Sajber-prostor se razlikuje od stvarnog prostora i zahteva drugačiji oblik upravljanja. U pravnoj oblasti, sajber-škola smatra da se postojeći zakoni o jurisdikciji, sajber-kriminalu i ugovorima ne mogu primenjivati na internet i da se moraju doneti novi zakoni. Sve više, stari-realni pristup postaje značajniji i na regulatornom i na političkom planu.

Decentralizovana nasuprot centralizovanoj strukturi upravljanja internetom

Prema decentralizovanom stavu, struktura upravljanja internetom trebalo bi da odražava samu prirodu interneta: mrežu mreža. Ovo gledište naglašava da je internet toliko kompleksan da se ne može staviti pod jedan upravljački kišobran, kao što je neka međunarodna organizacija, i da je decentralizovano upravljanje jedan od glavnih faktora koji omogućava brz razvoj interneta. Ovaj stav uglavnom podržavaju tehnička internetska zajednica i razvijene zemlje.

Centralizovani pristup, s druge strane, delimično se zasniva na praktičnoj poteškoći zemalja sa ograničenim ljudskim i finansijskim resursima da prate rasprave o upravljanju internetom u jako decentralizovanom i multiinstitucionalnom ambijentu. Takvim zemljama je teško da prisustvuju sastancima u glavnim diplomatskim centrima (Ženeva, Njujork), a kamoli da prate aktivnosti drugih institucija, kao što su ICANN, WWW konzorcijum i WGIG. Ove zemlje, uglavnom u razvoju, zalažu se za obradu na jednom mestu (one-stop shop), po mogućnosti u okviru neke međunarodne organizacije.

Zaštita javnih interesa na internetu

Jedna od glavnih moći interneta jeste njegov javni karakter, koji mu je omogućio brz razvoj i koji, takođe, podstiče kreativnost i uključenost. Kako da se zaštiti javni karakter interneta, ostaće jedno od suštinskih pitanja debate o upravljanju internetom. Ovaj problem je posebno komplikovan obzirom na to da se znatan deo osnovne strukture interneta – od transkontinentalnih okosnica do lokalnih mreža – nalazi u privatnom vlasništvu. Da li se od privatnih vlasnika može tražiti da upravljaju ovim vlasništvom u javnom interesu i koji delovi interneta se mogu smatrati globalnim javnim dobrom, teška su pitanja kojima se moramo baviti. U najnovije vreme, pitanje javnog karaktera interneta ponovo je otvoreno kroz raspravu o mrežnoj neutralnosti.

Za detaljniju raspravu o mrežnoj neutralnosti videti Drugi deo

Geografija i internet

Jedna od ranih pretpostavki u vezi s internetom bila je da je on prevazišao državne granice i da je narušio princip suvereniteta. Obzirom na činjenicu da je komunikacija internetom lako prelazila državne granice i da je anon-

imnost korisnika ukorenjena u sam smisao interneta, mnogima se činilo, da citiramo poznatu Deklaraciju o nezavisnosti sajber-prostora,[11] da vlade 'nemaju nikakvo moralno pravo da vladaju nama (korisnicima)', niti da 'imamo pravi razlog da se plašimo bilo kojeg metoda prisile'.

Međutim, najnoviji tehnički momenti, uključujući geolokacijski softver, sve više osporavaju stav o kraju geografije u eri interneta. Danas je još uvek teško tačno identifikovati onoga ko se nalazi iza ekrana, ali je prilično lako identifikovati preko kojeg provajdera se povezao s internetom.

Što više internet bude vezan za geografiju, to će manje jedinstveno biti njegovo upravljanje. Na primer, sa mogućnošću lociranja internet korisnika i transakcija, složeno pitanje sudske nadležnosti na internetu može se rešavati preko postojećih zakona

Politička neizvesnost

Rasprava o upravljanju internetom vodi se u kontekstu visoke neizvesnosti u vezi sa budućim tehničkim razvojem interneta, tako da ova neizvesnost pogađa program rada na upravljanju internetom. Na primer, 2002. godine, kada je pokrenut rad WSIS-a,[12] Gugl je bio samo jedna od mnogih mašina za pretraživanje. Na kraju ovog procesa u novembru 2005, Gugl je uspostavljen kao glavna kompanija koja oblikuje korišćenje interneta. Godine 2002, korišćenje blogova bilo je u povojima. Danas blogeri obaraju vlade, pomeraju granice slobode izražavanja i imaju znatan uticaj na društveni i ekonomski život. Spisak tehnoloških rešenja koja imaju značaj za upravljanje internetom uključuje Fejsbuk, Skajp, Ju tjub, Tviter i Viki.

Danas mnogi misle da tradicionalna suštinska pitanja u vezi s upravljanjem internetom (pitanja koja se odnose na ICANN) postepeno gube značaj u poređenju s pitanjima u vezi sa mrežnom neutralnošću, s približavanjem različitih tehnologija (npr. telefonije, TV-a i interneta), i u vezi s pitanjima upravljanja koja se odnose na društvene mreže (Fejsbuk i Tviter), kao i na ulogu Gugla i Vikipedije kao čuvara digitalizovanog znanja i informacija.

Rešenja s političkim balansiranjem

Balansiranje je verovatno najpogodnija grafička ilustracija rasprava o upravljanju internetom i njegovoj politici. Po mnogim pitanjima upravljanja internetom, mora se uspostaviti ravnoteža između različitih interesa i pristupa. Uspostavljanje ove ravnoteže vrlo često predstavlja osnov za kompromis. Područja balansiranja politike uključuju:

Rešenja s političkim balansiarnjem u istoriiji (uramiti)

Još 1875. godine, Međunarodna telegrafska unija (prethodnica današnje Međunarodne telekomunikacione unije) održala je konferenciju u Sankt Peterburgu, koja je uticala na budući razvoj telegrafa. Jedno od najspornijih pitanja bila je kontrola sadržaja telegrafskih poruka. Dok su se učesnici konferencije iz SAD i UK zalagali za princip privatnosti telegrafske korespondencije, Rusija i Nemačka su insistirale na ograničavanju privatnosti da bi se zaštitili državna bezbednost, javni red i javni moral. Postignut je kompromis posredstvom stare diplomatske tehnike – diplomatskom dvosmislenošću. Dok je član 2 Sanktpeterburške kovencije garantovao privatnost telegrafske komunikacije, član 7 je ograničavao ovu privatnost i uvodio je mogućnost državne cenzure. SAD su odbile da potpišu Konvenciju zbog člana o cenzuri.

- Slobodu izražavanja nasuprot zaštiti javnog reda: poznata rasprava između člana 19 (sloboda izražavanja) i člana 27 (zaštita javnog reda) Univerzalne deklaracije o ljudskim pravima, proširena je na internet. O tome se često raspravlja u kontekstu kontrole sadržaja i cenzure na internetu.

- Sajber-bezbednost nasuprot privatnosti: kao što je slučaj sa bezbednošću u stvarnom životu, tako i sajber-bezbednost može da ugrozi neka ljudska prava, kao što je pravo na privatnost. Ravnoteža između sajber-bezbednosti i privatnosti neprestano varira, u zavisnosti od globalne političke situacije. Posle 11. septembra, obzirom na potrebu za jačanjem globalne bezbednosti, ova ravnoteža se pomerila prema sajber-bezbednosti.

Za detaljniju raspravu o sajber-bezbednosti videti Drugi deo

- Intelektualna svojina – zaštita autorskih protiv poštenog korišćenja građe: još jedna 'realna' zakonska dilema koja je poprimila novu perspektivu u onlajn svetu.

Za detaljniju raspravu o intelektualnoj svojini videti Treći deo

Mnogi kritikuju ove 'balansirajuće parove', smatrajući ih lažnim dilemama. Postoje, na primer, snažni argumenti da više sajber-bezbednosti ne znači nužno manje privatnosti. Postoje pristupi koji teže ka jačanju i sajber-bezbednosti i privatnosti. Iako su ovi stavovi čvrsti, realnost politike upravljanja internetom jeste da je oblikuju u pomenute 'binarne' političke opcije.

Vodeći principi

Vodeći principi predstavljaju izvesne vrednosti i interese koji su bitni za pojavu režima upravljanja internetom. Neke od tih principa usvojio je WSIS, kao što su transparentnost i uključnost. Drugi principi su uvedeni uglavnom prećutno, preko rasprava o upravljanju internetom.

Ne izmišljajte točak

Svaka inicijativa u oblasti upravljanja internetom treba da počne od postojećih propisa, koji se mogu podeliti na tri velike grupe:

1. propisi izmišljeni za internet (npr. ICANN);
2. propisi koji zahtevaju znatno prilagođavanje u cilju bavljenja pitanjima vezanim za internet (npr. zaštita marki, elektronsko oporezivanje); i
3. propisi koji se mogu primenjivati na internet bez znatnih prilagođavanja (npr. zaštita slobode izražavanja).

Korišćenje postojećih pravila značajno bi povećalo pravnu stabilnost i smanjilo složenost razvoja režima upravljanja internetom.

Ako nije u kvaru, ne popravljajte ga

Upravljanje internetom mora zadržati tekuću funkcionalnost i krepkost interneta, a da ipak ostane dovoljno fleksibilan da usvaja promene koje vode ka povećanoj funkcionalnosti i većoj legitimnosti. Postoji opšti konsenzus da funkcionalnost i stabilnost interneta treba da bude jedan od vodećih principa upravljanja internetom. Stabilnost interneta treba da se sačuva preko ranog internet pristupa 'funkcionalnog koda' (running code), što podrazumeva postepeno uvođenje proverenih promena u tehničku infrastrukturu.

Međutim, neki akteri se plaše da će parola 'ako nije u kvaru, ne popravljajte ga' dovesti do otpornosti na sve promene u aktuelnom upravljanju internetom, uključujući i promene koje se ne odnose nužno na infrastrukturu. Jedno od rešenja je da se ovaj princip koristi kao kriterijum za vrednovanje specifičnih odluka koje se odnose na upravljanje internetom (npr. uvođenje novih protokola i promena mehanizma donošenja odluka).

Promovisanje celovitog pristupa i određivanje prioriteta

Celovit pristup bi trebalo da olakša bavljenje ne samo tehničkim nego i pravnim, društvenim, ekonomskim i razvojnim aspektima razvoja interneta. Ovaj pristup bi trebalo da uzme u obzir sve veće približavanje digitalnih tehnologija, uključujući seobu telekomunikacionih servisa prema internet protokolima.

Pri zadržavanju celovitog pristupa pregovorima o upravljanju internetom, trebalo bi da akteri identifikuju prioritetna pitanja u zavisnosti od svojih partikularnih interesa. Ni zemlje u razvoju ni razvijene zemlje ne čine homogene grupe. Među zemljama u razvoju postoje znatne razlike u prioritetima, nivou razvoja i IT opremljenosti (npr. između naprednih IKT zemalja, kao što su Indija, Kina i Brazil, i nekih najnerazvijenijih zemalja u podsaharskoj Africi).

Celoviti pristup i određivanje prioriteta programa upravljanja internetom trebalo bi da pomognu akterima i iz razvijenih i iz zemalja u razvoju da se koncentrišu na naročiti niz pitanja. Ovo bi trebalo da vodi ka suštinskijim i verovatno manje politizovanim pregovorima. Trebalo bi da se akteri grupišu oko pitanja pre nego oko tradicionalno visokopolitizovanih jazova (npr. razvijene zemlje-zemlje u razvoju, vlade-civilno društvo).

Princip tehnološke neutralnosti

Prema principu tehnološke neutralnosti, ne bi trebalo da se politika određuje za specifična tehnološka ili tehnička sredstva. Na primer, propisi za zaštitu privatnosti trebalo bi da određuju šta treba da se zaštiti (npr. lični podaci, zdravstveni dosijei), a ne kako da se zaštiti (npr. pristup bazama podataka, kriptozaštita). Korišćenje principa tehnološke neutralnosti čini da je nekoliko zaštitinih instrumenata privatnosti i podataka, kao što su Smernice Organizacije za ekonomsku saradnju i razvoj (OECD) iz 1980. godine, jednako značajno danas kao i u godini donošenja.

Tehnološka neutralnost obezbeđuje mnogo upravljačkih prednosti. Ona osigurava stalan značaj upravljanja, bez obzira na budući tehnološki napredak i verovatno približavanje glavnih tehnologija (telekomunikacije, mediji, internet, itd). Tehnološka neutralnost se razlikuje od mrežne neutralnosti: prva pokazuje da je naročita politika nezavisna od tehnologije koju reguliše; druga se koncentriše uglavnom na neutralnost internetskog saobraćaja.

Za detaljniju raspravu o mrežnoj neutralnosti videti Drugi deo

Pretvorite prećutna tehnološka rešenja u eksplicitne političke principe

Postoji opšta saglasnost unutar internetske zajednice da se neke društvene vrednosti, kao što je slobodna komunikacija, olakšavaju načinom na koji je internet tehnološki osmišljen. Na primer, princip mrežne neutralnosti, prema kojem mreža treba samo da prenosi podatke između dve krajnje tačke bez uvođenja posrednika, često se pozdravlja kao garancija slobodnog govora na internetu. Ovaj stav bi mogao dovesti do pogrešnog zaključka da su tehnološka rešenja dovoljna za promovisanje i zaštitu društvenih vrednosti. Najnovija internetska dostignuća, kao što je korišćenje tehnologija mrežne barijere za ograničavanje protoka informacija, dokazuju da se tehnologija može koristiti na mnogo, naizgled kontradiktornih načina. Kad god je moguće, principi kao što je slobodna komunikacija treba da budu jasno izneti na nivou politike, a ne da se prećutno podrazumevaju na tehničkom nivou. Tehnološka rešenja treba da jačaju političke principe, ali ne treba da budu jedini način njihovog promovisanja.

Izbegavajte opasnost vođenja društva preko programerskog koda

Jedan ključni aspekt odnosa između tehnologije i politike identifikovao je Lorens Lesing, koji je zapazio da moderno društvo, sve većom zavisnošću od interneta, može da završi tako da će njime upravljati softverski kod umesto prateći zakoni. U krajnjem slučaju, neke zakonodavne funkcije parlamenta i vlade mogle bi de facto preuzeti kompjuterske kompanije i kreatori softvera. Kombinovanjem softvera i tehničkih rešenja, oni bi mogli da utiču na život u društvima koja se sve više baziraju na internetu. Ako bi ikada došlo do toga da se društvom upravlja kodom umesto zakonima, to bi u suštini dovelo u pitanje sam osnov političkog i pravnog organizovanja modernog društva.

Analogije

Iako je analogija često varljiva,
ona je najmanje varljiva od svega što imamo.

Semjuel Batler, britanski pesnik (1835-1902)

Analogija nam pomaže da razumemo novo na osnovu već poznatoga. Povlačenje paralela između prošlih i sadašnjih primera, uprkos opasnosti koje nosi, jedan je od ključnih spoznajnih procesa u pravu i politici. Većina pravnih predmeta u vezi s internetom rešava se putem analogija, naročito u anglosaksonskom pravnu sa presedanima sistemu.

Korišćenje analogija u upravljanju internetom ima nekoliko značajnih ograničenja. Prvo, 'internet' je širok pojam koji obuhvata mnoštvo usluga, uključujući elektronsku poštu (analogno telefoniji), veb usluge (analogno televiziji) i baze podataka (analogno bibliotekama). Analogija sa bilo kojim specifičnim aspektom interneta može da preterano uprosti njegovo razumevanje.

Drugo, sa sve većim približavanjem različitih telekomunikacijskih i medijskih usluga, zamagljuju se tradicionalne razlike između njih. Na primer, uvođenjem prenosa glasa preko IP (VoIP), sve je teže praviti razliku između interneta i telefonije.

Uprkos ovim ograničavajućim faktorima, analogije su još uvek moćne; one su još uvek glavno kognitivno sredstvo za rešavanje pravnih predmeta i za razvijanje režima upravljanja internetom.

Internet – telefonija

Sličnosti: U prvim danima interneta, ova analogija se nalazila pod uticajem činjenice da se telefonija koristila za pristup internetu. Osim toga, na snazi je i dalje funkcionalna analogija između telefona i interneta (i-mejl i četovanje), budući da su oboje sredstvo za direktnu i ličnu komunikaciju.

Razlike: Internet koristi pakete umesto kola (telefon). Za razliku od telefonije, internet ne može garantovati usluge; on može garantovati jedino 'najbolji napor'. Ova analogija ističe samo jedan aspekt interneta: komunikaciju putem i-mejla ili četovanje. Druge velike internetske aplikacije, kao što je WWW, interaktivne usluge, itd, ne dele zajedničke elemente sa telefonijom.

Poštanski sistem i ICANN

Pol Tumi, bivši direktor ICANN-a, koristio je sledeću analogiju između funkcije poštanskog sistema i ICANN-a: Ako razmišljate o internetu kao o pošti ili poštanskom sistemu, ime domena i IP adresa u suštini obezbeđuju funkcionisanje adresa na prednjem delu koverta. Oni nemaju ništa sa sadržajem koverta, s tim ko šalje koverat, ko može da čita taj sadržaj, koliko je potrebno kovertu da stigne, koja je cena koverta. Nijedno od tih pitanja nije bitno za funkcionisanje ICANN-a.

Korisnici: Ovu analogiju koriste oni koji se protive regulisanju internet sadržaja (uglavnom u Sjedinjenim Državama). Kada bi internet bio analogan telefoniji, sadržaj internetske komunikacije ne bi se mogao kontrolisati, kao što je to slučaj s telefonom. Koriste je i oni koji tvrde da internetom treba da upravljaju, kao i sa ostalim komunikacionim sistemima (npr. telefonijom, poštom), državne vlasti uz koordinirajuću ulogu međunarodnih organizacija, kao što je ITU. Po ovoj analogiji, trebalo bi da se DNS organizuje i da se njime rukovodi kao brojevnim sistemom telefonije.[13]

Internet – mejl/pošta

Sličnosti: Postoji analogija u funkcionisanju, to jest u dostavljanju poruka. Sam naziv, i-mejl, ističe ovu sličnost.

Razlike: Ova analogija pokriva samo jednu internetsku uslugu: i-mejl. Štaviše, poštanska usluga ima mnogo finiju posredničku strukturu između pošiljaoca i primaoca od i-mejl sistema, gde aktivnu posredničku funkciju vrše provajderi internet usluga ili i-mejl servis provajderi kao Jahu! ili Hotmejl.

Korisnici: Univerzalna poštanska konvencija povlači ovu analogiju između pošte i i-mejla: 'Elektronska pošta predstavlja poštansku uslugu koja za prenos koristi telekomunikacije.' Ova analogija može imati posledice u vezi sa dostavlajnjem službenih dokumenata. Na primer, prijem neke sudske odluke putem i-mejla smatrao bi se službenom dostavom.

Porodice američkih vojnika koji su poginuli u Iraku takođe su pokušale da koriste analogiju između pošte (pisama) i i-mejla da bi dobile pristup privatnim i-mejlovima i blogovima svojih voljenih, tvrdeći da bi trebalo da im se dozvoli da naslede i-mejlove i blogove kao što je slučaj sa dnevnicima i pismima.

Provajderi internet usluga nisu imali snage da se bave ovim veoma emocionalnim problemom. Umesto da poštuju analogiju između pisama i i-mejlova, većina provajdera nije dozvolila pristup na osnovu ugovora o privatnosti koji su potpisali sa svojim korisnicima.

Internet – televizija

Sličnosti: Početna analogija odnosila se na fizičku sličnost između ekrana kompjutera i televizije. Finija analogija poziva se na korišćenje oba medija – veb i TV – za emitovanje.

Razlike: Internet je širi medij od televizije. Osim sličnosti između kompjuterskog i TV ekrana, postoje velike strukturne razlike između njih. Televizija je medij jedan-mnogima, za prenošenje gledaocima, dok internet olakšava mnoštvo različitih vrsta komunikacije (jedan-jednome, jedan-mnogima, mnogi-mnogima).

Korisnici: Ovu analogiju koriste oni koji žele da uvedu strožu kontrolu sadržaja internetu. Po njihovom mišljenju, zahvaljujući moći koju ima kao sredstvo masovnog medija slično televiziji, internet treba da bude pod strogom kontrolom. Američka vlada je pokušala da iskoristi ovu analogiju u sporu Rino protiv ACLU. Ovaj spor je pokrenut na osnovu Zakona o pristojnosti komunikacija donetog u Kongresu, koji predviđa strogu kontrolu radi sprečavanja izlaganja dece pornografskim sadržajima preko interneta. Sud je odbio da prizna analogiju s televizijom.

Internet – biblioteka

Sličnosti: Internet se ponekad sagledava kao ogromno skladište informacija, pa se za njegov opis često koristi termin ‘biblioteka’: na primer, ‘velika digitalna biblioteka', ‘sajber-biblioteka', ‘Aleksandrijska biblioteka XXI veka', itd.

Razlike: Skladištenje informacija i podataka predstavlja samo jedan aspekt interneta, a između biblioteka i interneta postoje znatne razlike:

- Tradicionalne biblioteke imaju za cilj da služe pojedincima koji žive u naročitom mestu (grad, zemlja, itd), dok je internet globalan.
- Knjige, članci i novine objavljuju se s namerom da obezbede kvalitet (urednici). Internet nema uvek urednike.
- Biblioteke se organizuju prema specifičnim klasifikacionim shemama, omogućujući korisnicima da svrstaju knjige u svojim kolekcijama. Ne postoji takva klasifikaciona shema za informacije na internetu.

- Osim opisa ključnih reči, sadržaj biblioteke (tekst u knjigama i člancima) nije dostupan sve dok korisnik ne posudi naročitu knjigu ili novine. Sadržaj interneta automatski je dostupan preko pretraživača.

Korisnici: Ovu analogiju koriste razni projekti čiji je cilj stvaranje sveobuhvatnog sistema informacija i znanja po naročitim pitanjima (portali, baze podataka, itd). U poslednje vreme, analogija sa bibliotekom koristi se u kontekstu Guglovog projekta čiji je cilj digitalizacija i štampanje knjiga.

Internet – video rikorder (VCR), fotokopirni aparat

Sličnosti: Ova analogija koncentriše se na reprodukciju i širenje sadržaja (npr. tekstova i knjiga). Kompjuteri su pojednostavili reprodukciju postupkom 'iskopiraj & prelepi'. To je u velikoj meri pojednostavilo širenje informacija preko interneta.

Razlike: Kompjuter ima mnogo širu funkciju nego što je kopiranje građe, iako je samo kopiranje mnogo jednostavnije na internetu nego video rikorderom ili fotokopirnim aparatom.

Korisnici: Ova analogija je korišćena u kontekstu američkog Zakona o digitalnim autorskim pravima, koji kažnjava institucije koje doprinose kršenju autorskih prava (razvijanje softvera za narušavanje zaštite autorskih prava, itd). Kontraargument u takvim slučajevima bio je da stvaraoci softvera, kao što su proizvođači kompjutera i fotokopirnih aparata, ne mogu da predvide da li će njihovi proizvodi biti ilegalno korišćeni.

Autoputevi i internet

Hamadun Ture, generalni sekretar ITU, koristio je analogiju između autoputeva i interneta upoređujući autoputve sa telekomunikacijama i internetski saobraćaj s kamionima ili automobilima: *Davao sam jednostavan primer, upoređujući internet i telekomunikacije s kamionima ili automobilima i autoputevima. To što ste vlasnik autoputeva ne znači da ćete biti vlasnik svih kamiona ili automobila koji njima putuju, a svakako ne robe koju oni prevoze, ili obrnuto. Reč je o jednostavnoj analogiji. Međutim, da biste lagano upravljali svojim saobraćajem, potrebno je da znate, prilikom izgradnje puteva, težinu, visinu i brzinu kamiona, tako da shodno tome izgradite mostove. Inače, sistem neće funkcionisati. Tako meni izgleda odnos između interneta i sveta telekomunikacija. A oni su osuđeni da rade zajedno.*[14]

Ova analogija korišćena je u sporovima protiv proizvođača softvera tipa Napster za međukorisničko deljenje fajlova (P2P), kao što su Grokster i StrimKast.

Internet – autoput

Sličnosti: Ova analogija povezane je s američkom opčinjenošću otkrivanjem novih prostora. Železnižke pruge i autoputevi obično su deo tog procesa. Internet, u virtuelnom svetu, metaforički odgovara autoputevima u stvarnom svetu.

Razlike: Pored transportnog aspekta interneta, ne postoje nikakve druge sličnosti između interneta i autoputeva. Internet prenosi neopipljivu građu (podatke), dok autoputevi olakšavaju prevoz robe i ljudi.

Korisnici: Analogija s autoputevima mnogo je korišćena sredinom devedesetih godina, pošto je Al Gor navodno izmislio termin 'informatički superautoput'. Termin 'autoput' koristila je i nemačka vlada da bi opravdala uvođenje strožeg zakona o kontroli sadržaja interneta u junu mesecu 1997:

> *Ovo je liberalni zakon koji nema nikakve veze sa cenzurom, ali koji jasno postavlja uslove za ono šta provajder može i šta ne može da radi. Internet je sredstvo prenošenja i širenja znanja. . . baš kao kod autoputeva, treba da postoje smernice za obe vrste saobraćaja.*[15]

Internet – otvoreno more

Sličnosti: U početku, ova analogija podsticana je činjenicom da, poput otvorenog mora, internet takođe deluje kao prostor van bilo koje nacionalne jurisdikcije. Danas je jasno da se najveći deo interneta nalazi unutar nekog nacionalnog pravosuđa. Tehnička infrastruktura kojom se kanališe internetski saobraćaj vlasništvo je privatnih ili državnih kompanija, naročito telekomunikacionih operatera. Najbliža analogija internetu bili bi transportni kontejneri neke brodske kompanije.

Razlike: Morski prevoz reguliše se širokim spektrom međunarodnih konvencija, počev od Konvencije o zakonu o moru, i granajući se u brojne konvencije Međunarodne pomorske organizacije koje se odnose na pitanja kao što su bezbednost ili zaštita okoline. Ove konvencije regulišu aktivnosti van nacionalog pravosuđa, kao što su one na otvorenom moru. Ne postoji ništa analogno tome u oblasti internet telekomunikacija.

Korisnici: Ovu analogiju koriste oni koji se zalažu za međunarodno regulisanje interneta. Govoreći konkretno, ova analogija sugeriše korišćenje starog koncepta iz rimskog prava *res communis onmium* (tj. prostor kao zajedničko nasleđe čovečanstva koje treba da regulišu i koriste sve države) na internetu kao što se isti koristi za regulisanje otvorenog mora.

Klasifikacija pitanja upravljanja internetom

Upravljanje internetom je kompleksna nova oblast koja zahteva početno pojmovno određivanje i klasifikaciju. Njegova kompleksnost povezana je s njegovom multidisciplinarnom prirodom, koja obuhvata mnoštvo aspekata, uključujući tehnologiju, socio-ekonomiju, razvoj, pravo i politiku.

Praktična potreba za klasifikacijom jasno je pokazana u toku WSIS-a. U prvoj fazi, za vreme uvoda u Ženevski samit (2003), mnogi igrači, uključujući države, imali su poteškoća da shvate složenost upravljanja internetom. Pojmovno određivanje, koje je dato u naučnim prilozima i u Izveštaju WGIG-a, doprinelo je efikasnijim pregovorima u kontekstu procesa WSIS-a. Izveštaj WGIG-a (2004) identifikovao je četiri glavne oblasti:

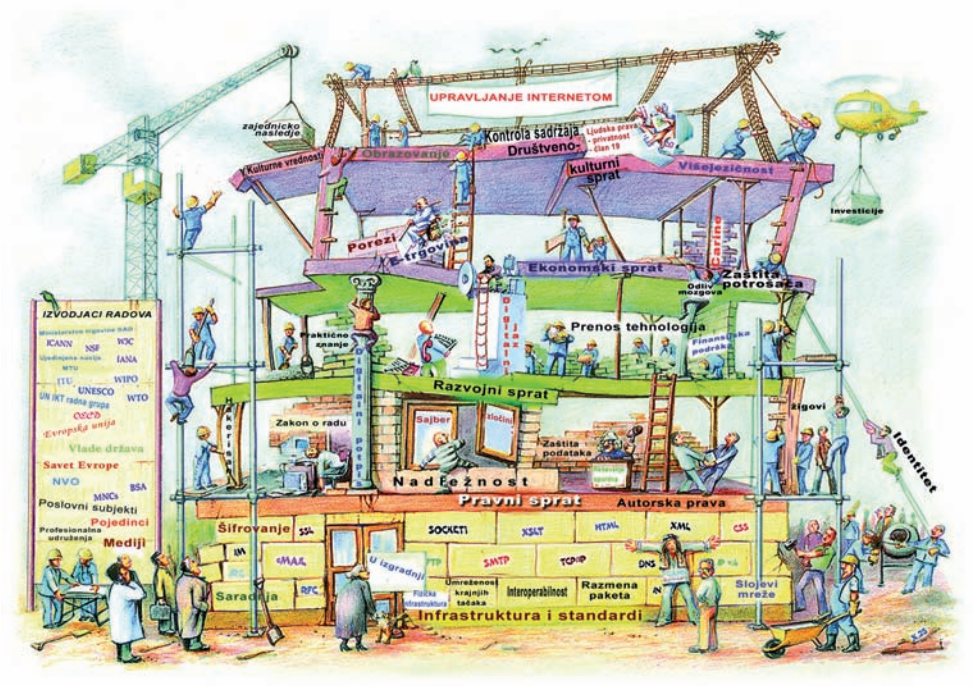
1. Pitanja koja se odnose na infrastrukturu i rukovođenje kritičnim resursima interneta.
2. Pitanja koja se odnose na korišćenje interneta, uključujući spem poruke, mrežnu bezbednost i sajber-kriminal.
3. Pitanja relevantna za internet, čiji je uticaj mnogo širi od interneta i za koja su odgovorne postojeće organizacije, kao što su prava na intelektualnu svojinu ili međunarodna trgovina.
4. Pitanja koja se odnose na razvojni aspekt upravljanja internetom, posebno na podizanje kapaciteta i zemljama u razvoju.

Dnevni red prvog IGF-a održanog u Atini (2006) sačinjen je oko sledećih tematskih oblasti:

1. Pristup
2. Bezbednost
3. Otvorenost
4. Raznovrsnost

Na drugom IGF-u u Rio de Žaneiru (2007), dnevnom redu je dodata peta tematska oblast.

5. Rukovođenje kritičnim internet resursima



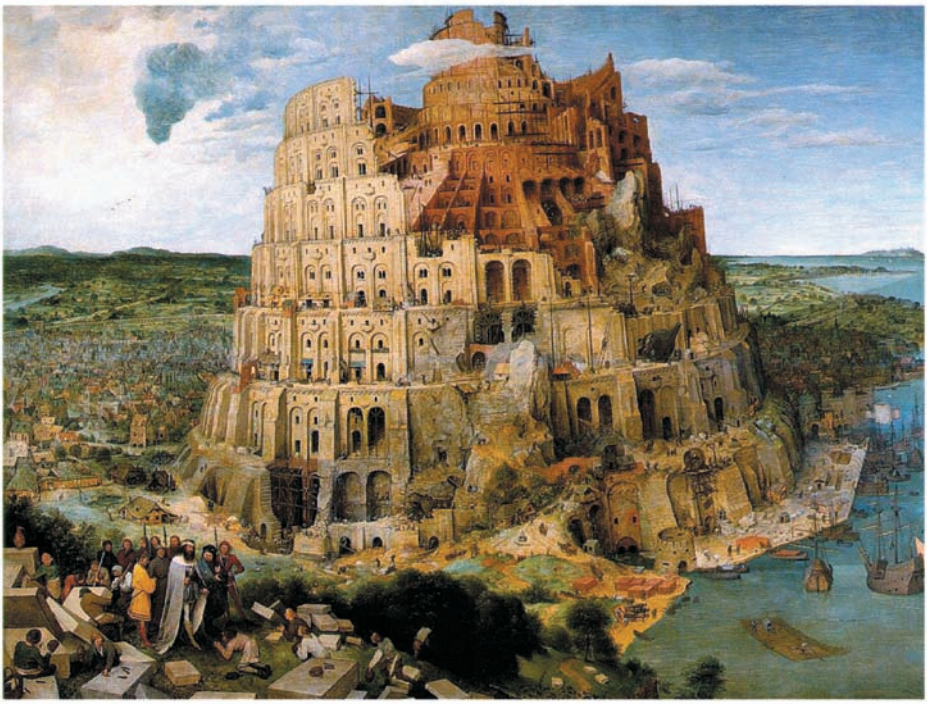
Iako se klasifikacija menja, upravljanje internetom bavi se, manje-više, istim nizom od 40 do 50 specifičnih pitanja, pri čemu se značaj naročitih pitanja menja. Na primer, dok se spem naročito isticao u klasifikaciji 2004. godine, njegov politički značaj splasnuo je na sastancima IGF-a, gde je postao jedna od beznačajnijih tema u okviru bezbednosne tematske oblasti.

Klasifikacija upravljanja internetom DiploFondacije grupiše glavnih 40–50 pitanja u sledećih pet korpi:[16]

1. Infrastrukturna i standardizaciona
2. Pravna
3. Ekonomska
4. Razvojna
5. Društveno-kulturna

Ova klasifikacija odražava i gorepomenute (WGIG, IGF) pristupe i naučna istraživanja u ovoj oblasti. Sama klasifikacija se se razvija od 1997, sa stalnim prilagođavanjima zasnovanim na povratnoj informaciji dobijenoj od studenata (850 diplomiranih zaključno sa 2010. godinom), na rezultatima istraživanja i uvidima iz političkog procesa.

Ova klasifikacija upravljanja internetom pomoću pet korpi metaforički je predstavljena slikom zgrade u izgradnji (videti gore) koju su sačinili istraživači DiploFondacije.



Zgrada u izgradnji: Gradimo li Vavilonsku kulu XXI veka?

Slika Pitera Brojgela Starijeg (1563), izložena u Muzeju istorije umetnosti u Beču, pokazuje izgradnju Vavilonske kule (videti gore). Jedna druga, manja slika, iz iste godine i na istu temu, nalazi se u Muzeju Bojmans van Bojningen u Roterdamu. Biblijska *Knjiga postanja* (11.7) govori o gradnji Vavilonske kule:

> *Hajde da siđemo, i da im pometemo jezik da ne razumiju jedan drugoga šta govore.*

Analogija gradnje Vavilonske kule deluje prikladno kada se posmatraju izazovi koje postavlja internet i navodi nas na razmišljanje o drugoj zgradi u izgradnji – čiji cilj nije da dosegne nebo nego da barem stigne do svakoga na planeti. DiploFondacija je sačinila okvir za raspravu o upravljanju internetom, koji je ilustrovan na prethodnoj stranici. O svakom spratu ove zgrade govori se u delovima knjige koji slede. Važno je shvatiti da su svi spratovi povezani, i da se gradnja nastavlja u nedogled.

Fusnote

1 Rezolucija Generalne skupštine UN 56/183 (od 21. decembra 2001) podržala je održavanje Svestkog samita o informacionom društvu (WSIS) u dve faze. Prva faza se odigrala u Ženevi od 10. do 12. decembra 2003, a druga u Tunisu, od 16. do18. novembra 2005. Cilj prve faze bio je da se dođe do razvijanja i podsticanja jasne izjave o političkoj volji i do preduzimanja konkretnih poteza za postavljanje temelja informatičkog društva za sve, odražavajući sve različite interese koji su u pitanju
(Izvor: **http://www.itu.int/wsis/basic/about.html**)

2 Definicija WGIG-a sledi obrazac često korišćenih definicija u teoriji režima. Osnivač teorije režima, Stiven D. Krasner, piše: *Režimi se mogu definisati kao nizovi implicitnih i eksplicitnih principa, normi, pravila i postupaka donošenja odluka, oko kojih se očekivanja aktera stapaju u datom području međunarodnih odnosa. Principi su uverenja u činjenice, uzroke i ispravnost. Norme su standardi ponašanja određeni u smislu prava i obaveza. Pravila su specifični recepti ili zabrane akcija. Postupci donošenja odluka predstavljaju preovlađujuću praksu za vršenje i primenu kolektivnog izbora. Krasner S (1983), Uvod, International regimes.* Krasner, SD (ur), Cornell University Press: Ithaca, NY, USA.

3 Shannon V (2006) What's in an 'i? (Šta se nalazi u jednom 'i'?) *International Herald Tribune*, 3. decembar 2006. Dostupno na:
http://www.iht.com/articles/2006/12/03/technology/btitu.php

4 Terminološka zbrka bila je pojačana načinom na koji su termin 'upravljanje' koristile neke međunarodne organizacije. Na primer, termin 'dobro upravljanje', Svetska banka koristi da bi promovisala reformu država uvođenjem više transparentnosti, smanjenjem korupcije i povećanjem efikasnosti administracije. U tom kontekstu, termin 'upravljanje' nalazi se u direktnoj vezi sa suštinskim funkcijama vlade.

5 Barlow JP (1996) *A Declaration of the independence of cyberspace (Deklaracija o nezavisnosti sajber-prostora)*. Dostupno na: **http://projects.eff.org/~barlow/Declaration-Final.htlm**

6 Za evoluciju upotrebe reči 'internet' prilikom pripremanja Ženevskog samita, videti: DiploFoundation (2003) *The Emerging Language of ICT Diplomacy – Key Words*. Dostupno na: **http://www.diplomacy.edu/IS/Language/htlm/words.htm**

7 Juna 2010, ICANN je odobrio ime domena .xxx top level za građu za odrasle.

8 Mrežna neutralnost je princip namenjen pristupnim mrežama korisnika koje učestvuju u internetu koji se zalaže za ukidanje svih ograničenja od strane internet provajdera i vlada u vezi sa sadržajem, sajtovima, platformama, sa vrstama opreme koja se može pridodati, kao i za ukidanje ograničenja u vezi sa dozvoljenim modusima komunikacije. Ovaj princip utvrđuje da ukoliko dati korisnik plaća za izvestan nivo pristupa internetu, a drugi korisnik plaća za isti nivo pristupa, onda toj dvojici korisnika treba omogućiti da se međusobno povežu na pretplaćenom nivou pristupa (Izvor: Vikipedija).

9 Dostupno na: **http://www.state.gov/secretary/rm/2010/01/135519.htm**

10 Ovaj deo ne bi bio završen bez razgovora sa Aldom Mateučijem, višim naučnim saradnikom DiploFondacije, čiji 'oprečni' stavovi o savremenim pitanjima upravljanja predsatavljaju stalnu proveru realnosti u nastavnim i istraživačkim aktivnostima DiploFondacije.

11 Barlow (1996), *nav. delo*.

12 WSIS proces započeo je prvim pripremnim sastankom održanim jula meseca 2002. u Ženevi. Prvi samit održan je u Ženevi (decembra 2003), a drugi samit u Tunisu (novembra 2003).

13 Folker Kic daje argument za analogiju između upravljanja sistemima telefonije i internetskim imenima i brojevima. Kitz F (2004) *ICANN je možda jedina igra u gradu, ali Marina del Rej nije jedini grad na svetu: Some thoughts on the so-called 'uniqueness' of the Internet*. Dostupno na: **http://smu.edu/stlr/articles/2004/Winter/Kitz.pdf**

14 Odlomci iz govora generalnog sekretara održanog na zasedanju ICANN-a u Kairu (6. novembar 2008). Dostupno na: **https://cai.icann.org/files/meetings/cairo2008/toure-speeche-06nov08.txt**

15 Navedeno u Mock K, Armony L (1998) *Hate on the Internet*. Dostupno na: **http://www.media-awareness.ca/english/resources/articles/online_hate/hate_on_internet.cfm**

16 termin 'korpa' uveden je u diplomatsku praksu za vreme pregovora Organizacije o evropskoj bezbednosti i saradnji (OEBS)

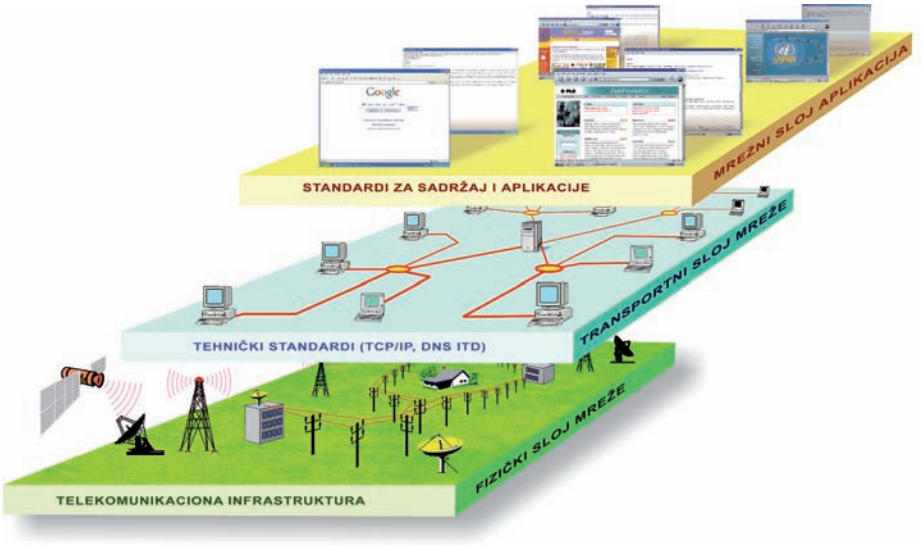
Drugi deo

Infrastrukturna i standardizaciona korpa

Infrastrukturna i standardizaciona korpa

Infrastrukturna i standardizaciona korpa uključuje osnovna, uglavnom tehnička pitanja koja se odnose na vođenje interneta. Glavni kriterijum za klasifikovanje nekog pitanja u ovoj korpi predstavlja njegov značaj za bazičnu funkcionalnost interneta. Ovde postoje dve grupe pitanja.

Prva grupa uključuje suštinska pitanja bez kojih internet i WWW ne bi mogli postojati.[2] Ova pitanja su grupisana u tri sloja:



1 Telekomunikaciona infrastruktura, kroz koju protiče sav internetski saobraćaj.
2 Internetski tehnički standardi i usluge, infrastruktura koja pokreće internet (npr. TCP/IP: kontrolni protokol prenosa/internet protokol; DNS: servisi imena domena; SSL: dodatni nivo zaštite).
3 SStandardi sadržaja i aplikacija (npr. HTML: hipertekstualni markirni jezik; XML).

Druga grupa sastoji se od pitanja koja se odnose na očuvanje bezbednog i stabilnog rada strukture interneta, a uključuje sajber-bezbednost, šifrovanje i spem.

Telekomunikaciona infrastruktura

Trenutna situacija

Internetski podaci mogu da putuju preko širokog dijapazona komunikacionih medija: telefonskim žicama, optičkim kablovima, satelitima, mikrotalasima i bežičnim vezama. Čak se i strujna mreža može koristiti za prenošenje internet sadržaja korišćenjem strujnih provodnika.[2]

Kako telekomunikacioni sloj prenosi internetski saobraćaj, svi novi propisi povezani s telekomunikacijama neminovno će se odražavati i na internet. Telekomunikacionu infrastrukturu reguliše i na državnom i na međunarodnom nivou mnoštvo javnih i privatnih organizacija. Glavne međunarodne organizacije uključene u regulisanje telekomunikacija uključuju Međunarodnu telekomunikacionu uniju (ITU), koja je donela razrađena pravila za pokrivanje odnosa između nacionalnih operatera, za dodelu radio spektra i za rukovođenje pozicioniranjem satelita, i Svetska trgovinska organizacija (STO), koja je odigrala ključnu ulogu u liberalizaciji telekomunikacionih tržišta širom sveta.[3]

Međunarodna regulativa ITU

Međunarodna regulativa ITU iz 1998. olakšala je međunarodnu liberalizaciju određivanja cena i usluga i omogućila je inovativnije korišćenje osnovnih servisa u oblasti interneta, kao što su međunarodne linije koje se daju na lizing. Ona je obezbedila jednu od infrastrukturnih baza za brz razvoj interneta devedesetih godina XX veka. đ

Uloge STO i ITU sasvim su različite. ITU postavlja detaljne tehničke standarde, donosi međunarodne propise specifične za telekomunikacije i pruža pomoć zemljama u razvoju. STO obezbeđuje okvir za opšta tržišna pravila.[4]

Liberalizacija nacionalnih telekomunikacionih tržišta omogućila je velikim telekomunikacionim kompanijama, kao što su AT&T, Kabl i Radio, Telekom Francuska, Sprint i SvetKom, da pokrivaju tržišta na globalnom planu. Kako se najveći deo internetskog saobraćaja prenosi preko telekomunikacionih infrastruktura ovih kompanija, one imaju značajan uticaj na razvoj interneta.

Pitanja

'Lokalna petlja' ili 'poslednja milja'

'Lokalna petlja' (ili 'poslednja milja') naziv je za vezu između internet servisnih provajdera (ISP-ova) i njihovih individualnih korisnika. Problemi s lokalnim petljama predstavljaju prepreku za raširenije korišćenje interneta u mnogim zemljama, uglavnom onima u razvoju. Bežična komunikacija je jedno moguće, jeftino rešenje za problem lokalne petlje. Osim sve dostupnije raspoloživosti tehnoloških opcija, rešenje problema lokalne petlje takođe zavisi od liberalizacije ovog segmenta telekomunikacionog tržišta.

Liberalizacija telekomunikacionih tržišta

Znatan broj zemalja liberalizovao je svoje telekomunikaciono tržište. Međutim, mnoge zemlje u razvoju suočene su s teškim izborom: da liberalizuju i učine telekomunikaciono tržište efikasnijim ili da sačuvaju važan budžetski prihod od postojećih telekomunikacionih monopola.[5] Strana pomoć, postepena tranzicija i povezivanje liberalizacionog procesa sa zaštitom javnog interesa, mogli bi biti putevi izlaska iz ove zavrzlame.

Uspostavljanje standarda tehničke infrastrukture

Tehničke standarde sve više određuju privatne i profesionalne institucije. Na primer, WiFi standard, IEEE 802.11b, razvio je Institut elektroinženjera i elektroničara. Sertifikate za kompatibilnu WiFi opremu izdaje WiFi alijansa. Sama funkcija postavljanja ili primenjivanja standarda na tako dinamičnom tržištu omogućuje ovim insititucijama značajan uticaj.

Protokol kontrole prenosa/Internet protokol (TCP/IP)

Tekuća situacija

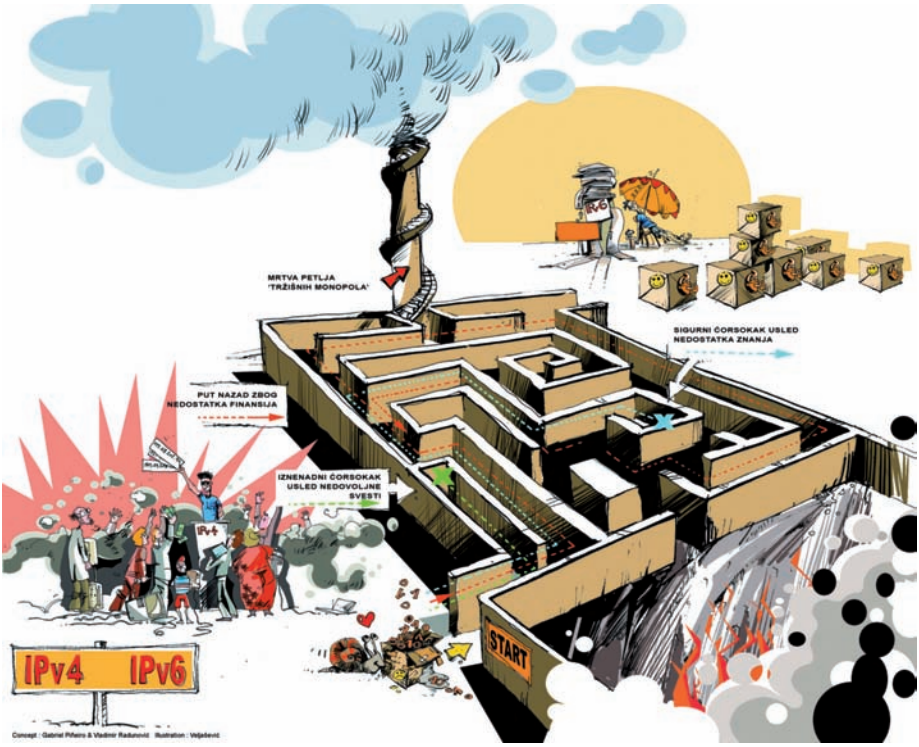
TCP/IP je glavni internetski tehnički standard, koji određuje kako se podaci kreću kroz internet; zasniva se na tri principa: usmeravanje paketa, celokupno umrežavanje i izdržljivost. Upravljanje internetom, budući da se odnosi na TCP/IP, ima dva važna aspekta: uvođenje novih standarda i raspodelu IP brojeva.

TCP/IP standarde postavlja Radna grupa za inženjering interneta (Internet Engineering Task Force – IETF). Obzirom na suštinski značaj ovih protokola za internet, IETF ih pažljivo čuva. Sve promene TCP/IP zahtevaju intenzivne prethodne rasprave i dokaz da predstavljaju efikasno rešenje (princip 'running code').

IP brojevi predstavljaju jedinstvene numeričke adrese koje moraju imati svi kompjuteri koji su povezani s internetom. Ne postoje dva kompjutera povezana s internetom sa istim IP brojem, što ih čini potencijalno oskudnim resursom. Sistem za raspodelu IP brojeva organizovan je hijerarhijski. Na vrhu se nalazi IANA (Internetska uprava za dodeljene brojeve – pomoćna ispostava ICANN-a – Internetske korporacije za dodeljena imena i brojeve), koja raspodeljuje blokove IP brojeva na pet regionalnih internet regisatara (RIR).[6] Regionalni registri dodeljuju IP brojeve lokalnim internetskim registrima (LIR) i nacionalnim internetskim registrima (NIR) koji sa svoje strane dodeljuju IP brojeve manjim internetskim provajderima, kompanijama i pojedincima koji se nalaze niže u skali.

Pitanja

Kako izaći na kraj sa ograničenjem IP brojeva (prelazak na Ipv6)
Sadašnji fond IP brojeva po IPv4 (Internetski protokol, verzija 4) sadrži oko četiri milijarde brojeva i mogao bi da se istroši tokom sledećih nekoliko godina uvođenjem naprava koje je omogućio internet, kao što su mobilni telefoni, mikrokompjuteri, konzole za igrice i kućni aparati. Zabrinutost da bi moglo da nestane IP brojeva i da tako dođe do sprečavanja daljeg razvoja interneta navela je tehničku zajednicu da preduzme sledeće velike akcije:



- Racionalizaciju korišćenja postojećeg fonda IP brojeva uvođenjem prevođenja mrežne adrese (NAT).
- Bavljenje algoritmima rasipne dodele adresa koje koriste RIR, uvođenjem besklasnog međudomenskog usmeravanja (CIDR).
- Uvođenje nove verzije TCP/IP – IPv6 – koja omogućuje mnogo veći fond IP brojeva (340 000 000 000 000 000 000).

Odgovor internetske tehničke zajednice na problem moguće nestašice IP brojeva predstavlja primer efikasnog i aktivnog menadžmenta. Iako su i NAT i CIDR obezbedili brzo rešavanje problema, pravo dugoročno rešenje predstavlja IPv6. Iako je IPv6 uveden još 1996, njegovo ugrađivanje teče veoma sporo. Kako se približava iscrpljivanje fonda IPv4 brojeva, ovo sporo instaliranje poprima elemente krize u nastajanju.

Jedan od glavnih izazova s kojima se suočava uvođenje IPv6 jeste nedostatak povratne kompatibilnosti između IPv6 i IPv4. Mreže koje koriste IPv6 ne mogu komunicirati direktno sa onima, još uvek dominantnim, koje koriste IPv4. Kako je vrlo verovatno da će mreže koje koriste IPv4 i IPv6 koegzistirati u narednom periodu, važno je obezbediti da nove mreže – zasnovane na IPv6 – ne ostanu ostrva. Tehničko rešenje podrazumevaće specijalno 'tunelisanje' između ova dva tipa mreža, što će uzrokovati složenije usmeravanje na internetu i još nekoliko 'kolateralnih problema'.

Instaliranje je takođe odloženo slabom zainteresovanošću ISP-ova i korisnika. Iako su svesni opasnosti nestanka IP brojeva, draža im je taktika čekanja. Na primer, nedavna anketa u Japanu pokazala je da je preko 70% ISP-ova svesno opasnosti nestanka IPv4, a samo se njih 30% priprema za prelazak na IPv6. U takvoj situaciji, kada tržišna motivacija ne može da obezbedi rešenje, postoji sve veći pritisak na vlade i druge javne vlasti da odigraju istaknutiju ulogu u promovisanju prelaska na IPv6 preko povećane svesti o opasnostima gašenja IPv4, davanjem finansijske podrške prelasku na IPv6 i korišćenjem IPv6 za vladine mreže.

S obzirom na kompleksnost prelaska na IPv6, zemlje u razvoju, uglavnom u Africi, mogu profitirati iz odloženog početka i mogućnosti uvođenja mreža zasnovanih na IPv6 od samog početka. U ovom procesu, zemljama u razvoju biće potrebna tehnička pomoć.[7]

Pored problema prelaska, politički okvir za distribuciju IPv6 zahtevaće pravilnu raspodelu IP brojeva, nalažući uvođenje otvorenih i konkurentnih mehanizama za izlazak u susret potrebama krajnjih korisnika na najoptimalniji način.

Promene kod TCP/IP i sajber-bezbednost

Bezbednost nije bila važno pitanje za osnivače interneta, jer se u to vreme on sastojao od zatvorene mreže istraživačkih institucija. Ekspanzijom interneta na 2 milijarde korisnika i njegovim sve većim značajem u smislu komercijalnog sredstva, pitanje bezbednosti našlo se visoko na listi pitanja upravljanja internetom.

Kako arhitektura interneta nije sačinjena imajući bezbednost u vidu, stvaranje suštinske sajber-bezbednosti zahtevaće bitne promene kod same baze interneta: TCP/IP. Novi IPv6 protokol daje neka poboljšanja bezbednosti, ali još uvek ne nudi obuhvatno rešenje. Takva zaštita zahtevaće znatne modifikacije TCP/IP.[8]

Promene kod TCP/IP i problem ograničenog propusnog opsega

Da bi se olakšalo dostavljanje multimedijalnog sadržaja (npr. internetske telefonije, videa po zahtevu) potrebno je obezbediti kvalitet usluge (QoS) koji će garantovati minimalni nivo izvršenja. QoS je naročito značajan kod aplikacija osetljivih na odlaganje, kao što je prenos događaja uživo, i često ga je teško postići zbog ograničenja propusnog opsega. Uvođenje QoS može zahtevati promene kod IP, uključujući moguće iskušenje za princip mrežne neutralnosti.

Tehnologija, standardi i politika

Rasprava o mrežnim protokolima pokazuje kako standardi mogu biti politika vođena drugim sredstvima. Dok se druge intervencije vlade u privredi i tehnologiji (kao što su propisi o bezbednosti i antimonopolske aktivnosti) odmah posmatraju kao političke i društvene, tehnički standardi se obično poimaju kao društveno neutralni i zato kao istorijski nezanimljivi. Međutim, tehničke odluke mogu imati dalekosežne ekonomske i društvene posledice, menjajući ravnotežu snaga između konkurentskih kompanija ili država i ograničavajući slobodu korisnika. Napori da se stvore formalni standardi uvode privatne tehničke odluke graditelja sistema u javnu oblast; na taj način, bitke za standard mogu da izvedu na svetlo dana neizrečene pretpostavke i sukobe interesa. Sama strast kojom jaz osporavaju odluke o standardima morala bi da nas upozori na dublje značenje koje leži ispod važnih praktičnih detalja.[9]

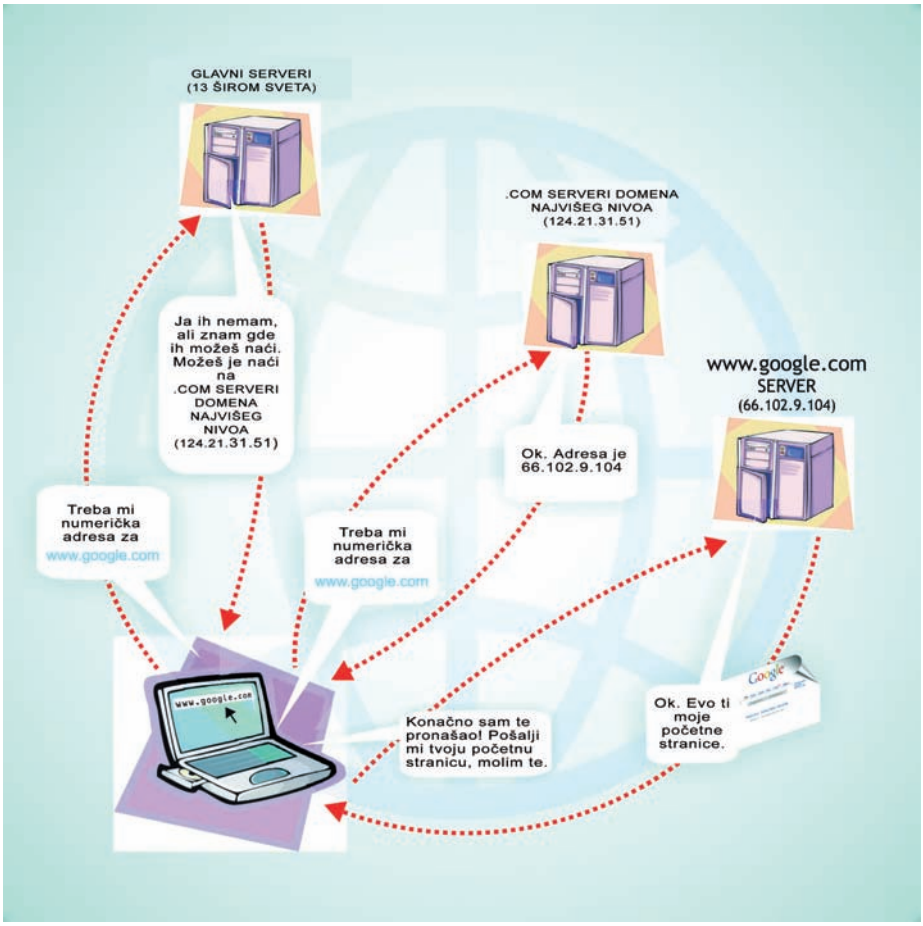
Sistem imena domena (DNS)

Trenutna situacija

DNS se bavi internetskim adresama (kao što je **www.google.com**) i pretvara ih u IP brojeve (pojednostavljena shema ovog procesa predstavljena je grafički na drugoj strani). DNS se sastoji od osnovnih servera, servera domena najvišeg nivoa (TLD) i velikog broja DNS servera koji se nalaze širom sveta. Upravljanje DNS-om predstavlja teško pitanje u raspravi o upravljanju internetom. Jedna od glavnih kontroverzi podrazumeva krajnju vlast Vlade SAD (preko Ministarstva trgovine) nad glavnim serverima, vrhunskim nizom hijerarhijski organizovanog DNS-a. Ovo dodatno otežava činjenica da je 10 od 13 postojećih glavnih servera smešteno u Sjedinjenim Državama (sa još tri u Evropi i Aziji). U cilju bavljenja ovim problemom i povećanja dijapazona sistema osnovnih servera, razvijen je program 'Enikast', koji sada ima oko sto servera širom sveta na svim kontinentima.

DNS uključuje tri vrste domena najvišeg nivoa: generički (opšti) (gTLD), državnog koda (ccTLD) i sponzorisani (sTLD). gTLD-ovi uključuju domene koje bi mogao dobiti ko god želi (.com, .info, .net and .org). sTLD-ovi su ograničeni na specifičnu grupu. Na primer, sTLD '.aero' je otvoren za registraciju samo za avionsku industriju. ccTLD-ovi su ograničeni na naročitu zemlju (.uk, .cn, .in).

Za svaki gTLD postoji jedan registar koji sadrži spisak adresa. Na primer, .com gTLD nalazi se pod upravom VeriSign-a. Funkciju 'pro-



davca' vrše administratori. ICANN obezbeđuje ukupnu koordinaciju DNS-a zaključivanjem ugovora i akreditovanjem registara i administratora. On takođe određuje cene na veliko po kojima registar (VeriSign) 'iznajmljuje' imena domena administratorima i postavlja određene uslove u vezi sa uslugama koje pružaju registri i administratori. To znači da ICANN deluje kao ekonomski i pravni regulator poslova u vezi s imenom domena za gTLD.

Važan deo rukovođenja DNS-om predstavlja zaštita zaštitnih znakova i rešavanje sporova. Princip 'prvi došao – prvi uslužen' kod dodele imena domena u prvim danima interneta izazvao je pojavu poznatu kao 'sajber-skvotovanje', praksu registrovanja imena domena koja su kasnije mogla da se preprodaju. Jedinstvena politika rešavanja sporova u vezi sa imenima domena (UDRP) koju su uspostavili ICANN i Svetska organizacija za intelektualnu svojinu (WIPO) imala je za cilj smanjenje sajber-svotovanja.

Drugi važan element kod razmatranja tekuće organizacije upravljanja DNS-om predstavlja upravljanje ccTLD-ovima. Trenutno, nekim državnim kodovima još rukovode razne institucije ili pojedinci koji su dobili akreditaciju u prvim danima interneta, kada neke vlade nisu uopšte bile zainteresovane za takve stvari.

Pitanja

Stvaranje novih generičkih imena domena

U tehničkom smislu, stvaranje novih TLD-ova je gotovo neograničen. Međutim, uvođenje novih gTLD-ova išlo je veoma sporo, pri čemu su neki novi gTLD-ovi uvedeni tek nedavno. Trenutno je aktivno 20 gTLD-ova, a još tri nalaze se u razmatranju.[10] Glavni otpor stvaranju novih gTLD-ova dolazi od lobija zaštitnih znakova, koji se plaši da bi povećanje broja domena otežalo zaštitu njihovih zaštitnih znakova i povećalo sajber-skvotovanje.

Pod pritiskom za uvođenje novih gTLD, ICANN je otpočeo konsultacije radi osmišljavanja nove politike u ovoj oblasti koja bi se, između ostalog, bavila rešavanjem konkurentskih zahteva za gTLD-ove, opasnošću od sajber-skvotovanja, pitanjima javnog morala, taksama za registraciju, itd.

Generička imena domena vezana za sadržaj

Drugo pitanje politike ICANN-a vezano je za donošenje odluke o stvaranju novih domena, koji bi mogli podrazumevati povezivanje imena domena sa sadržajem.[11] Najilustrativnija situacija jeste predlog da se uvede .xxx domen za sadržaj za odrasle. Upravni odbor ICANN-a odbacio je ovaj predlog u martu 2007. Glavna kritika ove odluke bila je da je to ICANN uradio pod pritiskom Vlade SAD, koja se snažno suprotstavljala tom uvođenju.[12] Zanimljivo je da su mnoge vlade podržale Vladu SAD, uključujući i one koje su obično kritički raspoložene prema poziciji SAD u upravljanju internetom, kao što su Brazil i Kina. Ovo pitanje je ponovo pokrenuto u junu 2010, na zasedanju ICANN-a u Briselu, gde je Upravni odbor ICANN-a pozitivno razmotrio aplikaciju za .xxx domen i započeo pregovore o njegovom uvođenju. Ova odluka je takođe obnovila raspravu o ulozi ICANN-a u stvarima javne politike.

Generička imena domena za kulturne i jezičke zajednice

Godine 2003, ICANN je uveo novi .cat domen za katalonski jezik. Ovo je prvi domen uveden za neki jezik.([13] Španska vlada nije se protivila ovoj odluci.

U vreme kada je uveden, izazvao je mnoga strahovanja da bi mogao da se koristi kao presedan za druge jezike, ili još kontroverznije, za jezičke i kulturne zajednice koje možda imaju ambicija da stvaraju države. Iz retrospektive zapažamo da se to nije dogodilo.

Rukovođenje državnim domenima

Rukovođenje ccTLD-ovima podrazumeva tri važne stvari. Prva se tiče, politički često kontroverzne odluke u vezi s tim koje državne kodove treba registrovati kada su u pitanju zemlje i entiteti s nejasnim ili spornim međunarodnim statusom (npr. zemlje koje su tek stekle nezavisnost i pokreti otpora). Jedno kontroverzno pitanje bilo je dodeljivanje imena domena palestinskim vlastima. Prilikom obrazlaganja odluke da se dodeli .ps TLD, IANA je ponovila princip dodele imena domena u skladu sa standardom ISO 3166, kao što je predložio Džon Postel, jedan od osnivača interneta.[14]

Druga stvar odnosi se na to ko treba da rukovodi ccTLD-ovima. Mnoge zemlje pokušavaju da preuzmu kontrolu nad svojim domenima, koji se smatraju nacionalnim resursom. Nacionalne vlade se opredeljuju za veoma različite političke pristupe.[15] Prenos ('redelegiranje') na novu instituciju koja će rukovoditi ccTLD-om ('delegant') ICANN odobrava jedino ako postoji konsenzus svih zainteresovanih aktera unutar zemlje. Obzirom na važnost ovog pitanja i na veliku raznovrsnost pristupa, postojale su dve značajne inicijative na međunarodnom nivou da se uvede izvestan nivo harmonizacije. Prva se zvala GAC principi, a usvojio ju je Državni savetodavni komitet ICANN-a, koji je predložio politiku i odredio postupke za redelegiranje uprave ccTLD-a.[16] Druga je bila Najbolja praksa, koju je predložila Svetska zajednica domena najvišeg nivoa (jun 2001).

Treća stvar odnosi se na neraspoloženje mnogih operatera državnih domena da postanu deo sistema ICANN-a. Do sada, ICANN nije uspeo da okupi operatere državnih domena pod svoj kišobran. Operateri državnih domena organizovani su na regionalnom nivou (Evropa – CENTR, Afrika – AFTLD, Severna Amerika – NATLD, i Južna Amerika – LACTLD). Na globalnom nivou, glavni forum je Svetska zajednica domena najvišeg nivoa. ICANN radi na Okvirima odgovornosti kao manje formalnom načinu razvijanja veza sa operaterima državnih domena.

Internacionalizovana imena domena

Internet je u početku bio prvenstveno medij na engleskom jeziku. Zahvaljujući brzom razvoju, postao je sredstvo globalne komunikacije sa sve većim brojem korisnika koji ne govore engleski. Dugo vremena,

nedostatak multijezičkih karakteristika u infrastrukturi interneta bio je jedan od glavnih ograničavajućih faktora za budući razvoj.

U maju 2010, posle dugog perioda testiranja i političkih neizvesnosti, ICANN je započeo odobravanje novih imena domena na mnogo različitih pisama, uključujući kinesko, arapsko i ćirilično. Uvođenje internacionalizovanih imena domena (IDN-ova) smatra se jednim od glavnih uspeha režima upravljanja internetom.

Glavni serveri

Na vrhu hijerarhijske strukture DNS-a, glavni serveri privlače veliku pažnju. Oni su deo većine praktičnih i akademskih rasprava o pitanjima upravljanja internetom.

Trenutna situacija

Funkcija čvrstine DNS-a može se ilustrovati analizom zabrinutosti da bi se internet raspao ako bi se onesposobili glavni serveri. Prvo, postoji 13 glavnih servera raspoređenih po svetu (10 u SAD i po jedan u Švedskoj, Holandiji i Japanu; od njih 10 u SAD, nekoliko se nalazi pod upravom agencija američke vlade), što je tehnički maksimalno moguć broj. Ako bi propao jedan server, preostalih 12 bi nastavilo da funkcioniše. Čak i ako bi svih 13 servera propalo istovremeno, razrešenje imena domena (glavna funkcija glavnih servera) nastavilo bi se na drugim serverima imena domena, koji su hijerarhijski raspoređeni po celom internetu.[17]

Zbog toga na hiljade servera imena domena sadrži kopije glavnog zonskog fajla, pa do neposredne i katastrofalne propasti interneta ne bi moglo da dođe. Potrajalo bi malo duže pre nego što bi bile primećene bilo kakve ozbiljne funkcionalne posledice, a za to vreme bi bilo moguće reaktivirati originalne servere ili stvoriti nove.

Osim toga, sistem glavnih servera je znatno ojačan planom Enikast, koji izrađuje kopije glavnih servera po celom svetu. Ovo pruža mnoge prednosti, uključujući čvrstinu kod DNS-a i bržu raspodelu internet adresa (sa planom Enikast, dodatni serveri su bliže krajnjim korisnicima).

Sa 13 glavnih servera rukovodi više raznih organizacija: akademske/državne institucije, kompanije i vladine institucije. Institucije koje rukovode glavnim serverima primaju fajl sa osnovnim internet adresama za smeštanje u zonu glavnih servera koji predlaže IANA (ICANN), a odobrava Vlada SAD (Ministarstvo trgovine). Kada Ministarstvo trgovine jednom odobri sadržaj, on se ubacuje u glavni server kojim upravlja VeriSign po ugovoru s Ministarstvom.

Fajl u ovom serveru automatski se presnimava u svim drugim glavnim serverima. Tako je teorijski moguće da Vlada SAD uvede jednostrane promene u ceo DNS. Ovo je izvor zabrinutosti mnogih vlada.

Pitanja

Internacionalizacija kontrole glavnih servera

Mnoge zemlje izražavaju zabrinutost zbog važećeg aranžmana po kojem krajnje donošenje odluka u vezi sa sadržajem glavnih servera ostaje odgovornost jedne zemlje (Sjedinjenih Država). Postojali su različiti predlozi u procesu upravljanja internetom, uključujući usvajanje Glavne konvencije, koja bi zadužila međunarodnu zajednicu za politiku nadgledanja glavnih servera, ili barem garantovala državama prava nad sopstvenim imenima domena. Nove mogućnosti su otvorene Izjavom o obavezama,[18] koja se bavi pitanjem institucionalne nezavisnosti ICANN-a od Ministarstva trgovine SAD, uključujući buduću internacionalizaciju ICANN-a. O aranžmanu IANA ponovo će se pregovarati tokom 2011. godine. Neki elementi rešenja u nastajanju sastojali bi se od dve faze:

1. Reforma ICANN-a, inicirana Izjava o obavezama, koja vodi ka stvaranju međunarodne organizacije *sui generis*, a koja bi bila prihvatljiv institucionalni okvir za sve zemlje.

2. Prenošenje kontrole nad glavnim serverima sa Ministarstva trgovine SAD na ICANN, kao što je prvobitno predviđeno.

Alternativni glavni serveri – mogućnosti i rizici

Stvaranje alternativnog glavnog servera tehnički je otvoreno. Glavno pitanje je koliko bi sledbenika imao alternativni server, ili još preciznije, koliko bi se kompjutera na internetu usmerilo prema njemu kada bi došlo do razrešenja imena domena. Bez korisnika, svaki alternativni DNS postaje beskoristan. Bilo je nekoliko pokušaja stvaranja alternativnog DNS-a: Open NIC, New.net i Name.space. Većina ih je bila neuspešna, odgovarajući samo za nekoliko procenata korisnika interneta.

Uloga SAD u rukovođenju glavnim serverima – paradoks vlasti

Od usvajanja Izjave o obavezama, pitanje vlasti SAD nad glavnim serverima moglo je postepeno postati istorijsko. Potencijalna moć skidanja neke zemlje sa interneta (brisanjem njenog imena domena) jedva da se može karakterisati kao moć, budući da nema nikakvu efektivnu upotrebu. Ključni element moći prisiljava drugu stranu da se ponaša na način koji želi držalac moći. Korišćenje vlasti SAD nad infrastrukturom interneta moglo bi stvoriti neplanirane posledice, uključujući i to da zemlje i regioni osnuju sopstvene internete. Kod takvog scenarija, internet bi mogao da se raspadne i da američki interesi budu ugroženi (prevlast američkih vrednosti na internetu, engleski kao jezik interneta i prevlast kompanija sa sedištem u SAD u oblasti elektronske trgovine). S obzirom na prve političke inicijative u upravljanju internetom (npr. Izjava o obavezama) čini se da je Obamina administracija svesna ovog paradoksa vlasti. To je dobar znak za budući razvoj globalnog režima upravljanja internetom.

Mrežna neutralnost[19]

Šta bi se desilo da je konkurencija ograničila pristup na Gugl u njegovim prvim danima? Ili da su operateri Telekoma usporili Skajpovo uvođenje internetske telefonije? Ili da je Vlada SAD imala internetski pristup neprijateljskim zemljama?[20] Najverovatnije bismo imali kompjutersku mrežu koja je nastavak logike iz osamdesetih godina sa, na primer, mrežnim protokolom X25 umesto TCP/IP, gde bi se podaci između nacionalnih kompjuterskih mreža razmenjivali na državnim granicama.

Uspeh interneta leži u njegovoj konstrukciji, koja se zasniva na principu mrežne neutralnosti. Sav prenos podataka na internetu u to vreme, bilo da su dolazili od početničkih ili velikih kompanija, vršen je bez diskriminacije. Novim kompanijama i inovatorima nije bila potrebna dozvola ili tržišna moć da bi uvodili inovacije u internet.

Značaj mrežne neutralnosti za uspeh interneta, do sada je bio ključ. Zbog toga je ova rasprava privukla veoma raznolike aktere: od predsednika Sjedinjenih Država do aktivista za ljudska prava. Mrežna neutralnost predstavlja jedan od najviših prioriteta tehnološkog programa predsednika Obame i o njoj se raspravlja u mnogim političkim telima, uključujući Kongres SAD. U samom početku, rasprave o mrežnoj neut -

ralnosti vodile su se na području Sjedinjenih Država, ali zahvaljujući novim tokovima, o mrežnoj neutralnosti se sve više razgovara širom sveta.

Zbog čega se sada toliko razgovara o mrežnoj neutralnosti?

Nema nikakve zavere. Internet je postao žrtva sopstvenog uspeha. Sa 2 milijarde korisnika i sve većim pomeranjem naše svakodnevne privredne i političke realnosti na internet, ulozi postaju veoma visoki. Internet ima veliki komercijalni i razvojni potencijal. Za neke od komercijalnih stvari, posebno za one koje se odnose na pružanje video i multimedijalnih usluga, mrežna neutralnost bi mogla značiti prepreku.

Trenutna situacija

Paradoksalno, mrežna neutralnost nije nikada strogo primenjena. Od prvih dana dial-up modemskih veza, postoji rivalstvo između raspoloživog prenosnog opsega i potreba korisnika. Da bi se bavili ovim izazovom i obezbedili kvalitetnu uslugu, internetski operateri koriste razne tehnike rukovanja mrežama da bi dali prednost nekom saobraćaju. Na primer, internetski saobraćaj koji prenosi razgovor preko Skajpa morao bi da ima prednost nad saobraćajem koji prenosi običnu elektronsku poštu: dok kod razgovora na Skajpu čujemo odlaganje, u razmeni i-mejlom nećemo primetiti mala odlaganja. Potreba za rukovođenjem mrežom naročito je važna danas, kada je povećana kvota korisnika mnogo traženih usluga kao što je skidanje, internetska telefonija, onlajn igrice, itd.

Sve veća tražnja propusnog opsega

Tokom 2009, kao ilustraciju sve veće tražnje propusnog opsega, gledaoci Ju tjuba pratili su 1.2 milijarde video snimaka dnevno,[21] i prenosili su skoro 20 časova video materijala u minuti![22]

Upravljanje mrežom postaje sve komplikovanije pri usmeravanju internetskog saobraćaja na najoptimalniji način u cilju pružanja kvalitetne usluge: sprečavanja zagušenostii eliminacije kašnjenja i nestabilnosti. Prvo nesalaganje u tumačenju principa mrežne neutralnosi fokusirase na to da li uopšte treba dozvoliti bilo kakvo upravljanje mrežom. Čistunci mrežne neutralnosti tvrde da su 'svi delovi stvoreni jednaki' i da internetski saobraćaj treba jednako tretirati. Telekomi i provajderi internet usluga osporavaju ovaj stav tvrdeći da korisnici moraju imati jednak pristup internetskim uslugama, pa ako to mora da se desi, onda internetski saobraćaj ne može da se tretira jednako. Ako se video i i-mejl saobraćaj tretiraju jednako, onda korisnici neće imati dobar video prijem, a ipak ne bi primetili nekoliko sekundi zakašnjenja kod prijema elektronske pošte. Čak i čistunci mrežne neutralnosti ne mogu da dovedu u

pitanje ovu argumentaciju. Oni se plaše da svaki kompromis o mrežnoj neutralnosti može da otvori Pandorinu kutiju, pokrećući pitanje razlikovanja između opravdanog upravljanja mrežom i moguće manipulacije.

Pitanja

U raspravi o mrežnoj neutralnosti, pojavljuje se konsenzus da postoji potreba za *celishodnim* upravljanjem mrežom. Glavno pitanje jeste kako tumačiti pridev 'celishodan'. Pored tehničkih problema, postoje još tri područja – ekonomska, pravna i pitanja ljudskih prava – gde je rasprava o upravljanju mrežom i mrežnoj neutralnosti naročito vrela.

Ekonomska pitanja

Tokom nekoliko proteklih decenija, mnogi značajni mrežni operateri – uključujući telekome i internetske provajdere – proširili su svoj posao i na ponudu usluga: pored toga što prodaju internetske veze različitih propusnih opsega domaćinstvima i firmama, oni su uveli i sopstveni VoIP (prenos glasa preko IP; telefon preko interneta) ili IP TV usluge (televizija preko interneta), video po zahtevu (slično iznajmljivanju filmova), muzičke ili video portale, itd. Oni se sada takmiče ne samo sa konkurentima za jeftinije, brže i bolje konekcije, nego i sa provajderima usluga i sadržaja – kao što su Skajp, Gugl i Epl.

Upravljanje mrežom – nešto dostupno operaterima ali ne ostalima – može da bude važno sredstvo pri nadmetanju u obezbeđivanju usluga i sadržaja davanjem prioriteta paketima u zavisnosti od poslovnih preferencijala. Na primer, neki operater može da odluči da uspori ili da potpuno zabrani protok paketa podataka konkurentske kompanije (kao što je Skajp ili Gugl Vojs) prema krajnjim korisnicima kroz svoju mrežu, dajući istovremeno prednost paketima podataka svoje unutrašnje usluge (kao što je IP telefonija ili internetska televizija koje nudi klijentima).[23]

Pravna pitanja

Drugu sivu zonu upravljanja mrežom predstavlja pravo internet operatera da blokiraju materijale koji mogu prekršiti autorska prava. Da li provajderi internet usluga imaju pravo i obavezu da zaustave, na primer, saobraćaj na mrežama računara jednakih nadležnosti (P2P) koje se obično koriste za distribuciju materijala sa zaštićenim autorskim pravima? Da li oni imaju prerogative sudskih i administrativnih tela?

Neka od ovih pitanja nalaze se u fokusu spora između Savezne komisije za komunikacije (FCC) i internetskog operatera Comcast. Godine 2007, dve advokatske grupe podnele su žalbu FCC, regulatornom telu

SAD, tvrdeći da je Comcast, operater, narušio mrežnu neutralnost time što je usporio pristupnicu BitTorenta (P2P softver za skidanje fajlova – obično muzike, videa i igrica, iako ne samo njih) za svoje korisnike.[24]

Politička pitanja

Mogućnost upravljanja mrežnim saobraćajem zasnovana na izvoru ili destinaciji, usluzi ili sadržaju, može dati vladama priliku da nametnu takvu praksu domaćim telefonskim kompanijama i da pritom efektivno uvedu filtere za nezgodne ili osetljive sadržaje u odnosu na političke, ideološke, verske, kulturne ili druge vrednosti. Ovo sa sobom nosi opasnosti od zloupotrebe onih koji upravljaju mrežom, za cenzuru, naročito u zemljama sa autoritarnim režimima.

Opasnosti

Ako oni koji upravljaju mrežom izlaze iz okvira *celishodnog nivoa,* čiji je cilj obezbeđivanje jednakih usluga za sve korisnike interneta, biće ugrožen sistem mrežne neutralnosti. To bi moglo da vodi ka stvaranju slojevitog interneta. Prema korisničkim grupama kao što je Spasite internet[25] i Kokus upravljanja internetom,[26] internet bi mogao postati set komercijalnih paketa koje nude provajderi, kod kojih bi korisnici mogli da pristupe samo nekim onlajn uslugama i sadržajima unutar izvesnog odabranog paketa[27] – mnogo nalik kablovskoj televiziji.

Shodno tome, oni upozoravaju da će, ukoliko telefonske kompanije budu počele da opterećuju provajdere sadržaja ili aplikacija, to ubiti konkurenciju za uslugama samih provajdera i ugroziti male kompanije[28] nekomercijalne ponude, kao što su aplikacije za ljude sa invaliditetom koji obično zahtevaju visok propusni opseg.

Ko su glavni igrači i koji su njihovi argumenti?

Pozicija glavnih igrača neprestano se menja. Na primer, najnovije naznake da će Gugl možda potpisati specijalni ugovor s Verizonom za srednji pristup mrežnoj neutralnosti promenile bi pozicije glavnih igrača.[29] Gugl je do sada smatran jednim od glavnih pobornika mrežne neutralnosti; u druge spadaju zastupnici potrošača, onlajn kompanije, neke tehnološke kompanije, mnoge kompanije za internetske aplikacije, kao što su Jahu!, Vonidž, Ibej, Amazon, ErtLink, i softverske kompanije kao Majkrosoft.

U protivnike mrežne neutralnosti spadaju glavne telekomske kompanije, provajderi internet usluga, proizvođači mrežne opreme i hardvera, te proizvođači video i multimedijalnih materijala. Njihovi argumenti su fokusirani na tržište, počev od potrebe da ponude ono što potrošači žele.

U raspravi o mrežnoj neutralnosti postoje četiri glavna argumenta:

	Pobornici	Protivnici
Argument o budućnosti	Mrežna neutralnost će sačuvati arhitekturu interneta koja je do sada omogućavala njegov brz i inovativan razvoj. Većina pobornika su nove internetske kompanije koje su se razvile zahvaljujući otvorenoj arhitekturi interneta.	Onlajn kompanije moraju imati mogućnost da dalje razvijaju internet i nude usluge za koje će korisnici biti zainteresovani. Ovo može podrazumevati brži internetski saobraćaj.
Ekonomski argument	Bez mrežne neutralnosti, internet će ličiti na kablovsku televiziju. Šačica gigantskih kompanija kontrolisala bi pristup i distribuciju sadržaja, odlučujući o tome šta korisnici dobijaju da vide i koliko to košta. Dok bi to retkima donelo korist, mnoge bi oštetilo, i na kraju uništilo ekonomsku budućnost interneta.	Ako ne bude mogućnosti ponude novih usluga i ekonosmkih modela, to će smanjiti ekonomsko interesovanje za internet, zaustaviti ulaganja i na kraju, ugroziti čak i infrastrukturu interneta.
Etički argument	Internet je rezultat rada mnogih volontera tokom više decenija. Oni su uložili vreme i kreativnost u razvijanje glavne memorije interneta, od tehničkih protokola do sadržaja. Ne može se opravdati da većina dobiti od tako velikih ulaganja pripadne nekolicini kompanija koje će zatvoriti internet u ograničene poslovne modele kršenjem mrežne neutralnosti. Internet se razvio otvoreno i javno. Javni interesi moraju se obezbediti. Mrežna neutralnost jedan je od načina da se to ostvari.	Mrežna neutralnost je etički sumnjiva zato što internetski operateri moraju da investiraju u održavanje strukture interneta; većinu dobiti ubiru kompanije internetskog 'sadržaja', kao što su Gugl, Fejsbuk i Amazon. Internetski i telekomski operateri tvrde da kolač treba da se podeli ravnopravnije.
Regulativni argument	Mrežnu neutralnost mora da nametne vlada. Svaki oblik samoregulative ostaviće otvoreno telekom i kablovskim kompanijama da krše princip mrežne neutralnosti.	Internet se razvio zbog vrlo lake ili nikakve regulative. Teška vladina regulativa može da uguši kreativnost, a regulacija mrežne neutralnosti može ugušiti budući razvoj interneta.

Osnovni principi

Poslednjih godina, neki donosioci zakonskih odredbi – kao što su oni u Norveškoj, SAD ili EU – ubacili su se i formulisali ključne principe za mrežnu neutralnost na osnovu tekućih diskusija:[30]

- **Transparentnost:** Internetski operateri moraju obezbediti korisnicima kompletne i tačne informacije o upravljanju mrežom, o njenom kapacitetu i kvalitetu usluga.
- **Pristup:** Korisnici bi morali imati (jednak) pristup svim (pravnim) sadržajima, uslugama ili aplikacijama (sa minimalnim kvalitetom garantovanih usluga, kao što je propisao donosilac odredbi) ili da spoje bilo koji hardver koji ne nanosi štetu mreži (bez obzira na finansijske mogućnosti ili društveni status).
- **(Ne)diskriminacija:** Internetski operateri ne bi trebalo da vrše nikakvu diskriminaciju (ili razumnu diskriminaciju) saobraćaja na osnovu:
  - porekla pošiljaoca ili primaoca;
  - vrste sadržaja aplikacije ili usluge (sa fer konkurencijom – bez diskriminacije neželjenih konkurenata);
  - tamo gde bi za javnu korist mogao biti 'razuman' svaki postupak (koji osigurava kvalitet usluga, bezbednost i elastičnost mreže, inovacije i dalja ulaganja, smanjenje troškova, itd);

U druge principe o kojima se najčešće raspravlja na međuanrodnim forumima, kao što su sastanci IGF i EuroDIG dijalog,[31] spadaju:

- očuvanje slobode izražavanja, pristup informacijama i mogućnost izbora;
- osiguravanje kvaliteta usluga i bezbednosti i elastičnosti mreže;
- očuvanje inicijativa za ulaganja;
- podsticanje inovacija (uključujući mogućnosti za nove poslovne modele i inovativne kompanije). Definisanje prava, uloga i odgovornosti svih uključenih strana (provajdera, donosioca uredbi, korisnika) uključujući pravo na žalbu i odštetu;
- sprečavanje antikonkurentskih postupaka;
- stvaranje tržišnog ambijenta koji bi omogućio korisnicima da lako biraju i menjaju mrežnog operatera;
- zaštita interesa hendikepiranih, kao što su osobe sa invaliditetom i korisnici i kompanije u zemljama u razvoju;
- održavanje raznolikosti sadržaja i usluga.

Korisnici ili kupci?

Rasprava o mrežnoj neutralnosti stvara i jezički diskurs. Pobornici mrežne neutralnosti govore o 'korisnicima' interneta, dok ih drugi – uglavnom komercijalni igrači – opisuju kao 'kupce'. Korisnici interneta su više od običnih kupaca; termin 'korisnik' podrazumeva aktivno učešće u razvoju interneta preko društvenih mreža, blogovanja i drugih sredstava, i kroz važnu ulogu koju imaju u odlučivanju o budućnosti interneta. Kupci, s druge strane, kao bilo koji kupci, mogu da odlučuju da li će kupovati usluge koje se nude ili neće. Njihov status na internetu zasnovan je na ugovoru sa provajderima internet usluga i na pravilima o zaštiti kupaca. Izvan toga, od kupaca se ne očekuje da imaju bilo kakvu ulogu u odlučivanju o vođenju interneta.

Pristupi politici

Raspravom o mrežnoj neutralnosti, u prvi plan je izbilo još jedno pitanje: koja je uloga donosioca zakonskih odredbi u politici dodele frekvencija i prakse operatera?

Razvijen zemlje

U znak odgovora na slučaj Comcast, FCC SAD je usvojila Smernice o mrežnoj neutralnosti kao osveženje svog dokumenta o politici iz 2005,[32] koje odražavaju potrebu za pristupom i izborom sadržaja i sredstava, i pozabavila se pitanjima diskriminacije i transparentnosti. Radna grupa japanskog ministarstva unutrašnjih poslova i komunikacija podnela je izveštaj o izboru i pristupu, kao i o diskriminaciji, ali se pored toga pozabavila nepristrasnošću u raspodeli troškova i upotrebe mreže.[33] Švedska poštanska i telekomska agencija (ŠPT) podvlači da je otvorenost – koja se unapređuje nediskriminacijom i konkurencijom – preduslov za inovacije, ali i da mora da bude balansirana u odnosu na ulaganja i bezebdnost mreže.[34] Regulatorni okvir elektronskih komunikacija EU teži ka zaštiti slobode izražavanja, izbora korisnika i pristupnih prava, skupa sa principom transparentnosti; ipak, on takođe ističe potrebu za ulaganjima, fer konkurencijom bez ikakve diskriminacije i mogućnostima za nove poslovne modele, uključujući inovativnost.[35]

Najcenjeniji model dolazi od Uprave Norveških pošta i telekomunikacija (NPT), koji traži da se obezbede: transparentnost poslovnih ponuda i postupaka, izbor korisnika i pristup sadržajima, usluge i hardver, te nediskriminacija zasnovana na aplikaciji, uslugama, sadržaju, pošiljaocu ili primaocu.[36] Ne ističe se, međutim, samo sadržaj nego i proces postizanja konsenzusa o ovim smernicama: zauzimanjem širokog pristupa zasnovanog na multiakterstvu prema osmišljavanju suodredaba koje se temelje na postizanju konsenzusa svih strana u vezi sa obavezujućim ugovorima; na taj način NPT je uverila potrošače i kompanije da se tržište može regulisati bez krutih zakona.[37]

Međutim, u nekim zemljama postoji praksa da se ne sprečava diskriminacija koju diktira biznis. Pobornici mrežne neutralnosti nazivaju ih 'ostrvima antineutralnosti', gde svakako može da se vidi koje su perspektive 'neneutralnog interneta'.

Zemlje u razvoju

Zahvaljujući ograničenoj infrastrukturi i propusnom opsegu, donosioci zakonskih odredbi više se fokusiraju na fer politiku korišćenja – pristupačne cene i fer pristup za sve. Neki izražavaju bojazan zbog prekogranične nediskriminacije, govoreći da bi trebalo da se saobraćaj iz svih zemalja tretira na isti način, bez ikakvih preferencijala zasnovanih na završnim troškovima. Isto tako, neke zemlje imaju više osećaja za unutrašnje kulturne, političke ili etičke aspekte, razumevajući pritom '(ne)celishodno korišćenje' i rukovođenje drugačije od nekih drugih. Izražena je zabrinutost da bi inovativni modeli razvijenog sveta mogli sputati tržišta u razvoju: davanjem prednosti uslugama velikih globalnih kompanija; nove kompanije i konkurencija bili bi dodatno oštećeni, što bi ugrozilo raznolikost i inovacije. Međutim, još uvek nije došlo do pojave formalne politike ili regulatorne prakse iz zemalja u razvoju.

Međunarodne organizacije i NVO

Mnoge međunarodne organizacije i korisničke grupe takođe su razvile pozicije u odnosu na mrežnu neutralnost. Savet Evrope naglašava osnovna prava na slobodu izražavanja i informacije; Internet društvo (ISOC) forsira korisničkocentrički pristup koji se prvenstveno bavi pitanjima pristupa, izbora i transparentnosti kroz 'otvorenu inter-mrežnu' raspravu, pre nego kroz raspravu o mrežnoj neutralnosti.[38] Transatlantski potrošački dijalog (TACD), forum potrošačkih organizacija SAD i EU, dodatno ističe zahteve za nediskriminatorno ponašanje telekomunikacionih kompanija, pozivajući SAD i EU da ovlaste donosioce zakonskih odredbi da se ponašaju kao zaštitnici korisničkih prava.[39] Mnoge nevladine organizacije naročito su zabrinute za budućnost nekomercijalnih i nekonkurentnih onlajn sadržaja i usluga, zahtevajući da one budu prenošene preko svih telekomunikacionih mreža kao i komercijalne. Oni ističu prava marginalizovanih grupa – naročito ljudi sa invaliditetom – da koriste sadržaje, usluge i aplikacije (uključujući i one koje traže visoki propusni opseg) za svoje potrebe bez ikakvih ograničenja.

Otvorena pitanja

Postoji više otvorenih pitanja u vezi s raspravom o mrežnoj neutralnosti:

- Gde bi trebalo da bude ravnoteža između dobrih javnih efekata interneta i korisničkih (ljudskih) prava s jedne strane, i prava internet operatera da unose inovacije u mreže čiji su vlasnici, s druge strane?

- Da li bi neregulisano tržište sa otvorenom konkurencijom, kako smatraju telekomunikacione kompanije, pružalo neograničen (ili dovoljan) izbor za korisnike? Ili bi donosioci zakonskih odredbi neminovno bili ovlašćeni kao zaštitnici, i sa kojim ovlašćenjima?
- Koje su implikacije mrežne (ne)neutralnosti za zemlje u razvoju?
- Da li će potreba za upravljanje mrežom iz tehničkih (kvalitativnih) razloga biti zastarela u budućnosti, zahvaljujući napretku u telekomunikacionoj tehnologiji?
- Koje su implikacije stepenastog interneta za konkurenciju, inovacije, ulaganja i ljudska prava?
- Kako će era servisa u oblaku i sve veća zavisnost od virtuelnih servera uticati na raspravu o mrežnoj neutralnosti i obrnuto?
- Da li bi trebalo da se rasprava proširi sa rukovođenja saobraćajem na telekomunikacionom nivou na rukovođenje sadržajem i aplikacijama na nivou sadržaja i aplikacija kod provajdera, kao što su Gugl, Epl i Fejsbuk?
- Da li će zaštita potrošača i dalje biti suštinski povezana sa mrežnom neutralnošću? Ako mrežna neutralnost bude 'poražena', koji će principi podržavati zaštitu potrošača u budućnosti?

Provajderi internet usluga (ISP)

Kako ISP-ovi povezuju krajnje korisnike sa internetom, oni pružaju najdirektniju opciju za sprovođenje pravnih pravila na internetu. Sa sve većim komercijalnim značajem interneta i sve većim brigama vezanim za sajber-bezbednost, mnoge države su počele da koncentrišu svoje napore na donošenju zakona na ISP-ove.

Pitanja

Za dalju raspravu o digitalnom jazu videti Peti deo

Telekomunikacioni monopoli i ISP-ovi
Uobičajeno je u zemljama s telekomunikacionim monopolima da ti isti monopoli obezbeđuju pristup internetu. Monopoli sprečavaju druge ISP-ove da uđu na ovo tržište, i uništavaju konkurenciju. To rezultira višim cenama, često nižim kvalitetom usluga i ne uspeva da smanji digitalni jaz. U nekim slučajevima, telekomunikacijski monopoli tolerišu postojanje drugih ISP-ova, ali prave smetnje na operativnom nivou (npr. dajući niže propusne opsege ili uzrokujući prekide usluga).

Odgovornost ISP-ova za autorska prava

Zajednički svim pravnim sistemima jeste princip da jedan ISP ne može biti odgovoran za držanje materijala koji krše zakon o autorskim pravima ako taj ISP nije svestan tog kršenja. Glavna razlika leži u zakonskom postupku koji se preduzima pošto ISP bude obavešten da materijal koji drži krši autorska prava.

Zakon EU i SAD koristi postupak obaveštenja o skidanju, koji zahteva od ISP-a da ukloni takav materijal da bi izbegao gonjenje. Japanski zakon preduzima uravnoteženiji pristup, preko obaveštenja o skidanju, koji pruža korisniku materijala pravo da se žali na zahtev za skidanje.

Pristup nametanja ograničene odgovornosti ISP-ovima uglavnom ima podršku pravosuđa. Neki od najvažnijih slučajeva u kojima su ISP-ovi bili oslobođeni odgovornosti za držanje materijala kojima su kršili autorska prava su sledeći: Sajentološki slučaj (Holandija), RIAA vs Verizon (Sjedinjene Države), SOCAN vs CAIP (Kanada) i Sabam vs Tiscali (Belgija).

Uloga ISP-ova u politici sadržaja

PPod sve većim javnim pritiskom, ISP-ovi se postepeno, iako nerado, uključuju u politiku sadržaja. Čineći to, možda bi morali da slede dva moguća puta. Prvi je da sprovode vladinu regulativu. Drugi, zasnovan na samoregulaciji, jeste da ISP-ovi sami odlučuju šta je prikladan sadržaj. Ovim se dolazi u opasnost privatizovanja kontrole sadržaja, pri čemu ISP-ovi preuzimaju odgovornosti vlada.

Uloga ISP-ova u politici suzbijanja spema

ISP-ovi se obično sagledavaju kao primarne institucije uključene u inicijative za suzbijanje spema. Oni obično imaju sopstvene inicijative za smanjenje spema, bilo preko tehničkog filtriranja ili preko uvođenja antispemne politike. Izveštaj ITU o spemu konstatuje da bi trebalo da ISP-ovi budu odgovorni za spem i predlaže antispemni kodeks ponašanja, koji bi trebalo da uključi dve glavne odredbe: svaki ISP mora da zabrani svojim korisnicima upotrebu spema i ne sme da se povezuje sa drugim ISP-ovima koji ne prihvataju sličan kodeks ponašanja.[40]

Problem sa spemom izlaže ISP-ove novim poteškoćama. Na primer, Verizonovo antispemno filtriranje dovelo je do sudskog spora budući da je blokiralo i dozvoljene poruke, uzrokujući tako neugodnosti za korisnike koji nisu dobijali svoju legitimnu elektronsku poštu.[41]

Provajderi za pružanje širokopojasnih internet usluga (IBP)

Pristupna arhitektura interneta sastoji se od tri sloja. ISP-ovi koji povezuju krajnje korisnike čine sloj 3. Slojevi 1 i 2 sastoje se od IBP-ova. Prenosnici sloja 1 glavni su IBP-ovi. Oni obično imaju ujednačene aranžmane sa drugim IBP-ovima iz sloja 1.[42] Glavna razlika između provajdera za pružanje širokopojasnih internet usluga sloja 1 i sloja 2 počiva u tome što IBP-ovi sloja 1 razmenjuju saobraćaj putem ravnopravnog povezivanja, dok IBP-ovi sloja 2 moraju da plaćaju proviziju provajderima sloja 1.[43]

Sloj 1 obično vode velike kompanije, kao što su MCI, AT&T, Kejbl vajerles i Frans telekom.

Pitanja

Da li internetska infrastruktura treba da bude javni servis?
Internetski podaci mogu da putuju preko bilo kojeg telekomunikacionog medija. U praksi, kapaciteti kao što su prenosni putevi sloja 1 (tj. glavne trase za prenos podataka između velikih, strateški međusobno povezanih mreža i glavnih rutera interneta), koji obično imaju optičke kablove ili satelitske linkove, postali su presudni za rad interneta. Njihova ključna pozicija unutar internetske mreže daje njihovim vlasnicima tržišnu moć da nameću cene i uslove za pružanje usluga. U krajnjem slučaju, funkcionisanje interneta moglo bi da zavisi od odluka koje donesu vlasnici centralnih trasa. Da li je moguće da globalna internetska zajednica traži garancije za pouzdano funkcionisanje kritične infrastrukture interneta od glavnih telekomunikacionih operatera? U raspravama se teži ka tome da se nametnu neki javni zahtevi operaterima privatne infrastrukture interneta.

Provajderi za pružanje širokopojasnih internet usluga (IBP-ovi) i kritična infrastruktura

Početkom 2008. godine, došlo je do prekida jednog od glavnih internet kablova u Sredozemnom moru, u blizini Egipta. Ovaj incident doveo je u opsanost pristup internetu u velikom području koje se prostiralo do Indije. Dva slična incidenta dogodila su se 2007 (prekidi internetskog kabla u blizini Tajvana i glavnog internetskog kabla za Pakistan), jasno pokazujući da je infrastruktura interneta deo nacionalne i globalne kritične infrastrukture. Prekid internet usluga može da pogodi ukupan privredni i društveni život nekog regiona. Mogućnost takvog prekida pokreće više pitanja.

- Da li su glavni internetski kablovi temeljito zaštićeni?
- Koja je uloga nacionalnih vlada, međunarodnih organizacija i pri - vatnih kompanija u zaštiti internetskih kablova?

- Kako možemo da rešavamo opasnosti vezane za potencijalni prekid glavnih internet kablova?

Telekomunikaciona liberalizacija uloge ISP-ova i IBP-ova

Postoje suprotstavljeni stavovi u vezi sa stepenom do kojeg ISP-ovi i IBP-ovi treba da budu potčinjeni postojećim međunarodnim instrumentima. Razvijene zemlje tvrde da liberalizovana pravila koja je STO garantovala telekomunikacionim operaterima mogu da se prošire i na ISP-ove. Ovo restriktivno tumačenje osvetljava činjenicu da se telekomunikacioni režim STO primenjuje samo na telekomunikaciono tržište. Regulisanje tržišta ISP-ova zahteva nova pravila STO.

Ekonomski model povezivanja internetom

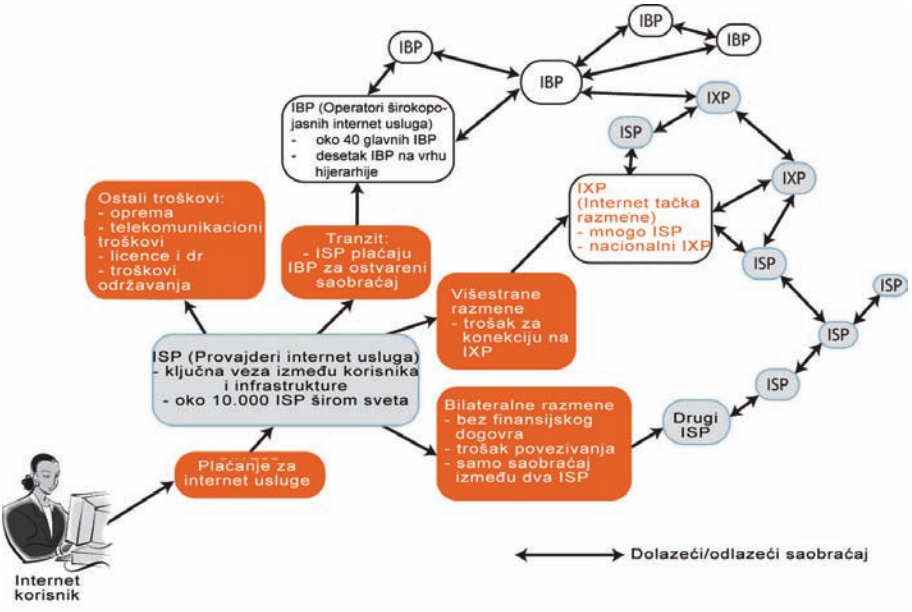
Mi znamo kako da usmeravamo pakete,
ali ne znamo kako da usmeravamo dolare.

Dejvid Klark

Trenutna situacija

Rasprave o pitanjima vezanim za upravljanje najčešće se završavaju analizom raspodele novca.[44] Ko plaća internet? Veći broj finansijskih transakcija odvija se između mnogo strana povezanih s internetom. Individualni pretplatnici i kompanije plaćaju ISP-ovima za pristup internetu i za pružene usluge. Kako se ovaj novac deli drugima u raznim lancima pružanja internet usluga, drugim rečima, kako se kreće internetski dolar?[45]

- ISP-ovi plaćaju telekomunikacionim operaterima i za propusni opseg interneta;
- ISP-ovi plaćaju RIR-ovima (regionalnim internet registrima) ili LIR-ovima (lokalnim internet registrima), od kojih se dobijaju fondovi IP adresa za dalju raspodelu;
- ISP-ovi plaćaju prodavcima za opremu, softver i održavanja (uključujući dijagnostifikujuće instrumente kao i za izdržavanje osoblja koje rukuje njihovim uređajima, servisima za pomoć i pruža administrativne usluge);
- strane koje registruju ime domena kod administratora plaćaju administratoru i IUDB za njene usluge; i
- telekomunikacioni operateri plaćaju proizvođačime kablova i satelita i provajderima telekomunikacionih usluga za snabdevanje potrebnim linkovima. (Kako su ovi operateri često zaduženi, oni sa svoje strane plaćaju kamate raznim bankama i konzoricijumima).



Ovaj spisak se nastavlja, a sve se u stvari svodi na to da 'nema džabe ni kod babe'. Na kraju krajeva, krajnji korisnici interneta, bilo da je reč o pojedincima ili institucijama, plaćaju troškove u ovom lancu.

Pitanja

Da li je ekonomiji interneta potrebna reforma?
Jedno od zaveštanja interneta je njegova tekuća ekonomska politika i praksa, koja se razvija kroz veći broj ponavljanja. Ekonomska praksa interneta trenutno se smatra uspešnom zbog njegove tečne funkcionalnosti i zbog uglavnom podnošljivih troškova. Glavne kritike tekućih ekonomskih mera koncentrišu se na dva aspekta:

1. Internet ne izbegava monopol glavnih igrača na polju internetske povezanosti i na taj način daje mogućnost za poremećaj na tržištu.
2. Ne omogućava ravnopravno učešće u prihodima i rashodima svih onih koji su uključeni u ekonomiju interneta.

U akademskim krugovima, bilo je mnogo pokušaja da se za internet uvedu prave mere ekonomske politike. Nuven i Armitidž tvrde da internet treba da ima optimalnu ravnotežu između tri elementa: tehnička efikasnost, ekonomska efikasnost i društveni efekti.[46] Drugi ističu

izazove vezane za zamenu postojeće, jednostavne, paušalne strukture određivanja cena složenijom, kao što je računovodstvo zasnovano na saobraćaju paketa. U vezi sa praktičnim promenama, neki smatraju da bi promena važeće ekonomske politike interneta mogla da otvori Pandorinu kutiju.

Sprečavanje mogućih monopola na tržištu internet resursa

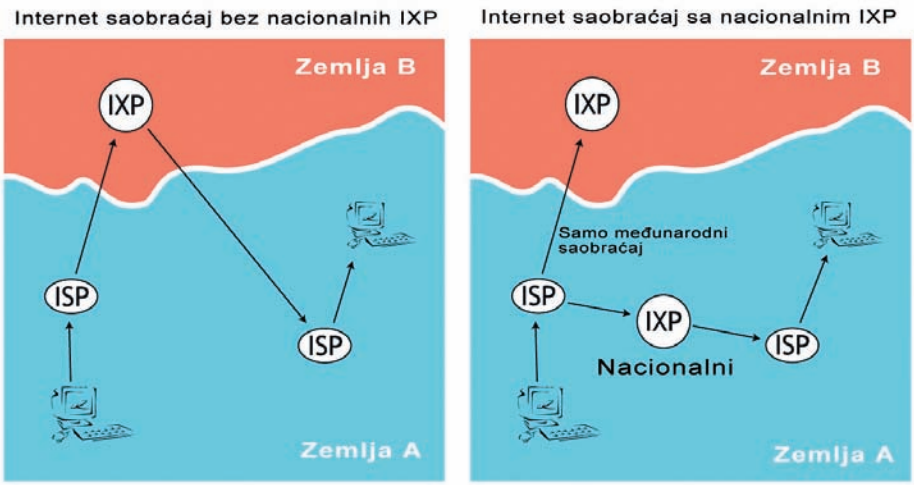
Moguće je da zahvaljujući preuzimanjima, nekoliko monopola zavlada celim tržištem internetskog saobraćaja.[47] Ovaj problem postoji i u razvijenim i u nerazvijenim zemljama. Neki se nadaju da će proces liberalizacije telekomunikacionih tržišta rešiti problem monopola (naročito onih koji uključuju važeće operatere). Međutim, liberalizacija bi mogla dovesti do zamene državnog monopola privatnim. Džef Hjuston tvrdi da bi uspostavljanje monopola i gubljenje raznovrsnog tržišta internet resursa neminovno uticalo na cenu i kvalitet internet usluga.[48]

Ko bi trebalo da pokriva troškove veza između zemalja u razvoju i razvijenih zemalja?

> *Kada krajnji korisnik u Keniji pošalje i-mejl komitentu u SAD, troškove međunarodnog povezivanja iz Kenije u SAD snosi kenijski provajder internet usluga (ISP). U suprotnom slučaju, kada američki krajnji korisnik šalje i-mejl u Keniju, opet troškove međunarodnog povezivanja snosi kenijski ISP, i u krajnjem slučaju, kenijski krajnji korisnik koji snosi glavni teret plaćanjem viših pretplata.*[49]

Trenutno, zemlje u razvoju pokrivaju troškove veza između zemalja u razvoju i razvijenog sveta.[50, 51] U poređenju sa sistemom tradicionalne telefonije, gde dve zemlje dele cenu svakog međunarodnog poziva, internetski model stavlja ceo teret na jednu stranu: na stranu zemalja u razvoju. Ove zemlje moraju snositi troškove povezivanja sa glavnim prenosnicima komunikacija koji se uglavnom nalaze u razvijenim zemljama. Posledica toga je da male i siromašne zemlje dotiraju internet u bogatim zemljama.

Glavni argument u raspravama o promenama trenutnog sistema internet opterećenja koristi analogiju finansijskog aranžmana u sistemu telefonije, koji deli troškove i prihode između krajnjih tačaka komunikacije. U sistemu telefonije, samo jedan artikal koji se može jasno identifikovati – telefonski poziv kojim se uspostavlja ljudski razgovori između dva telefonska aparata – ima cenu.[52] Internet nema odgovarajući, pojedinačni 'artikal', samo pakete koji kreću kroz mrežu različitim putevima. Ova suštinska razlika čini ovu analogiju neprikladnom. Ona je takođe glavni razlog zbog čega je teško primeniti na internet model finansijskog telefonskog aranžmana.



ITU je inicirala rasprave o mogućim poboljšanjima važećeg sistema za rešavanje internet troškova, da bi se dobila uravnoteženija raspodela troškova za pristup internetu. Zahvaljujući protivljenju razvijenih zemalja i telekomskih operatera, usvojena rezolucija ITU, D. 50, praktično nema dejstva.[53] Takođe je bilo neuspešnih pokušaja uvođenja ovog pitanja za vreme pregovora koje je vodila STO. Potreba za usaglašavanjima u vezi s opterećenjima ponovljena je u završnim dokumentima Svetskog samita o informacionom društvu (WSIS) i u izveštaju Radne grupe za upravljanje internetom (WGIG).

Veb-standardi

Krajem osamdesetih godina XX veka, bitka za mrežne standarde je završena. TCP/IP postepeno je postajao glavni mrežni protokol, dovodeći na marginu ostale standarde, kao što je X25 koji je imao podršku ITU, i mnogi drugi patentirani standardi, kao što je Aj-Bi-Em i SNA. Dok je internet olakšavao normalnu komunikaciju između različitih mreža preko TCP/IP-a, samom sistemu su još nedostajali zajednički standardi za aplikacije.

Rešenje su dali Tim Berners-Li i njegove kolege u CERN-u (Evropska organizacija za nuklearna istraživanja) u Ženevi, a sastojalo se od novog standarda za širenje informacija preko interneta, nazvanog HTML (koji je u stvari predstavljao samo pojednostavljenje ISO standarda zvanog SGML – standardni opšti markirni jezik). Sadržaj prikazan na internetu morao je najpre da se organizuje prema standardima HTML-a. HTML, kao baza WWW, trasirao je put za nagli razvoj interneta.

Od svoje prve verzije, HTML se neprestano unapređuje novim karakteristikama. Sve veći značaj interneta doveo je u žarište interesovanja standardizaciju HTML-a. Ovo je bilo naročito relevantno tokom 'pretraživačkog rata' između Netskejpa i Majkrosofta, kada je svaka od ove dve kompanije pokušala da ojača svoj tržišni položaj vršeći uticaj na standarde HTML-a. Dok je osnovni HTML radio samo sa tekstom i fotografijama, nove internetske aplikacije zahtevale su prefinjenije standarde za vođenje baza podataka, video sadržaja i animacija. Takva raznolikost aplikacija zahtevala je znatne napore na standardizaciji da bi se obezbedilo da internetski sadržaj može da propisno vidi većina pretraživača interneta.

Standardizacija aplikacija ušla je u novu fazu pojavom XML-a (proširljivog markirnog jezika), koji je omogućio veću fleksibilnost pri postavljanju standarda za internetski sadržaj. Uvedeni su i novi nizovi standarda XML-a. Na primer, standard za distribuciju bežičnog sadržaja zove se bežični markirni jezik (WML).

Standardizacija aplikacija vrši se uglavnom u okviru WWW konzorcijuma (W3C), na čijem čelu se nalazi Tim Berners-Li. Zanimljivo je primetiti da uprkos visokom značaju za internet, W3C nije do sada privukao mnogo pažnje u raspravi o upravljanju internetom.

Servisi u oblaku (cloud computing)

Termin 'cloud computing' koristi se za opis nove tendencije u kompjuterskoj industriji koja se zasniva na korišćenju kompjuterskih aplikacija kao usluga koje se pružaju iz velikih serverskih farmi (zbirka kompjuterskih servera koju održava inicijativa da se ostvare serverske potrebe koje daleko premašuju mogućnosti jedne mašine). Prva naznaka servisa u oblaku oseća se već prelaskom elektronske pošte sa naših hard diskova na mejl servere (Gmejl, Hotmejl, Jahu!) i na upotrebu onlajn tekst procesora (usluge Vikija i Gugla). Aplikacije društvenih mreža kao što su Fejsbuk i blogovi dodatno su ubrzale trend ka servisima u oblaku. Sve više našeg digitalnog kapitala prelazi sa hard diska na virtuelni server. Glavni igrači među servisima u oblaku su Gugl, Majkrosoft, Epl, Amazon i Fejsbuk; svi oni već imaju ili su planirali da razviju velike farme servera.

U početku su postojali moćni matični kompjuteri i neme radne stanice. Procesorska snaga se nalazila u sredini. Posle toga, dugo vremena, sa pi-sijevima i vindous aplikacijama, procesorska snaga pomerila se ka periferiji. Da li će servisi u oblaku zatvoriti krug? Da li ćemo imati nekoliko velikih cen-

tralnih kompjutera/serverskih farmi i na milijarde nemih jedinica u obliku malih kompjutera, monitora i mobilnih telefona? Za odgovor na ovo i druga pitanja biće potrebno malo više vremena. Trenutno, možemo identifikovati nekoliko pitanja u vezi sa upravljanjem internetom, koja će se vrlo verovatno pojaviti paralelno s razvojem servisa u oblaku.

1. Sa sve više usluga koje se budu dostavljale onlajn, moderno društvo će povećati zavisnost od interneta. U prošlosti, kada bi se internet prekinuo, nismo mogli da pošaljemo i-mejl ili da pretražujemo mrežu. U eri servisa u oblaku ne možemo čak ni da napišemo tekst ili da izvršimo proračun. Ova veća zavisnost od interneta podrazumevaće veći pritisak na njegovu čvrstinu i pouzdanost. Ona će neminovno voditi ka snažnijem režimu upravljanja internetom i većoj uključenosti vlada.
2. Sa sve više ličnih podataka smeštenih na virtuelnim serverima, pitanje zaštite privatnosti i podataka postaće centralno. Da li ćemo imati kontrolu nad svojim tekstualnim fajlovima, nad elektronskom poštom i drugim podacima? Da li bi operateri virtuelnih servera mogli da ih koriste bez naše dozvole? Ko će imati pristup našim podacima?
3. Sa sve većim obimom društvenog kapitala koji ide digitalno, zemljama može postati neprijatno da se njihov nacionalni kapital nalazi van državnih 'granica'. Možda će one pokušati da stvore nacionalne ili regionalne virtuelne servere ili da se uvere da postojeći virtuelni serveri imaju neki međunarodni nadzor. Nacionalizacija virtuelnih servera mogla bi još više da se ubrza činjenicom da su svi glavni operateri u ovoj oblasti smešteni u Sjedinjenim Državama. Neki tvrde da trenutna rasprava koncentrisana na ICANN može da bude zamenjena raspravom u vezi s upravljanjem internetom o regulisanju servisa u oblaku.
4. Sa različitim operaterima servisa u oblaku, pitanje standarda postaje veoma važno. Usvajanje zajedničkih standarda obezbediće lak prenos podataka između raznih virtuelnih servera (npr. sa Gugla na Epl). Jedna mogućnost o kojoj se raspravlja jeste usvajanje otvorenih standarda od strane mnogih igrača među servisima u oblaku.

Za detaljniju raspravu o Sporazumu o sigurnoj luci videti Šesti deo

Kada je reč o servisima u oblaku, ima više pitanja nego odgovora. Upravljanje internetom kod servisa u oblaku verovatno će se pojaviti u međusobnom delovanju raznih aktera i tela. Na primer, EU je zainteresovana za zaštitu privatnosti i podataka. Sporazum o sigurnoj luci, od kojega se očekivalo da reši problem različitih režima privatnosti u SAD i EU, ne funkcioniše dobro. Sa sve više digitalnih podataka koji prelaze Atlantik, EU i SAD će morati da se pozabave pitanjem zaštite privatnosti

prema standardima EU kod američkih kompanija, glavnih operatera servisa u oblaku. Kada je reč o standardima, veoma je verovatno da će se glavne kompanije međusobno sporazumeti. Gugl je već započeo snažan proboj prema otvorenim standardima osnivanjem organizacije Front za slobodu podataka (Data Liberation Front), s ciljem obezbeđivanja lakog prenosa podataka između virtuelnih servera. To su prvi građevinski blokovi koji će se pozabaviti pitanjem upravljanja internetom kod servisa u oblaku. Drugi će se verovatno pojaviti kao rešenje za konkretne probleme politike razvoja.

Konvergencija: internet – telekomunikacije – multimediji

Istorijski, telekomunikacije, televizija i druga srodna područja bili su odvojeni industrijski segmenti; koristili su različite tehnologije i nalazili su se pod različitim propisima. Široka i preovlađujuća upotreba IP započela je njihovo približavanje. Danas možemo telefonirati, gledati televiziju i uživati u muzici na svojim kompjuterima preko interneta. Samo pre nekoliko godina njima bi rukovodili različiti sistemi.

Na polju tradicionalnih telekomunikacija, glavna tačka konvergencije je VoIP. Sve veća popularnost sistema za prenos glasa preko IP kao što je Skajp zasniva se na niskoj ceni, mogućnosti integrisanja podataka i govornih linija komunikacije, i na upotrebi razvijenih alata zasnovanih na pi-siju. Kod Ju tjuba i sličnih servisa, internet se takođe spaja sa tradicionalnim multimedijima i zabavnim servisima. Dok tehnička konvergencija napreduje brzim koracima, njene ekonomske i pravne posledice zahtevaće malo više vremena da bi se razvile.

Pitanja

Ekonomske implikacije konvergencije
Na ekonomskom nivou, konvergencija je počela da preoblikuje tradicionalna tržišta dovodeći kompanije koje su ranije delovale u raznim domenima u direktnu konkurenciju. Kompanije koriste različite strategije. Najčešći pristup je fuzionisanje i kupovina. Na primer, fuzionisanje Amerike onlajn i Tajm Vornera imalo je za cilj spajanje telekomunikacija s medijima/zabavom. Sada je AOL/Tajm Vorner okupio ISP-ove, televiziju, muziku i razvoj softvera pod jedan korporativni kišobran.

Potreba za pravnim okvirom
Pravni sistem bio je najsporiji kod prilagođavanja promenama uzrokovanim tehnološkom i ekonomskom konvergencijom. Svaki segment – telekomu-

nikacije, televizija i plasiranje informacija – ima sopstveni regulatorni okvir. Konvergencija otvara nekoliko pitanja vezanih za upravljanje i regulativu:

- Šta će se desiti sa postojećim nacionalnim i međunarodnim režimima u takvim oblastima kao što su telefonija i televizija?
- Da li će se razviti novi režimi koji će se koncentrisati uglavnom na internet
- Da li bi trebalo da regulaciju konvergencije sprovode samo javne vlasti (države i međunarodne organizacije) ili da se ista vrši samoregulisanjem?

Neke zemlje, kao Malezija i Švajcarska, a i EU, počele su da daju odgovore na ova pitanja. Malezija je usvojila Zakon o komunikacijama i multimedijima 1998. godine, osnivanjem opšteg okvira za regulisanje konvergencije. Nove okvirne smernice EU, koje se sada ugrađuju u nacionalne zakone, takođe predstavljaju jedan korak u tom smeru, kao što je slučaj i sa švajcarskim zakonima i propisima o telekomunikacijama.

Rizik konvergencije: fuzija kablovskih operatera i ISP-ova

U mnogim zemljama, višefrekvencijski internet uveden je preko kablovskih mreža. Ovo posebno važi za SAD, gde je kablovski internet dominantniji od asimetrične digitalne pretplatničke linije (ADSL), koja predstavlja drugu glavnu višefrekvencijsku internetsku opciju. Koji su rizici povezani s ovom konvergencijom?

Neke strane tvrde da bi ubacivanje kablovskih operatera između korisnika i interneta moglo ugroziti princip mrežne neutralnosti.

Glavna razlika između ADSL-a i kabla počiva u tome što se kabl ne nalazi pod regulativom pravila tzv. 'običnih prenosnika'. Ova pravila, primenjiva na telefoniju, preciziraju da pristup mora biti nediskriminatoran. Kablovski operateri nisu podvrgnuti ovim pravilima, pa tako imaju potpunu kontrolu nad pristupom internetu svojih pretplatnika. Oni mogu da blokiraju korišćenje nekih aplikacija i kontrolisati pristup nekim materijalima. Nadzorne mogućnosti i shodno tome mogućnost ugrožavanja privatnosti mnogo su veći kod kablovskog interneta budući da se pristup kontroliše preko sistema koji je sličan lokalnim područnim mrežama, što omogućava visok nivo direktne kontrole korisnika.

U dokumentu po ovom pitanju, Unija američkih građanskih sloboda daje sledeći primer za rizik od monopola kablovskog interneta:

> *Ovo je kao telefonska kompanija kojoj je dozvoljeno da poseduje restorane i da onda daje dobre usluge i jasne signale mušterijama koji nazovu Domino, a signale o zauzeću, prekide i zastoj onima koji nazovu Pizza Hut.*[54]

Ovaj problem konvergencije biće rešen kada se donese odluka o tome da li je kablovski internet 'informacioni servis' ili 'telekomunikacioni servis'. Ako bude ovaj potonji, moraće potpasti pod pravila običnih prenosnika.

Sajber-bezbednost

Trenutna situacija

Internet je originalno zamišljen kao sredstvo koje će se koristiti u zatvorenom krugu, uglavnom među učenim ljudima koji nisu opterećeni brigama za bezbednost. Oni su komunicirali otvoreno i bavili su se mogućim problemima bezbednosti na neformalan način.

Sajber-bezbednost je došla u žižu interesovanja zahvaljujući nagloj ekspanziji korisničke baze interneta. Internet je ponovio onu staru istinu da tehnologija može da bude i operativna i preteća. Ono što se može iskoristiti u korist društva može se iskoristiti i na njegovu štetu.

Propratni efekat nagle integracije interneta u skoro svim aspektima ljudske delatnosti jeste povećana ranjivost savremenog društva. Internet je deo kritične globalne infrastrukture. Drugi bitni servisi savremenog društva, kao što su električni dalekovodi, transportni sistemi, zdravstvene službe, sve više zavise od interneta. Oni su česta meta sajber-napada.

Pitanja sajber-bezbednosti mogu se svrstati prema tri kriterijuma:

1. **Vrsta akcije.** Klasifikacija zasnovana na vrsti akcije može podrazumevati presretanje podataka, ometanje prijema podataka, ilegalni pristup, špijuniranje, uništavanje podataka, sabotažu, uskraćivanje usluga i krađu identiteta.
2. **Vrsta počinioca.** U moguće počinioce mogli bi spadati hakeri, sajber-kriminalci, sajber-ratnici i sajber-teroristi.
3. **Vrsta cilja.** Mogući ciljevi su brojni, a kreću se od pojedinaca, privatnih kompanija i javnih institucija do kritične infrastrukture, vlada i vojnih sredstava.

Inicijative politike sajber-bezbednosti

Mnoge nacionalne, regionalne i globalne inicijative koncentrišu se na sajber-bezbednost. Na nacionalnom nivou, sve veći obim zakonodavstva i pravosuđa bavi se sajber-bezbednošću. Najistaknutije pravne inicijative jesu one u SAD koje su povezane sa borbom protiv terorizma, gde je

Ministarstvo državne bezbednosti glavna institucija koja se bavi pitanjima sajber-bezbednosti. Teško je naći bilo koju razvijenu zemlju bez nekih inicijativa koje se koncentrišu na sajber-bezebdnost.

Na međunarodnom nivou, ITU je najaktivnija organizacija; ona je stvorila veliki broj bezbednosnih okvira, arhitektura i standarda, uključujući X.509, koji obezbeđuje bazu za glavnu javnu infrastrukturu, koja se, na primer, koristi u bezbednoj verziji HTTP (hipertekstulanog transfernog protokola). Nedavno je ITU izašla iz strogo tehničkih aspekata i pokrenula je program globalne sajber-bezbednosti.[55] Ova inicijativa obuhvata zakonske mere, kooperativnost u sprovođenju politike i izgradnju kapaciteta.

Grupa G8 takođe ima nekoliko inicijativa na polju sajber-bezbednosti, čija je svrha poboljšanje saradnje između agencija koje sprovode zakon. Ona je formirala Podgrupu za visokotehnički kriminal, da bi se bavila uspostavljanjem neprestanih komunikacija između centara za sajber-bezbednost država članica, obukom osoblja i poboljšanjem državnih pravnih sistema za borbu protiv sajber-kriminala i unapređenje saradnje između IKT industrije i agencija za sprovođenje zakona.

Generalna skupština Ujedinjenih nacija donosi nekoliko rezolucija godišnje o 'razvoju na polju informatike i telekomunikacija u kontekstu međunarodne bezbednosti', posebno rezolucije 53/70 (1998), 54/49 (1999), 55/28 (2000), 56/19 (2001), 57/239 (2002) i 58/199 (2003). Od godine 1998, sve potonje rezolucije uključile su sličan sadržaj, bez bilo kakvih značajnih poboljšanja. Osim ovih rutinskih rezolucija, glavni proboj bio je u nedavnom setu preporuka za pregovore o ugovoru o sajber-bezbednosti, koje su podnete generalnom sekretaru UN od strane 15 država, ukllјučujući stalne članice Saveta bezbednosti.

Za detaljniju raspravu o sajber-kriminalu videti Treći deo

Važan međunarodni pravni instrument koji se odnosi na sajber-bezbednost predstavlja Konvencija o sajber-kriminalu Saveta Evrope, koja je stupila na snagu 1. jula 2004. Neke zemlje su uspostavile bilateralne aranžmane; na primer, Sjedinjene Države imaju bilateralne sporazume o pravnoj saradnji po pitanjima kriminala sa preko 20 država.[57] Ovi sporazumi se takođe primanjuju u slučajevima sajber-kriminala.

Jedan pokušaj naučnika i nedržavnih aktera da se izradi nacrt međunarodnog sporazuma predstavlja Stenfordski nacrt konvencije o zaštiti od sajber-kriminala i terorizma. Ovaj nacrt preporučuje osnivanje jednog međunarodnog tela: Agencije za zaštitu informatičke infrastrukture (AIIP).

Pitanja

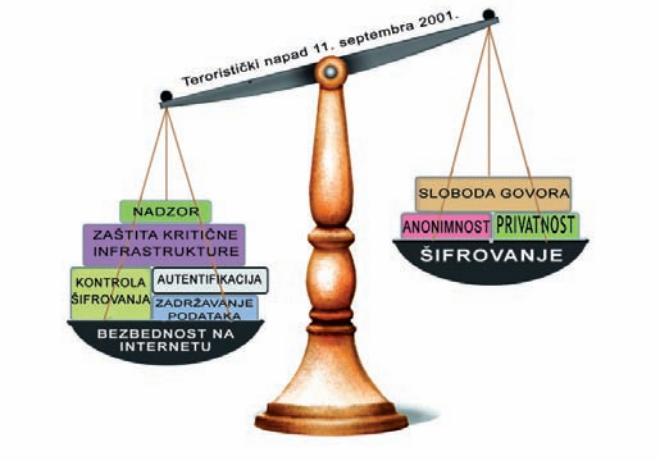
Uticaj arhitekture interneta na sajber-bezbednost

Sama priroda organizacije interneta pogađa njegovu bezbednost. Da li da nastavimo sa sadašnjim pristupom izgradnje bezbednosti na postojećim nebezbednim temeljima ili da promenimo bazu infrastrukture interneta? Kako bi se takva promena odrazila na druge karakteristike interneta, naročito na njegovu otvorenost i transparentnost? Najveći deo dosadašnjeg razvoja internet standarda imao je za cilj poboljšanje performansi ili uvođenje novih aplikacija; bezebdnost nije bila prioritet.

Nije jasno da li će WGIG biti sposobna da promeni standarde elektronske pošte za obezbeđivanje prave autentičnosti, da bi u krajnjem slučaju smanjila zloupotrebu interneta (npr. spem, sajber-kriminal). Obzirom na debatu koja okružuje sve promene vezane za osnovne standarde interneta, verovatno će poboljšanja kod osnovnog internetskog protokola u vezi sa bezebdnošću biti postepena i spora.

Budući razvoj elektronske trgovine zahteva visok nivo sajber-bezebdnosti

Sajber-bezbednost se često pominje kao jedan od preduslova za brz razvoj elektronske trgovine. Bez bezbednog i pouzdanog interneta, kupci neće biti raspoloženi da daju poverljive informacije, kao što su brojevi kreditnih kartica. Isto važi za onlajn bankarstvo i za korišćenje elektronskog novca. Ako se opšta sajber-bezbednost bude sporo poboljšavala (sa, na primer, nedostatkom standarda), verovatno će poslovni sektor tražiti brže promene. To može voditi ka daljim izazovima u odnosu na princip mrežne neutralnosti i ka razvoju 'novog interneta', koji bi, između ostaloga, omogućio bezbedniju komunikaciju.



Sajber-bezebdnost i privatnost

Drugo pitanje o kojem se raspravlja jeste odnos između bezbednosti i privatnosti. Da li će dodatne mere u vezi sa sajber-bezbednošću podrazumevati izvestan gubitak privatnosti? Kakva regulativa bi trebalo da se primeni na softver kodiranja, koji se može koristiti i za legitimnu zaštitu komunikativne privatnosti i za zaštitu komunikacije od terorista i kriminalaca? Odgovori na ova i druga pitanja zavise od stalnog pomeranja balansa između sajber-bezebdnosti i privatnosti.

Posle terorističkog napada u Njujorku, septembra 2001, bezbednost je postala prioritet, što se odrazilo u usvajanju raznih nacionalnih zakona koji su, između ostalog, određivali više nivoe kontrole interneta. Reakcija civilnog društva koncentrisala se na opasnosti po privatnost i na koncept pojam izražavanja.

Za dalju raspravu o slobodi izražavanja videti Šesti deo

Na međunarodnom nivou, pitanje balansiranja sajber-bezbednosti sa zaštitom privatnosti našlo se u centru rasprava vezanih za proširenje Konvencije Saveta Evrope o sajber-kriminalu na globalni nivo. Glavna primedba boraca za ljudska prava odnosi se na činjenicu da se Konvencija bavi pitanjima sajber-bezbednosti na uštrb zaštite privatnosti i drugih ljudskih prava.

Kodiranje

Jedno od centralnih pitanja rasprave o bezbednosti interneta jeste kodiranje, koje se bavi sredstvima koja se mogu koristiti za zaštitu podataka komunikacije.

Softver za kodiranje ispretura elektronske komunikacije (mejlove, slike) u nečitak tekst koristeći matematičke algoritme. Ovde problem ostaje balans između potrebe da neke informacije ostanu poverljiva i potrebe vlada da nadgledaju mogući kriminal i terorističku aktivnost.

Međunarodni aspekti politike kodiranja relevantni su za raspravu o upravljanju internetom utoliko što bi trebalo da regulativa kodiranja bude globalna, ili barem da uključi one zemlje koje mogu da proizvode sredstva kodiranja.

Na primer, američka politika izvozne kontrole softvera kodiranja nije bila mnogo uspešna zato što nije mogla da kontroliše svoju međunarodnu distribuciju. Američke softverske kompanije inicirale su snažnu kampanju lobiranja, tvrdeći da izvozne kontrole ne povećavaju nacionalnu bezbednost, već da pre podrivaju američke poslovne interese.

Međunarodni režimi za sredstva kodiranja

Kodiranje je predmet bavljenja u dva konteksta: u okviru Vasenarskog sporazuma i OECD-a. Vasenarski sporazum je međunarodni režim koji su usvojile 33 industrijske zemlje da bi ograničile izvoz konvencionalnog naoružanja i tehnologija koje se mogu zloupotrebiti u zemlje koje se nalaze u ratu ili se smatraju 'neprijateljskim zemljama'. Ovim sporazumom osnovan je sekretarijat u Beču. Lobiranje SAD kod Vasenarske grupe imalo je za cilj širenje 'kliperovskog pristupa'[58] na međunarodni plan, kontrolisanjem softvera kodiranja preko tajnog algoritma (key escrow). Ovome su se suprotstavile mnoge zemlje, naročito Japan i skandinavske države.

Do kompromisa je došlo 1998. godine uvođenjem kriptografskih smernica, što je podrazumevalo kontrolnu listu dvojne upotrebe proizvoda hardverske i softverske kriptografije iznad 56 bita. Ovo proširenje uključivalo je internetska sredstva, kao što su pretraživači veba i elektronske pošte. Interesantno je zapaziti da ovaj aranžman ne pokriva 'nedodirljive' transfere, kao što je preuzimanje fajlova. Propust da se uvede međunarodna verzija Klipera doprineo je povlačenju ovog predloga i unutar samih SAD. U ovom primeru veze između nacionalnih i međunarodnih arena, međunarodni tokovi imali su odlučujući uticaj na nacionalne.

OECD je drugi forum za međuanrodnu saradnju na polju kodiranja. Iako OECD ne donosi pravno obavezujuće dokumente, njegove smernice po raznim pitanjima veoma se cene. One su rezultat stručnog pristupa i procesa donošenja odluka koji se zasniva na konsenzusu. Većina ovih smernica na kraju je ugrađena u nacionalne zakone. Pitanje kodiranja bilo je veoma prisutna tema u aktivnostima OECD-a. Ono je inicirano 1996, s predlogom Sjedinjenih Država za usvajanje tajnog algoritma kao međunarodnog standarda. Slično Vasenaru, pregovori o američkom predlogu da se usvoji tajni algoritam kod međunarodnih standarda naišli su na žestoko protivljenje Japana i skandinavskih zemalja. Rezultat toge bila je kompromisna specifikacija glavnih elemenata politike kodiranja.

Nekoliko pokušaja da se razvije međunarodni režim kodiranja, uglavnom u kontekstu Vasenarskog sporazuma, nije rezultiralo razvojem efektivnog međunarodnog režima. Još uvek je moguće dobiti snažan kodni softver na internetu.

Spem

Trenutna situacija

Spem se obično definiše kao netražena elektronska pošta, koja se prosleđuje velikom broju korisnika interneta. Iako se uglavnom koristi za komercijalnu promociju, ostale njene upotrebe podrazumevaju društvene aktivnosti, političke kampanje i distribuciju pornografskog materijala. Spem se svrstava u infrastrukturnu korpu zato što pogađa normalno funkcionisanje interneta ometajući jednu od glavnih aplikacija interneta: elektronsku poštu. Predstavlja jedno od pitanja vezanih za upravljanje internetom koje pogađa gotovo sve one koji su povezani na internet. Prema statistici iz 2009. godine, 81% saobraćaja elektronske pošte predstavlja spem. Obim spema između 2008. i 2009. povećao se za 24%. Pored činjenice da je neugodan za korisnike, spem uzrokuje znatne ekonomske gubitke, kako u pogledu korišćenog propusnog obima tako i u pogledu izgubljenog vremena na njegovoj proveri/brisanju.

Protiv spema se može boriti tehničkim i pravnim sredstvima. Što se tiče tehničke strane, na raspolaganju se nalaze mnoge aplikacije za filtriranje poruka i otkrivanje spema. Glavni problem kod sistema za filtriranje jeste da su poznati i po brisanju poruka koje ne spadaju u spem. Antispem industrija je sektor u naglom razvoju, sa sve više prefinjenih aplikacija koje su sposobne da razlikuju spem od pravih poruka. Tehnički metodi imaju samo ograničen efekat i zahtevaju dodatne zakonske mere.

Što se tiče pravne strane, mnoge su države reagovale uvođenjem zakona protiv spema. U SAD, zakon Can-Spam uključuje finu ravnotežu između promocije zasnovane na elektronskoj pošti i sprečavanja spema.[59] Iako ovaj zakon propisuje stroge kazne za distribuciju spema, uključujući i zatvor do pet godina, neke od njegovih odredbi, po mišljenju kritičara, tolerišu ili čak podstiču spem aktivnosti. Početna, pogrešna pozicija izneta u ovom zakonu glasi da je spem dozvoljen dok primalac spem poruka ne kaže 'stop', tj. koristi se klauzula ili-ili. Od usvajanja ovog zakona 2003, statistika korišćenja spema ne pokazuje smanjenje broja spem poruka.

U julu 2003, EU je uvela sopstveni antispem zakon kao deo uputstva o privatnosti i elketronskim komunikacijama. Zakon EU podstiče inicijative samoregulisanja i privatnog sektora koje bi dovele do smanjenja

Spem i 'politički metod'

Spem je ilustrativan primer trendova i ponekad metoda u globalnoj politici. Godine 2005, spem je naveden kao važno pitanje vezano za upravljanje internetom u Izveštaju WGIG-a. O spemu se raspravljalo na WSIS-u u Tunisu, kao i na brojnim međunarodnim susretima. O njemu se često raspravljalo i u medijima.

Od 2005. godine, obim spema se povećao šest puta, i to prema opreznim procenama (2005: 30 milijardi poruka dnevno; 2010: 183 milijarde poruka dnevno). Politički značaj spema ne prati ovaj trend. Sada spem ima vrlo nisku vidljivost u procesima globalne politike. Na IGF-u 2009. u Šarm el Šeiku, nije bilo nijedne radionice ili sesije koja je raspravljala o spemu. Značaj spema za globalnu politiku očito tek treba da se otkrije.

spema.[60] U novembru 2006, Evropska komisija usvojila je Saopštenje o borbi protiv spema, špijuniranja i zlоćudnog softvera. Ovo saopštenje identifikuje veći broj akcija za promovisanje primene i sprovođenja postojećeg zakonodavstva, navedenog gore, budući da se nedostatak sprovođenja sagledava kao glavni problem.[61]

Međunarodni odgovor

I antispem zakoni usvojeni u SAD i oni u EU imaju jednu slabost: nedostatak odredbe za sprečavanje prekograničnog spema. Ovo pitanje naročito je značajno za neke zemlje, kao što je Kanada, koja prema najnovijoj ststistici dobija 19 od 20 spem poruka iz inostranstva. Kanadski ministar industrije, Lisjen Robijar, konstatovao je da se ovaj problem ne može rešiti na bazi pojedinačnog odnosa između država. Potrebno je globalno rešenje, koje će se primenjivati kroz jedan međunarodni ugovor ili preko nekog sličnog mehanizma.

Memorandum o razumevanju (MoU) koji su potpisale Australija, Koreja i UK jedan je od prvih primera međunarodne saradnje u antispem kampanji.

OECD je osnovao radnu grupu za spem i pripremio antispem alat. ITU je takođe bila aktivna organizovanjem Tematskog sastanka o suzbijanju spema (2004) radi razmatranja raznih mogućnosti osnivanja MoU za borbu protiv spema. Na regionalnom nivou, EU je osnovala Mrežu agencija za borbu protiv spema, a APEK (Azijsko-pacifička ekonomske kooperacija) je pripremio set smernica za potrošače.

Drugi mogući antispem pristup preduzele su vodeće internetske kompanije koje daju elektronske računovodstvene izveštaje: Amerika onlajn, Britiš telekom, Komkast, ErtLink, Majkrosoft i Jahu! One su osnovale Antispem tehničku alijansu (ASTA) sa glavnim zadatkom da koordinira tehničke i antispem aktivnosti vezane za politiku.

Pitanja

Različite definicije spema

Različita razumevanja spema štetno deluju na antispem kampanju. U SAD, opšta zainteresovanost za zaštitu slobode govora i Prvi amandman pogađaju antispem kampanju. Američki zakonodavci smatraju da je spem samo 'netražena elektronska pošta', izostavljajući druge vrste spema u koje spada politički aktivizam i pornografija. U većini zemalja, spem se smatra 'preobimnom netraženom elektronskom poštom' bez obzira na sadržaj. Kako najveći deo spema nastaje u SAD, ova razlika u definiciji ozbiljno ograničava svaku mogućnost uvođenja efikasnog međunarodnog antispem mehanizma.

Spem i ustanovljenje autentičnosti elektronske pošte

Jedna od strukturnih prednosti spema jeste mogućnost slanja mejlova s lažnom adresom pošiljaoca. Postoji mogućnost za tehničko rešenje ovog problema, koje bi zahtevalo promene postojećih internet standarda vezanih za elektronsku poštu. RGUI radi na uvođenju promena u protokol elektronske pošte, što bi obezbedilo ustanovljenje autentičnosti mejlova. Ovo je primer kako tehnička pitanja (standardi) mogu da utiču na politiku. Moguće rešenje koje bi uvođenje ustanovljenja autentičnosti elektronske pošte donelo jeste ograničenje anonimnosti na internetu.

Potreba za globalnom akcijom

Najveći deo spema dolazi u dotičnu zemlju spolja. U pitanju je globalni problem koji zahteva globalno rešenje. Postoje razne inicijative koje bi mogle dovesti do poboljšane globalne saradnje. Neke od njih, kao što su bilateralni MoU, već su pomenute. Druge podrazumevaju akcije kao što je izgradnja kapaciteta i razmena informacija. Obuhvatnije rešenje podrazumevalo bi neku vrstu globalnog antispem instrumenta. Do sada, razvijene zemlje radije se opredeljuju za nacionalne zakonske propise, skupa sa bilateralnim ili regionalnim antispem kampanjama. Obzirom na nepovoljnu poziciju primanja 'globalnog javnog đubreta', većina zemalja u razvoju zainteresovana je za oblikovanje globalnog odgovora na problem sa spemom.

Fusnote

1 Termini 'internet' i 'WWW' ponekad se koriste naizmenično; međutim, postoji razlika. Internet je ogromna mreža mreža; ona pokriva više različitih servisa. Ponekad se termin 'internet' koristi da obuhvati sve, uključujući infrastrukturu, aplikacije (mejlove, ftp, Veb) i sadržaj. WWW je samo jedna od mnogih internet aplikacija, sistem međusobno povezanih dokumenata koji se povezuju uz pomoć HTTP-a (protokola prenosa hipertekstualnih dokumenata).

2 Prenos interneta preko električne mreže zove se komunikacija preko dalekovoda (PLC). Korišćenje strujne mreže učinilo bi internet pristupačnijim mnogim korisnicima. Za tehnički i organizacioni pregled ovog mehanizma pogledati: Internet Society (2003) *Addressing the digital divide Ipvb-enabled broadband power line communications.* ISOC Member Briefing No. 13. Dostupno na: **http://www.isoc.org/briefings/013/**

3 Liberalizacija telekomunikacionih tržišta članica STO formalizovana je 1998. godine u Osnovnom telekomunikacionom sporazumu (BTA). Posle usvajanja BTA, preko 100 zemalja započelo je proces liberalizacije, koji karakterišu privatizacija nacionalnih telekomunikacionih monopola, uvođenje konkurencije i osnivanje nacionalnih nadležnih organa. Ovaj sporazum se formalno naziva Četvrti protokol opšteg ugovora o trgovini u uslugama (usvojen 30. aprila 1996. i stupio na snagu 5. februara 1998). Dostupno na: **http://www.wto.org/english/tratop_e/serv_e/4prote_e.htm**

4 Za više informacija o ulozi STO u oblasti telekomunikacija, videti: **http://www.wto.org/english/tratop_e/serv_e/telecom_e/telecom_e.htm**

5 Vlada uverenje da države mogu da dobiju više prihoda od tržišnog monopola nacionalnih operatera; protivnici tvrde da liberalizacijom tržišta ukupna tržišna vrednost raste, donoseći tako više prihoda državi nego u slučaju monopola.

6 Važeći regionalni internetski registri su: ARIN (American Registry for Internet Numbers), APNIC (the Asia Pacific Network Information Centre), LACNIC (the Latin American and Carribean IP Address Regional Registry), RIPE NCC (Reseaux IP Européens Network Coordination Centre – koji pokriva Evropu i Srednji istok) i AFRINIC (the African Network Information Centre). Detaljno objašnjenje sistema RIR dostupno je na: **https://www.ripe.net/info/resource-admin/rir-system.html**

7 Za detaljnu raspravu o IPv6, videti: Kissangou JP, Guthrie M, Njiraini M (2005) *IP allocation and IPv6*, deo programa o izgradnji kapaciteta upravljanja internetom. Dostupan na: **http://textus.diplomacy.edu/Textusbin/portal/Ghome.asp?IDspace=84**

8 Obuhvatan i visokotehnički pregled TCP/IP bezbednosti, videti: Chambers C, Dolske J, Iyer J (ND) *TCP/IP Security, Department of Computer and Inforamtion Science*, Ohio State University: Columbus, OH, USA. Dostupno na: **http://www.linuxsecurity.com/resource_files/documentation/tcpip-security.html**

9 Abbate J (1999) *Inventing the Internet.* MIT Press: Cambridge, MA, USA.

10 Opšti pregled gTLD povezan sa spiskom svih TLD (domena najvišeg nivoa) dostupan je na: **http://www.icann.org/registries/about.htm**

11 Jedan prethodni primer domena koji se odnose na sadržaj je kids.us domain. Američki kongres usvojio je zakon kojim je uveo domen rezervisan za sadržaje za decu. Glavnu poteškoću u vezi s ovim predlogom predstavlja određenje činjenice šta je sadržaj poželjan za decu. Moglo bi da dođe do konceptualnih i praktičnih problema koji se odnose na kontrolu sadržaja. Do sada je 'kids' domen korišćen samo kao deo domena SAD.

12 Za vreme rasprava o .xxx domenu, Vlada SAD nije sledila procedure ICANN-a o donošenju odluka. Američko protivljenje izraženo je pismom koje je Ministarstvo trgovine uputilo predsedavajućem ICANN-a.

13 Obrazac aplikacije za registraciju .cat domena dostupan je na: **http://www.icann.org/tlds/stld-apps-19mar04/cat.htm**

14 Izveštaj IANA o ccTLD-u za Palestinu dostupan je na: **http://www.iana.org/reports/ps-report-22mar00.htm**

15 Na primer, Južna Afrika je iskoristila svoja suverena prava kao argument za vraćanje kontrole nad svojim državnim domenom. Novodoneti zakon precizira da će se korišćenje državnog domena van parametara koje je propisala južnoafrička vlada smatrati kriminalom. Brazilski model upravljanja državnim domenom obično se navodi kao uspešan primer multiakterskog pristupa. Nacionalno telo odgovorno za brazilski domen otvoreno je za sve ključne igrače, uključujući vladine predstavnike, poslovni sektor i civilno društvo. Kambodžanski prenos upravljanja državnim domenom sa nevladine na vladinu kontrolu često se navodi kao primer neuspešne tranzicije. Vlada je smanjila kvalitet usluga i uvela veće takse, što je otežalo registraciju kambodžanskih domena. Za više informacija, videti: Alfonso CA (2004) BR: CCTLD An Asset of the commons, na *Internet Governance: A grand collaboration.* MacLean D (ed.). UNICT Task Force: New York, NY, USA, str. 291-299; Klein N (2004) Internet governance: Perspectiev from Cambodia, na *Internet Governance: A grand collaboration.* op. cit.

16 ICANN (2000) *Principles for the Delegation andAdministartion of Country Code Top-Level Domains,* trenutno u fazi prerade. Dostupno na: **http://www.icann.org/committees/gac/gac-cctldprinciples-23feb00.htm**

17 Spisak glavnih zonskih servera, njihovih režima i položaja, kao i rukovodećih organizacija dostupan je na: **http://www.root-servers.org/**

18 ICANN (2009) Dostupno na: **http://www.icann.org/en/announcement/announcement-30sep09-en.htm**

19 Deo o mrežnoj neutralnosti zasnovan je na radovima Vladimira Radunovića, koordinatora projekta o upravljanju internetom DiploFondacije.

20 U dugoj istoriji interneta, Sjedinjene Države nisu nikad blokirale pristup nekoj drugoj zemlji, uključujući sukobljene strane. U nekim slučajevima, kao što je rat na Kosovu, režim sankcija UN dao je Sjedinjenim Državama pravnu mogućnost presecanja telekomunikacionih veza sa Srbijom. One nisu iskoristile ovu pravnu mogućnostn i Srbija je imala pristup internetu tkom celog konflikta.

21 Arington M (2009) JuTjub video dostiže vrhunac sa 1.2 miliona dnevno. Dostupno na: **http://techcrunch.com/2009/06/09/youtube-video-streams-top-1-billionday/**

22 Broadcasting Ourselves. The office YouTube Blog (2009) Zoinks! 20 časova video zapisa prenosi se svakog minuta! Dostupno na: **http://youtube-global.blogspot.com/2009/05/zoinks-20-hours-of-video-uploaded-every_20.htlm**

23 Amerika insistira na neutralnosti mreže: prava bita. The Economist 24 September 2009.

24 Ovaj slučaj imao je nekoliko preokreta. Za dodatne informacije o pozadini predmeta, videti: Broache A (2008) FCC wants to know: Is degrading P2P traffic 'reasonable'? Cnet News Blog. Dostupno na: **http://news.cnet.com/8301-10784_3-9850611-7.html?tag=mncol;txt**
Najnovije ažuriranje predstavljala je odluka suda protiv prethodne odluke FCC. Videti: Kang C (2010) Court rules for Comcast over FCC in 'net neutrality' case. The Washington Post, 7 April. Dostupno na: **http://www.washingtonpost.com/wp-dyn/content/article/2010/04/06/AR2010040600742.html**

25 Grupa Spasi internet je naročito aktivna u propagiranju mrežne neutralnosti kao očuvanja slobodnog i otvorenog interneta. Dostupno na: **http://www.savetheinternet.com/**

26 Kokus upravljanja internetom (IGC) originalno su stvorili individualni i organizacioni aktivisti civilnog društva koji su se spojili u kontekstu WSIS-a da bi propagirali ciljeve globalnog javnog interesa u kreiranju politike upravljanja internetom. Dostupno na: **www.igcaucus.org**

27 Džon Herman ilustruje ponude paketa koje često koriste zagovornici mrežne neutralnosti. Dostupno na: **http://gizmodo.com/5391712/net-neutrality-worst-case**

28 *La Quadrature du Net,* zastupnička grupa koja propagira prava i slobode građana na internetu, navodi u otvorenom pismu Evropskom parlamentu o mrežnoj neutralnosti: *svako na svetu ima pristup istom internetu, pa se čak i najmanji preduzetnici nalaze na ravnoj nozi s vodećim globalnim preduzetnicima.* Dostupno na: **http://www.laquadrature.net/en/we-must-protect-net-neutrality-in-europe-open-letter-to-the-european-parliament#**

29 Ogg E (2010) Report: Google, Verizon reach Net neutrality deal. Cnet 4. avgust. Dostupno na: **http://news.cnet.com/8301-31021_3-20012703-260.htlm?tag=mncol;mlt_related**

30 Oni elementi koji su još sporni i o kojima će se pregovarati u budućnosti nalaze se u uglatim zagradama.

31 Izveštaji sa ovih susreta, kao i drugi relevantni materijali o mrežnoj neutralnosti, dostupni su na: **www.diplomacy.edu/ig/nn**

32 FCC (2005) Referat o vođenju mreže i o njenoj neutralnosti. Dostupno na: **http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-05-151A1.pdf**

33 Ministarstvo unutrašnjih poslova i komunikacija, Japan (2007) *Report on Network Neutrality.* Dostupno na: **www.soumu.go.jp/main_sosiki/joho_tsusin/eng/pdf/070900_1.pdf**

34 PTS (2009) *Open Networks and Services.* Dostupno na: **http://www.pts.se/en-gb/Documents/Reports/Internet/2009/Open-Networks-and-Services---PTS-ER-200932/**

35 Kroes N (2010) *Net neutrality in Europe.* Govor koji je održao potpredsednik Evropske komisije za digitalni program. Dostupno na: **http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/10/153&format=HTML&aged=0&language=EN&guiLanguage=en**

[36] NPT (2009) *Net neutrality: Guidelines for Internet neutrality.* Dostupno na: **http://www.npt.no/ikbViewer/Content/109604/Guidelines%20for%20network%neutrality.pdf**

[37] Anderson N (2009) Norway gets net neutrality – voluntary, but broadly supported. *Ars Technica*. Dostupno na: **http://arstechnica.com/tech-policy/news/2009/02/norway-gets-voluntary-net-neutrality.ars**

[38] ISOC smatra da je mrežna neutralnost prilično loša definicija, pa govori o trajnom otvorenom mrežnom međupovezivanju. Dostupno na: **http://www.isoc.org/pubpolpillar/usercentricity/openinternetworking.shtml.** U njegovim javnim konsultacijama o mrežnoj neutralnosti od 16. maja 2010. navodi se: *Umesto prostog fokusiranja na dijapazon mogućih definicija mrežne neutralnosti, Internetsko društvo veruje da je prikladnije koncentrisati se šire na imperativ očuvanja otvorenog internetskog modela usmerenog na korisnike, koji je do sada bio tako uspešan.* Dostupno na: **http://www.isoc.org/regions/europe/docs/neutrality_20100516_en.pdf**

[39] *TACD calls for Net Neutrality.* Dostupno na: **http://tacd.org/index.php?option=com_content&task=view&id=162&Itemid=43**

[40] Williams F (2006) ISP-ovi bi trebalo da budu odgovorni za spem, kaže se u izveštaju UN. Financial Times, 8. novembar. Dostupno na: **http://www.qlinks.net/quicklinks/spam.htm**

[41] Shannon V (2006) The end user: Junk payout in spam case. *Internet Herald Tribune*, 13. april. Dostupno na: **http://www.iht.com/articles/2006/04/12/business/PTEND13php**

[42] Izjednačavanje (uređaja) je 'bilateralni sporazum koji sklapaju mrežni operateri da bi međusobno garantovali pristup svojih klijenata bez ikakvih troškova', kako je definisala HSC grupa (**www.hscgroup.co.uk**). Ovakav aranžman pruža obostranu korist i često se sklapa među provajderima internetskih usluga, kao i među telekomskim operaterima.

[43] IBP-ovi sloja 2 obično se nazivaju tačke internetskog povezivanja (ICP) ili internetske kapije (gejtveji).

[44] Endru Odlisko sagledava pitanje određivanja cena i arhitekture na internetu iz istorijske perspektive. Vukući nit politike cena iz određivanja cena u transportnim sistemima starog sveta, on je povezuje sa trenutnom politikom cena na internetu. Odlyzko A (2004) *Pricing and architecture of the Internet: Historical perspectives from telecommunications and transportation.* University of Minnesota: Minneapolis, MN, USA. Dostupno na: **http://www.dtc.umn.edu/~odlyzko/doc/pricing.arhitecture.pdf**

[45] Šon O'Donel, u članku *An economic map of the Internet,* daje analizu protoka internetskog dolara, objašnjavajući kud ide novac korisnika provajdera internet usluga. Dostupno na: **http://ebusiness.mit.edu/research/papers/162_ODonnell_Map.pdf**

[46] Nguyen TT, Armitage GJ (2005) Evaluating Internet pricing schemes: A three-dimensional visual model. *ETRI Journal* 27:64-74.

[47] Vebsajt tržišta propusnog opsega je onlajn tržište internet resursa, koje nudi propusni opseg, pristup internetu i druge resurse interneta. Dostupno na: **http://www.bandwidthmarket.net/**

[48] Huston G (2005) Gde je novac? Internetska međupovezanost i finansijski aranžmani. ISP Column, Internet Society. Dostupno na: **http://ispcolumn.isoc.org/2005-01/interconns.pdf**

49 AfrISPA (2002) Kompromisan predlog: Propratni referat o obrnutim subvencijama zemalja G8 od strane afričkih PIU, pročitan na Konferenciji afričkih ministara finansija, planiranja i ekonomskog razvoja, u Johanezburgu, Južna Afrika, 19. oktobar 2002. Dostupno na: **http://www.wougnet.org/WSIS/ug/WSIS2005/docs/HalfwayProposition_Draft4.pdf**

50 Za iscrpan uvid u troškove međupovezivanja, videti: Esmat B, Fernandez J (2006) International Internet Connection Costs, u Drake WJ (2006) *Reforming Internet Governance: Perspectives from the Working Group on Internet Governance (WGIG)*. WGIG: New York, NY, USA, str. 73-86. Dostupno na: **http://www.wgig.org/book-Launch.html**

51 Iscrpnu analizu ove teme možete naći kod Jensen M (2005) Interconnection Costs. APC: Melville, Južna Afrika. Dostupno na: **http://www.apc.org/en/pubs/issue/accessibility/all/interconnection-costs**

52 Huston (2005) *op. cit.* str. 7-9.

53 Jedno od ograničenja pregovora o ovom pitanju između vlada jeste to što se sporazumi o međupovezivanju zaključuju između privatnih telekomunikacionih operatera. Oni su često poverljivi

54 ACLU White paper (ND) *No Competition: How monpoly control of broadband Internet threatens free speech*. ACLU: New York, NY, USA.

55 Za iscrpnije informacije o Programu ITU za globalnu sajber-bezebdnost, videti: **http://www.itu.int/osg/csd/cybersecurity/gca/**

56 Tekst Konvencije dostupan je na: **http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm**

57 Zvaničan naziv ovih instrumenata glasi Ugovori o uzajamnoj pravnoj pomoći po krivičnim pitanjima (MLAT).

58 Kliperovski pristup je predložila Vlada SAD još 1993. godine. Njegova suština svodila se na upotrebu kliperovskog čipa koji je trebalo da bude upotrebljen kod svih telefona i drugih govornih sredstava komunikacije. Kliperovski čip je imao 'zadnja vrata' koja su vlade mogle da koriste za zakonitu kontrolu. Posle snažnog suprotstavljanja boraca za ljudska prava i javnog mnjenja, Vlada SAD je odustala od ovog predloga 1995. godine. Videti: Denning D (1995) The Case of clipper. *MIT Technology Review*. MIT: Cambridge, MA, USA. Dostupno na: **http://encryption_policies.tripod.com/us/denning_0795_clipper.htm**

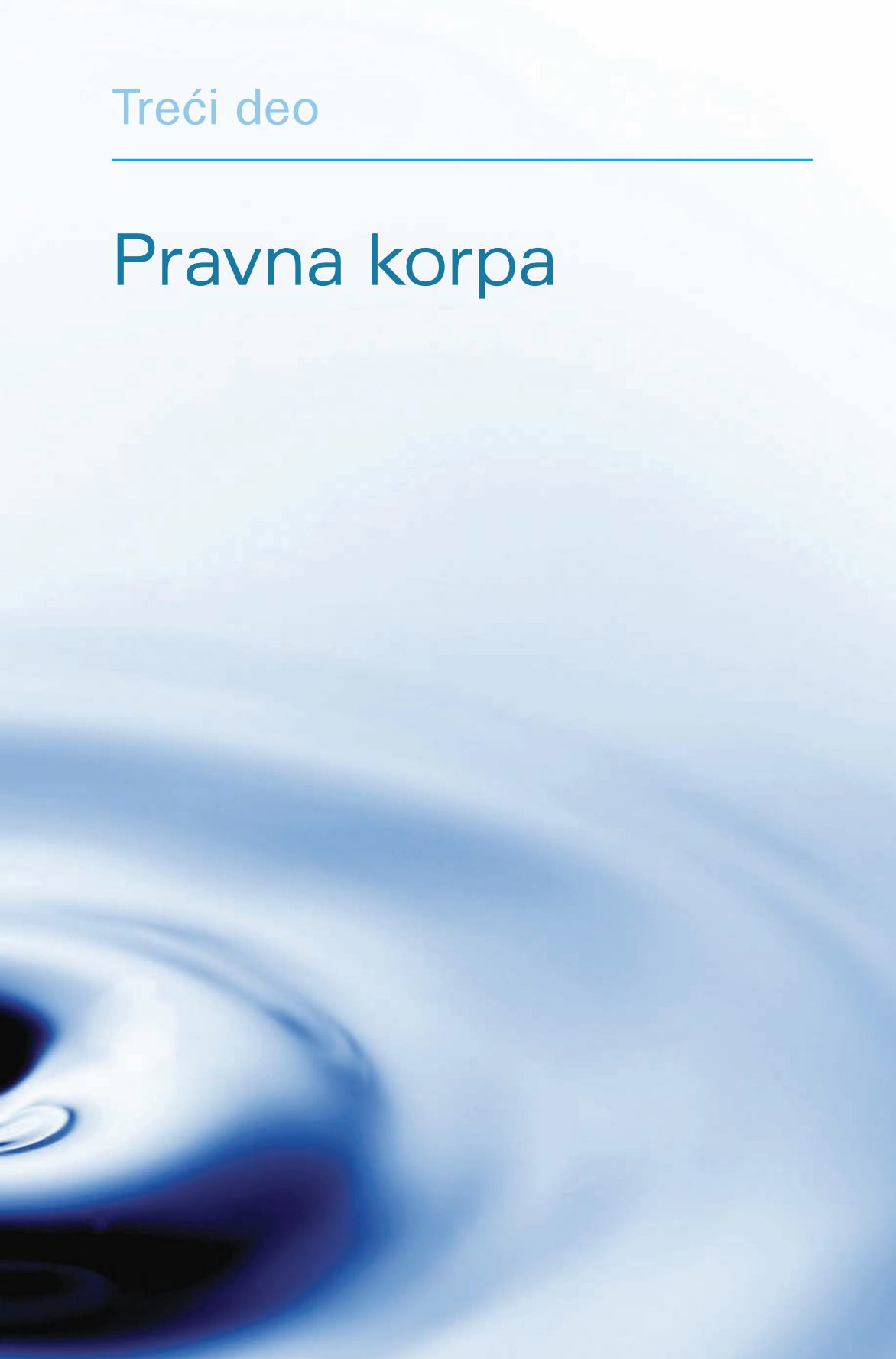
59 Više informacija o zakonu Can-Spam dostupno na: **http://www.ftc.gov/bcp/edu/pubs/business/ecommerce/bus61.shtm**

60 Kontaktnu mrežu između vlasti za suzbijanje spema (CNSA) osnovalo je u februaru 2005. trinaest zemalja EU (Francuska, Austrija, Belgija, Kipar, Češka Republika, Danska, Grčka, Irska, Italija, Litvanija, Malta, Ujedinjeno Kraljevstvo i Španija). Njen cilj je unapređenje saradnje među ovim državama i koordinacija sa organizacijama van EU, kao što su OECD i ITU.

61 European Commission, Information Society (2010). Unsolicited communication: fighting spam. Dostupno na: http://ec.europa.eu/information_society/policy/ecomm/todays_framework/privacy_protection/spam/index_en.htm

Treći deo

Pravna korpa



Pravna korpa

Gotovo sva pitanja u vezi sa upravlajnjem internetom imaju pravni aspekt, pa ipak oblikovanje pravnog okvira u cilju usmeravanja brzog razvoja interneta još se nalazi u ranim fazama.

1. Pristup 'postojećeg prava', gde se internet u suštini tretira jednako kao prethodne telekomunikacione tehnologije, u dugoj evoluciji od dimnih signala do telefona. Iako brži i obuhvatniji, internet još uvek podrazumeva komunikaciju između pojedinaca na daljinu. Sledstveno tome, sva postojeća pravna pravila mogu se primeniti i na internet.[1,2]
2. 'Sajber-pravo' se zasniva na pretpostavci da internet uvodi nove vrste društvenih odnosa u sajber-prostoru. Shodno tome, postoji potreba za formulacijom sajber-zakona da bi se olakšalo regulisanje sajber-prostora. Jedan argument za ovaj pristup predstavlja činjenica da sama brzina i obim prekogranične komunikacije putem interneta sprečava primenu postojećih pravnih propisa.

Iako oba pristupa sadrže valjane elemente, prednost se daje 'postojećem pravu'. Postoji opšte shvatanje da znatan deo postojećeg zakonodavstva može da se primeni na internet. Za neka pitanja, postojeći zakoni bi morali da se prilagode da bi mogli da se primenjuju na sajber-svet. Za neka, ograničena pitanja, moraju se osmisliti nova pravila.

Pravni instrumenti

Postoji mnogo pravnih instrumenata koji se već primenjuju ili bi mogli da se primenjuju na upravljanje internetom

Pravni instrumenti na nivou država i širih zajednica

Zakonodavstvo

Svako zakonodavstvo sastoji se od propisa i sankcija. Propisi predviđaju neka društveno prihvatljiva ponašanja (npr. ne čini prekršaje, plaćaj poreze), a sankcije određuju kazne u slučaju da se propisi ne poštuju (npr. novčane kazne, zatvor, u nekim društvima i smrtne kazne).

Zakonodavne aktivnosti sve više se pojačavaju u oblasti interneta. To je posebno slučaj u zemljama Organizacije za ekonomsku saradnju i razvoj (OECD), gde je internet raširen i gde ima visok stepen uticaja na ekonomske i društvene odnose. Prioritetna područja zakonodavne regulative su privatnost, zaštita podataka, intelektualna svojina, oporeziavnje i sajber-kriminal.

Ipak, društveni odnosi su odveć složeni da bi ih mogli regulisati samo zakonodavci. Društvo je dinamična kategorija i zakonodavstvo uvek zaostaje iza promena. To je naročito uočljivo u ovom našem vremenu, kada tehnološki razvoj preoblikuje društvenu stvarnost mnogo brže nego što zakonodavci uspevaju da reaguju. Ponekad propisi postaju zastareli i pre nego što budu usvojeni. Opasnost od zakonske zastarelosti predstavlja važnu činjenicu kod regulisanja interneta.

Društvene norme (običaji)

Poput zakonodavstva, društvene norme propisuju određen način ponašanja. Za razliku od zakonodavstva, ove norme ne nameće nikakva državna vlast. Njih nameće zajednica vršeći pritisak preko ravnopravnih računara. Korišćenje interneta u početku je bilo regulisano nizom društvenih normi nazivanih 'netikecija', gde su pritisak ravnopravnih računara i isključivanje bili glavne sankcije. Tokom tog perioda, u kojem su internet koristile relativno male, uglavnom akademske zajednice, uglavnom su se poštovali društveni propisi. Razvoj interneta učinio je te propise neefikasnim. Međutim, ova vrsta regulative može se još koristiti unutar ograničenih grupa sa jakim zajedničkim vezama.

Postojeće pravo nasuprot sajber-pravu

Bez obzira na to koji pristup je prikladniji – postojeće ili sajber-pravo – opšti princip ostaje da **zakoni ne onemogućavaju zabranjeno ponašanje, već ga samo čine kažnjivim.** Činjenica da je podvala zabranjena i u stvarnom i u sajber-svetu ne znači da će zato podvala biti iskorenjena. Ova distinkcija je važna zato što jedan od čestih argumenata za stvaranje posebnih sajber-propisa glasi da zabranjeno ponašanje (podvala, kriminal itd.) već preovlađuje u sajber-prostoru i da se propisi iz realnog prava ne mogu efikasno koristiti.

Samoregulisanje

Bela knjiga o upravljanju internetom američke vlade (iz 1998. godine) predlaže samoregulisanje kao poželjan regulatorni mehanizam za internet. Samoregulisanje ima elemenata koji se poklapaju sa prethodno opisanim društvenim normama. Glavna razlika leži u tome što se samoregulisanje, za razliku od društvenih normi koje tipično podrazumevaju difuzni regulatorni sistem, zasniva na ciljanom i dobro organizovanom pristupu. Samoregulativni propisi se obično kodifikuju u praktične kodekse ili kodekse dobrog ponašanja.

Težnja ka samoregulativi naročito je primetna kod provajdera internet usluga (ISP-ova). U mnogim zemljama, ISP-ovi se nalaze pod sve većim pritiskom vlasti za nametanje propisa koji se odnose na politiku sadržaja; oni sve više koriste samoregulativu kao metod nametanja određenih standarda ponašanja i, u krajnjem slučaju, da spreče mešanje vlasti u njihove aktivnosti.

Iako samoregulisanje može biti korisna regulatorna tehnika, ostaju neke opasnosti pri njenom korišćenju kod regulisanja oblasti od visokog javnog interesa, kao što je politika sadržaja. Ostaje da se vidi u kojoj će meri ISP-ovi biti sposobni da regulišu sadržaj na svojim veb-sajtovima. Mogu li oni da donose odluke umesto zakonitih vlasti? Mogu li da određuju šta je prihvatljiv sadržaj? Treba se pozabaviti i drugim pitanjima; kao što su pitanja slobode izražavanja i privatnosti.

Pravosudna nadležnost

Pravosudna nadležnost (jurisdikcija) čini važan element pravnog sistema SAD, prvi koji se bavi pravnim pitanjima interneta. U ovom sistemu, presedan stvara zakon, naročito u predmetima koji podrazumevaju regulisanje novih pitanja, kao što je internet. Sudije moraju da odlučuju u predmetima čak i ako nemaju potreban alat – zakonske propise.

Prvo zakonsko sredstvo koje sudije koriste jeste pravna analogija, gde se nešto novo dovodi u vezu s nečim poznatim. Većina pravnih predmeta u vezi s internetom rešava se putem analogija.

Međunarodni pravni instrumenti

Razlika između međunarodnog privatnog i međunarodnog javnog prava
Potreba za korišćenjem međunarodnog prava često se pokreće u raspravama o upravljanju internetom. Termin ‘međunarodno pravo’ uglavnom se koristi kao sinonim za međunarodno ‘javno pravo', koje uspostavljaju nacionalne države i međunarodne organizacije, obično usvajanjem ugovora i konvencija. Međutim, većina mogućih pravnih predmeta povezanih sa internetom

uključuje snažnu crtu privatnog prava, podrazumevajući takva pitanja kao što su ugovori i delikti. Za resavanje takvih predmeta, postoji potreba za korišćenje međunarodnog privatnog prava, za propisima koji su predviđeni u nacionalnom zakonodavstvu, ne u međunarodnim ugovorima.(3) Propisi međunarodnog privatnog prava preciziraju kriterijume za uspostavljanje primenjive jurisdikcije i prava u pravnim slučajevima sa stranim elementima (npr. pravni odnosi koji uključuju više subjekata iz različitih zemalja). Kriterijumi za sagledavanje primenjive jurisdikcije i prava uključuju vezu između individualne i nacionalne jurisdikcije (npr. nacionalnost, mesto boravka) ili vezu između naročite transakcije i nacionalne sudske nadležnosti (npr. gde je zaključen ugovor, gde je došlo do razmene).

Međunarodno privatno pravo

Obzirom na globalni karakter interneta, pravne rasprave u kojima učestvuju pojedinci i institucije iz različitih nacionalnih jurisdikcija vrlo su česte. Međutim, vrlo retko se međunarodno privatno pravo koristi kod rešavanja pitanja vezanih za internet, verovatno zato što je reč o procesima koji su obično složeni, spori i skupi. Glavni mehanizmi međunarodnog privatnog prava razvijeni su u vreme kada su prekogranične transakcije bile ređe i manje intenzivne, tako da je proporcionalno bilo manje predmeta koji su uključivali pojedince i pravne subjekte iz različitih jurisdikcija.

Međunarodno javno pravo

Međunarodno javno pravo reguliše odnose između država. Neki instrumenti međunarodnog javnog prava već se bave oblastima koje su od značaja za upravljanje internetom (npr. propisi vezani za telekomunikacije, konvencije o ljudskim pravima i međunarodni trgovinski ugovori). U ovom delu, analiza će se fokusirati na elemente međunarodnog javnog prava koji bi se mogli koristiti u oblasti upravljanja internetom, uključujući ugovore i konvencije, 'meko pravo' i *ius cogens* (obavezujuće pravo – bezuslovan norma).

Međunarodne konvencije

Glavni set konvencija o pitanjima vezanim za internet usvojila je ITU, pri čemu su Međunarodni telekomunikacioni propisi (1998) najvažniji za pripremu okvira telekomunikacione politike za dalji razvoj interneta. Pored konvencija ITU, jedina konevncija koja se bavi direktno pitanjima vezanim za internet jeste Konvencija o sajber-kriminalu Saveta Evrope. Međutim, mnogi drugi međunarodni pravni instrumenti bave se širim aspektima upravljanja internetom, kao što su ljudska prava, trgovina i prava na intelektualnu svojinu.

Međunarodno običajno pravo

Razvoj običajnih pravila uključuje dva elementa: opštu praksu *(consuetudo)* i priznanje da je takva praksa pravno obavezujuća *(opinio iuris)*. Za kristalizaciju opšte prakse obično je potreban dugi vremenski period.

Neki elementi običaja u nastajanju pojavljuju se u načinu na koji Vlada SAD vrši nadzor nad glavnim Internet serverima. Ona ima doslednu praksu neintervenisanja po pitanju nacionalnih domena u fajl sa osnovnim internet adresama smešten u zoni glavnih servera. Opšta praksa je prvi element kod sagledavanja običajnog prava. Ostaje da se vidi da li je takva praksa bila zasnovana na svesti Vlade SAD da je ona u skladu sa međunarodnim pravnim propisima (postojanje *opinio iuris*). Ako je to slučaj, postoji mogućnost prepoznavanja međunarodnog običajnog prava kod upravljanja delovima glavnog serverskog sistema interneta koji se bave državnim domenima drugih zemalja. Bilo bi teško proširiti takvo rezonovanje na pravni status gTLD-ova – generičkih domena najvišeg nivoa – (.com, .org, .edu, .net) koji ne uključuju druge zemlje.

Meko pravo

'Meko pravo' je često korišćen termin u raspravama o upravljanju internetom. Većina definicija mekog prava koncentriše se na ono što ono nije: nije pravno obavezujući instrument. Instrumenti mekog prava sadrže principe i norme pre nego naričite propise. Ono se obično nalazi u međunarodnim dokumentima kao što su deklaracije, smernice i ogledni zakoni.

Glavni dokumenti Svetskog samita o informacionom društvu (WSIS), uključujući Završnu deklaraciju, Plan akcije i regionalne deklaracije, imaju potencijal za razvoj nekih normi mekog prava. Ovi dokumenti nisu pravno obavezujući, ali su obično rezultat dugotrajnih pregovora i prihvatanja od svih zemalja. Opredeljenost koju države i drugi akteri ulažu u dogovaranje o instrumentima mekog prava i u postizanje potrebnog konsenzusa stvara prvi element kod sagledavanja, da takvi dokumenti znače nešto više od običnih političkih deklaracija.[4]

Meko pravo pruža izvesne prednosti pri bavljenju pitanjima upravljanja internetom. Prvo, ono predstavlja manje formalan pristup, ne zahtevajući zvaničnu opredeljenost država i, pritom, ne zahtevajući dugotrajne pregovore. Drugo, dovoljno je fleksibilno da olakšava proveru novih pristupa i prilagođava se brzim promenama u oblasti upravljanja internetom. Treće, meko pravo pruža veću šansu za višeakterski pristup nego što je to slučaj sa međunarodnim pravom koje je ograničeno na države i međunarodne organizacije.

Ius cogens

Ius cogens se opisuje u Bečkoj konvenciji o ugovronom pravu na sledeći način:

> *...norma, koju prihvata i priznaje međunarodna zajednica država u celini, od koje nije dozvoljeno nikakvo odstupanje i koja se može promeniti samo potonjom normom opšteg međunarodnog prava sa istim karakterom.*[5]

Profesor Braunlaj navodi sledeće primere pravila ius cogens:[6]

- Zabrana korišćenja sile.
- Zakon o genocidu.
- Princip rasne nediskriminacije.
- Zločini protiv čovečnosti.
- Propisi koji zabranjuju trgovinu robljem i gusarenje.

Kod upravljanja internetom, *ius cogens* bi moglo da se koristi za uvođenje nekih propisa, kao što je zabrana dečije onlajn pornografije.

Sudska nadležnost

Broj sporova vezanih za internet stalno se povećava i zato je pitanje sudske nadležnosti jedan od vrućih aspekata upravljanja internetom. Konfuzija u vezi sa sudskom nadležnošću može da ima dve neposredne i istovremene posledice:

1. nemoć države da vrši svoju zakonsku vlast kao odgovoran subjekt kod regulisanja društvenih odnosa na svojoj teritoriji; i
2. nemoć pojedinaca i pravnih subjekata da koriste svoja prava na pravdu (negacija pravde).

Druge posledice dvosmislene jurisdikcije mogle bi biti:

- Pravna nesiguirnost na internetu, uključujući 'forum shoping'.
- Sporiji razvoj elektronske trgovine.
- Povlačenje interneta u pravno sigurne zone.

Zbog ovih posledica, razjašnjenje jurisdikcije i njenih postupaka od vitalnog je značaja za upravljanje internetom.

Odnos između jurisdikcije i interneta

Odnos između jurisdikcije i interneta ima ugrađenu dvosmislenost, obzirom na to da jurisdikcija počiva prvenstveno na geografskoj podeli globusa na nacionalne teritorije. Svaka država ima suvereno pravo da vrši jurisdikciju na svojoj teritoriji. S druge strane, internet olakšava veliki deo prekogranične razmene, koju je teško (iako nije nemoguće) nadgledati pomoću tradicionalnih vladinih mehanizama. Pitanje jurisdikcije na internetu skreće pažnju na jednu od glavnih dilema povezanih sa upravljanjem internetom: kako je moguće 'usidriti' internet unutar postojeće pravne i političke geografije?[7]

Jurisdikcija – osnovne tehnike

Kada razmišljamo o jurisdikciji, moguća su tri glavna razmatranja:

1. Koja sudska ili državna vlast ima pravu nadležnost (proceduralna jurisdikcija).
2. Koji propisi će se primenjivati (stvarna jurisdikcija).
3. Kako će se primenjivati sudske odluke (izvršna jurisdikcija).

U naročitim slučajevima, jurisdikciju uspostavljaju sledeći glavni kriterijumi:

- **Teritorijalni princip –** pravo države da odlučuje o licima i imovini na svojoj teritoriji.
- **Personalni princip –** pravo države da odlučuje o svojim državljanima ma gde se nalazili (princip državljanstva).
- **Princip potraživanja –** pravo države da odlučuje o ekonomskim i pravnim efektima na svojoj teritoriji, koji prositiču iz aktivnosti vođenih u inostranstvu.

Još jedan važan princip koji je uvelo savremeno međunarodno pravo jeste princip opšte jurisdikcije.[8]

> *Koncept opšte jurisdikcije u svom širokom smislu (predstavlja) pravo države da kažnjava neka zlodela, ma gde i ma ko ih počinio, bez ikakve nužne veze sa teritorijom, državljanstvom ili naročitim državnim interesom.*[9]

Opšta jurisdikcija pokriva takva zlodela kao što su gusarenje, ratni zločini i genocid.

Sukob nadležnosti

Principi za uspostavljanje jurisdikcije neminovno dovode do situacija u kojima pravo na nju polažu sudovi nekoliko država. Problemi s jurisdikcijom pojavljuju se kada sporovi uključuju vanteritorijalnu komponentu (npr. učešće pojedinaca iz različitih zemalja ili međunarodne transakcije). Kako su svi sadržaji na internetu dostupni odsvuda, svaki korisnik interneta može biti izložen bilo kojoj nacionalnoj jurisdikciji. Prilikom postavljanja sadržaj na internet, teško je znati koji bi nacionalni zakon mogao biti prekršen, ako se uopšte krši. U ovom kontekstu, gotovo svaka aktivnost na internetu ima međunarodni aspekt koji bi mogao dovesti do uključivanja više nacionalnih jurisdikcija.[10]

Jedan od najilustrativnijih i najčešće navođenih slučajeva koji služe kao primer za problem jurisdikcije, predstavlja slučaj Jahu! u Francuskoj iz 2001. godine. Slučaj Jahu! koji je procesuiran u francuskim sudovima ponovo je ukazao na značaj problema višestrukih jurisdikcija.(11) Pokrenut je zbog kršenja francuskog zakona o nacističkim materijalima, koji zabranjuje izlaganje i prodaju takvih predmeta, bez obzira što se veb-sajt koji je ponudio ove stvari – the Yahoo.com auction website – nalazio u SAD, gde je izlaganje takvog materijala bilo – i još uvek jeste – legalno. Ovaj sudski spor razrešen je korišćenjem tehničkog rešenja (geolociranje softvera i filtriranje pristupa). Jahu! je morao da identifikuje korisnike koji su se kačili iz Francuske i da blokira njihov pristup veb-stranicama sa nacističkim materijalima.[12]

Osim tehničkih rešenja (geolociranje i filtriranje), u druge pristupe rešavanju sukoba jurisdikcija spadaju usaglašavanje nacionalnih zakona i korišćenje arbitraže i drugih rešenja u sporovima.

Za iscrpniju raspravu o sajber-bezbednosti i spemu videti Drugi deo

Usaglašavanje nacionalnih zakona moglo bi rezultirati uspostavljanjem seta jednakih propisa na globalnom nivou. Time bi pitanje jurisdikcije postalo bi manje urgentno. Usaglašavanje bi se moglo postići u oblastima u kojima već postoji visok nivo globalnog konsenzusa; na primer, u vezi sa dečijom pornografijom, piraterijom, ropstvom, terorizmom i sajber-kriminalom. Stavovi se približavaju i po drugim pitanjima, kao što su spem i sajber-bezbednost. Međutim, u nekim oblastima, uključujući politiku sadržaja, malo je verovatno da će doći do globalnog konsenzusa u odnosu na osnovna pravila, budući da kulturne razlike nastavljaju da se žilavije sukobljavaju u onlajn nego u stvarnom svetu.[13] Drugu moguću posledicu nedostatka usaglašavanja predstavlja prebacivanje sadržaja u zemlje sa nižim nivoom internetske regulative. Neke zemlje mogle bi postati ofšor centri nastajućeg internetskog sveta.

Kratak pregled glavnih razlika između tradicionalnih sudskih sistema i arbitraže

Elementi	Sudska nadležnost	Arbitraža
Organizacija	Određuje se zakonima/ugovorima - stalna	Određuju je strane (privremena, ad hok) Određuje se konvencijama (stalna)
Primenjivo pravo	Pravo suda (sudija odlučuje o pravu koji će se primeniti)	Strane mogu da biraju pravo; ako to ne učine, onda će biti po pravu označenom u ugovoru; ako oznake nema, onda se primenjuje pravo arbitražnog tela
Postupak	Sudski postupci određeni zakonima/ugovorima	Određuju ga strane (privremeni, ad hok) Određuje ga regulativa arbitražnog tela (stalni)
Kompetentnost/ Predmet spora	Određena zakonima/ugovorima u odnosu na predmet spora	Određuju je strane
Odluka	Obavezujuća	Obavezujuća

Arbitraža

Arbitraža predstavlja mehanizam rešavanja sporova, koji podrazumeva jednog ili više nezavisnih arbitara koje biraju strane u sporu. Međunarodna arbitraža u poslovnom sektoru ima dugu tradiciju. Arbitražni mehanizam obično je izložen u privatnom ugovoru, gde se strane slažu da će sve buduće sporove rešavati arbitražom. Postoji mnoštvo različitih arbitražnih ugovora, koji preciziraju takva pitanja kao što je mesto arbitraže, procedura i izbor prava.

U poređenju sa tradicionalnim sudovima, arbitraža nudi mnogo prednosti, uključujući veću fleksibilnost, manje troškove, brzinu, izbor jurisdikcije i lakše izvršenje naplata strane arbitraže. Jedna od glavnih prednosti arbitraže jeste da ona prevazilazi problem biranja proceduralne i materijalne jurisdikcije. Njih unapred biraju strane u sporu. Arbitraža ima naročite prednosti u odnosu na jedan od najtežih zadataka kod sudskih predmeta u vezi s internetom: izvršenje odluka. Njujorška konvencija o priznavanju i izvršenju stranih arbitražnih naplata reguliše izvršenje arbitražnih naplata.[14] Prema ovoj konvenciji, nacionalni sudovi su obavezni da izvrše arbitražne naplate. Lakše je izvršiti takve naplate u stranim zemljama korišćenjem režima Njujorške konvencije nego korišćenjem presuda redovnih sudova.

Glavno ograničenje arbitraže leži u činjenici da ona ne može da se bavi pitanjima od višeg javnog interesa; ta pitanja zahtevaju intervenciju državnih sudova.

Arbitraža se mnogo koristi u trgovačkim sporovima. Uspostavljen je razvijeni sistem propisa i institucija koje se bave trgovačkim sporovima. Glavni međunarodni resurs je Ogledni zakon o međunarodnoj trgovačkoj arbitraži, koji je sačinila Komisija UN za međunarodno trgovačko pravo (UNCITRAL) 1985. godine, uz dopunske instrumente UNCITRAL-a.([15] Vodeća međunarodna arbitražna tela obično se pridodaju trgovačkim komorama i organizovana su na međunarodnom (npr. Međunarodni arbitražni sud), regionalnom (npr. Evropski arbitražni sud) i nacionalnom nivou.

Arbitraža i internet

Arbitraža i drugi alternativni sistemi za rešavanje sporova koriste se mnogo da bi popunili jaz koji je nastao usled nemoći važećeg međunarodnog privatnog prava da se bavi predmetima vezanim za internet. Naročit primer alternativnog metoda rešavanja sporova u vezi s internetom predstavlja Jedinstvena politika rešavanja domenskih sporova (UDRP), koju je razvila Svetska organizacija za intelektualno svojinu (WIPO), a koju primenjuje ICANN kao glavni postupak u rešavanju spoprova.[16]

Za iscrpniju raspravu o DNS-u videti Prvi deo

UDRP se, unapred ,predviđa kao mehanizam rešavanja sporova u svim ugovorima koji podrazumevaju registraciju gTLD-ova (.com, .edu, .net) i neke domene najvišeg nivoa državnih kodova. Jedinstven aspekt ovog dokumenta počiva u tome što se naplate arbitraže vrše direktno preko promena sistema imena domena (DNS-a), bez pribegavnja izvršenju preko nacionalnih sudova.

Arbitraža omogućuje brži, jednostavniji i jeftiniji način rešavanja sporova. Međutim, korišćenje arbitraže kao glavnog mehanizma za rešavanje sporova vezanih za internet ima nekoliko ograničenja.

Prvo, budući da se arbitraža obično uspostavlja prethodnim sporazumom, ona ne pokriva široku oblast pitanja kada se sporazum između strana ne sklapa unapred (kleveta, razne vrste odgovornosti, sajberkriminal).

Drugo, mnogi sagledavaju važeću praksu dodavanja klauzule o arbitraži stalnim ugovorima kao štetnu za slabiju ugovornu stranu (obično korisnik interneta ili kupac preko elektronske pošte).

Treće, neki su zabrinuti zbog toga što arbitraža širi precedentno pravo (pravni sistem SAD/UK) na globalnom nivou i tako potiskuje druge nacionalne pravne sisteme. U slučaju trgovačkog prava, ovo bi se moglo pokazati kao prihvatljivije, obzirom na već postojeći visok nivo jednoobraznosti materijalnih propisa. Međutim, radi se o delikatnijem predlogu kada je reč o sadržajnim i društveno-kulturnim aspektima, gde nacionalni pravni sistem odražava specifičan kulturni sadržaj.

Autorska prava

Pod autorska prava spada samo izražavanje ideje, kada se ona materijalizuje u raznim oblicima, kao što je knjiga, CD, kompjuterski program, itd. Sama ideja nije zaštićena sistemom autorskog prava. U praksi je ponekad teško napraviti jasnu razliku između ideje i njenog izraza.

Sistem autorskih prava dosledno prati tehnološku evoluciju. Svaki novi izum, kao što je štamparska mašina, radio, televizija, video rikorder, uticao je i na oblik i na primenu autorskih prava. Internet nije nikakav izuzetak. Tradicionalni koncept autorskih prava došao je u iskušenje na više načina, od prostog preuzimanja teksta sa veba do složenijih aktivnosti, kao što je distribucija muzike i video fajlova preko interneta bez značajnog troška.

Paradoksalno je da internet pomaže nosiocima autorskih prava, snabdevajući ih moćnijim tehničkim sredstvima za zaštitu i praćenje

Prava na intelektualnu svojinu (IPR)

Znanje i ideje su ključni resursi u globalnoj ekonomiji. Zaštita znanja i ideja preko prava na intelektualnu svojinu postala je jedno od dominatnih pitanja u raspravi o upravljanju internetom, i ima snažnu komponentu razvoja.

Prava na intelektualnu svojinu pogođena su razvojem interneta, uglavnom preko digitalizacije znanja i informacija, kao i preko novih mogućnosti njihovom manipulacijom. Ova prava u vezi s internetom uključuju autorska prava, zaštitne znakove i patente. Druga prava na intelektualnu svojinu uključuju dizajn, poslovne tajne, geografske oznake i vrste biljaka.

korišćenja materijala koji je predmet zaštite. U najekstremnijem slučaju, nosioci autorskih prava mogu da zabrane pristup materijalu u celini, što bi ceo koncept zaštite učinilo irelevantnim.

Ovakav tok događaja dovodi u opasnost delikatnu ravnotežu između prava autora i zaštite javnog interesa, što je sam osnov zakona o zaštiti autorskih prava.

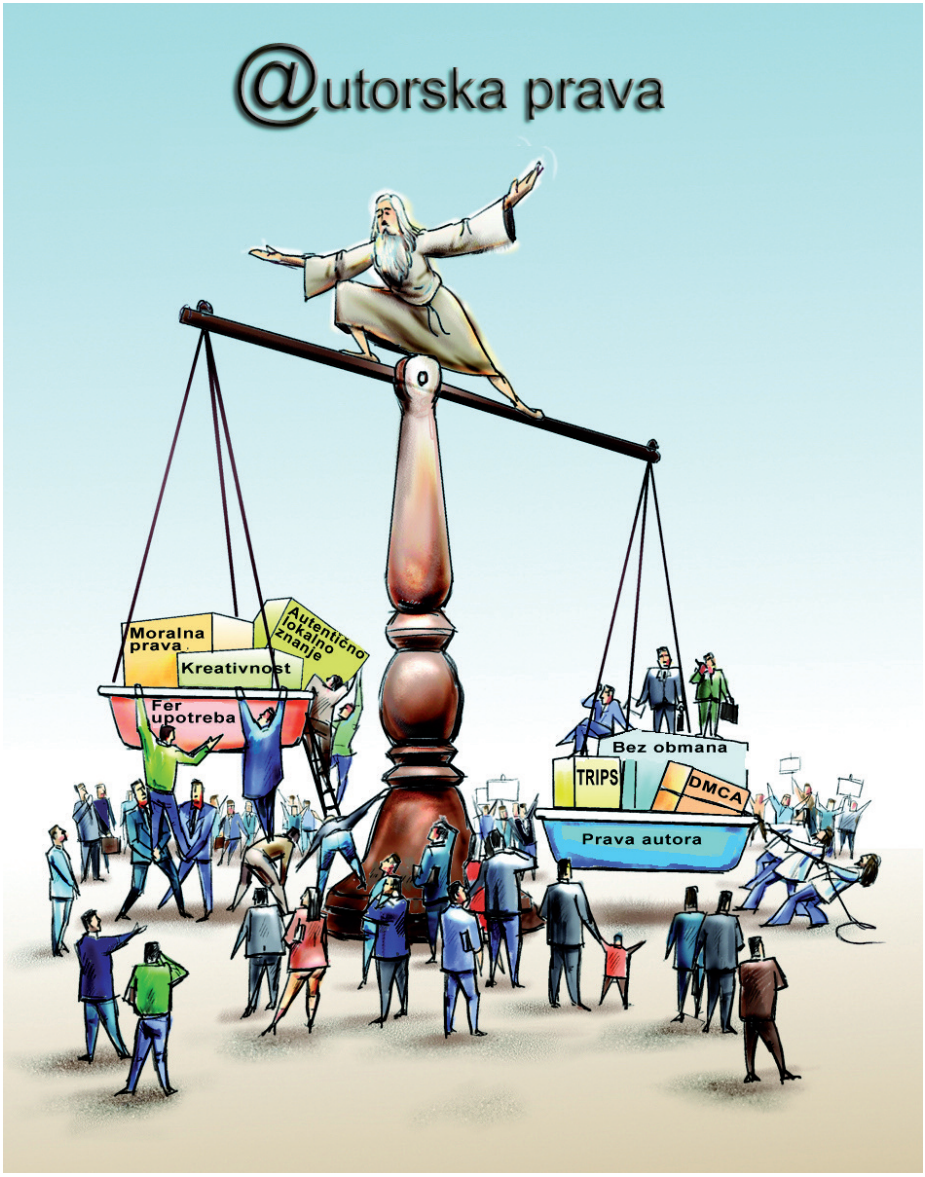
Do sada su nosioci autroskih prava, koje su predstavljale velike multimedijalne kompanije, bili aktivniji u zaštiti svojih interesa. Javni interes bio je samo donekle shvaćan i nedovoljno zaštićen. Ovo se, međutim, postepeno menja, uglavnom preko brojnih globalnih inicijativa koje se fokusiraju na pristup znanju i informacijama.

Trenutna situacija

Stroža zaštita autorskih prava na nacionalnom i međunarodnom nivou
Filmska i muzička industrija sve intenzivnije lobiraju na nacionalnom i međunarodnom nivou da pojačaju zaštitu autorskih prava. U SAD, stroža zaštita autorskih prava uvedena je Zakonom o digitalnim milenijumskim autorskim pravima iz 1998. godine. Na međunarodnom nivou, zaštita digitalnih umetnina uvedena je Ugovorom o autorstvu, 1996, koji je sačinila Svetska organizacija za intelektualnu svojinu. Ovaj ugovor takođe sadrži odredbe za ograničenja ekskluzivnih prava autora, zabranu izigravanja tehnološke zaštite autorskih prava i druge srodne mere.

Sve veći broj sudskih predmeta

Samo tokom 2003. godine, na osnovu američkog zakona o digitalnim autorskim pravima, poslato je 1000 opomena provajderima internet usluga (ISP), kojima se zahtevalo da obustave aktivnosti svojih pretplatnika vezane za preuzimanje fajlova, a pokrenuto je preko 500 sudskih postupaka protiv pojedinaca. Naročito relevantan slučaj za buduću zaštitu autorskih prava na internetu predstavlja predmet protiv Grokstera i StrimKasta, dve kompanije koje proizvode softver P2P za preuzimanje fajlova. U skladu s odredbama američkog zakona o digitalnim autorskim pravima, Filmsko-muzička asocijacija SAD zahtevala je od ovih kompanija da odustanu od razvoja tehnologije za preuzimanje fajlova koja doprinosi povredi autorskih prava. U početku su se američki sudovi opredeljivali za odbijanje odgovornosti softverskih kompanija za povredu autorskih prava, pod razumnim okolnostima. Međutim, u junu 2005, Vrhovni sud SAD zaključio je da su proizvođači softvera odgovorni za svaku zloupotrebu njihovog softvera.



Softver protiv povrede autorskih prava

Sredstva koja koriste prekršioci mogu koristiti i oni koji brane autorska prava. Tradicionalno, državne vlasti i kompanije sprovodile su svoju odgovornost preko legalnih mehanizama. Međutim, poslovni sektor sve više koristi sredstva 'alternativnog' softvera protiv kršioca autorskih prava.

U jednom članku objavljenom u Njujork tajmsu navedene su sledeće taktike koje koriste snimateljske/zabavne kompanije, u cilju zaštite svojih autorskih prava:[17]

- **Trojanski konj** preusmerava korisnike veb-sajtova tamo gde mogu legitimno da kupe pesmu koju su pokušali da skinu.
- **'Freeze'** softver blokira kompjutere na neko vreme i prikazuje upozorenje o skidanju piratske muzike.
- **'Silence'** softver skenira hard diskove, a radi se i na tome da se skinu svi zatečeni piratski fajlovi.
- **'Indirection'** softver sprečava pristup mreži za one koji pokušaju da snime piratsku muziku.

Profesor Lorens Lensig sa Stenfordskog pravnog fakulteta upozorava da bi takve mere mogle biti nelegalne. On je zapazio da među merama donetim protiv povreda autorskih prava, ove nisu uključene. Da li kompanije koje su pribegle takvim merama krše zakon?

Tehnologije za rukovođenje digitalnim pravima

Kao dugoročan i strukturniji pristup, poslovni sektor je uveo razne tehnologije za rukovođenje pristupom zaštićenim materijalima. Majkrosoft je uveo softver digitalnog rukovođenja pravima (DRM) da bi rukovodio preuzimanjem zvučnih fajlova, filmova i drugih autorskih maetrijala. Slične sisteme razvili su Kseroks (CiontentGuard), Filips i Soni (InterTrust).

Korišćenje tehnoloških sredstava za zaštitu autorskih prava dobilo je podršku i na međunarodnom nivou (WIPO Copyright Treaty) i u američkom zakonu o digitalnim autorskim pravima (DMCA). Štaviše, DMCA je proglasio kriminalnom aktivnost čiji je cilj izigravanje tehnološke zaštite autorskih materijala.

Pitanja

Da li dopuniti postojeće ili razviti nove mehanizme zaštite autorskih prava? Kako bi trebalo da se mehanizmi zaštite prilagode tako da odražavaju duboke promene do kojih su doveli informaciona i komunikaciona tehnologija (IKT) i razvoj interneta? Jedan od odgovora koje sugeriše *Bela knjiga o intelektualnoj svojini i nacionalnoj informacionoj infrastrukturi,*[18] koju je izdala Vlada SAD, glasi da su potrebne samo manje promene, uglavnom preko 'dematerijalizacije' autorskih koncepata fiksiranja, distribucije, prenosa i objavljivanja. Ovaj pristup je praćen u glavnim međunarodnim ugovorima vezanim za autorska prava, uključujući trgovačke aspekte prava na intelektualnu svojinu (TRIPS) i konvencije Svetske organiazcije za intelektualnu svojinu (WIPO).

Međutim, suprotno stanovište tvrdi da promene u pravnom sistemu moraju biti duboke, budući da se autorska prava u digitalnoj eri više ne odnose na 'pravo sprečavanja kopiranja' nego i na 'pravo sprečavanja pristupa'. Najzad, sa sve većim tehničkim mogućnostima ograničavanja pristupa digitalnim materijalima, možemo se zapitati da li je zaštita autorskih prava uopšte potrebna. Ostaje da se vidi kako će javni interes, drugi deo jednačine autorskih prava, biti zaštićen.

Zaštita javnog interesa – 'fer korišćenje' zaštićenih autorskih sadržaja

Autorska prava su u početku zamišljena kao podsticaj kreativnosti i izuma. To je razlog zbog čega su ona kombinovala dva elementa: zaštitu autorskih prava i zaštitu javnog interesa. Glavni izazov bio je da se utvrdi kako bi javnost mogla da dobije zaštićeni materijal radi povećanja kreativnosti, znanja i opšte dobrobiti. Govoreći operativno, ovaj javni interes bio je zaštićen preko koncepta 'fer korišćenja' zaštićenih materijala. Fer korišćenje se definiše kao 'korišćenje zaštićenih sadržaja bez traženja dozvole od nosilaca prava, kao što je za komentare, kritiku, novinsko izveštavanje, istraživanje, podučavanje i učenje'.[19]

Autorska prava i razvoj

Svako ograničenje fer korišćenja moglo bi da oslabi poziciju zemalja u razvoju. Internet služi istraživačima, studentima i drugima iz zemalja u razvoju kao moćno sredstvo za učestvovanje u globalnoj akademskoj i naučnoj razmeni. Restriktivan zaštitni režim autorskih prava mogao bi da ima negativan uticaj na razvoj mnogih siromašnih zemalja.

Drugi aspekt predstavlja sve veća digitalizacija kulturnih i umetničkih dobara iz zemalja u razvoju. Paradoksalno je, ali i sasvim moguće, da se može desiti da zemlje u razvoju budu kupovale digitialne verzije svog kulturnog i umetničkog nasleđa nakon što je ono digitalizovano i spremljeno za komerciajlizaciju od strane velikih kompanija.

WIPO i TRIPS

Kao što smo već pomenuli, postoje dva glavna međunarodna režima za prava na intelektualnu svojinu. WIPO rukovodi tradicionalnim režimom prava na intelektualnu svojinu, koji se zasniva na Bernskoj i Pariskoj konvenciji. Drugim, novijim režimom rukovodi Svetska trgovinska organizacija (STO) a zasniva se na trgovačkim aspektima prava na intelektualnu svojinu (TRIPS). Prebacivanje međunarodne koordinacije prava na intelektualnu svojinu sa WIPO na TRIPS izvršeno je da bi se ojačala zaštita tih prava, naročito u oblasti izvršenja. Ovo je bila jedna od glavnih dobiti razvijenih zemalja tokom urugvajske runde pregovora STO.

Mnoge zemlje u razvoju zabrinute su zbog ovakvog toka stvari. Strogi mehanizmi izvršenja STO mogli bi smanjiti manevarski prostor zemalja u razvoju i mogućnost balansiranja razvojnih potreba sa zaštitom međunarodnih prava na intelektualnu svojinu, smeštenih uglavnom u SAD. Do sada je glavna orijentacija STO i TRIPS bila na razna tumačenja prava na intelektualnu svojinu za farmaceutske proizvode. Veoma je verovatno da će se buduće rasprave proširiti na prava na intelektualnu svojinu i internet.

Odgovornost ISP-ova za povrede autorskih prava

Međunarodni mehanizmi izvršenja na polju intelektualne svojine dodatno su pojačani činjenicom da su provajderi internet usluga postali odgovorni za držanje sadržaja kojima se krše autorska prava ukoliko dotični sadržaji ne budu uklonjeni po obaveštenju o povredama. Ovim je, prethodno nedefinisan režim prava na intelektualnu svojinu, postao direktno sprovodljiv u oblasti interneta.

Zaštitni žigovi

Zaštitni žigovi su značajni za internet zbog registrovanja imena domena. U ranoj fazi razvoja interneta, registrovanje imena domena odvijalo se u stilu 'ko prvi devojci, njegova devojka'. Ovo je dovelo do sajberskvotovanja, prakse registrovanja imena kompanija i njihove potonje prodaje po višim cenama.

Ova situacija prisilila je poslovni sektor da postavi pitanje zaštite zaštitnih znakova u centar reforme upravljanja internetom, dovodeći do osnivanja ICANN-a 1998. U Beloj knjizi o osnivanju ICANN-a, Vlada SAD zahtevala je da ICANN razvije i da primeni mehanizam za zaštitu zaštitnih znakova u oblasti imena domena. Ubrzo po formiranju, ICANN je uveo jednoobraznu politiku rešavanja sporova u vezi sa imenima domena (UDRP), koju je razvio WIPO.

Patenti

Tradicionalno, patent štiti novi proces ili proizvod uglavnom tehničkog karaktera; tek nedavno su patenti odobreni na softver. Što je više registracija patenata, to je više sudskih predmeta među američkim softverskim kompanijama, što podrazumeva ogromne iznose novca.

Neki patenti odobreni za poslovne procese bili su sporni, kao što beše sa zahtevom Britiš telekoma da naplaćuje taksu za licencu za patent o hipertekstualnim linkovima, koji je registrovao osamdesetih godina XX veka. Avgusta 2002, ovaj zahtev je odbačen.[21] Da je Britiš telekom dobio ovaj spor, korisnici interneta bi morali da plaćaju taksu za svaki hipertekstualni link, bilo da je kreiran ili korišćen. Praksa odobravanja patenata za softver i za procedure koje se odnose na internet nije prihvaćena u Evropi i drugim regionima.[22]

Sajber-kriminal

Dihotomija između realnog i sajber-prava postoji u raspravi o sajber-kriminalu. Realno-pravni pristup ističe da je sajber-kriminal isto što realni kriminal, ali se obično vrši pri korišćenju kompjutera koji je najverovatnije povezan sa internetom. Kriminal je isti, samo se razlikuju sredstva izvršenja. Sajberpravni pristup ističe da jedinstveni elementi sajber-kriminala garantuju poseban tretman, naročito kada je reč o izvršenju ili prevenciji.

Tvorci Konvencije o sajber-kriminalu Saveta Evrope bili su bliži realno pravnom pristupu, naglašavajući da je jedini specifičan aspekt sajber-kriminala korišćenje IKT kao sredstva za počinjenje zlodela. Ova konvencija, koja je stupila na snagu 1. jula 2004, glavni je međunarodni instrument u ovoj oblasti.[23]

Pitanja

Definicija sajber-kriminala

Definicija sajber-kriminala jedno je od glavnih pitanja sajber-prava, budući da će ona podržati praktičan pravni rezultat, vršeći i uticaj na praćenje sajber-kriminala. Ako je reč o prekršajima počinjenim protiv kompjuterskih sistema, sajber-kriminal bi uključivao: neovlašćen pristup; oštećenje kompjuterskih podataka i programa; sabotažu u cilju sprečavanja funkcionisanja nekog kompjuterskog sistema ili mreže; neovlašćeno presretanje podataka ka, od ili unutar nekog sistema ili mreže; kao i kompjutersku špijunažu. Definicija sajber-kriminala kao 'svih nedela počinjenih preko interneta i kompjuterskih sistema' podrazumevala bi širi dijapazon nedela, uključujući i ona navedena u Konvenciji o sajber-kriminalu: kompjutersku podvalu, povrede autorskih prava, dečiju pornografiju i mrežnu bezbednost.

Sajber-kriminal i zaštita ljudskih prava

Konvencija o sajber-kriminalu pojačala je raspravu o ravnoteži između bezbednosti i ljudskih prava. Pojavile su se mnoge sumnje, prvenstveno u artikulaciji civilnog društva, da ova konvencija daje državnim vlastima preširoka ovlašćenja, uključujući pravo na proveru hakerskih kompjutera, kontrolu komunikacija i štošta drugog. Ova široka ovlašćenja mogla bi dovesti do ugrožavanja ljudskih prava, naročito privatnosti i slobode izražavanja.(24) Konvenciju o sajber-kriminalu usvojio je Savet Evrope, jedan od najaktivnijih propagatora ljudskih prava. Ovo može biti od pomoći kod uspostavljanja potrebne ravnoteže između borbe protiv sajber-kriminala i zaštite ljudskih prava.

Prikupljanje i čuvanje dokaza

Jedan od glavnih izazova kod borbe protiv sajber-kriminala predstavlja prikupljanje dokaza za sudske predmete. Brzina današnje komunikacije zahteva brz odgovor agencija zaduženih za sprovođenje zakona. Jedna mogućnost za čuvanje dokaza nalazi se na mrežnim logovima, koji daju informacije o tome ko je pristupio naročitim internetskim resursima, i kada je to učinio. Konvencija o sajber-kriminalu precizira obavezu čuvanja podataka iz internetskog saobraćaja. Ovo pravilo moglo bi uticati na ulogu ISP-ova u aktivnostima izvršenja zakona koje se odnose na internet.

Radni odnosi

Često se govori da internet menja način na koji radimo. Iako ovaj fenomen zahteva širu elaboraciju, sledeći aspekti imaju direktan značaj za upravljanje internetom:

- Internet je uveo veliki broj privremeno i kratkoročno zaposlenih. Naziv ‘stalnoprivremeni’ uveden je za zaposlene koji rade u dužim vremenskim periodima, pri čemu redovno obnavljaju kratkoročne ugovore. Ovo dovodi do nižeg nivoa socijalne zaštite radne snage.
- Telerad postaje sve značajniji kako napreduje razvoj telekomunikacija, naročito sa kablovskim pristupom internetu.
- Rad po ugovoru sa drugim zemljama u IKT servisnom sektoru, kao što su kol centri i odeljenja za obradu podataka, sve je prisutniji. Znatan deo ovih delatnosti već je prenet na zemlje sa jeftinijom radnom snagom, uglavnom u Aziji i Latinskoj Americi.

IKT je dovela do zamagljenja tradicionalne podele na rad, slobodno vreme i spavanje (8+8+8 časova). Sve teže je razlikovati gde rad počinje a gde se završava. Ove promene u radnim obrascima mogu zahtevati novo radno zakonodavstvo, koje će se baviti pitanjima kao što je radno vreme, zaštita interesa radnika i nagrađivanje.

U oblasti radnog prava, važno je pitanje privatnosti na radnom mestu. Da li je poslodavcu dozvoljeno da nadgleda korišćenje interneta od strane zaposlenih (kao što je sadržaj poruka elektronske pošte ili pristup veb-sajtovima)? Pravosuđe se postepeno razvija na ovom polju, sa mnoštvom novih rešenja.

U Francuskoj, Portugalu i Ujedinjenom Kraljevstvu, zakonske smernice i nekoliko sudskih predmeta pokazuju tendenciju ograničavanja kontrole elektronske pošte zaposlenih. U Danskoj, jedan sud je vodio predmet u kojem je došlo do otpuštanja radnika zbog toga što je slao privatne mejlove i ulazio na veb-sajt sa seksualno orijentisanim razgovorima. Sud je doneo odluku da je ovo otpuštanje bilo nezakonito zato što zaposleni nije imao obaveštenje kojim se zabranjuje neslužbeno korišćenje interneta. Drugi argument koji je primenio ovaj danski sud bila je činjenica da se korišćenje interneta nije negativno odrazilo na rad zaposlenog.

Radno pravo je tradicionalno državno pitanje. Međutim, globalizacija uopšte, a naročito internet, doveli su do internacionalizacije radnih pitanja. Sa sve većim brojem pojedinaca koji rade za strane firme i s radnim timovima na globalnoj bazi, javlja se sve veća potreba za odgovarajućim međunarodnim regulatornim mehanizmima. Ovaj aspekt je prihvaćen u deklaraciji WSIS-a, koja u članu 47 zahteva poštovanje svih relevantnih međunarodnih normi u oblasti radnog tržišta IKT-a.

Fusnote

1 Jedan od najvećih pristalica 'realnopravnog' pristupa je sudija Frenk Isterbruk, za koga kažu da je rekao: 'Idite kući; sajber-pravo ne postoji.' U članku *Cyberspace and the law of the horse,* on tvrdi da uprkos tome što su konji bili važni, nikad nije postojao 'Zakon o konjima'. Sudija Isterbruk tvrdi da postoji potreba za fokusiranjem na glavne pravne instrumente, kao što su ugovori, odgovornost, itd. Dostupno na: **http://www.law.upenn.edu/law619/f2001/week15/easterbrook.pdef**

2 Argumentacija sudije Isterbruka izazvala je nekoliko reakcija, uključujući i reakciju Lorensa Lesiga u članku *The law of the horse: What cyberlaw might teach*. Dostupno na: **http://www.lessig.org/content/articles/works/finalhls.pdf**

3 Bilo je nekoliko međunarodnih pokušaja da se usaglasi međunarodno privatno pravo. Glavni globalni forum predstavlja Haška konferencija o međunarodnom privatnom pravu, koja je usvojila brojne konvencije u ovoj oblasti.

4 Postoji velika učestalost korišćenja reči 'should' (trebalo bi da) u dokumentima Svetskog samita o informatičkom društvu (WSIS), što je jedna od karakteristika instrumenata mekog prava. Za iscrpnije informacije, videti: *The emerging language of ICT diplomacy – Qualitative analysis of terms and concepts*. Dostupno na: **http://www.diplomacy.edu/IS/Language/htlm/words.htm**

5 Član 53 Bečke konvencije o ugovornom pravu

6 Brownlie I (1999) *Principles of Public International Law, 5th Edn.* Oxford University Press: Oxford, UK, str. 513.

7 Za iscrpnije informacije, videti:
- Salis RP (2001) *A summary of the American Bar Association's (ABA) Jurisdiction in Cyberspace Project: Achieving legal and business order in cyberspace: A report on global jurisdiction issues created by the Internet*. Dostupno na: **http://www.lex-electronica.org/articles/v7-1/Salis.htm**
- Zittrain J (2006) *Jurisdiction in cyberspace,* Internet Law Program, Harvard Law School. Dostupno na: **http://cyber.law.harvard.edu/ilaw/mexico_2006_module_9_jurisdiction**
- ABA (2002) *Jurisdiction over Internet disputes: Different perspectives under American and European law in 2002, ABA Section on International Law and Practice*. Godišnji prolećni susret, New York, NY, USA, 8. maj 2002. Dostupno na: **http://www.howardice.com/uploads/content/jurisdiction_internet.pdf**

8 Među najvažnije izvore u ovoj oblasti spada rad P*rinceton Principles on Universal Jurisdiction* (2001). Dostupno na: **http://www1.umn.edu/humanrts/instree/princeton.htlm**

9 Malanczuk P (1997) *Akehurst's Modern Introduction nto International Law.* Routledge: London, UK, str. 113.

10 Za pregled predmeta vezanih za vanteritorijalnu sudsku nadležnost koja se odnosi na internetske sadržaje, videti: Timofeeva YA (2005) Worldwide perspective jurisdiction in Internet content controversies: A comparative analysis. *Connecticut Journal of International Law* 20: 199. Dostupno na: **http://ssrn.com/abstract=637961**

[11] Da biste pratili tok ovog slučaja, videti:
http://w2.eff.org/legal/Jurisdiction_and_sovereignty/

[12] Drugi sudski predmeti uključuju predmet na Nemačkom saveznom sudu pravde protiv Frederika Tobena, bivšeg nemačkog državljanina sa australskim državljanstvom koji je postavio sadržaje koji dovode pod sumnju postojanje holokausta, na veb-sajt sa sedištem u Australiji. Dostupno na:
http://www.ihr.org/jhr/v18/v18n4p-2_Toben.html

[13] Rasistički sadržaji i pornografija (u predmetima pod fusnotama 11 i 12) nisu jedina sporna pitanja – u druge primere spadaju ilegalno kockanje, reklamiranje duvana i prodaja droge

[14] Celokupan tekst Konvencije dostupan je na:
http://www.uncitral.org/uncitral/en/uncitral_texts/arbitration/NYConvention.html

[15] U druge instrumente UNCITRAL-a spadaju UNCITRAL Arbitration Rules (1976), UNCITRAL Concilation Rules (1980), UNCITRAL Notes on Organising Arbitral Proceedings (1996) i UNCITRAL Model Law on International Commercial Conciliation (2002).

[16] Uniform Domain-Name Dispute-Resolution Policy, ICANN, 26. avgust 1999. Dostupno na: **http://www.icann.org/udrp/udrp-policy-24oct99.htm**

[17] Sorkin AR (2003) Software bulletis sought to kill musical piracy. New York Times, 4. maj. Dostupno na: **http://www.nytimes.com/2003/05/04/business/04MUSI.html**

[18] Dostupno na: **http://www.uspto.gov/web/offices/com/doc/ipnii/**

[19] Dostupno na: **http://en.wikipedia.org/wiki/Fair_use**

[20] Za obuhvatan pregled glavnih pitanja u vezi sa UDRP, videti: *WIPO's Overview of WIPO panel views on selected UDRP questions*. Dostupno na:
http://arbiter.wipo.int/domains/search/overview/index.html

[21] Loney M (2002) *Hyperlink patent case fails to click*. CNET News.com. Dostupno na: **http://news.com.com/2100-1033-955001.html**

[22] Za iscrpnije informacije o debati u Evropi o mogućnosti softverskih patenata, videti: **http://swpat.ffii.org**

[23] Celokupan tekst Konvencije dostupan je na:
http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm

[24] Za kritičke stavove o *Konvenciji o sajber-kriminalu* kojima se izražava zabrinutost civilnog društva i boraca za ljudska prava, videti:
- Bailey C (2002) *Report on the Cybercrime Convention*. The Association for Progressive Communication. Dostupno na:
http://rights.apc.org/privacy/treaties_icc_bailey.shtml
- TreatyWatch.org website (2010). Dostupno na: **http://www.treatywatch.org/**

Četvrti deo

Ekonomska korpa

Ekonomska korpa

Elektronska trgovina predstavlaj jednu od glavnih lokomotiva razvoja interneta tokom poslednjih 15 godina. Njen značaj ilustruje naslov dokumenta koji je započeo reformu upravljanja internetom i osnovao ICANN: Okvir za globalnu elektronsku trgovinu (1997), koji navodi da 'privatni sektor treba da vodi' proces upravljanja internetom i da će glavna funkcija ovog upravljanja biti da 'nametne predvidljiv, minimalistički, dosledan i jednostavan pravni ambijent za elektronsku trgovinu'. Ovi principi predstavljaju temelj režima upravljanja internetom, koji se nalazi u ICANN-u.

Definicija elektronske trgovine

Izbor definicije za elektronsku trgovinu ima mnogo praktičnih i pravnih implikacija.[1] Koriste se specifični propisi u zavisnosti od toga da li se neka transakcija klasifikuje kao elektronska trgovina, kao što su propisi koji regulišu poreze i carinu.

Za Vladu SAD, ključni element u razlikovanju tradicionalne od elektronske trgovine predstavlja 'onlajn opredeljenje za prodaju robe ili usluga'. To znači da bi trebalo da se svaka trgovačka pogodba koja se zaključi onlajn, smatra elektronskom transakcijom, čak i ako realizacija pogodbe podrazumeva fizičku dostavu. Na primer, kupovina knjige preko Amazon.com smatra se elektronskom trgovačkom transakcijom uprkos tome što se knjige obično isporučuju tradicionalnom poštom. Svetska trgovinska organizacija (STO) definiše elektronsku trgovinu kao 'proizvodnju, distribuciju, marketing, prodaju ili dostavljanje robe i usluga elektronskim sredstvima'.[2]

Elektronska trgovina poprima mnogo formi.

- **Firma potrošaču (B2C) –** najpoznatija vrsta elektronske trgovine (npr. Amazon.com).
- **Firma firmi (B2B) –** ekonomski najintenzivnija, sa preko 90% svih transakcija elektronske trgovine.
- **Firma vladi (B2G) –** veoma značajna u oblasti nabavne politike.
- **Potrošač potrošaču (C2C) –** na primer, aukcije putem interneta.

Mnoge zemlje razvijaju regulatorni ambijent za trgovinu preko interneta. Usvajaju se zakoni u oblastima digitalnih potpisa, rešavanja sporova, sajber-kriminala, zaštite potrošača i oporezivanja. Na međunarodnom planu, sve je veći broj inicijativa i režima koji se odnose na elektronsku trgovinu (tj. trgovinu preko interneta).

STO i elektronska trgovina

Ključni politički igrač u modernoj globalnoj trgovini, STO, reguliše mnoga relevantna pitanja trgovine preko interneta, uključujući telekomunikacionu liberalizaciju, prava na intelektualnu svojinu i neke aspekte informatičke i komunikacione tehnologije. Elektronska trgovina pojavljuje se u sledećim aktivnostima i inicijativama STO:

- Privremenom moratorijumu na carinjenje elektrosnkih transakcija koji je uveden 1998. godine. Ovaj moratorijum oslobodio je carine sve transakcije preko interneta.
- Utvrđivanju Radnog programa STO za elektronsku trgovinu, koji se zalaže za raspravu o elektronskoj trgovini.
- Mehanizmu za rešavanje sporova. Elektronska trgovina bila je naročito značajna u sudskom sporu USA/Antigva povodom onlajn kockanja.[4]

Iako se trgovina preko interneta nalazila na diplomatskoj margini STO, pojavile su se razne inicijative i uočeno je više ključnih pitanja. Takva dva pitanja pominju se ovde.

Da li transakcije putem interneta treba kategorisati pod usluge (koje reguliše GATS – Opšti ugovor o trgovini uslugama) ili pod roba (koju reguliše GATT – Opšti ugovor o carinama i trgovini)?

Da li se kategorizacija muzike kao robe ili usluga menja u zavisnosti od toga da li se ona dostavlja na CD-u (opipljivo) ili preko interneta (neopipljivo)? Najzad, ista pesma bi mogla imati različit trgovački status (i biti podložna carini i porezima) u zavisnosti od načina isporuke.

Pitanje kategorizacije ima značajne implikacije zbog različitih regulatornih mehanizama za robu i usluge.

Šta bi trebalo da bude veza između TRIPS (trgovinskog aspekta prava na intelektualnu svojinu) i zaštite prava na intelektualnu svojinu (IPR) na internetu?

Kako TRIPS sporazum STO obezbeđuje mnogo jače mehanizme prinude za IPR, razvijene zemlje pokušavaju da prošire TRIPS na elektronsku trgovinu i na internet, koristeći dva pristupa. Prvo, navođenjem principa 'tehnološke neutralnosti', one tvrde da bi trebalo da TRIPS, kao i drugi propisi STO, bude proširen na sve telekomunikacione medije, uključujući internet. Drugo, neke razvijene zemlje zahtevaju neposredniju integraciju 'digitalnih ugovora' WIPO u TRIPS sistem. TRIPS nudi jače mehanizme prinude od konvencija STO. Oba pitanja ostaju otvorena i postajaće sve važnija u budućim pregovorima STO. U trenutnoj fazi trgovinskih pregovora, nije mnogo verovatno da će elektronska trgovina dobiti značajnu pažnju na dnevnom redu STO. Nedostatak globalnih aranžmana elektronske trgovine biće delimično kompenzovan nekim naročitim inicijativama (na primer, u vezi sa ugovorima i potpisima) i raznim regionalnim sporazumima, uglavnom u EU i azijsko-pacifičkom regionu.

Druge međunarodne inicijative u vezi sa elektronskom poštom

Jednu od najuspešnijih i najpodržavanijih međunarodnih inicijativa u oblasti elektronske trgovine predstavlja Ogledni zakon o elektronskoj trgovini UNCITRAL-a (Komisije UN za međunarodno trgovačko pravo). Ogledni zakon se fokusira na mehanizme integracije elektronske trgovine sa tradicionalnim trgovinskim pravom (npr. priznavanje valjanosti elektronskih dokumenata). Ogledni zakon se koristi kao osnov za regulisanje elektronske trgovine u mnogim zemljama. Drugu inicijativu, osmišljenu radi razvijanja elektronske trgovine, predstavlja uvođenje e-business XML (ebXML) od strane Centra UN za olakšanje trgovine i elektronskog poslovanja (UN/CEFAT), koji je set standarda zasnovanih na XML tehnologiji. U stvari, ebXML bi mogao uskoro postati glavni standard za razmenu dokumenata elektronske trgovine, zamenjujući ovaj tekući – razmenu elektronskih podataka (EDI).

EU je pokrenula širok niz akcija u oblasti elektronske trgovine, sa glavnom orijentacijom na mala i srednja preduzeća.[5] Aktivnosti OECD-a (Organizacije za ekonomsku saradnju i razvoj) dotiču razne aspekte koji se odnose na elektronsku trgovinu, uključujući zaštitu potrošača i digitalne potpise. Aktivnosti OECD-a stavljaju akcenat na razvoj i istraživanja u vezi sa elektronskom trgovinom pomoću preporuka i smernica.

UNCTAD (Konferencija UN o trgovini i razvoju) naročito je aktivan u istraživanjima i izgradnji kapaciteta, usmerenih na značaj elektronske trgovine za razvoj. Svake godine objavljuje E-Commerce and Development Report (Izveštaj o elektronskoj trgovini i razvoju) koji sadrži i pregled trenutne situacije i predloge za budući razvoj.

U poslovnom sektoru, najaktivnije međunarodne organizacije su Međunarodna trgovinska komora (ICC), koja objavljuje veliki broj preporuka i analiza iz oblasti elektronske trgovine, i Global Business Dialogue, koji promoviše elektronsku trgovinu i u međunarodnom i u nacionalnom kontekstu.

Regionalne inicijative

Za dodatnu raspravu o o opštem pristupu videti Peti deo

EU je razvila startegiju elektronske pošte na takozvanom 'Dot kom samitu' svojih lidera u Lisabonu (mart 2000). Iako je prihvatila privatni tržišno orijentisani pristup elektronskoj trgovini, EU je takođe uvela nekoliko korektivnih mera za zaštitu društvenih interesa (propagiranje opšteg pristupa, konkurentska politika koja podrazumeva razmatranje javnog interesa i restrikciju u distribuciji štetnih sadržaja). EU je usvojila Uputstvo o elektronskoj trgovini, kao i set drugih uputstava koja se odnose na elektronske potpise, zaštitu podataka i elektronske finansijske transakcije. U Azijsko-pacifičkom regionu, žarišnu tačku saradnje u elektronskoj trgovini predstavlja Azijsko-pacifička ekonomska kooperacija (APEK). APEK je osnovao Nadzorni odbor za elektronsku trgovinu, koja se bavi raznim pitanjima iz ove oblasti, uključujući zaštitu potrošača, spem i sajber-bezbednost. Najistaknutija inicijativa je APEK-ov Individualni akcioni plan za trgovinu bez papira, koji ima za cilj stvaranje trgovine robom u regionu bez ikakvih papira do 2010. godine.

Za dodatnu raspravu o spemu i sajber-bezbednosti videti Drugi deo

Zaštita potrošača

Poverenje potrošača jedan je od glavnih preduslova za uspeh elektronske trgovine. Ova vrsta trgovine je još relativno nova i potrošači nemaju poverenja u nju kao u 'stvarnu' kupovinu. Zaštita potrošača važan je pravni metod za razvijanje poverenja u elektronsku trgovinu. Trebalo bi da regulativa elektronske trgovine zaštiti potrošače u više oblasti:

- onlajn manipulacija informacijama sa platne kartice;
- obmanjujuće reklamiranje; i
- isporuka neispravnih proizvoda.

Novu karakteristiku elektronske pošte predstavlja internacionalizacija zaštite potrošača, koja ne spada u bitno pitanje kod tradicionalne trgovine. U prošlosti, potrošačima je retko bila potrebna međunarodna zaštita. Kupovali su lokalno i bila im je potrebna lokalna zaštita. Sa elektronskom poštom, sve veći broj transakcija odvija se preko međunarodnih granica.

Sudska nadležnost je značajno pitanje vezano za zaštitu potrošača. Ona uključuje dva glavna pristupa. Prvi favorizuje prodavca (uglavnom elektronsko poslovanje) i drži se pristupa koji propisuje prodavac/zemlja porekla. Po ovom scenariju, kompanije koje se bave elektronskom trgovinom imaju prednost u tome što se oslanjaju na predvidljiv i poznat pravni ambijent. Drugi pristup, koji favorizuje kupca, vezan je za zemlju odredišta.

Glavni nedostatak za kompanije koje trguju elektronskim putem predstavlja mogućnost izlaganja mnoštvu različitih jurisdikcija. Jedno od mogućih rešenja za ovu dilemu predstavlja intenzivnije usaglašavanje propisa za zaštitu potrošača, čime vi pitanje sudske nadležnosti postalo manje relevantno.

Za dodatnu raspravu o jurisdikciji videti Treći deo

U pogledu elektronske trgovine, OECD je preuzeo vodeću ulogu usvajanjem Smernica za zaštitu potrošača u kontekstu elektronske trgovine (2000) i Smernica za zaštitu potrošača od prevarne i obmanjujuće prekogranične trgovačke prakse (2003). Glavne principe koje je uspostavio OECD usvojile su druge poslovne asocijacije, uključujući Međunarodnu rgovinsku komoru (ICC) i Savet biroa za razvoj poslovanja.

EU nudi visok nivo zaštite potrošača u elektronskoj trgovini. Problem sudske nadležnosti razrešen je preko Briselske konevncije, koja predviđa da se potrošači uvek mogu osloniti na lokalnu zakonsku zaštitu. Na globalnom nivou, nisu ustanovljeni prikladni međunarodni pravni instrumenti. Jedan od najprikladnijih, Konvencija UN o ugovorima za međunarodnu prodaju robe (1980), ne pokriva potrošačke ugovore, ni zaštitu potrošača.

Neka privatna udruženja i nevladine organizacije (NVO) takođe se fokusiraju na zaštitu potrošača u elektronskoj trgovini, uključujući Međunarodne potrošače, Potrošački projekat o tehnologiji, Međunarodnu potrošačku mrežu za zaštitu i izvršenje i Kontrolu potrošačkih sajtova. Budući razvoj elektronske trgovine zahtevaće usaglašavanje nacionalnih zakona ili novi međunarodni režim zaštite elektronskih potrošača.

Oporezivanje i takse

> *Gospodo, ja ne znam zbog čega je to dobro. Međutim, u jedno sam sasvim siguran, jednog dana ćete ga oporezovati.*
>
> **Odgovor Majkla Faradeja skeptičnim političarima o svrsi njegovog otkrića elektromagnetske indukcije 1831. godine.[6]**

Kako internet sve više ulazi u glavne pore savremenog društva, pitanje oporezivanja i taksi se sve oštrije nameće kao problem. Ono je postalo još značajnije od finansijske krize iz 2008. godine. Mnoge vlade pokušavaju da povećaju budžetske prihode da bi smanjile sve veći javni dug. Oporezivanje ekonomskih aktivnosti na internetu postalo je jedna od prvih mogućnosti za povećanje budžetskih prihoda. Jedan od najčešćih zahteva predstavlja ograničavanje onlajn kockanja da bi se zaustavilo odlivanje poreskih prihoda iz tradicionalnih kockarskih centara. U druge predloge spada uvođenje posebnih taksi za pristup internetu.

Dilema upravljanja internetom da li sajber pitanja treba tretirati drukčije od pitanja iz stvarnog života jasno se ogleda u pitanju oporezivanja.[7] Od samog početka, SAD pokušavaju da proglase internet bezporeznom zonom. Godine 1998, američki Kongres usvojio je Zakon o oslobađanju od poreza, koji je u decembru 2004. produžen na još tri godine. Oktobra 2007, važenje ovog zakona produženo je do 2014, uprkos nekim strahovanjima da bi on mogao da dovede do znatnih gubitaka u prihodima.[8]

OECD i EU zastupaju suprotan stav, to jest da ne bi trebalo da internet ima specijalan tretman oporezivanja. Otavski principi OECD-a preciziraju da ne postoji nikakva razlika između tradicionalnog i elektronskog oporezivanja koja bi zahtevala posebne propise. Primenjujući ovaj princip, EU je 2003. uvela regulativu kojom se traži od elektronskih kompanija iz zemalja koje nisu članice EU, da plaćaju porez na dodatu vrednost (PDV) ukoliko prodaju robu unutar Evropske unije. Glavni razlog za ovu odluku EU bio je što su spoljne kompanije (uglavnom američke) imale prednost nad evropskim kompanijama, koje su morale da plaćaju PDV na sve transakcije, uključujući i elektronske.

Drugo pitanje u vezi sa elektrosnkim oporezivanjem koje ostaje nerešeno između EU i SAD je pitanje mesta oporezivanja. Otavski principi uveli su princip oporezivanja po 'odredištu' umesto po 'poreklu'. Američka vlada je snažno zainteresovana da oporezovanje ostane tamo gde transakcije nastaju, budući da se većina kompanija koje trguju elektronski nalazi u SAD. Nasuprot tome, intetres EU za oporezivanje prema odredištu uveliko je inspirisan realnošću da EU ima više elektronskih potrošača nego prodavaca.

Digitalni potpisi

Uopšteno govoreći, digitalni potpisi su povezani sa ustanovljenjem autentičnosti pojedinaca na internetu, što utiče na mnoge aspekte interneta, uključujući jurisdikciju, sajber-kriminal i elektronsku trgovinu. Korišćenje digitalnih potpisa trebalo bi da doprinese izgradnji poverenja na internetu. Digitalno ustanovljenje autentičnosti uopšte deo je okvira elektronske trgovine. Ono bi trebalo da olakša transakcije u elektronskoj trgovini putem zaključivanja elektronskih ugovora. Na primer, da li je jedan ugovor valjan i obavezujući ako se ostvari preko mejla ili veb-sajta? U mnogim zemljama, zakon zahteva da ugovori moraju biti 'pisani' ili 'potpisani'. Šta to znači u smislu interneta? Suočene sa ovim dilemama i izložene pritisku da oforme ambijent za razvoj elektronske trgovine, mnoge vlade su započele usvajanje zakonodavstva o digitalnim potpisima.

Kada je reč o digitalnim potpisima, glavni izazov je što vlade ne regulišu postojeći problem, kao što je sajber-kriminal ili kršenje autorskih prava, već stvaraju novi regulatorni ambijent u kojem nemaju nikakvog praktičnog iskustva. Ovo je rezultiralo mnoštvom rešenja i opštom maglovitošću kod odredaba u vezi sa digitalnim potpisima. Pojavila su se tri glavna pristupa regulisanju digitalnih potpisa.[9]

Prvi je 'minimalistički' pristup, koji precizira da elektronski potpisi ne mogu da se osporavaju zato što su u elektronskoj formi. Ovaj pristup određuje veoma široku upotrebu digitalnih potpisa i usvojen je u zemljama običajnog prava: Sjedinjenim Državama, Kanadi, Australiji i Novom Zelandu.

Drugi pristup je 'maksimalistički', određujući okvir i procedure za digitalne potpise, uključujući kriptografiju i korišćenje garanta javnih ključeva. Ovaj pristup obično precizira uspostavljanje posvećenih atestnih vlasti, koje mogu da potvrđuju buduće korisnike digitalnih potpisa. Ovaj pristup preovlađuje u zakonima evropskih zemalja, kao što su Nemačka i Italija.

Treći pristup, koji je usvojen u okviru Uputstva za digitalne potpise EU, predstavlja kombinaciju ova dva pristupa.[10] On ima minimalističku odredbu za prepoznavanje potpisa koji se dostavljaju elektronskim putem. Priznat je i maksimalistički pristup garancijom da će 'napredni elektronski potpisi' imati jače pravno dejstvo u pravnom sitemu (npr. lakše je dokazati ove potpise u sudskim sporovima).

Na globalnom nivou, UNCITRAL je 2001. godine usvojio Ogledni zakon o elektronskim potpisima, koji garantuje isti status digitalnim i rukom pisanim potpisima, pod uslovom da su zadovoljeni neki tehnički uslovi. Međunarodna trgovinska komora (ICC) izdala je dokument Opšta upotreba u digitalno obezbeđenoj trgovini (GUIDEC), koji daje pregled najbolje prakse, regulativa i atestiranja.[11] U direktnoj vezi sa digitalnim potpisima stoje inicijative javne šifarske infrastrukture (PKI). Dve organizacije, ITU i IETF, bave se standardizacijom javne šifarske infrastrukture (PKI).

Pitanja

Privatnost i digitalni potpisi

Digitalni potpisi su deo šireg razmatranja odnosa između privatnosti i ustanovljenja autentičnosti na internetu. Oni su samo jedna važna tehnika (ali ne i jedina) za identifikaciju pojedinaca na internetu.[12] Na primer, ustanovljenje autentičnosti SMS poruka preko mobilnog telefona koriste banke u nekim zemljama za odobravanje onlajn transakcija klijenata, tamo gde zakonodavstvo ili standaradi i procedure u vezi sa digitalnim potpisima još nisu uspostavljeni.

Potreba za preciznim standaradima implementacije

Iako su mnoge razvijene zemlje usvojile opšte zakonodavstvo u vezi sa digitalnim potpisima, njemu često nedostaju standardi i procedure za implementaciju. Obzirom na novinu ovih složenih pitanja, mnoge zemlje čekaju da vide smer u kojem će se razvijati konkretni standardi. Inicijative za standardizaciju odvijaju se na raznim nivoima, uključujući međunarodne organizacije (ITU) i profesionalne asocijacije (IETF).

Opasnost od nekompatibilnosti

Raznolikost pristupa i standarda u oblasti digitalnih potpisa mogla bi voditi ka nekompatibilnosti između različitih nacionalnih sistema. Ovakva rešenja mogla bi ograničiti razvoj elektronske trgovine na globalnom nivou. Nužno usaglašavanje bi trebalo obezbediti preko regionalnih i globalnih organizacija.

Elektronska plaćanja: elektronsko bankarstvo i elektronski novac

Zajednički element u raznim definicijama elektronskog jeste da se finansijske transakcije odvijaju u onlajn ambijentu korišćenjem sistema onlajn plaćanja. Postojanje sistema elektronskog plaćanja preduslov je za uspešan razvoj elektronske trgovine. Oblast elektronskih plaćanja zahteva diferencijaciju između elektronskog bankarstva i elektronskog novca.

Elektronsko bankarstvo podrazumeva korišćenje interneta za vođenje konvencionalnih bankarskih operacija, kao što je plaćanje karticama ili prebacivanje sredstava. Jedina novina je medij; bankarske usluge ostaju u suštini iste. Elektronsko bankarstvo pruža prednosti klijentima uvođenjem novih usluga i smanjenjem troškova transakcija. Na primer, transakcije koje staju 1 američki dolar u tradicionalnom bankarstvu, staju samo 0.02 dolara kod internetskog bankarstva.[13] U smislu upravljanja, elektronsko bankarstvo postavlja nove izazove kada dođemo na pitanje davanja licenci bankama od strane finansijskih vlasti. Kako bi trebalo da se daju licence virtuelnim bankama? Drugo pitanje u vezi sa upravljanjem jeste zaštita klijenata na međunarodnom nivou.

Elektronski novac, s druge strane, uvodi značajne inovacije. Američki Bord saveznih rezervi definiše elektronski novac kao 'novac koji se kreće elektronski'. Elektronski novac se obično povezuje sa tzv. pametnim karticama, koje izdaju kompanije kao što su Mandeks, Viza Keš i SajberKeš. Sav elektronski novac ima sledeće karakteristike:

- Dostavlja se elektronski, tipično na karticu s magnetnim zapisom ili mikroprocesorskim čipom.
- Prebacuje se elektronski. U većini slučajeva, to se događa između potrošača i trgovaca. Ponekad je moguće vršiti transfere između pojedinaca.
- Transakcije podrazumevaju kompleksan sistem, uključujući izdavača vrednosti elektronskog novca, mrežne operatere i isplatioca transakcija.

Elektronski novac se još uvek nalazi u ranoj fazi razvoja. Ne koristi se mnogo zbog ograničene sigurnosti i zbog nedostatka privatnosti. Mogao bi da krene u dva smera.

Prvi je evolutivni razvoj, koji bi uključio prefinjenije metode za elektronske transakcije, uključujući razvoj efikasnog mikroplaćanja. U krajnjem slučaju, sve te transakcije bile bi uklopljene u postojeći bankarski i monetarni sistem.

Drugi je revolucionarni razvoj, koji bi izvukao elektronski novac van kontrole centralne banke. Banka za međunarodna plaćanja već je identifikovala smanjenu kontrolu nad protokom kapitala i dotokom novca kao opasnosti koje su povezane sa elektronskim novcem. Koncepcijski, izdavanje elektronskog novca bilo bi slično štampanju novca bez kontrole centralne bankarske institucije. Takav pristup bi omogućio privatnim institucijama da izdaju novac prvenstveno za elektronsku trgovinu. Nedavno uvođenje virtuelne berze na Fejsbuku izazvalo je zebnje da bi zahvaljujući obimu svojih onlajn aktivnosti, on mogao u budućnosti da *de facto* preuzme neke monetarne funkcije.[14] U kontekstu nedavne finansijske krize i pokušaja vlada da ponovo steknu kontrolu nad finansijskim sistemom, nije mnogo verovatno da će eksperimenti sa elektronskim novcem imati podršku.

Pitanja

Promene u svetskom bankarskom sistemu

Dalje korišćenje elektronskog bankarstva i novca moglo bi dovesti do promena u svetskom bankarskom sistemu, dajući klijentima dodatne mogućnosti uz istovremeno smanjenje bankarskih troškova. Tradicionalni bankarski metodi naći će se pred ozbiljnim izazovom elektronskog bankarstva[15] Treba primetiti da su mnoge tradicionalne banke već usvojile elektronsko bankarstvo. U 2002. godini bilo je samo 30 virtuelnih banaka u Sjedinjenim Državama. Danas je teško naći banku bez usluga elektronskog bankarstva.

Sajber-prostor

Sajber-bezbednost predstavlja jedan od glavnih izazova široj upotrebi elektronskog plaćanja. Kako se može obezbediti sigurnost finansijskih transakcija preko interneta? Po tom pitanju, važno je istaći odgovornost banaka i drugih finansijskih institucija za sigurnost onlajn transakcija. Glavni događaj u tom smislu bilo je donošenje Sarbans-Okslijevog zakona, koji je usvojio američki Kongres u znak reakcije na finansijske skandale Enrona, Artura Andersena i WorldKoma. Ovaj zakon jača finansijsku kontrolu i povećava odgovornost finansijskih institucija za sigurnost onlajn transakcija. On takođe deli teret odgovornosti za sigurnost između klijenata, koji moraju da pokažu izvesnu obazrivost, i finansijskih institucija.[16]

Nedostatak metoda plaćanja

Ankete o elektronskoj trgovini navode nedostatak metoda plaćanja (npr. kartica) kao treći razlog, posle bezbednosti i privatnosti, za nekorišćenje elektronske trgovine. Trenutno, elektronska trgovina se vrši uglavnom kreditnom karticom. Ovo je značajna prepreka za zemlje u razvoju koje

nemaju razvijeno tržište kreditnim karticama. Vlade u tim zemljama morale bi uvesti potrebne zakonske promene da bi omogućile brže uvođenje plaćanja karticama.

Digitalna gotovina

Da bi pospešile razvoj elektronske trgovine, vlade širom sveta trebalo bi da podstiču sve oblike bezgotovinskog plaćanja, uključujući kreditne kartice i elektronski novac. Brže uvođenje elektronskog novca zahtevaće dodatne regulatorne aktivnosti vlada. Posle Hongkonga, koji je prvi uveo celokupno zakonodavstvo za elektronski novac, EU je 2000. godine usvojila Uputstvo za elektronski novac.[17] Vlade nerado uvode elektronski novac zbog mogućih opasnosti po autoritet centralnih banaka. Ozbiljna upozorenja stižu od stavova kao što je stav koji je izrazio ekonomist Dejvid Sekston: 'Digitalna gotovina predstavlja pretnju svakoj vladi na ovoj planeti koja želi da upravlja sopstvenom valutom.'[18] Vlade su takođe zabrinute zbog potencijalnog korišćenja elektronskog novca za pranje novca.

Male transakcije

Neki analitičari veruju da je stvarna ekspanzija elektronske trgovine povezana sa uvođenjem efikasnih i pouzdanih usluga za male transakcije. Na primer, korisnici interneta još nisu spremni da koriste kreditne kartice za mala plaćanja (od nekoliko evra/dolara), koja se obično uzimaju za pristup člancima ili drugim internetskim uslugama. Sistem mikroplaćanja, zasnovan na elektronskom novcu, može ponuditi potrebno rešenje. Zanimljivo je primetiti da je WWW konzorcijum (WC3), glavno telo za veb standardizaciju, obustavio svoje aktivnosti na polju elektronske trgovine/mikroplaćanja, što je predstavljalo zastoj u globalnim naporima prema standardizaciji u ovoj oblasti.[19]

Bavljenje ovim pitanjem na međunarodnom nivou

Zahvaljući karakteru interneta, verovatno će elektronski novac postati globalni fenomen – koji će dati razlog da se ovo pitanje podigne na međunarodni nivo. Jedan mogući igrač u oblasti elektronskog novca jeste Grupa za elektronsko bankarstvo Bazelskog komiteta. Ova grupa je već počela da se bavi ovlašćenjima, standardima obazrivosti, transparentnošću, privatnošću, pranjem novca i prekograničnom kontrolom, svim ključnim pitanjima za uvođenje elektronskog novca.[20]

Veza sa sprovođenjem zakona

Nedavni zahtev glavnog tužioca države Njujork PejPelu i Sitibanci da ne izvrše plaćanja internetskim kasinima direktno povezuje elektronsko plaćanje sa sprovođenjem zakona.[21] Ono što vlasti za sprovođenje zakona nisu mogle da postignu preko zakonskih mehanizama, mogle bi postići preko kontrole elektronskih plaćanja.

Fusnote

1 Pravna relevantnost uspostavljanja jasne definicije otvoreno se objašnjava na interaktivnoj stranici EU o elektronskoj trgovini: *Normalno, izbegavamo definisanje elektronske trgovine, osim maglovite ne-definicije da elektronska trgovina ima veze sa elektronskim poslovanjem. Međutim, postoji potreba za jednom pravnom definicijom za pravna dokumenta.* Izvor: **http://ec.europa.eu/archives/ISPO/ecommerce/drecommerce/answers/000025.html**

2 STO (1998) Radni program za elektronsku trgovinu. Dostupno na: **http://www.wto.org/english/tratop_e/ecom_ehtm**

3 Ovaj deo sajta STO fokusira se na elektronsku trgovinu: **http://www.wto.org/english/tratop_e/ecom_e.htm**

4 Za dodatne informacije o sporu SAD/Antigva vezanom za onlajn kockanje, videti: **http://www.wto.org/english/tratop_e/dispu_e/cases_e/ds285_e.htm**

5 Za dodatne informacije o inicijativama EU vezanim za elektronsku trgovinu, videti: **http://ec.europa.eu/information_society(eeurope/2002/action_plan/ecommerce/index_en.htm**

6 Mastrihtski institut za ekonomska istraživanja o inovacijama i tehnologiji (MERIT). Dostupno na: **http://www.merit.unimaas.nl/cybertax/**

7 Detaljniju raspravu o raznim aspektima politike oporezivanja i interneta, videti:
- Cockfield AJ (2001) Transforming the Internet into a taxable forum: A Case study in e-commerce taxation, *Minnesota Law Review* **85:**1171-1236. Dostupno na: **http://post.queensu.ca/~ac24/MinnLRevArtcle.pdf**
- Morse EA (1997) State taxation of Internet commerce: Something new under the sun? *Creighton Law review.* **30:**1124-1127.
- Williams WR (2001) The role of Caesar in the next millenium? Taxation of e-commerce: An overview and analysis, *Wm. Mitchell Law Review* **27:**1703-1707.

8 Mazerov M (2007) *Making the 'Internet Tax Freedom Act' permanent could lead to a substantial revenue loss for states and localities.* Dostupno na: **http://www.cbpp.org/7-11-07sfp.htm**

9 Za iscrpnije objašnjenje ova tri pristupa, videti *Survey of Electronic and Digital Signature Initiatives* koji je obezbedio Internet Law & Policy Forum. Dostupno na: **http://www.ilpf.org/groups/survey.htm#IB**

10 Uputstvo 1999/93/EC Evropskog parlamenta i Saveta, od 13. decembra 1999. o Zajedničkom okviru za elektronske potpise. Dostupno na: **http://eur-lex.europa.eu/LexUriServ.do?uri=CELEX:31999L0093:en:HTML**

11 GUIDEC (General Usage for International Digitally Ensured Commerce) Međunarodne trgovinske komore. Dostupno na: **http://cryptome.org/jya/guidec2.htm**

[12] Longmuir G (2000) *Privacy and digital authentication*. Dostupno na: http://caligula.anu.edu.au/~gavin/ResearchPaper.htm. Ovaj rad se bavi ličnim, komunalnim i vladinim aspektima potrebe za ustanovljenjem autentičnosti digitalnog sveta.

[13] Nsouli SM, Schaechter A (2002) Challenges of the e-banking revolution. *Finance and Development* **39(3).** Dostupno na: **http://www.imf.org/external/pubs/ft/fandd/2002/09/nsouli.htm**

[14] Radi upoznavanja sa aspektima uvođenja virtuelnog novca na Fejsbuku, videti: Claburn T (2010) Virtual money presents some legal problems, **Information week.** Dostupno na: **http://www.informationweek.com/news/security/app-security/showArticle.jhtml?articleID=223101009**

[15] Bankrate.com (2002) *What is online banking?* Dostupno na: **http://www.bankrate.com/brm/olbstep2.asp.** Ovaj članak daje uvod u onlajn bankarstvo i pregled prednosti i nedostataka u poređenju sa tradicionalnim bankarstvom.

[16] Za dodatne informacije, videti: Jacobs E (ND) *Security as a legal obligation: About EU legislation related to security and Sarbanes-Oxley in the European Union.* Dostupno na: **http://www.arraydev.com/commerce/JIBC/2005-08/security.htm**

[17] Uputstvo 2000/46/EC Evropskog parlamenta i saveta od 18. septembra 2000. o preuzimanju, praćenju i obazrivoj kontroli poslovanja institucija elektronskog novca. Dostupno na: **http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000L0046:EN:HTML**

[18] Holland K, Cortese A (1995) *The future of money: e-cash could transform the world's financial life*. Dostupno na: **http://www.businessweek.com/1995/24/b3428001.htm**

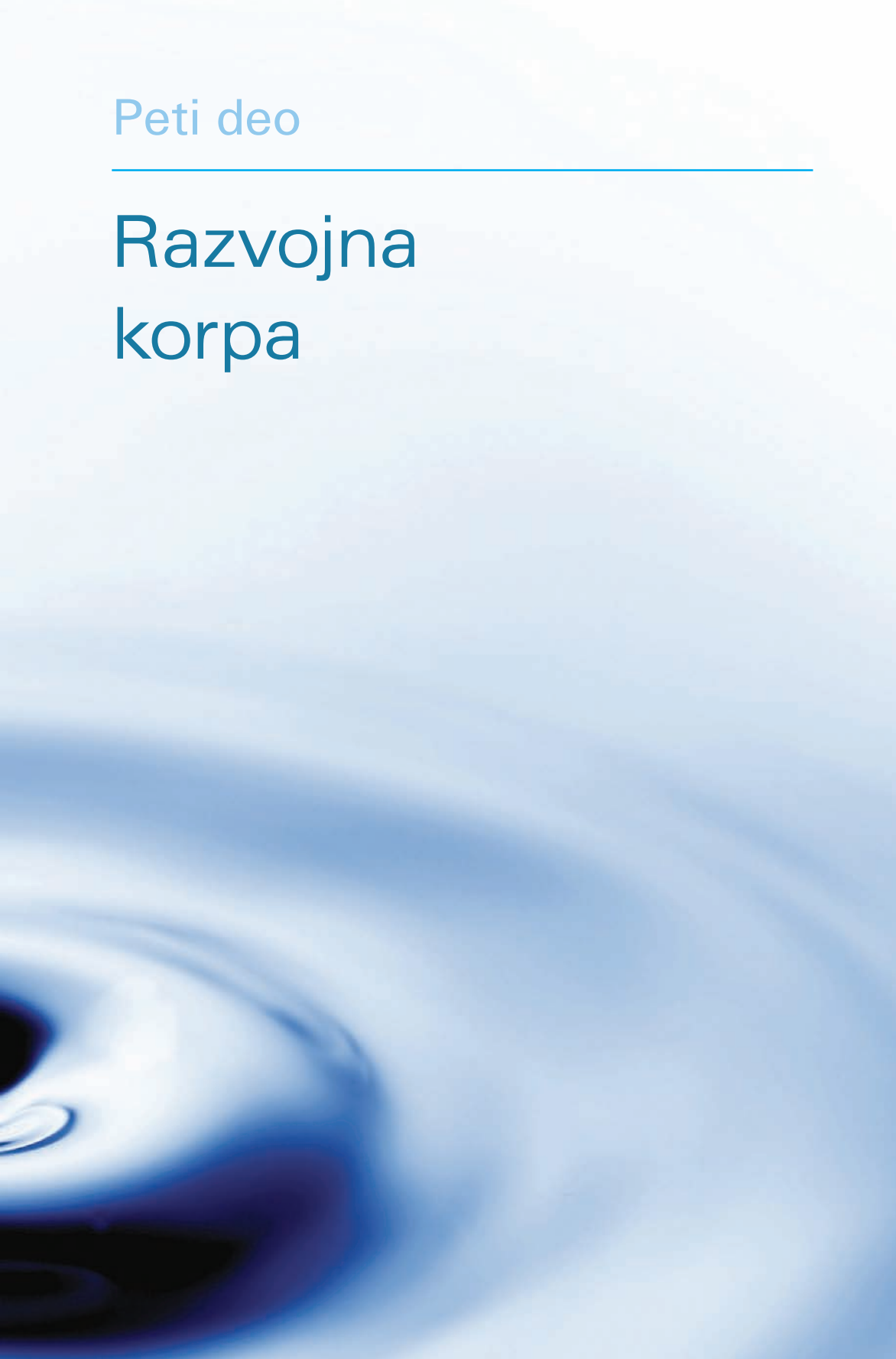
[19] U vezi sa argumentima protiv mikroplaćanja, videti: Shirky C (2000) *The case against micropayments*. Dostupno na: **http://www.open2p.com/pub/a/p2p/2000/12/19/micropayments.html**

[20] Bazelska grupa nalazi se u Banci za međuanrodna plaćanja. Izdaje redovan *Survey of Developments in Electronic Money and Internet and Mobile Payments*. Dostupno na: **http://www.bis.org/publ/cpss62.pdf**

[21] Za iscrnije informacije, videti: **http://www.ag.ny.gov/media_center/2002/aug/aug21a_02-html**

Peti deo

Razvojna korpa



Razvojna korpa

Tehnologija nije nikada neutralna. Istorija ljudskog društva pruža mnogo primera u kojima je tehnologija jačala neke pojedince, grupe ili narode, a isključivala druge. Internet se po ničem ne razlikuje u tom smislu. Od individualnog do globalnog nivoa, došlo je do dubokih promena u raspodeli bogatstva i moći. Uticaj IKT/interneta na raspodelu moći i razvoja doveo je do mnogih pitanja:

- Kako će promene koje ubrzava IKT/internet uticati na već postojeći jaz između Severa i Juga? Da li će IKT/internet smanjiti ili povećati taj jaz?
- Kako i kada će zemlje u razvoju uspeti da dostignu IKT nivo industrijski razvijenijih zemalja?

Odgovor na ova i druga pitanja zahteva analizu značaja razvoja u kontekstu upravljanja internetom.

Gotovo svako pitanje upravljanja internetom ima razvojni aspekt.

- Postojanje telekomunikacione infrastrukture olakšava pristup, prvi preduslov za prevlazilaženje digitalnog jaza.
- Trenutni ekonomski model za pristup internetu postavlja nesrazmeran teret na one zemlje u razvoju koje moraju da finansiraju pristup glavnim serverima smeštenim u razvijenim zemljama.
- Spem ima komparativno veći negativni uticaj na zemlje u razvoju zbog njihovog ograničenog propusnog opsega i nedostatka sposobnosti da se njime bave.

Za dalju raspravu o infrastrukturi videti Drugi deo

Za dalju raspravu o ekonomskim aspektima videti Četvrti deo

- Globalno regulisanje prava na intelektualnu svojinu (IPR) direktno utiče na razvoj zbog smanjene mogućnosti zemalja u razvoju da pristupe znanju i informacijama preko interneta.

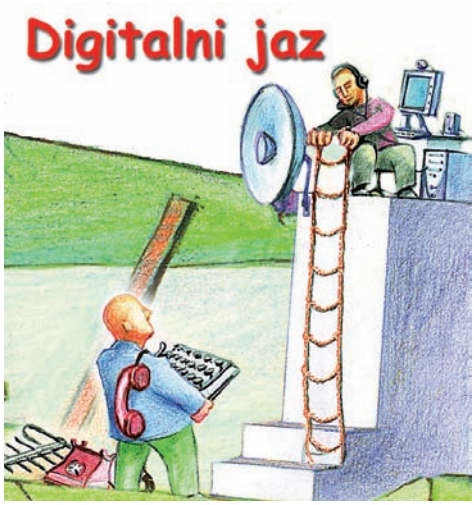
Razvojni aspekt Svetskog samita o informacionom društvu (WSIS) često se podvlači, počev od Rezolucije Generalne skupštine UN o WSIS-u, koja je istakla da WSIS treba da 'podstiče razvoj, naročito u odnosu na pristup tehnologiji i na njen transfer'. Ženevska deklaracija WSIS-a i Plan akcije istakli su razvoj kao prioritet i povezali ga sa Milenijumskom rezolucijom i njenim podsticanjem 'pristupa svih zemalja informacijama, znanju i komunikacionim tehnologijama radi razvoja'. S obzirom na vezu sa milenijumskim ciljevima, WSIS ima snažnu poziciju u kontekstu razvoja.

Kako IKT utiče na razvoj društva?

Glavne dileme u vezi sa IKT i razvojem sažeto su izražene u jednom članku *Ekonomista*.[1] Ovaj članak daje argumenta za i protiv teze da IKT daje poseban podsticaj razvoju.

IKT ne olakšava razvoj	IKT olakšava razvoj
• 'Mrežne eksternalije' pomažu prvodošlima da uspostave dominantnu poziciju. Ovo pogoduje američkim kolosima tako da bi lokalne firme u nerazvijenim ekonomijama bile efikasno izbačene iz elektronske trgovine.	• IKT smanjuje troškove rada; jeftinije je ulagati u zemljama u razvoju.
• Pomeranje moći sa prodavca na kupca (internet neminovno dovodi do scenarija u kojem se alternativni dobavljač nalazi udaljen samo za jedno pomeranje miša) naneće štetu siromašnim zemljama. Ono će naneti štetu proizvođačima uglavnom iz zemalja u razvoju.	• U poređenju s pređašnjim tehnologijama, IKT se veoma brzo širi preko granica. Pređašnjim tehnologijama (železnica i struja) bilo je potrebno više decenija da stignu u zemlje u razvoju, a IKT napreduje u velikim skokovima
• 'Veća zainteresovanost za deonice visoke tehnologije u bogatim ekonomijama smanjiće zainteresovanost investitora za zemlje u razvoju.	• Prilika da se preskaču stare tehnologije izbegavnjem posrednih elemenata, kao što su bakarne žice analogni telefoni, podstiče razvoj.
	• Karakteristika IKT da smanjuje optimalnu veličinu firme u većini delatnosti mnogo je bliža potrebama zemalja u razvoju.

Digitalni jaz



Digitalni jaz može se definisati kao procep između onih koji, usled tehničkih, političkih, socijalnih ili ekonomskih razloga, imaju pristup i mogućnosti da koriste IKT/internet, i onih koji nemaju. O veličini i značaju digitalnog jaza izraženi su različiti stavovi.

Digitalani jaz postoji na raznim nivoima: unutar zemalja i između njih; između seoskog i gradskog stanovništva; između starih i mladih; kao i između muškaraca i žena. Digitalni jazovi nisu nezavisne pojave. One odražavaju postojeće društveno-ekonomske nejednakosti u obrazovanju, zdravstvenoj zaštiti, kapitalu, stanovanju, zaposlenosti, čistoj vodi i hrani. Ovo je jasno iznela Radna grupa G8 za dgitalni razvoj (G8 DOT):

> *Ne postoji nikakva dihotomija između digitalnog jaza i širih društvenih i ekonomskih razlika kojima bi razvojni proces trebalo da se bavi; digitalni jaz treba shvatati i njime se baviti u kontekstu širih razlika.*[2]

Da li se digitalni jaz povećava?

Kretanja u IKT/internetu uzrokuju mnogo brže zaostajanje zemalja u razvoju od napredovanja u drugim oblastima (npr. u poljoprivrednoj ili medicinskoj tehnici), a kako razvijeni svet ima potrebne instrumente za uspešno korišćenje ovih tehnoloških dostignuća, ispostavlja se da se digitalna jaz neprestano i brzo širi. Ovo je često izražen stav u različitim vrlo cenjenim dokumentima, kao što je Izveštaj o ljudskom razvoju Razvojnog programa Ujedinjenih nacija (UNDP) i *Izveštaj o svetskom zapošljavanju* Međunarodne organizacije rada (ILO).

Neka suprotna mišljenja tvrde da je statistika u vezi sa digitalnim jazom često varljiva i da se ona uopšte ne širi. Po ovom mišljenju, tradicionalno fokusiranje na broj kompjutera, broj sajtova na internetu ili na dostupni propusni opseg, treba da bude zamenjeno fokusiranjem na širi uticaj IKT/interneta na društva u zemljama u razvoju. Često navođeni primeri su digitalni uspesi Brazila, Kine i Indije.

Opšti pristup

Pored digitalnog jaza, drugi često pominjan koncept u debati o razvoju predstavlja opšti pristup, tj. pristup za sve. Iako bi on morao da bude kamen-temeljac svake politike razvoja IKT, različite percepcije i koncepcije u vezi s karakterom i opsegom politike ovog opšteg pristupa ostaju na snazi. Često pozivanje na opšti pristup u preambulama međunarodnih deklaracija i rezolucija, bez potrebne političke i finansijske podrške, čini ovaj nejasni princip beznačajnim u praktičnom smislu. Pitanje opšteg pristupa na globalnom nivou ostaje u velikoj meri političko, zaviseći u krajnjem slučaju od spremnosti razvijenih zemalja da investiraju u realizaciju ovog cilja.

Za razliku od globalnog nivoa, u nekim zemljama opšti pristup predstavlja razvijen ekonomski i pravni koncept. Obezbeđivanje telekomunikacionog pristupa svim građanima čini osnov američke telekomunikacione politike. Rezultat toga je veoma razvijen sistem različitih političkih i finansijskih mehanizama, čija je svrha davanje subvencija za troškove pristupa u udaljenim područjima sa visokim troškovima za konektovanje. Subvencije finansiraju područja sa niskim troškovima konektovanja, prvenstveno veliki gradovi. I Evropska unija je preduzela jedan broj konkretnih koraka ka ostvarenju opšteg pristupa.

Strategije za prevazilaženje digitalnog jaza

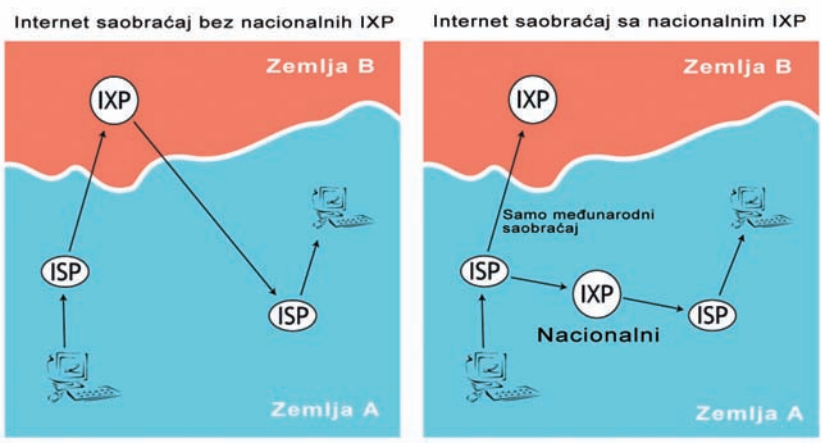
Teorija razvoja oslonjena na tehnologiju, koja dominira u akademskim i političkim krugovima poslednjih 50 godina, tvrdi da razvoj zavisi od dostupnosti tehnologije. Što je više tehnologije, više je razvoja. Među - tim, ovaj pristup je propao umnogim zemljama (uglavnom bivšim socijalističkim), gde je postalo očito da je razvoj društva mnogo složeniji proces. Tehnologija je nužan, ali ne i samodovoljan preduslov za razvoj. Drugi elementi podrazumevaju regulatorni okvir, finansijsku podršku, raspoložive ljudske resurse i druge socio-kulturne uslove. Čak i ako su svi ovi elementi prisutni, ostaju ključni izazovi: kako i kada bi trebalo da budu korišćeni, kombinovani i međusobno preplitani.

Pristup: Razvijanje telekomunikacija i internetske infrastrukture

Pristup internetu jedan je od glavnih izazova za prevazilaženje digitalnog jaza. Stopa pokrivenosti internetom u Africi iznosi 5,6%, u poređenju sa

73,8% u Japanu ili 60,7% u Evropi.[3] Postoje dva glavna aspekta pristupa internetu u zemljama u razvoju. Prvi je pristup glavnim međunarodnim strukturama interneta. Drugi je povezanost unutar zemalja u razvoju.

Pristup glavnim međunarodnim strukturama interneta zavisi uglavnom od podmorskih optičkih kablova. Dugo vremena samo je zapadna Afrika, do južne Afrike, opsluživana podmorskim kablom SAT-3. Zatim je i istočna Afrika dobila pristup podmosrkim kablovima: Istočnoafrički podmorski sistem (EASSY) počeo je da radi u julu 2010.[4] Nekoliko dodatnih podmor - skih kablova trebalo bi da bude naručeno tokom sledećih nekoliko godina. Tako će se formirati snažan digitalni prsten oko Afrike, koji bi trebalo da znatno poveća dostupni internetski propusni opseg za ceo afrički kontinent.[5]



Drugo je uvođenje internet tačaka razmene (IXP-ova) koje održavaju lokalni saobraćaj unutar jedne zemlje i smanjuju i korišćenje i cenu međunarodne kablovske veze.[6] Ipak, mnoge zemlje u razvoju nemaju IXP-ove, što znači da se znatan deo saobraćaja između klijenata unutar jedne zemlje odvija preko neke druge zemlje. Ovo povećava obim podataka međunarodnog saobraćaja i troškove za obezbeđivanje inter- net usluga. Razne inicijative traže da se IXP-ovi uspostave i u zemljama u razvoju. Jedna od njih koja je postigla izvestan uspeh jeste Asocijacija afričkih provajdera internet usluga. Ova asocijacija odgovorna je za osnivanje nekoliko IXP-ova u Africi.[7]

Povezanost unutar zemalja u razvoju drugi je veliki izazov. Većina korisnika interneta bila je koncentrisana u velikim gradovima. Seoska područja obično su bila bez ikakvog pristupa internetu. Situacija je počela da se menja naglim razvojem mobilne telefonije i bežičnih

komunikacija. Patrik Gelzinger iz Intela savetovao je zemlje u razvoju da kažu 'ne' telekomunikacionoj infrastrukturi zasnovanoj na bakru i da koriste bežične veze kao rešenje. Bežična komunikacija mogla bi biti rešenje za problem razvijanja tradicionalne zemaljske komunikacioen infrastrukture (polaganje kablova kroz velika prostranstva mnogih azijskih i afričkih zemalja). Na ovaj način, problem lokalne petlje, jedne od glavnih prepreka za brži razvoj interneta može biti prevaziđen.

Za dalju raspravu o infrastrukturi videti Drugi deo

Finansijska podrška

Zemlje u razvoju dobijaju finansijsku podršku raznim kanalima, uključujući bilateralne ili multilateralne razvojne agencije, kao što su UNDP ili Svetska banka, kao i regionalne razvojne inicijative i banke. S povećanom liberalizacijom telekomunikacionog tržišta, porasla je tendencija za razvijanje telekomunikacionih infrastruktura preko direktnih stranih ulaganja. Kako su telekomunikaciona tržišta zemalja u razvoju prezasićena, mnoge međunarodne telekomunikacione kompanije vide tržišta zemalja u razvoju kao područje budućeg rasta.

Tokom trajanja WSIS-a, značaj finansijske podrške za prevazilaženje digitalnog jaza bio je jasno prepoznat. Jedna ideja predložena na SSID-u bila je osnivanje Fonda digitalne solidarnosti pod upravom Ujedinjenih nacija, koji bi pomagao tehnološki zaostalim zemljama da izgrade telekomunikacionu infrastrukturu. Međutim, ovaj predlog nije dobio široku podršku razvijenih zemalja, koje su favorizovale direktna ulaganja umesto osnivanja jednog centralizovanog razvojnog fonda. Posle WSIS-a, osnovan je Fond digitalne solidarnosti u Ženevi kao nezavisna fondacija, koja uglavnom ima podršku gradova i lokalnih vlasti širom sveta.

Društveno-kulturni aspekti

Društveno-kulturni aspekti digitalnih vo - dodelnica obuhvataju mnoštvo pitanja, uključujući pismenost, IKT veštine, obuče - nost, obrazovanje i zaštitu jezika.

Za dalju raspravu o društveno-kulturnim aspektima videti Šesti deo

Za zemlje u razvoju, jedno od glavnih pitanja predstavlja 'odliv mozgova', koji se opisuje kao odlazak visokoobrazovane radne snage iz zemalja u razvoju u razvijene zemlje. Odlivom mozgova, zemlje u razvoju gube na više načina. Glavni

gubitak je u stručnoj radnoj snazi. Zemlje u razvoju takođe gube svoja ulaganja u obuku i obrazovanje stručnih kadrova koji se sele. Sva je verovatnoća da će se odliv mozgova nastaviti, obzirom na razne planove u vezi sa zapošljavanjem doseljenika kojin postoje u SAD, Nemačkoj i drugim razvijenim zemljama, da bi se privukla obrazovana radna snaga, uglavnom ona koja je obučena u IKT.

Jedna stvar koja može da zaustavi, ili u nekim slučajevima, čak da okrene odliv mozgova u suprotnom smeru, jeste povećanje davanja IKT zadataka zemljama u razvoju. Najuspešniji primeri za to su centri softverske industrije u Indiji, kao što su Bangalor i Hajderabad.

Na globalnom nivou, UN su pokrenule Digitalnu mrežu dijaspore za pospešivanje razvoja u Africi, kroz mobilizaciju tehnoloških, preduzetničkih i profesionalnih veština i resursa afričke dijaspore u oblasti IKT.

Telekomunikaciona politika i regulativa

Pitanja telekomunikacione politike su u mnogočemu blisko povezana sa prevazilaženjem digitalnog jaza.

- Ni privatni investitori i, sve više, ni javni donatori nisu spremni da investiraju u zemlje bez pravog institucionalnog i zakonskog ambijenta za razvoj interneta.
- Razvoj nacionalnih IKT sektora zavisi od stvaranja potrebnog regulatornog okvira.
- Telekomunikaciona politika bi trebalo da olakša uspostavljanje efikasnog telekomunikacionog tržišta sa više konkurentnosti, nižim troškovima i širim dijapazonom usluga.

Za dalju raspravu o pravu videti Treći deo

Stvaranje povoljnog ambijenta predstavlja zahtevan zadatak, koji za sobom povlači postepenu monopolizaciju telekomunikacijskog tržišta, uvođenje zakona koji se odnose na internet (pokrivajući sajber-kriminal, autorska prava, privatnost, elektronsku trgovinu, itd.) i garantovanje pristupa svim građanima bez ograničenja.

Institucionalno govoreći, jedan od prvih koraka jeste da se osnuju nezavisne i profesionalne telekomunikacione regulatorne vlasti. Iskustvo iz razvijenih zemalja pokazuje da su solidni nadležni organi preduslov za brz razvoj telekomunikacijske infrastrukture. U zemljama u razvoju, ra-

zvoj regulatornih vlasti nalazi se u sasvim početnoj fazi. Regulatorni organi su obično slabi, nedostaje im nezavisnost i često su deo sistema u kojem su državni operateri uticajni u regulativnim i političkim procesima.

Drugi veliki izazov predstavlja liberalizacija telekomunikacijskog tržišta. Indija i Brazil se obično pominju kao zemlje u razvoju u kojima je takva liberalizacija olakšala razvoj interneta i IKT sektora. Ona je takođe doprinela ukupnom ekonomskom razvoju u ovim zemljama. Za druge zemlje, naročito za one najnerazvijenije, liberalizacija telekomunikacionog tržišta pokazala se kao veliki izazov. Gubitkom telekomunikacijskih monopola, vlade u tim zemljama izgubile su važan izvor budžetskih prihoda. Niži budžeti su pogodili sve druge sektore društvenog i ekonomskog života. U nekim slučajevima, iako su izgubile telekomunikacijske prihode, ove zemlje nisu požnjele korist od liberalizacije u vidu nižih troškova i boljih telekomunikacionih usluga. U mnogim slučajevima, ovo je bilo zbog toga što privatizaciju telekomunikacionih kompanija nije pratilo osnivanje efikasnog tržišta i konkurencije. Takva praksa navela je Svetsku banku da podvuče da zemlje otvore glavne tržišne segmente konkurenciji, pre ili istovremeno sa privatizacijom operatera u vlasništvu vlada; na ovaj način, one će smanjiti troškove brže nego zemlje koje najpre privatizuju a potom uvode konkurenciju.[8]

Fusnote

1 Falling through the Net? *The Economist*, 21. septembar 2000.

2 DOT Force (2001) *Digital opportunities for all: Meeting the challenge*. Izveštaj Radne grupe za digitalizaciju (DOT Force), uključujući predlog za Đenovski plan akcije. Dostupno na: **http://www.g7.utoronto.ca/www./summit/2001genoa/dot-force1.htm**

3 *Internet World Stats*. Dostupno na: **http://www.internetworldstats.com/stats.htm**

4 **http://www.eassy.org/**

5 Mapa podmorskih kablova oko Afrike dostupna na: **http://manypossibilities.net/african-undersea-cables/**

6 Tačke internetske razmene (IXP-ovi) predstavljaju tehničke instalacije preko kojih provajderi internet usluga razmenjuju internetski saobraćaj (bez plaćanja). IXP-ovi se obično uspostavljaju da bi se internetski saobraćaj odvijao unutar manjih zajednica (npr. grad, region, zemlja), izbegavajući nepotrebno usmeravanje preko udaljenih geografskih lokacija.

7 MTN (2008) We are MTN. Dostupno na: **http://www.mtn.co.za/?pid=8049**

8 Ismail S (2006) Analyzing the World Bank's blueprint for promoting 'information and communications. Federal Communications Law Journal 59(1). Dostupno na: **http://www.law.indiana.edu/fclj/pubs/v59/no1/13-Book%20ReviewFINAL.pdf**

Šesti deo

Društveno-kulturna korpa

Društveno-kulturna korpa

Internet je izvršio značajan uticaj na društveno i kulturno tkivo savremenog društva. Teško je naći bilo koji segment društvenog života koji nije pod uticajem interneta. On uvodi nove obrasce komuniciranja, ruši jezičke barijere i stvara nove oblike kreativnog izražavanja. Danas, internet sve više postaje društveni nego tehnološki fenomen.

Ljudska prava

Osnovni set ljudskih prava koji se odnosi na internet uključuje privatnost, slobodu izražavanja, pravo na dobijanje informacija, različita prava koja štite kulturnu, jezičku i manjinsku raznolikost, i pravo na obrazovanje. Nije iznenađujuće to što se o pitanjima u vezi sa ljudskim pravima vrlo često žestoko raspravlja i na Svetskom samitu informacionog društva (WSIS-u) i na Forumu o upravljanju internetom (IGF-u). Iako se o ljudskim pravima obično govori eksplicitno, i ona su uključena u prateća pitanja koja se pojavljuju prilikom bavljenja mrežnom neutralnošću (pravo na pristup, sloboda izražavanja, anonimnost), sajber-bezbednošću (poštovanje ljudskih prava prilikom izvođenja aktivnosti vezanih za sajber-bezbednost i zaštitu), kontrolom sadržaja, itd. WSIS je prepoznao značaj ljudskih prava, naročito prava na razvoj i prava na slobodu izražavanja.

Za dodatnu raspravu o mrežnoj neutralnosti i sajber -bezbednosti videti Drugi deo

Važeća prava nasuprot sajber-pravima

Paralelno sa koncepcijskom pravnom raspravom koja se vodi o tome da li je važeće pravo dovoljno da reguliše internet ili da li postoji potreba za sajber-pravom, odvija se rasprava u krugovima boraca za ljudska

prava o tome da li koncepti tradicionalnih ljudskih prava treba da budu revidirani s obzirom na njihovo korišćenje interneta. Asocijacija za progresivnu komunikaciju (APK) u Povelji o internetskim pravima tvrdi da su ljudska prava koja se odnose na internet snažno uklopljena u sistem ljudskih prava UN koji se zansiva na Univerzalnoj deklaraciji o ljudskim pravima i drugim srodnim instrumentima.[1]

Takođe postoji predlog da se uspostavi pravo na komunikaciju kao nova vrsta ljudskog prava koje je uglavnom inspirisano novim oblicima komunikacija zasnovanim na internetu.

Pregled inicijativa o ljudskim pravima i internetu

Glavna inicijativa o sajber-pravima koja se trenutno odvija jeste Internetska povelja o pravima (IBR), koju sponzoriše italijanska vlada i civilno društvo. Ovaj projekat je pokrenuo proces koji trenutno podržava Dinamična koalicija za internetska prava i principe[2] a uključuje i druge tokove kao što je Nadgledanje internet prava. O IBR se raspravljalo na svim prethodnim forumima o upravljanju internetom. U pokušaju da definiše sajber-prava, APK je izradila nacrt Povelje o internetskim pravima.[3] Drugu prvenstveno akademsku inicijativu predstavlja Povelja o slobodi umreženih komunikacija koju je predložio Pravni fakultet Torontskog univerziteta.

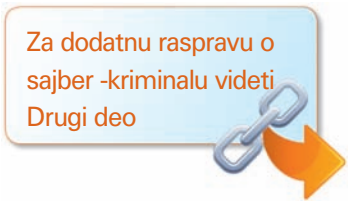
Pravo pristupa internetu

Finska je jedna od prvih zemalja koja zakonski garantuje pravo pristupa internetu. Od jula 2010. svi građani Finske imaju pravo na konekciju od 1 megabita.

Gugl, Majkrosoft i nekoliko drugih internet kompanija pokrenuli su Inicijativu globalne mreže (GNI) u novembru 2008, sa glavnim ciljem promovisanja ljudskih prava, naročito slobode izražavanja i privatnosti. Ova inicijativa posebno je važna zato što komercijalne aktivnosti velikih internet kompanija mogu direktno da utiču na način zaštite ljudskih prava.[4]

Aktivnosti Saveta Evrope posvećene ljudskim pravima i internetu

Savet Evrope je jedan od glavnih igrača u oblasti ljudskih prava. Savet je glavna institucija koja se bavi panevropskim ljudskim pravima, sa Evropskom konvencijom o zaštiti ljudskih prava i fundamentalnih slo-



boda (195)[5] kao svojim glavnim instrumentom. Od 2003. godine, Savet Evrope je usvojio nekoliko deklaracija koje ističu značaj ljudskih prava na internetu.[6] Savet je takođe zaštitnik Konvencije o sajber-kriminalu kao glavnog instrumenta u ovoj oblasti. Ovo može svrstati Savet Evrope kao jednu od ključnih institucija za pronalaženje prave ravnoteže pri razmatranju ljudskih prava i sajber-bezbednosti u budućem razvoju interneta.

Sloboda izražavanja i pravo na traženje, dobijanje i davanje informacija

Jedno od najspornijih područja ljudskih prava na internetu podrazumeva slobodu izražavanja. Ovo je jedno od fundamentalnih ljudskih prava, koje obično dolazi u žižu interesovanja kada se razgovara o kontroli sadržaja i cenzuri. U Univerzalnoj deklaraciji o ljudskim pravima (UDHR), slobodi izražavanja (član 19) suprotstavljeno je pravo države da ograniči slobodu izražavanja zbog morala, javnog reda i opšte dobrobiti (član 29). Na taj način, i razgovor i primena člana 19 moraju se staviti u kontekst uspostavljanja prave ravnoteže između ove dve potrebe. Ova dvosmislena situacija otvara mnoge mogućnosti za različita tumačenja normi i, u krajnjem slučaju, za razne implementacije. Polemika u vezi s pravom ravnotežom između članova 19 i 29 u 'realnom' svetu ogleda se u raspravama o postizanju ravnoteže na internetu.

Sloboda izražavanja nalazi se posebno u žiži interesovanja nevladinih organizacija (NVO) kao što su Amnesti internešenel i Fridom haus. Jedna novija studija Fridom hausa bavi se procenama nivoa slobode na internetu i u mobilnoj telefoniji kroz prizmu iskustava prosečnih korisnika na uzorku od 15 zemalja u 6 regiona. Pokrivajući kalendarske godine 2007. i 2008, ova studija bavi se nizom faktora koji bi mogli uticati na takvu slobodu, uključujući stanje telekomunikacione infrastrukture, vladina ograničenja na pristup tehnologiji, regulatorni okvir za provajdere usluga, cenzuru i kontrolu sadržaja, pravni ambijent, nadzor i vanpravne napade na korisnike ili proizvođače sadržaja. Navedeni indikatori odražavaju ne samo akcije vlada nego i snagu, raznolikost i aktivizam novog medijskog domena u svakoj zemlji, bez obzira na – ili uprkos – naporima države da ograniči upotrebu.[7]

Politike sadržaja

Jedno od glavnih društveno-političkih pitanja predstavlja politika sadržaja, koja je često predmet interesovanja sa stanovišta ljudskih prava (sloboda izražavanja i pravo na komuniciranje), vlade (kontrola sadržaja) i tehnologije (sredstva za kontrolu sadržaja). Rasprave se obično koncentrišu na tri grupe sadržaja.

1. Sadržaj za čiju kontrolu postoji globalni konsenzus. Ovde su uključeni dečija pronografija, opravdavanje genocida i podsticanje ili organizovanje terorističkih akcija, što je sve zabranjeno međunarodnim pravom (*ius cogens*). [8]
2. Sadržaj koji je osetljiv za naročite zemlje, regione ili etničke grupe usled njihovih naročitih verskih i kulturnih vrednosti. Globalizovana onlajn komunikacija postavlja izazove lokalnim, kulturnim i verskim vrednostima u mnogim društvima. Najveći deo kontrole sadržaja u srednjoistočnim i azijskim državama zvanično se pravda zaštitom specifičnih kulturnih vrednosti. To često znači da je pristup pornografskim i kockarskim sajtovima blokiran.[9]
3. Politička cenzura na internetu. Godine 2007, Reporteri bez granica izvestili su da 12 zemalja vrši političku cenzuru na internetu.[10]

Kako se vodi politika sadržaja

Stavke za politiku upravljanja sadržajem sadrže sledeće zakonske i tehničke opcije, koje se koriste u različitim kombinacijama.

Vladino filtriranje sadržaja

Zajednički element za vladino filtriranje je internetski indeks sajtova koji su blokirani za pristup građana.[11] Ako je sajt uključen u internetski indeks, pristup neće biti dozvoljen. Tehnički govoreći, filtriranje najviše koristi blokiranje internetskog protokola (IP) smeštenog na ruteru, ovlašćene servere i preusmeravanje sistema domena imena (DNS-a).[12] Pored zemalja koje se obično povezuju sa ovom praksom, kao što su Kina, Saudijska Arabija i Singapur, i druge zemlje sve više je usvajaju. Na primer, Australija ima sistem filtriranja za specifične nacionalne stranice, iako ne one međunarodne.[13]

Sistemi za privatno ocenjivanje i filtriranje

Suočeni sa potencijalnom opasnošću od raspada interneta usled postavljanja različitih nacionalnih barijera (sistema za filtriranje), W3C (WWW konzorcijum) i druge slične institucije preduzeli su aktiven poteze predlažući primenu sistema za ocenjivanje i filtriranje koji će biti pod kontrolom korisnika.[14] U ovim sistemima, filterski mehanizmi ugrađuju se u internetske pretraživače. Etiketa označava mogućnost dostupnosti naročitog sadržaja na naročitom sajtu. Korišćenje ove vrste filtriranja posebno se favorizuje na dečijim sajtovima.

Filtriranje sadržaja zasnovano na geografskom položaju

Drugo tehničko rešenje koje se odnosi na sadržaj predstavlja geolocirajući softver, koji filtrira pristup naročitom sadržaju sajta prema geografskom ili nacionalnom poreklu korisnika. U tom smislu, važan je bio slučaj Yahoo! budući da je grupa umešanih stručnjaka, uključujući Vinta Serfa, da u 70 do 90% slučajeva Yahoo! može da odredi da li se na delove jednog od njegovih sajtova, na kojima su se nalazile nacističke uspomene, pristupilo iz Francuske.[15] Ova procena je pomogla sudu da dođe do konačne odluke, koja je zahtevala od Jahua! da filtrira pristup nacističkim sadržajima iz Francuske. Kompanije koje proizvode geolocirajući softver tvrde da mogu da identifikuju zemlju porekla bez ikakve greške, a grad u 85% slučajeva, naročito ako je reč o nekom velikom gradu.[16]

Za detaljniju raspravu o jurisdikciji videti Treći deo

Kontrola sadržaja preko pretraživača

Most između krajnjeg korisnika i sadržaja sajta obično predstavlja pretraživač. Objavljeno je da su kineske vlasti započele jedan od prvih primera kontrole sadržaja preko pretraživač. Ako bi korisnici ubacili zabranjene reči u Gugl serč, gubili bi vezu sa internetskim protokolom (IP) na nekoliko minuta.[17] Odgovor kineskog ministarstva za informisanja:

> *. . . savim je normalno kod nekih sajtova na internetu da nekad možete da stupite na njih a nekad ne možete. Ministarstvo nije dobilo nikakve informacije da je Gugl blokiran.*[18]

Filtriranje pretraga bilo je jedan od razloga koji stoje iza nedavne tenzije između Gugla i kineskih vlasti.[19]

Da bi se prilagodio lokalnim zakonima, Gugl je odlučio da ograniči neke sadržaje na nacionalnim sajtovima. Na primer, na nemačkoj i francuskoj verziji Gugla nije moguće naći nacističke sadržaje. Ovo podrazumeva izvestan nivo samocenzure da bi se izbegli potencijalni sudski sporovi.[20]

Izazov Veba 2.0: korisnici kao učesnici

Razvojem platformi Veba 2.0 – blogova, foruma, sajtova za razmenu dokumenata i virtuelnim svetovima – razlika između korisnika i autora zamaglila se. Korisnici interneta mogu da kreiraju velike delove sadržaja sajta, kao što su blogerski postovi, video snimci na Jutjubu i foto galerije.

Identifikovanje, filtriranje i etiketiranje 'neprikladnih' sajtova postaje sve teže. Iako tehnike automatskog filtriranja već postoje, automatsko prepoznavanje, filtriranje i etiketiranje vizuelnih sadržaja ne postoji.

Jedan pristup, koji su u nekoliko prilika koristili Maroko, Pakistan, Turska i Tunis, jeste da se blokira pristup Ju tjubu u celoj zemlji. Međutim, ovaj maksimalistički pristup rezultira i blokadom dozvoljenog sadržaja, uključujući i obrazovni.

Potreba za odgovarajućim zakonskim okvirom

Pravni vakuum u oblasti politike sadržaja pruža vladama visok nivo slobode izbora pri odlučivanju o tome koji sadržaj treba da bude blokiran. Kako je politika sadržaja osetljivo pitanje za svako društvo, usvajanje zakonskih instrumenata je od vitalnog značaja. Nacionalna regulativa u oblasti politike sadržaja može obezbediti bolju zaštitu ljudskih prava i razrešiti ponekad dvosmislenu ulogu provajdera internetskih usluga, agencija i drugih igrača. Poslednjih godina, mnoge zemlje su uvele zakonske propise u vezi s politikom sadržaja.

Međunarodne inicijative

Na međunarodnom nivou, glavne inicijative javljaju se u evropskim zemljama sa strogim zakonskim propisima u oblasti govora mržnje, uključujući antirasizam i antisemitizam. Evropske regionalne institucije pokušavaju da nametnu ove propise i za sajber-prostor. Glavni pravni instrument koji se bavi pitanjem sadržaja jeste Dodatni protokol Saveta Evrope Konvenciji o sajber-kriminalu.

EU je inicirala kontrolu sadržaja, usvajajući Preporuku Evropske komisije protiv rasizma putem interneta. Na praktičnijem planu, EU je uvela Akcioni plan EU za bezbedniji internet, koji sadrži sledeće glavne tačke:

- Uspostavljanje evropske mreže hotlajna za izveštavanje o nezakonitim sadržajima.
- Podsticanje samoregulative.
- Razvijanje klasiranja sadržaja, filtriranja i standardizacije filtriranja.
- Razvijanje softvera i usluga.
- Podizanje svesti o bezbednijem korišćenju interneta.[21]

Organizacija za bezbednost i saradnju u Evropi takođe je aktivna na ovom polju. Od 2003. godine, ona je organizovala više konferencija i sastanaka s naročitim naglaskom na slobodu izražavanja i potencijalnu zloupotrebu interneta (npr. rasistička, ksenofobična i antisemtiska propaganda).

Pitanja

Kontrola sadržaja protiv slobode izražavanja

Kada je reč o kontroli sadržaja, druga strana medalje vrlo često je ograničavanje slobode izražavanja. Ovo je naročito važno u SAD, gde Prvi amandman garantuje široku slobodu izražavanja, čak i pravo objavljivanja sadržaja koji se odnose na nacizam i slično.

Sloboda izražavanja uveliko određuje poziciju SAD u međunarodnoj debati o pitanjima vezanim za sadržaj na internetu. Na primer, iako su SAD potpisale Konvenciju o sajber-kriminalu, one ne mogu da potpišu Dodatni protokol ove konvencije koji se bavi govorom mržnje i kontrolom sadržaja. Pitanje slobode izražavanja bilo je dugo iznošeno u kontekstu sudskog predmeta Jahu! U svojim međunarodnim inicijativama, SAD neće preći liniju koja bi mogla kompromitovati slobodu izražavanja kako je ona određena u Prvom amandmanu.

Nezakoniti oflajn – nezakoniti onlajn

Ovo dovodi raspravu o sadržaju do dileme o stvarnom i o sajber svetu. Postojeći propisi o sadržaju mogu se primeniti na internet. To se često ističe u okviru evropskog konteksta. Okvirna odluka Saveta Evrope o borbi protiv rasizma i ksenofobije izričito ukazuje da je 'ono što je nezakonito oflajn, nezakonito i onlajn'. Jedan od argumenata sajber pristupa regulativi interneta jeste da količina (intenzitet komunikacija, broj poruka) pravi kvalitativnu razliku. Prema ovom stavu, problem govora mržnje nije u tome što nisu doneti nikakvi propisi protiv njega, nego u tome što njegovo širenje preko interneta predstavlja drugačiju vrstu pravnog problema. Opasnosti je izloženo više pojedinaca i teško je sprovesti postojeće propise. Zbog toga se razlika koju donosi internet uglavnom odnosi na probleme sprovođenja, ne na same propise.

Efikasnost kontrole sadržaja

U raspravama o politici interneta, ključni argument je da decentralizovani karakter interneta može da zaobiđe cenzuru. Internet sadrži mnoge tehnike i tehnologije koje mogu da obezbede efikasnu kontrolu. Međutim, tehnički govoreći, kontrolni mehanizmi se mogu zaobići.

U zemljama u kojima kontrolom sadržaja upravlja vlada, tehnički daroviti korisnici pronašli su način da zaobiđu takvu kontrolu. Ipak, kontrola sadržaja nema veze sa ovom malom grupom tehnički darovitih korisnika; ona je okrenuta prema široj populaciji. Prema Lesigu, 'jedan propis ne mora biti apsolutno efikasan da bi bio dovoljno efikasan'.[22]

Ko bi trebalo da bude odgovoran za politiku sadržaja?

Glavni igrači u oblasti kontrole sadržaja jesu vlade. One propisuju koje sadržaje treba a koje ne treba kontrolisati, i na koji način. Provajderi internet usluga (ISP-ovi), kao kapije interneta, obično se smatraju odgovornim za primenu filtriranja sadržaja, bilo prema propisima vlade ili preko samoregulisanja (barem u vezi s pitanjima za koja postoji širok konsenzus, kao što je pornografija).[23] Neke grupe individualnih korisnika, kao što su roditelji, oštro se zalažu za uvođenje efikasnije politike kontrole sadržaja u cilju zaštite dece. Razne ocenjivačke inicijative pomažu roditeljima da nađu sadržaje povoljne za decu. Nove verzije softvera za pretraživanje interneta obično sadrže mnoge opcije za filtriranje. Privatne kompanije i univerziteti takođe vrše kontrolu sadržaja. U nekim slučajevima, sadržaj se kontroliše preko softverskih paketa; na primer, Sajentološki pokret je distribuirao softverski paket svojim pripadnicima – Scienositter – koji sprečava pristup sajtovima koji se kritički odnose prema sajentologiji.[24]

Privatnost i zaštita podataka[25]

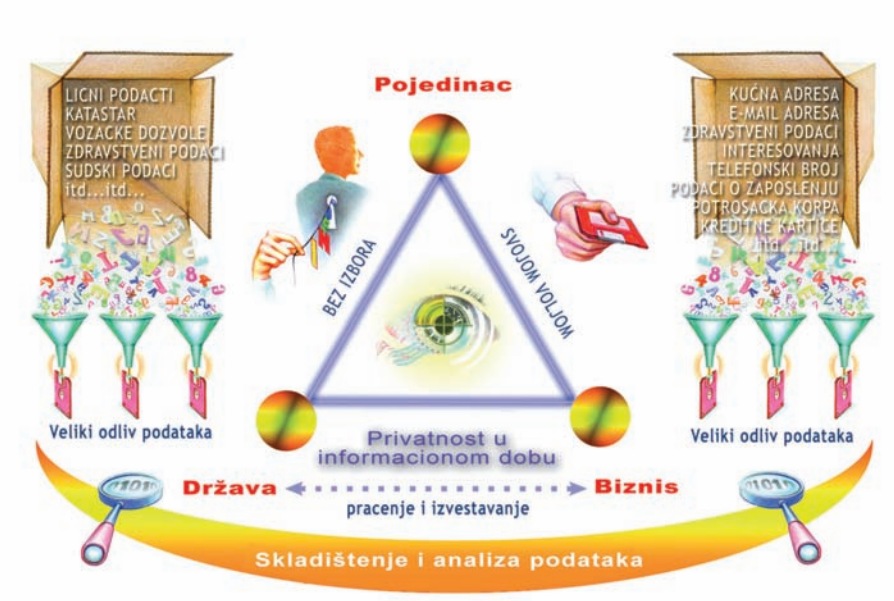
Privatnosti i zaštita podataka predstavljaju dva međusobno povezana pitanja upravljanja internetom. Zaštita podataka je zakonski mehanizam koji obezbeđuje privatnost. Ipak, šta je privatnost? Ona se obično definiše kao pravo svakog građanina da kontroliše svoje lične informacije i da odlučuje o njima (da ih čuva ili otkriva). Privatnost je fundamentalno ljudsko pravo. Priznaju ga Univerzalna deklaracija o ljudskim pravima (UDHR), Međunarodni sporazum o građanskim i političkim pravima imnoge druge međunarodne i regionalne konvencije o ljudskim pravima.

Nacionalne kulture i načini života utiču na praksu privatnosti. Iako je ovo pitanje važno u zapadnim društvima, ono ima možda manji značaj u drugim kulturama. Savremeni postupci u vezi sa privatnošću fokusiraju se na privatnost komunikacije (nema nadgledanja komunikacije) i na privatnost informacija (nema manipulisanja informacijama o pojedincima). Pitanja privatnosti, koja su se obično fokusirala na aktivnosti vlada, proširila su se i sada uključuju poslovni sektor, kao što je prikazano na trouglu privatnosti čija se ilustracija nalazi na drugoj strani.[26]

Zaštita privatnosti: pitanja

Pojedinci i države

Informacije su oduvek bitno sredstvo kojim države vrše vlast nad teritorijama i stanovništvom. Vlade prikupljaju veliki broj ličnih informacija (podaci o rođenju i bračnom stanju, brojevi socijalnog osiguranja, izborni spiskovi,



krivični dosijei, informacije o porezima, o stanovanju, posedovanju kola, itd). Pojedinac ne može da izbegne davanje ličnih podataka, osim da emigrira u neku drugu zemlju, gde ga očekuje isti problem. Informatička tehnologija, kao što je ona koja se koristi za otkrivanje podataka, pomaže u prikupljanju i upoređivanju podataka iz mnogih specijalizovanih sistema (npr. oporezivanje, podaci o stanovanju, posedovanju kola) u cilju vršenja složenih analiza, traganja za uobičajenim i neuobičajenim obrascima i nedoslednostima. Jedan od glavnih izazova inicijativa za elektronsko upravljanje jeste da se obezbedi prava ravnoteža između modernizacije vladinih funkcija i garancije prava građana na privatnost.

Posle događaja u SAD od 11. septembra 2001, Patriotski zakon Sjedinjenih Država i slično zakonodavstvo u drugim zemljama proširili su ovlašćenja vlada na prikupljanje informacija, uključujući odredbu za zakonsko presretanje informacija.[27] Koncept zakonskog presretanja pri prikupljanju dokaza takođe je uključen u Konvenciju o sajber-kriminalu (član 20 i 21) Saveta Evrope.

Pojedinci i kompanije

U trouglu privatnosti koji je gore prikazan, drugi i sve važniji odnos jeste onaj između pojedinaca i poslovnog sektora. Ljudi otkrivaju lične podatke kada otvaraju bankovni račun, kada rezervišu let ili hotel, kada vrše onlajn plaćanja kreditnom karticom, kada pretražuju internet. Mnoštvo tragova podataka često se ostavlja u tim aktivnostima.

U informatičkoj ekonomiji, informacije o potrošačima, uključujući njihove sklonosti i kupovni profil, postaju važan tržišni artikal. Za neke kompanije, kao što su Gugl i Amazon, informacije o sklonostima potrošača čine kamen-temeljac njihovog poslovnog modela. Uspeh i održivost elektronske trgovine, bilo u odnosima kompanija-potrošač ili u odnosima kompanija-kompanija, zavise o uspostavljanju velikog poverenja i u politiku poslovne privatnosti i u bezbednosne mere koje uspostavljaju u cilju zaštite poverljivih informacija o klijentima, od krađe do zloupotrebe.[28]

Države i kompanije

O trećoj strani trougla privatnosti najmanje se govori, a možda je reč o najznačajnijem pitanju privatnosti. I države i kompanije prikupljaju znatan broj podataka o pojedincima. Neki od tih podataka razmenjuju se sa drugim državama i kompanijama da bi se sprečile terorističke aktivnosti. U nekim situacijama, međutim, kao u onima na koje se primenjuje Uputstvo u zaštiti podataka EU, država kontroliše i štiti podatke o pojedinicima koje drže kompanije.

Pojedinci i pojedinci

Poslednji aspekt zaštite privatnosti, koji nije predstavljen u trouglu privatnosti, jeste potencijalna opasnost za privatnost od pojedinaca. Danas svaki pojedinac sa dovoljno novca može da poseduje moćna sredstva za nadzor. Čak i običan mobilni telefon s kamerom može postati sredstvo praćenja. Tehnologija je 'demokratizovala nadzor', da citiramo Ekonomist. Dolazi do mnogo slučajeva napada na privatnost, od običnog voajerizma do prefinjenog korišćenja kamera za snimanje brojeva u bankama i za elektronsku špijunažu. Glavni problem za zaštitu od ove vrste povrede privatnosti počiva u tome što se zakonodavstvo fokusira na opasnosti po privatnost koje dolaze od države. Suočene sa ovom novom realnošću, nekoliko vlada je preduzelo neke početne korake. Kongres SAD usvojio je Zakon o sprečavanju video voajerizma, zabranjujući fotografisanje nagih ljudi bez njihovog odobrenja. Nemačka i nekoliko drugih zemalja usvojile su slične zakone o privatnosti, sprečavajući individualno praćenje.

Međunarodna regulativa privatnosti i zaštite podataka

Jedan od glavnih instrumenata u vezi sa privatnošću i zaštitom podataka predstavlja Konvencija SE za zaštitu pojedinaca u odnosu na automatsku obradu ličnih podataka iz 1981. godine. Iako je ovu konvenciju usvojio Savet Evrope, ona je otvorena za prihvatanje od drugih država, uključujući i vanevropske. Kako je konvencija tehnološki neutralna, izdržala je test vremena. U novije vreme ispituju se mogućnosti njene primene za prikupljanje i obradu biometrijskih podataka.

Uputstvo za zaštitu podataka EU (Directive 45/46/EC) takođe predstavlja važan zakonodavni okvir za obradu ličnih podataka u Evropskoj uniji i ima ogroman uticaj na razvoj nacionalnog zakonodavstva ne samo u Evropi, nego i globalno.

Još jedan ključni međunarodni – neobavezujući – dokument o privatnosti i zaštiti podataka jesu Smernice OECD-a o zaštiti privatnostin i prekograničnom protoku ličnih podataka, iz 1980. godine. Ove smernice i potonji rad OECD-a inspirisali su mnoge međunarodne, regionalne i nacionalne propise o privatnosti i zaštiti podataka. Danas praktično sve zemlje OECD-a imaju zakone o privatnosti i odgovarajuće organe vlasti za njihovu primenu.

Iako su principi smernica OECD-a široko prihvaćeni, glavna razlika se nalazi u načinu njihove primene, naročito između evropskog i američkog pristupa. U Evropi postoji opšte zakonodavstvo u vezi sa zaštitom podataka dok se u Sjedinjenim Državama regulativa u vezi sa privatnošću razvija za svaki sektor privrede, uključujući finansijsku privatnost (Greem-Lič-Blajlijev zakon)[29,30] i dečiju privatnost (Zakon o onlajn zaštiti dečije privatnosti),[31] i medicinsku privatnost (predloženi propisi za zdravstvene usluge).[32]

Druga velika razlika leži u tome što u Evropi zakonodavstvo u vezi sa privatnošću donose državne vlasti, dok u Sjedinjenim Državama donošenje uglavnom počiva na privatnom sektoru i samoregulativi. Kompanije određuju politiku privatnosti. Na kompanijama i pojedincima je da sami odlučuju o politici privatnosti. Glavna kritika za američkog pristupa odnosi se na to da se pojedinci stavljaju u relativno loš položaj; oni su retko svesni važnosti opcija koje im pruža politika privatnosti i obično je prihvataju bez pravog uvida u nju.

Sporazum o sigurnoj luci između SAD i EU

Ova dva pristupa – SAD i EU – zaštiti privatnosti počela su da se sukobljavaju. Glavni problem proističe iz korišćenja ličnih podataka od poslovnih kompanija. Kako može EU, na primer, da nametne svoje propise nekoj softverskoj kompaniji sa sedištem u SAD? Kako može EU da obezbedi da podaci o njenim građanima budu zaštićeni prema pravilima navedenim u Uputstvu o zaštiti podataka? Prema čijim se pravilima (EU ili SAD) rukuje podacima koji se prenose preko mreže kompanije iz EU u SAD? EU je zapretila da će blokirati prenošenje podataka u svaku zemlju koja ne može da obezebdi isti nivo zaštite privatnosti prema kriterijumima navedenim u njenom uputstvu. Ovaj zahtev je neminovno doveo do sudara sa američkim samoregulativnim pristupom zaštiti privatnosti.

Ova duboka razlika otežala je postizanje bilo kojeg mogućeg sporazuma. Štaviše, prilagođavanje američkog prava Uputstvu EU ne bi bilo moguće budući da bi zahtevalo promenu nekoliko važnih principa američkog pravnog sistema. Do značajnog napretka u došlo je kada je američki ambasador Aron predložio formulu 'sigurne luke'. Ovo je preoblikovalo celo pitanje i omogućilo izlaz iz ćorsokaka pregovora.

Do rešenja se došlo tamo gde propisi EU mogu da se primenjuju na američke kompanije unutar sigurne pravne luke. Američke kompanije koje raspolažu podacima građana EU mogu dobrovoljno da potpišu da će poštovati zahteve EU koji se odnose na zaštitu privatnosti. Kada to potpišu, kompanije moraju da poštuju formalne mehanizme izvršenja o kojima su EU i SAD postigle sporazum.

Kada je potpisan 2000. godine, Sporazum o sigurnoj luci prihvaćen je s velikom nadom kao zakonsko sredstvo koje bi moglo rešiti slične probleme s drugim zemljama. Međutim, podaci nisu mnogo ohrabrujući. Ovaj sporazum pretrpeo je kritike Evropskog parlamenta zbog toga što nedovoljno štiti privatnost građana EU. Američke kompanije nisu bile mnogo oduševljene mogućnošću korišćenja ovog pristupa. Prema studiji koju je sačinila Galeksija (Galexia), od 1597 kompanija registrovanih u Okviru sigurne luke, samo 348 ispunjava osnovne zahteve (tj. politiku privatnosti).[33] Obzirom na značaj privatnosti i zaštite podataka u EU, verovatno treba očekivati veći pritisak za pronalaženje nekog rešenja za nefunkcionisanje Sporazuma sigurne luke.

Multijezičnost i kulturna raznolikost

Od samog početka, internet je medij koji koristi prvenstveno engleski jezik. Prema nekim statistikama, približno 80% internetskog sadržaja na engleskom je jeziku, dok 80% svetskog stanovništva ne govori engleski. Ovakva situacija navela je mnoge zemlje da se posvete promovisanju multijezičnosti i zaštiti kulturne raznolikosti. Promovisanje multijezičnosti nije samo kulturno pitanje, nego se nalazi u direktnoj vezi s potrebom za daljim razvojem interneta.[34] Ako internet treba da koriste širi delovi društva ne samo nacionalne elite, sadržaj mora biti dostupan na više jezika.

Pitanja

Nelatinična pisma

Promocija multijezičnosti zahteva tehničke standarde koji olakšavaju korišćenje nelatiničnih pisama. Jednu od prvih inicijativa u vezi sa multijezičnim korišćenjem kompjutera preduzeo je Unikod konzorcijum – neprofitna institucija koja razvija standarde za olakšavanje korišćenja slovnih garnitura za razne jezike. Sa svoje strane, ICANN (Internetska korporacija za dodeljena imena i brojeve) i IETF (Radna grupa za razvijanje interneta) preduzeli su značajan korak za promovisanje Internacionalizovanog imena domena (IDN). IDN olakšava korišćenje imena domena ispisanih na kineskom, arapskom i drugim nelatiničnim pismima.[35]

Mašinsko prevođenje

U cilju poboljšanju mašinskog prevođenja čine se mnogi napori. Obzirom na politiku prevođenja svih zvaničnih aktivnosti na jezike država članica, EU podržava različite aktivnosti u oblasti mašinskog prevođenja. Iako je došlo do velikih pomaka, i dalje ostaju neka ograničenja.

Odgovarajući vladini okviri

Promovisanje multijezičnosti zahteva odgovarajuće vladine okvire. Prvi element režima upravljanja obezbedile su organizacije kao što je UNESKO (Obrazovna, naučna i kulturna organizacija UN). UNESKO je pokrenuo mnoge inicijative, koncentrišući se na multijezičnost, uključujući usvajanje važnih dokumenata, kao što je Univerzalna deklaracija o kulturnoj različitosti. Drugi ključni promoter multijezičnosti je EU, budući da ona odražava multijezičnost kao jedan od osnovnih političkih i radnih principa.

Razvoj i široka upotreba sredstava Veba 2.0, koja omogućuju običnim korisnicima da lako postanu autori priloga i kreatori sadržaja, pruža priliku za veću pristupačnost lokalnih sadržaja na mnoštvu jezika. Ipak, bez šireg okvira za unapređenje multijezičnosti, ova šansa bi mogla da se okonča stvaranjem još dubljeg jaza ako se ne preseče postojeća pozitivna petlja povratne sprege: 'novi korisnici interneta smatraju korisnim da uče engleski i da ga koriste onlajn, jačajući tako jezički prestiž i primoravajući potonje korisnike da takođe uče engleski'.[36]

Globalno javno dobro

Koncept globalnog javnog dobra može se povezati sa mnogim aspektima upravljanja internetom. Najdirektnije veze nalaze se u oblastima pristupa infrastrukturi interneta, zaštite znanja razvijenog preko intetrnetske interakcije, zaštite javnih tehničkih standarda i pristupa onlajn obrazovanju.

Infrastrukturom interneta uglavnom upravljaju privatne kompanije. Jedan od izazova predstavlja harmonizacija privatnog vlasništva nad infrastrukturom interneta sa statusom interneta kao globalnog javnog dobra. Nacionalni zakoni pružaju mogućnost da privatno vlasništvo bude ograničeno nekim javnim zahtevima, uključujući obezbeđivanje jednakih prava svim potencijalnim korisnicima i nemešanje u sadržaj koji se prenosi.

Jedna od glavnih karakteristika interneta jeste da preko svetske interakcije korisnika, dolazi do stvaranja novog znanja i informacija. Preko razmene na imejl listama, društvenim mrežama i blogovima, došlo je do stvaranja znatnog broja spoznaja. Sa izuzetkom organizacije "Zajednička kreativnost" (Creative Commons),[37] ne postoji nikakav zakonski mehanizam koji bi štitio takvo znanje. Ostavljeno u pravnom vakuumu, ono je dostupno za modifikacije i komercijalizaciju. Ovaj zajednički fond znanja, važna baza kreativnosti, nalazi se u opasnosti da bude izbrisan. Što se internetski sadržaj bude više komercijalizovao, to će promene postajati manje spontane. Ovo bi moglo dovesti do smanjene kreativne interakcije.

Koncept globalnog javnog dobra, u kombinaciji sa incijativama kao što su "Zajednička kreativnost", mogao bi da obezbedi rešenja koja bi istovremeno štitila trenutni kreativni ambijent interneta i čuvala znajnje nastalo na internetu za buduće genearcije.

U vezi sa standardizacijom, čine se gotovo stalni napori da se javni standardi zamene privatnim i vlasničkim. To je bio slučaj s Majkrosoftom (preko pretraživača i ASP) i Sun Microsystems (preko Jave). Internetski standardi (uglavnom TCP/IP: prenosni kiontrolni protokol/internetski protokol) otvoreni su za javnost. Režim upravljanja internetom trebalo bi da obezbedi zaštitu glavnih standarad interneta kao globalnog javnog dobra.

Pitanja

Ravnoteža između privatnih i javnih interesa

Jedan od glavnih izazova budućem razvoju interneta predstavlja uspostavljanje ravnoteže između privatnih i javnih interesa. Pitanje je kako sanbdeti privatni sektor pravim komercijalnim ambijentom i istovremeno obezbediti razvoj interneta kao globalnog javnog dobra. U mnogim slučajevima nije reč o 'nultom rezultatu' nego o situaciji u kojoj svi dobijaju. Gugl i mnoge druge kompanije talasa Veb 2.0 uspeli su da razviju poslovne modele koji istovremeno donose profit i omogućuju kreativan razvoj interneta.

Zaštita interneta kao globalnog javnog dobra[38]

Neka rešenja mogu se razviti na osnovu postojećih ekonomskih i zakonskih koncepata. Na primer, ekonomska teorija ima jako razvijen koncept javnih dobara, koji je na međunarodnom nivou proširen na globalna javna dobra. Javno dobro ima dva kritična svojstva: nekonkurentsku potrošnju i neisključivost. Prva znači da potrošnja jednog pojedinca ne oduzima ništa od potrošnje drugog; druga, da je teško, ako ne i nemoguće, isključiti pojedinca da uživa u tom dobru. Pristup materijalima na mreži i mnoge druge internetske usluge ispunjavaju oba kriterijuma: nekonkurentsku potrošnju i neisključivost.

Prava osoba sa invaliditetom[39]

Ujedinjene nacije procenjuju da danas u svetu ima 500 miliona ljudi sa invaliditetom. Ovaj broj se svake godine povećava zahvaljujući faktorima kao što su rat i razaranje, nezdravi životni uslovi, ili odsustvo znanja o invaliditetu, njegovim uzrocima, prevenciji i lečenju.[40] Internet pruža nove mogućnosti za društveno uključivanje (inkluziju) ljudi sa invaliditetom. Da bi se optimizovale tehnološke mogućnosti za ljude sa invaliditetom, postoji potreba za razvijanjem nužnog upravljanja internetom i političkog okvira. Glavni međunarodni instrument u ovoj oblasti jeste Konvencija o pravima lica sa invaliditetom, koju su Ujedinjene nacije usvojile 2006. godine i koju je potpisalo već 139 zemalja, što uspostavlja prava koja se sada nalaze u procesu uključivanja u nacionalna zakonodavstva, a što će ih za nekoliko godina učiniti sprovodljivim.[41]

Svest o potrebi za tehnološkim rešenjima koja uključuju ljude sa invaliditetom povećava se radom organizacija koje vrše podučavanje i stimulišu podršku zajednici invalida, kao što su Dinamična koalicija o

pristupačnosti i invaliditetu Foruma o upravljanju internetom[42] i Odeljak Internet društva o invaliditetu i specijalnim potrebama.[43]

Nedostatak pristupačnosti proističe iz jaza između sposobnosti potrebnih za korišćenje hardvera, softvera i sadržaja, i sposobnosti lica sa invaliditetom. Da bi se ovaj jaz suzio, postoje dva pravca akcija:

1. Uključivanje standarda pristupačnosti u zahteve za dizajniranje i razvoj opreme, softvera i sadržaja.
2. Stimulisanje dostupnosti pomagala kod hardvera i softvera koja povećavaju ili zamenjuju funkcionalne sposobnosti dotičnog lica.

U oblasti upravljanja internetom, glavni fokus odnosi se na sadržaj mreže, budući da se on naglo razvija i da predstavlja jednu vrstu infrastrukture. Mnoge veb-aplikacije nisu saobrazne sa standardima dostupnosti usled nedostatka svesti ili podrazumevane složenosti i visokih troškova (što je daleko od današnje realnosti). Međunarodne standarde veb-dostupnosti razvija W3C koji ih naziva Smernice za dostupnost veb-sadržaja (WCAG).[44]

Jedna programska akcija koja bi trebalo da poveća mogućnosti pristupa ljudi sa invaliditetom jeste Univerzalni dizajn za internet Internet društva:

> *Univerzalni dizajn za internet utvrđuje da prezentacija sadržaja na internetu i dizajn internetske tehnologije bude dovoljno fleksibilan da zadovolji potrebe najšireg mogućeg kruga korisnika, bez obzira na njihovu dob, jezik ili invaliditet.*[45]

Obrazovanje

Internet je otvorio nove mogućnosti za obrazovanje. Uvedene su razne inicijative vezane za elektronsko učenje i za učenje na daljinu; njihov glavni cilj jeste korišćenje interneta kao medija za držanje kurseva. Iako ne može da zameni tradicionalno obrazovanje, onlajn učenje pruža nove mogućnosti za učenje, naročito kada vremenska ili prostorna ograničenja sprečavaju lično pohađanje nastave. Neke procene prognoziraju da će se tržište onlajn učenja u SAD razviti do približno 10 milijardi dolara do kraja 2010.

Tradicionalno, obrazovanjem upravljaju nacionalne institucije. Akreditacija obrazovnih institucija, priznavanje kvalifikacija i uverenja o kvalitetu, svim tim se upravlja na nacionalnom nivou. Međutim, prekogranično obrazovanje zahteva razvijanje novih režima upravljanja. Mnoge međunarodne

inicijative imaju za cilj popunjavanje jaza upravljanja, naročito u oblastima kao što su garancija kvalitetu i priznavanje akademskih nivoa.

Pitanja

STO i obrazovanje

Sporno pitanje u pregovorima Svetske trgovinske organizacije (STO) predstavlja tumačenje članova 1 (3) (b) i (c) Opšteg sporazuma o trgovini i uslugama (GATS), koji navode izuzetke od režima slobodne trgovine za usluge koje pruža vlada. Prema jednom stavu, koji podržavaju uglavnom SAD i UK, ove izuzetke bi trebalo usko posmatrati, omogućujući de facto slobodnu trgovinu u višem obrazovanju. Ovaj se stav prvenstveno rukovodi interesima engleskog govornog obrazovnog sektora da bi se pokrilo globalno obrazovno tržište, tako da je naišao na ozbiljno suprotstavljanje mnogih zemalja.

Predstojeća debata, koja će se verovatno razviti u okviru STO i u drugim međunarodnim organizacijama, koncentrisaće se na dilemu u vezi s obrazovanjem kao robom ili javnim dobrom. Ako se obrazovanje bude smatralo robom, i u ovoj oblasti će se primenjivati pravila slobodnog tržišta. S druge strane, pristup koji obrazovanje smatra javnim dobrom sačuvao bi sadašnji model obrazovanja u kojem državni univerziteti dobijaju specijalni status kao institucije od značaja za nacionalnu kulturu.

Garancija kvaliteta

Raspoloživost sistema onlajn učenja i lak ulazak na ovo tržište otvorili su pitanje garancije kvaliteta. Usredsređenost na onlajn predavanja može prevideti značaj kvaliteta gradiva i didaktike. Mnoštvo mogućih poteškoća može ugroziti kvalitet obrazovanja. Jedna od njih je ulazak novih, uglavnom komercijalno inspirisanih obrazovnih institucija, koje često imaju malo potrebnih akademskih i didaktičkih kapaciteta. Drugi problem garancije kvaliteta leži u tome što jednostavan transfer postojećih papirnatih materijala na onlajn medij ne koristi prednost didaktičkih potencijala novog medija.

Priznavanje akademskih stepena i prenos ispita

Kada je reč o onlajn učenju, glavni izazov predstavlja priznavanje stepena van regionalnog konteksta, uglavnom na globalnom nivou.
EU je počela da razvija regulatorni okvir sa Evropskim sistemom prenosa ispita (ECTS). Azijsko-pacifički region sledi evropsko vođstvo uvođenjem sopstvenog regionalnog modela za razmenu studenata i odgovarajućeg ispitnog sistema (UCTS).

Standardizacija onlajn učenja

Ranu fazu onlajn učenja karakterisao je nagli razvoj i velika raznovrsnost gradiva, u smislu programa, sadržaja i didaktike. Postoji, međutim, potreba za razvijanjem zajedničkih standarda da bi se olakšala razmena onlajn kurseva i uveo određen standard kvaliteta.

Najveći deo standardizacije, u SAD vrše privatne i profesionalčne institucije. Druge inicijative, uključujući međunarodne, učestvuju u mnogo manjem obimu.

Bezbednost dece na internetu[46]

Deca su oduvek veoma ranjiva i lako postaju žrtve. Većina pitanja u vezi sa bezebdnošću na internetu prvenstveno se odnosi na omladinu, posebno na maloletnike. Ipak, zamagljene linije obično postaju oštrije kada se dođe do pitanja bezbednosti dece. Neprijatan sadržaj jasno je označen kao neprikladan i neodgovarajući, a podrazumeva širok spektar materijala uključujući pornografiju, sadržaje ispunjene mržnjom i nasiljem, zatim one koji su opasni za zdravlje, te savete za samoubistvo, anoreksiju i slično.

Pitanja

Maltretiranje predstavlja naročit izazov kada su u pitanju maloletnici. Oni su ranjivi pri korišćenju brojnih sredstava komunikacije koja im stoje na raspolaganju, kao što su razmena poruka, ćaskanje i društvene mreže. Deca mogu lako postati žrtve sajber-siledžijstva – najčešće od strane vršnjaka koji koriste IKT, kombinujući kamere mobilnih telefona, sisteme za razmenu fajlova i društvene mreže, kao pogodna sredstva.

Zlostavljanje i seksualno iskorišćavanje

Štetno ponašanje čija su meta maloletnici može biti naročito opasno kada ga ispoljavaju odrasli. Skriveni identitet jedan je od najčešćih pristupa koji koriste pedofili na internetu. Pretvarajući se da su vršnjaci, ovi ‘onlajn predatori’ prikupljaju informacije i uporno pripremaju dete, lako uspevajući da pridobiju njegovo poverenje, s ciljem da se čak i fizički sretnu. Tako se virtuelno praćenje pretvara u stvarni kontakt i može ići čak do zlostavljanja i iskorišćavanja, pedofilije, saletanja maloletnika u seksualne svrhe, pa čak i do trgovine decom.

Nasilne igre

Nasilne igre (naravno na internetu, recimo u tamnici) sve više dominiraju 'pasivno' nasilnim filmovima. O uticaju koji nasilje vrši na ponašanje mladih sve više se raspravlja. Najozloglašenije igre uključuju suptilno naoružanje (koje ima karakteristike stvarnog oružja i/ili osobine iz mašte) i krvoproliće, a obično se etiketira kao 'eliminatori stresa'. I zaista, 10 vrhunskih igara za razne hardverske platforme, uključujući Majkrosoft Iksboks, Nintendo DS, Nintendo Wii, PC, Plejstejšen, PSP, prepuno je akcionih/nasilnih igara.

Bavljenje izazovima

Glavni izazov s kojim se suočavaju pedagozi i roditelji kod onlajn zaštite dece predstavlja činjenica da su 'digitalni domoroci' mnogo upućeniji u načine korišćenja IKT; oni znaju više, pa ipak razumeju manje. Najvažnija je bliska saradnja među vršnjacima, roditeljima, pedagozima i sa zajednicom. Ipak, roditelji, kreatori politike i šira zajednica širom sveta polako postaju svesniji situacije i pokreću inicijative za zaštitu dece u kompjuterskim ambijentima.

Da bi se podigla svest među akterima, Evropska komisija je pokrenula projekat InSafe – evropsku mrežu za svest o e-bezbednosti koja nudi roditeljima i pedagozima brojne pomoćne materijale na nekoliko jezika, koji se besplatno preuzimaju i šire. Poljska medijska kampanja o sajber-siledžijstvu dala je rezultat u obliku paketa video-klipova i jednog elektronskog kursa o bezebdnosti dece na internetu. Inicijativa NetSafe na Novom Zelandu, osnovana 1998, spada među prve nacionalne inicijative o bezbednosti na internetu; ona okuplja glavne aktere, uključujući ministarstva, poslovni sektor i medije.

Među najuspešnijim modelima nacionalne svesti i kampanja obuke nalazi se egipatska Inicijativa za sajber-mir (CPI). Grupa mladih aktivista, Net-Aman, kao i grupa predstavnika roditelja, obučene su za vođenje daljih aktivnosti. Zajedno s roditeljima, uključujući Ministarstvo telekomunikacija i egipatski Majkrosoft, kao i međunarodne partnere kao što su ChildNet International, CPI je, za nekoliko prošlih godina, doprla do više desetina hiljada omladinaca i roditelja širom zemlje. Sačinila je nekoliko obrazovnih programa za decu, roditelje i pedagoge, koji su prevedeni na arapski.

Pored izgradnje svesti i obučavanja omladine, roditelja i pedagoga, nužan korak predstavlja izgradnja kapaciteta u oblasti bezbednosti na

internetu, orijentisane prema multiakterskom sastavu kreatora politike: vladinim zvaničnicima, poslovnom sektoru, medijima, akademijama, think-thank, NVO, itd. Razne međunarodne organizacije vode raspravu o mogućim modelima saradnje pri osnivanju takvih programa, među kojima se nalaze i Savet Evrope, ITU, CPI i DiploFondacija.

Posmatrano na duži rok, potrebno je osvežavanje obrazovnih programa, koji će uključiti pitanja bezbednosti na internetu kao što su: zaštita lične priavtnosti i bezbednosti, onlajn zaštita ličnog i drugog ugleda, etika, prijavljivanje zlostavljanja, prenošenje morala i veština iz stvarnog života u onlajn svet, itd. Nekoliko takvih inicijativa postoji širom sveta, kao što su Sajber Smart!, ajKipSejf, aj-Sejf i NetSmarc.

Neophodnu komponentu čine nacionalni i međunarodni pravni i politički mehanizmi. Dobar primer predstavlja uspešna Panevropska praška deklaracija za bezbedniji internet za decu, koja je usvojena na Ministarskoj konferenciji (april 2009). Globalni program sajber-bezbednosti (GCA) ITU predstavlja inicijativu Onlajn zaštita dece (COP) kao integralni deo. Postoji još mnogo međunarodnih foruma u kojima je zaštita dece veoma značajno pitanje, uključujući Forum o upravljanju internetom (IGF) sa svojom Dinamičnom koalicijom o onlajn bezbednosti dece.

Međunarodna saradnja u oblasti zaštite dece ima uspešnu istoriju u vezi sa međuanrodnim krizama i hot-line programima. Neke od uspešnih inicijativa su:

- Zvanična saradnja KOSPOLA na Projektu vezanom za materijale kojima se zloupotrebljavaju deca na internetu (CIRCAMP) koji je inicirala Radna grupa evropskih šefova policije.
- Rad NVO u saradnji s vladama, kao što je Internet Watch Foundation, Perverted Justice Foundation, ICMEC, ECPAT, Spasite decu, Asocijacija za sadržaj na internetu, Iskorišćavanje dece i Centar za onlajn zaštitu.
- Javno-privatna partnerstva, kao što je saradnja između norveškog Telekoma i norveške policije.

Fusnote

[1] Povelja o pravima na internetu APK. Dostupno na: **http://www.apc.org/en/node/5677/**

[2] Koalicija za internetska prava i principe (2010). Dostupno na: **http://internetrightsandprinciples.org/**

[3] Povelja o pravima na internetu APK podrazumeva: pristup internetu za sve; slobodu izražavanja; pristup znanju; zajedničko učenje i stvaranje – besplatan i otvoren izvorni softver i tehnološka dostignuća; privatnost, nadzor i kodiranje; upravljanje internetom; svest o pravima, njihova zaštita i ostvarenje. Dostupno na: **http://www.apc.org/en/node/5677**

[4] Inicijativa globalne mreže (2010) Dostupno na: **http://www.globalnetworkinitiative.org**

[5] Konvencija o sajber-kriminalu. Dostupno na: **http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm**

[6] Savet Evrope usvojio je sledeće glavne deklaracije od značaja za ljudska prava i internet: Deklaraciju o slobodi komunikacije na internetu (28.maj 2003); i Deklaraciju o ljudskim pravima i vladavini zakona u infromacionom društvu (13. maj 2005).

[7] Freedom House (2009) *Freedom on the Internet: A global assessment of Internet and digital media*. Dostupno na: **http://www.freedomhouse.org/uploads/specialreports/NetFreedom2009/FreedomOnTheNet_Fullreport.pdf**

[8] Zick T (1999) Kongres, internet i problem neuhvatljive pornografije: Zakon o onlajn zaštiti dece iz 1998. *Creighton Law Review* **32:**1147, 1153, 1201.

[9] Za raspravu o kockanju preko interneta, videti: Karadabil JF (2000) Beleška: Kasina sledećeg milenijuma: pogled u predloženu zabranu kockanja preko interneta. *Arizona Journal of International and Comparative Law* **17:**413, 437-38.

[10] *Internet under surveillance*. Dostupno na: **http://en.rsf.org/spip.php?page=recherche&lang=en&recherche=internet+enemies&image.x=47&image.y=13&image=%3E%3E**

[11] Zittrain J, Edelman B (2008) *Documentation of Internet filtering worldwide*. Open net Initiative. Dostupno na: **http://cyber.law.harvard.edu/filtering/**

[12] Zvanično saudijsko filtriranje obavlja se preko ovlašćenog sistema. Videti: **http://www.isu.net.sa/saudi-internet/content-filtring/filtring-mechanism.htm**

[13] Electronic Frnotiers Australia (2006) *Internet censorship laws in Australia*. Dostupno na: **http://www.efa.org.au/Issues/Censor/cens1.html**

[14] Resnick P. Miller J (1996) PICS: Kontrole pristupa internetu bez cenzure. *Communications of the ACM* **39(10):**87-93. Dostupno na: **http://www.w3.org/PICS/iacwcv2.htm**

15 Iako je Vint Serf učestvovao u raspravi, dao je primedbe na završni izveštaj, za koji je rekao da se nije fokusirao na nedostatke ili krupnije implikacije instaliranja onlajn kapija. Guersney L (2001) *Welcome to the world wide web. Passport please.* Dostupno na: **http://www.criminology.fsu.edu/transcrime/articles/Welcome%20to%20the%20World%20Wide%20Web-%20Passport,%20Please.htm**

16 Akami tvrdi da može da identifikuje geografsku lokaciju ljudi koliko i njihove ZIP kodove. Ovo je tehnološko ograničenje. Informacije o uličnim adresama ne mogu se dobiti iz IP brojeva. *Silicon Valleys Quova Inc., jedan od vodećih provajdera ove tehnologije, tvrdi da može da ispravno identifikuje zemlju korisnika kompjutera u 98 odsto vremenam, a grad u oko 85 odsto vremena, ali samo ako je reč o velikom gradu. Nezavisne studije su označile stopu preciznosti takvih programa, koje prodaju i kompanije kao što su InfoSplit, Digital Envoy, Netgeo o Akami, na 70 do 90 odsto.* Cha AE (2002) Rise of internet borders prompts fears of web's future. *Washington Post,* 4. januar. Dostupno na: **http://www.google-watch.org/geolocat.html**

17 Za pregled članaka o sporu Gugl-KIna, videti: **http://searchenginewatch.com/sereport/article.php/2165031**

18 Knight W (2002) Guglove ključne reči obaraju kineske surfere. New Scientist Internet edition, 13. septembar. Dostupno na: **http://www.newsscientist.com/article/dn2797-google-keywords-knock-chinese-surfers-offline-html**

19 Knight W (2002) On-off access for Google in China. *New Scientist Internet edition,* 13. septembar. Dostupno na: **http://www.newsscientist.com/article/dn2795-onoff-access-for-google-in-china.html**

20 Zittrain J, Edelman B (2002) *Localised Google search result exclusions: statement of issues and call of data.* Harvard Law School. Dostupno na: **http://cyber.law.harvard.edu/filtering/google**

21 EU Information Society (2005) *Safer Internet programme.* Dostupno na: **http://europa.eu/legislation_summaries/information_society/124190_en.htm**

22 Lessig L (1996) The zones of cyberspace (Zone sajber-prostora). *Standford Law Review* **48:**1403, 1405.

23 Asocijacija evropskih provajdera internet usluga (EuroISPA) usvojila je *Smernice o ljudskim pravima za provajdere internet usluga (*Human rights guidelines for Internet service providers). Ovo je zanimljiv primer samoregulative po pitanjima od šireg javnog značaja (ljudska prava). Dostupno na: **http://www.euroispa.org/files/human_rights_guidelines.pdf**

24 Operation Clambake (2010) *Church of Scientology censors net access for members.* Dostupno na: **http://www.xenu.net/archive/events/censorship**

25 Dragocene komentare i podatke dala je Katica Rodrigez.

26 Ovaj izveštaj objašnjava problem privatizacije nadzora i novih izazova koji su povezani sa zaštitom privatnosti: Stanley J (2004) *The surveillance-industrial complex: How the American government is conscripting business and individuals in the construction of surveillance society.* ACLU: New York, NY, USA. Dostupno na: **http://www.aclu.org/FilesPDFs/surveillance_report.pdf**

[27] USA Patriot Act (2001) Dostupno na: **http://www.epic.org/privacy/terrorism/hr3162.html**

[28] Za raspravu o poverenju potrošača u poslovnu zaštitu privatnosti, videti: Whiting R (2002) Wary customers don't trust business to protect privacy. *Information Week,* 19 avgust. Dostupno na: **http://www.informationweek.com/shared/printableArticle.jhtml?articleID=6503045**

[29] Opšti prikaz Grem-Li-Blajlijevog zakona. Dostupno na: **http://www.frbsf.org/publications/banking/gramm/grammpg1.htm**

[30] Grem-Lič-Blajlijev zakon: Privatnost finansijskih informacija potrošača. Dostupno na: **http://www.ftc.gov/privacy/glbact/glboutline.htm**

[31] Zakon o onlajn zaštiti dečije privatnosti iz 1998. Dostupno na: **http://www.ftc.gov/ogc/coppal1.shtm**

[32] Zakon o prenosivosti i odgovornosti za zdravstveno osiguranje iz 1996, *Public Law* 104-191, § 264; Department of Health and Human Services, Standards for Privacy of Individually Identifiable Health Information; Proposed Rule, 64 Fed. Reg. 59917. Dostupno na: **http://www.epic.org/privacy/medical/HHS_medical_privacy_regs.html**

[33] Connolly C (2008) *The US Safe Harbor – Fact or Fiction?* Galexia: Pyrmont, Australia. Dostupno na: **http://www.galexia.com/public/research/artices/research_articles_articles-pa08.html**

[34] Za detaljnije informacije u vezi sa multijezičnošću na internetu, videti: Al-Shatti Q, Aquirre R, Cretu V (2007) *Multilingualism – the communication bridge.* DiploFoundation Internet Governance Research Project. Dostupno na: **http://textus.diplomacy.edu/thina/TxFsetW.asp?URL=http://textus.diplomacy.edu/thina/txgetxdoc.asp?IDconv=3241**

[35] Za detaljnije informacije o IDN, videti: Marson C (2010) Internationalization in Names and Other Identifiers. *IEFT Journal* **5(3).** Dostupno na: **http://www.isoc.org/tools/blogs/ietfjournal/?p=1521**

[36] Vikipedija (2010) *English in computing.* Dostupno na: **http://en.wikipedia.org/wiki/English_on_theInternet#Internet_content**

[37] Creative Commons (CC) je neprofitna organizacija sa sedištem u San Francisku, Kalifornija, Sjedinjene Države, posvećena širenju lepeze kreativnih dela dostupnih drugima da na njima zakonski dograđuju i da ih dele. Ova organizacija je izdala nekoliko licenci za autorska prava poznatih kao Licence "Zajedničke kreativnosti" koje su besplatne za javnost. Ove licence omogućuju stvaraocima da saopšte koja prava rezervišu za sebe, a kojih se odriču u korist primalaca ili drugih stvaralaca (Izvor: Vikipedija).

[38] Arata S, Psaila S (2006) *Protection of Public Interest on the Internet.* DiploFoundation Governance Research Project. Dostupno na: **http://www.diplomacy.edu/ig/Reserach/display.asp?Topic=Research%20Themes%20II#Protection**

39 Dragocene komentare i podatke dao je Horhe Plano.

40 hrea.org (2010) *Human rights of persons with disabilities*. Dostupno na: **http://www.hrea.org/index.php?base_id=152**

41 UN Enable (2010) *Rights and dignity of persons with disabilities*. Dostupno na: **http://www.un.org/disabilities/**

42 IGF (2010) *Dynamic Coalition on Accessibility and Disability*. Dostupno na: **http://www.intgovforum.org/cms/dynamic-coalitions/80-accessibility-and-disability**

43 ISOC (2010) *Internet Society Disability andSpecial Needs Chapter*. Dostupno na: **http://www.isocdisab.org**

44 W3C (1999) *Web Content Accessibility Guidelines 1.0*. Dostupno na: **http://www.w3.org/TR/WCAG10/**

45 Burks M, Waddell C (2001) *Universal design for the Internet*. ISOCMember Briefing No.2. Dostupno na: **http://www.isoc.org/briefings/002/isocbriefing02.txt**

46 Ovaj tekst pripremio je Vladimir Radunović za napredni kurs o sajber-bezebdnosti i bezbednosti na internetu (Internet Governance Capacity Building Program – DiploFoundation).

Sedmi deo

Akteri upravljanja internetom

Akteri upravljanja internetom

Jednu od istaknutih karakteristika upravljanja internetom čini učešće mnoštva aktera, prirodna tema rasprava o o upravljanju internetom budući da nedržavni akteri igraju nadmoćnu ulogu u razvoju i rukovođenju internetom. Civilno društvo, naročito njegov akademski deo, bitan je igrač u oblasti interneta od samih početaka. Ono je osnovalo glavni internetski protokol (Protokol prenosa kontrole/ Internet protokol; TCP/IP) i usluge (i-mejl). Poslovni sektor razvija tehnološku infrastrukturu, uključujući kompjutere, mreže i softver. Vlade su relativne novajlije u oblasti upravljanja internetom.[1]

Glavna razlika između pregovora o upravljanju internetom i drugih globalnih pregovora, kao što su razgovori o ekologiji, počiva u tome što su se kod drugih pregovora međuvladini režimi postepeno otvarali prema nevladinim akterima, a kod pregovora o upravljanju internetom vlade su morale da uđu u postojeći nevladin režim, sazdan oko IETF-a (Radna grupa za razvoj interneta), ISOC-a (Internetsko društvo) i ICANN-a (Internetska korporacija za dodeljena imena i brojeve). Kada je u jednom momentu upravljanje internetom postalo globalno pitanje, ukazala se potreba za približavanjem ova dva režima (nevladin i tradicionalni diplomatski) preko razvoja politike multiakterskog okvira.

Prvi uspešan eksperiment u ovom smeru bila je Radna grupa za upravljanej internetom (WGIG) za vreme Svestkog samita o informacionom društvu (WSIS) koji je održan u periodu 2002-2005.(2) WSIS je bio više od ekspertske, savetodavne grupe, ali manje od tela koje donosi odluke.[3]

Upravljanje internetom – pristup promenljive geometrije

Upravljanje internetom zahteva uključivanje mnoštva aktera koji se razlikuju u mnogim aspektima, uključujući međunarodni pravni kapacitet, zainteresovanost za naročita pitanja upravljanja internetom i raspoloživu stručnost. Takva raznolikost može se smestiti u jedan okvir upravljanja internetom korišćenjem pristupa promenljive geometrije. Ovaj pristup, koji odražava interese aktera, prioritete i kapacitete za bavljenje pitanjima upravljanja internetom, sadržan je u članu 49 Deklaracije WSIS-a, koji navodi sledeće uloge glavnih aktera:

- Države – političko ovlašćenje za pitanja javne politike u vezi s internetom (uključujući međunarodne aspekte).
- Privatni sektor – razvoj interneta, kako u tehničkoj tako i u ekonomskoj oblasti.
- Civilno društvo – važna uloga po pitanjima interneta, naročito na nivou zajednice.
- Međuvladine organizacije – koordinacija pitanja državne politike u vezi s internetom.
- Međunarodne organizacije – razvoj tehničkih standarda i relevantne politike u vezi s internetom.[4]

Ona nije donela zvanična dokumenta UN, ali je suštinski uticala na pregovore WSIS-a o upravljanju internetom. WGIG je predstavljala kompromis u kojem su vlade naklonjene ICANN-u dozvolile da se pitanja upravljanja internetom zvanično pojave na multilateralnim diplomatskim programima i u kojem su druge vlade, uglavnom iz zemalja u razvoju, prihvatile učešće nedržavnih aktera. Ovaj kompromis rezultirao je uspehom WGIG-a.

Kao produžetak WSIS-a, upravljanje internetom ostaje na globalnom dnevnom redu preko Foruma za upravljanje internetom (IGF).

IGF prati strukturu učestvovanja WGIG-a. I WGIG i IGF ostaju korisni primeri za budući razvoj multiakterskog partnerstva na međunarodnom planu.

Vlade

Poslednjih sedam godina – od uvođenja upravljanja internetom u političke programe 2003. godine – predstavljaju proces učenja za mnoge vlade. Čak i za velike i bogate zemlje, bavljenje internetom

postavilo je brojne izazove, kao što je rukovođenje multidisciplinarnim karakterom interneta (tehnološki, ekonomski i društveni aspekti), i uključilo je široku raznolikost aktera. Mnoge vlade morale su da obučavaju činovnike, da razvijaju politiku i da aktivno učestvuju na raznim forumima o upravljanju internetom, a uz to se još hvatajući u koštac s novim fenomenom upravljanja internetom.

Nacionalna koordinacija

Godine 2003, na početku procesa WSIS-a, većina zemalja bavila se pitanjima upravljanja internetom preko 'tehničkih' ministarstava, obično onih koja su bila odgovorna za odnose sa Međunarodnom telekomunikacionom unijom (ITU). Postepeno, kako su shvatale da je upravljanje internetom više od 'žica i kablova', vlade su počele da uključuju činovnike iz drugih, manje tehničkih ministarstava, kao što su kultura, mediji i pravda.

Glavni izazov za mnoge vlade bilo je razvijanje strategije za dobijanje i efikasno koordiniranje podrške od nedržavnih aktera, kao što su univerziteti, privatne kompanije i nevladine organizacije (NVO) koje imaju potrebne stručnjake za za bavljenje pitanjima upravljanja internetom. Tokom procesa WSIS-a, većina velikih i srednjih država uspela je da razvije dovoljan institucionalni kapacitet da prati globalne pregovore o upravljanju internetom. Neke od njih, kao što je Brazil, razvile su inovativnu nacionalnu strukturu za praćenje debate o upravljanju internetom, uključujući ministarstva telekoma, diplomatiju, poslovni sektor, civilni sektor i akademske krugove.[5]

Kablovska 'geostrategija' i politička (ne)doslednost

Anglofrancuski savez osnovan je 1904. godine. Međutim, uspostavljanjem bliske saradnje s Nemačkom, Telegrafsko ministarstvo Francuske nije sledilo opštu politiku zemlje. Ministarstvo je želelo da oslabi britansku dominaciju u globalnoj 'kablovskoj geostrategiji' polažući nove telegrafske kablove u saradnji s Nemačkom. Francuski istoričar Šarl Lesaž dao je sledeći komentar o ovoj političkoj (ne)doslednosti:

Produženo neslaganje između opštih principa francuske diplomatije i procedura telegrafske politike potiče, verujem, iz činjenice da u ovoj zemlji svako ministarstvo vodi sopstvenu spoljnu politiku: Ministarstvo spoljnih poslova ima jednu, Ministarstvo finansija drugu. . . Poštanska i telegrafska uprava takođe, s vremena na vreme, vodi spoljnu politiku; tako se desilo da je, tokom poslednjih nekoliko godina, iako nije bila sasvim neprijateljska prema Engleskoj, pokazala snažnu naklonost prema Nemačkoj.[6]

Politička doslednost

Obzirom na multidisciplinarni karakter upravljanja internetom i na veliku raznolikost aktera i političkih foruma, poseba izazov predstavlja postizanje političke doslednosti. To zahteva od mnogih vlada da imaju fleksibilan oblik političke koordinacije, uključujući horizontalnu komunikaciju između različitih ministarstva, poslovnog sektora i drugih aktera. Tradicionalna struktura vlade, zasnovana na strogoj hijerarhiji, mogla bi predstavljati prepreku razvoju tako fleksibilne koordinacije.

Pored izazova rukovođenja, postizanje političke doslednosti obično je ograničeno postojanjem konkurentskih političkih interesa. Ovo je naročito slučaj u razvijenim i razgranatim internetskim privredama. Na primer, mrežna neutralnost je jedno od najnovijih pitanja u koje se umešala američka vlada delikatno izbalansiranim zakonom između internetskog sektora privrede (Gugl, Jahu!) koji snažno podržava mrežnu neutralnost i telekomunikacionog/zabavnog sektora (Verizon i AT&AT, Holivudski lobi), koji na nju gleda kao na prepreku za razvijanje novog poslovnog modela zasnovanog na bržem internetu, za distribuciju multimedijalnog sadržaja.

Tehnološko približavanje između različitih medija daće još jedan impuls postizanju političke doslednosti. Ranije različita politička područja, kao što su telekomunikacije i televizija, moraće da se integrišu da bi odražavala tehnološku konvergenciju.

Za dalju raspravu o konvergenciji videti Drugi deo

Značaj stalnih misija sa sedištem u Ženevi

Za mnoge vlade, stalne misije u Ženevi bile su važni, ako ne i vitalni, igrači u procesu WSIS-a i u procesu upravljanja internetom.Većina aktivnosti odvijala se u Ženevi, sedištu ITU koja je igrala važnu ulogu u ovim procesima. Prvi WSIS 2003. dogodio se u Ženevi i svi pripremni sasatanci, izuzev jednog, održani su u Ženevi, usled čega su stalne misije sa sedištem u tom gradu bile direktno uključene. Trenutno, Sekretarijat IGF-a ima sedište u Ženevi i svi pripremni sastanci održavaju se u ovom gradu.

Za velike i razvijene zemlje, stalne misije bile su deo široke mreže institucija i pojedinaca koji su se bavili procesima WSIS-a i upravljanja internetom. Za male i zemlje u razvoju, stalne misije bile su glavni, a u nekim situacijama i jedini učesnici u tim procesima. Portfelj WSIS-a pridodat je poslovima malih i obično prezauzetih misija zemalja u razvoju. U mnogim slučajevima, isti diplomata morao je da preuzme zadatke povezane sa WSIS-om zajedno s drugim pitanjima, kao što su ljudska prava, zdravlje, trgovina i rad.

'Diplomatizacija' procesa upravljanja internetom

WSIS je postavio internet na globalni diplomatski dnevni red. Pre WSIS-a, o internetu se raspravljalo prvenstveno u nevladinim krugovima ili na nacionalnom nivou. 'Diplomatizacija' pitanja politike interneta izazvala je različite reakcije. Kenet Nil Kukijer, tehnološki dopisnik *Ekonomista*, isticao je negativan aspekt 'diplomatizacije' rasprave o upravljanju internetom:

> *. . . podizanjem ovog pitanja na formalni samit Ujedinjenih nacija, to po svojoj prirodi širi značaj teme unutar vlada. Kao posledica toga, pitanja vezana za informaciono društvo, koja su ranije razmatrali manje politički i manje vidljivi delovi vlade – kao naučnu i tehnološku ili medijsku i kulturnu stvar – prebačena su u ministarstva spoljnih poslova i predata diplomatama sa iskustvom, koji su više naviknuti na politiku sile i manje upoznati sa tehnološkim pitanjima i suštinskim zahtevom interneta za saradnjom i međuzavisnošću.*[7]

Za detaljnu raspravu o ulozi Nitina Desaja i Markusa Kumera u IGF-u videti Osmi deo

Proces diplomatizacije imao je neke pozitivne efekte na rasprave u okviru WSIS-a. Na primer, diplomate su dale nepristrasan doprinos dugotrajnim debatama o pitanjima vezanim za ICANN: imena domena, internetski brojevi i glavni serveri. Doprinos diplomata bio je naročito vidljiv u raspravi WGIG-u. Diplomatsko vođstvo WGIG-a (predsedavajući Nitin Desaj i izvršni direktor Markus Kumer) stvorilo je prijatnu atmosferu u kojoj razlike među predstavnicima, uključujući one iz tehničke zajednice, nisu blokirale proces. Rad WGIG-a rezultirao je Završnim izveštajem koji je naglašavao razlike, ali je isto tako obezbeđivao rešenje u odnosu na proces za buduće rasprave, osnivanjem IGF-a.

Pozicija Vlade SAD

Internet se razvio kao deo projekta koji je finansirala Vlada SAD. Od nastanka interneta do danas, američka vlada uključena je u upravljanje internetom preko raznih ministarstava i agencija, u početku preko Ministarstva odbrane, kasnije preko Nacionalne fondacije za nauku, a u najnovije vreme preko Ministarstva trgovine. Savezna komisija za komunikacije takođe igra važnu ulogu u stvaranju zakonskog okvira za razvoj interneta.

Konstantu uključenosti američke vlade predstavlja njen pristup nemešanja, pri čemu se ona obično opisuje kao 'udaljeni staratelj'. Ona postavlja okvir a upravljanje internetom prepušta onima koji neposredno rade na njemu, što je uglavnom internetska zajednica. Međutim, Vlada SAD je u nekoliko navrata intervenisala direktnije, kao što beše sredinom devedesetih godina, kada je projekat CORE mogao da prebaci glavni server i rukovođenje glavnom strukturom interneta iz SAD u Ženevu. Ovaj proces je zaustavljen čuvenom – barem u istoriji interneta – diplomatskom notom koju je poslala državni sekretar Medlin Olbrajt generalnom sekretaru ITU.[8] Paralelno sa zaustavljanjem inicijative CORE, američka vlada je započela konsultacije koje su rezultirale osnivanjem ICANN-a.

Od stvaranja ICANN-a, američka vlada pokazuje nameru da se povuče iz nadgledanja ICANN-a kada on stekne institucionalnu i funkcionalnu čvrstinu. Ovaj proces povlačenja započet je početkom oktobra 2009, potpisivanjem Izjave o obavezama od strane Ministarstva trgovine SAD i ICANN-a. Prema ovom dokumentu, ICANN će postati nezavisna organizacija. Drugi element ovog specijalnog odnosa između Ministarstva trgovine SAD i ICANN-a – ugovor o IANA (Internetska uprava za dodeljene brojeve) – biće revidiran 2011. godine.

Na globalnoj sceni, tokom procesa WSIS-a, SAD su se suprotstavile mogućem preuzimanju funkcija ICANN-a od strane nekog međuvladinog tela. Međutim, u toku trajanja WSIS-a, američka vlada preduzela je prve korake ka internacionalizaciji uloge ICANN-a priznavanjem prava nacionalnim vladama nad odgovarajućim imenima domena i prihvatanjem nastavka međunarodnih rasprava preko osnivanja IGF-a.

Pozicija drugih vlada

Spektar politike upravljanja internetom počeo je nedavno da dobija konture razvojem nacionalnih pozicija vlada. Na jednoj strani ovog političkog spektra nalazio se stav da bi trebalo da jedna međuvladina organizacija, kao što je ITU, preuzme upravljanje internetom. Ovo je bila početna pozicija mnogih zemalja u razvoju. Najgrlatije zemlje u propagiranju istaknute uloge ITU bile su Kina, Iran i Rusija. Neke zemlje u razvoju zalagale su se za stvaranje nove međunarodne organizacije koja bi zamenila ITU, uključujući osnivanje nove ugovorne organizacije, kao što je možda 'Međuanrodna internetska organizacija'. Druge zemlje tvrdile su da bi upravljanje internetom trebalo da preuzme nova vrsta multiakterske organizacije.

U centru ovog političkog spektra nalazile su se vlade koje su tvrdile da ICANN treba da zadrži svoje tehničke funkcije, dok bi novo međunarodno telo imalo nadzornu političku funkciju. Ovo je pozicija koju je postepeno zauzela EU.

Na drugom kraju ovog političkog spektra, SAD su tvrdile da ne treba ništa da se menja u važećem režimu koji je smešten u ICANN-u. Kanada, Australija i Novi Zeland ponudili su slične stavove, dodatno se zalažući za veću internacionalizaciju ICANN-a. Ove zemlje, zajedno sa EU, Švajcarskom i nekoliko zemalja u razvoju, odigrale su značajnu ulogu u postizanju kompromisa po pitanju upravljanja internetom u toku procesa WSIS-a.

Pozicija malih zemalja

Složenost pitanja i dinamike aktivnosti gotovo da je onemogućila mnoge male zemlje, a posebno male zemlje u razvoju, da prate sva događanja, a kamoli da imaju bilo kakav bitan uticaj. Usled toga, neke male države podržavale su varijantu da se pitanja upravljanja internetom rešavaju na jednom mestu. Sam obim programa i ograničen politički kapacitet zemalja u razvoju, kako kod kuće tako u diplomatskim misijama, ostali su jedna od glavnih prepreka njihovom punom učešću u ovom procesu. Potreba za izgradnjom kapaciteta u oblasti upravljanja internetom i politici prepoznata je kao jedan od prioriteta za dnevni red informacionog društva WSIS-a u Tunisu.

Poslovni sektor[10]

Za dodatnu raspravu o zaštitnim znakovima videti Treći deo

Kada je ICANN osnovan, 1998, jedna od glavnih briga poslovnog sektora bila je zaštita zaštitnih žigova. Mnoge kompanije bile su suočene sa sajber-skvotovanjem i zloupotrebom svojih zaštitnih znakova od strane pojedinaca koji su bili dovoljno brzi da ih prvi ragistruju. U procesu stvaranja ICANN-a, poslovni krugovi su jasno dali prioritet bavljenju zaštitom zaštitnih znakova i, shodno tome, ovo pitanje je pokrenuto čim je osnovan ICANN.[11]

Danas, razvojem interneta, zainteresovanost poslovnog sektora za upravljanje internetom proširila se i razgranala, pri čemu imamo sledeće glavne grupe poslovnih kompanija: kompanije za imena domena, provajderi internet usluga (ISP), proizvođači softvera i kompanije za internetski sadržaj.

Međunarodna trgovinska komora (ICC)

Međunarodna trgovinska komora (ICC), poznata kao asocijacija koja predstavlja poslove preko sektora i geografskih granica, pozicionirala se kao jedan od glavnih predstavnika poslovnog sektora u procesu globalnog upravljanja internetom. ICC (MTK) je bila aktivno uključena u prve pregovore WGIG-a i WSIS-a, a i dalje je aktivan učesnik u procesu IGF-a.

Kompanije za imena domena

Kompanije za imena domena uključuju administratore i registre koji prodaju imena domena (npr. .com, .edu). U glavne igrače u ovom sektoru spadaju VeriSajn i Afilias. Njihov posao nalazi se pod direktnim uticajem političkih odluka ICANN-a u oblastima kao što su uvođenje novih domena i rešavanje sporova. To ih svrstava među najvažnije aktere u procesu stvaranja politike ICANN-a. Oni su takođe uključeni u širi politički proces upravljanja internetom (WSIS, WGIG, IGF) sa glavnim ciljem da se smanji opasnost od potencijalnog preuzimanja uloge ICANN-a od strane drugih igrača, uglavnom nacionalnih vlada i međunarodnih organizacija.

Provajderi internet usluga

Za dodatnu raspravu o ISP-ovima videti Drugi deo

ISP-ovi su kompanije ili organizacije koje deluju kao kapije kroz koje se pristupa internetu. Kako su ISP-ovi ključni onlajn posrednici, to ih čini naročito značajnim za upravljanje internetom. Njihova glavna angažovanost odvija se na nacionalnom nivou u poslovanju sa vladinim i zakonodavnim vlastima. Na globalnom nivou, neki ISP-ovi, naročito iz SAD i Evrope, bili su aktivni u procesima WSIS/WGIG/IGF individualno, a još više preko ICC (MTK) i njene OSNOVNE inicijative, te preko nacionalnih i regionalnih ili sektorskih poslovnih organizacija kao što su ETNO (Asocijacija evropskih telekomunikacijskih mrežnih operatera) i ITAA (Informaciono-tehnološka asocijacija Amerike) i druge.

Telekomunikacione kompanije

Ove kompanije olakšavaju internetski saobraćaj i rukovode infrastrukturom interneta. U glavne igrače spadaju kompanije kao što su Verizon i AT&T. Tradicionalno, telekomunikacione kompanije učestvuju u međunarodnoj telekomunikacionoj politici preko ITU. Sve više se uključuju u aktivnosti ICANN-a i IGF-a. Njihova primarna zainteresovanost

za upravljanje internetom jeste da obezbede poslovno prijatan globalni ambijent za razvoj internetske telekomunikacione infrastrukture.

Za dodatnu raspravu o IPR videti Treći deo

Softverske kompanije

Kompanije kao što su Majkrosoft, Adobe i Orekl uglavnom su uključene u aktivnosti različitih tela za standardizaciju (W3C – WWW konzorcijum; IETF). U samom početku procesa WSIS-a, glavna briga bila je mogućnost otvaranja rasprave o pravima na inletektualnu svojinu (IPR) na internetu. Pošto je bilo jasno da WSIS neće ulaziti u oblast IPR, interesovanje softverskih kompanija za proces WSIS-a oslabilo je. Ovakav trend traje od prvog samita.

Kompanije za internetski sadržaj

U njih spadaju glavne internetske marke kao što su Gugl, Fejsbuk i Tviter. Ova grupa kompanija postala je mnogo važna razvojem aplikacija Veba 2.0. Njihovi poslovni prioriteti blisko su povezani sa raznim pitanjima upravljanja internetom, kao što su intelektualna svojina, privatnost i sajber-bezbednost. Njihovo prisustvo se sve više zapaža u globalnim procesima upravljanja internetom.

Civilno društvo

NVO i WSIS

Učešće NVO na WSIS-u bilo je relativno slabo. Od blizu 3 000 NVO koje imaju konsultativni status Ekonomskog i društvenog saveta UN, samo njih 300 učestvovalo je na WSIS-u.

Civilno društvo je najglasniji i najaktivniji propagator multiakterskog pristupa upravljanja internetom. Uobičajena kritika učestvovanja civilnog društva na prethodnim multilateralnim forumima bila je nedostatak prave koordinacije i prisustvo previše, često disonantnih, glasova. Međutim, u procsu WSIS-a reprezentacija civilnog društvo uspela je obuzda ovu suštinsku složenost i raznolikost preko nekoliko organizacionih formi, uključujući Biro civilnog društva, Kvorum civilnog društva i Grupu za sadržaj i teme. Suočene sa ograničenim mogućnostima da utiču na formalni proces, grupe civilnog društva razvile su dvosmerni pristup. Nastavile su sa

prisustvovanjem u formalnom procesu koristeći raspoložive mogućnosti da učestvuju i lobiraju kod vlada. Paralelno s tim, pripremali su Deklaraciju civilnog društva kao alternativnu viziju glavnoj deklaraciji koja je usvojena na ženevskom samitu WSIS-a.

Zahvaljujući multiakterskom karakteru WGIG-a, civilno društvo je dostiglo visok nivo uključenosti. Grupe civilnog društva predložile su osam kandidata za WGIG, od kojih su svi kasnije imenovani od strane generalnog sekretara UN. U tuniskoj fazi (druga faza WSIS-a, posle Ženeve), glavni politički proboj organizacija civilnog društva pomerio se ka WGIG-u, gde su uticali na mnoge zaključke, kao i na odluku da se osnuje IGF kao multiakterski prostor za raspravu o pitanjima upravljanja internetom. Civilno društvo nastavlja da se angažuje na aktivnostima IGF-a.

Međunarodne organizacije

ITU je bila centralna međunarodna organizacija u procesu WSIS-a. Bila je domaćin Sekretarijatu WSIS-a i obezbedila je politički sadržaj za glavna pitanja. Angažovanje ITU u procesu WSIS-a bilo je deo njenog pokušaja da definiše i konsoliduje svoju novu poziciju u globalnoj telekomunikacionoj areni koja se naglo menjala, a koju je sve više oblikovao internet. Uloga ITU osporavana je na razne načine. Ona je gubila svoj tradicionalni politički domen zahvaljujući liberalizaciji globalnog telekomunikacionog tržišta koju je predvodila STO. Najnoviji trend prebacivanja telefonskog saobraćaja sa tradicionalnih komunikacija na internet (preko VoIP-a) dodatno je smanjio 'regulativni trag' ITU na polju globalnih telekomunikacija.

Mogućnost da bi ITU mogla da izađe iz procesa WSIS-a *de facto* kao 'Međunarodna internetska organizacija' izazvala je zabrinutost u SAD i nekim razvijenim zemljama, dobivši podršku od nekih zemalja u razvoju. Tokom celog trajanja WSIS-a, ova mogućnost stvarala je naglašene političke tenzije. To je bilo naročito očito u oblasti upravljanja internetom, gde je napetost između ICANN-a i ITU postojala još od osnivanja ICANN-a 1998. godine. WSIS nije razrešio ovu tenziju. Sa sve većom konvergencijom raznih komunikacionih tehnologija, vrlo je verovatno da će se pitanje aktivnije uloge ITU u oblasti upravljanja internetom ponovo pojaviti u raspravama o politici.

Drugo pitanje odnosilo se na uklapanje multidisciplinarnog programa WSIS-a u porodicu specijalizovanih agencija UN. Netehnički aspekti komu-

nikacija i internetske tehnologije, kao što su društvene, ekonomske i kulturne karakteristike, deo su mandata drugih organizacija UN. Najistaknutiji igrač u ovom kontekstu je UNESKO, koji se bavi pitanjima kao što je multijezičnost, kulturna raznolikost, naučna društva i pravo na informacije. Ravnotežom između ITU i drugih organizacija UN vrlo pažljivo se manipulisalo. Procesi nastali posle WSIS-a takođe odražavaju ovu ravnotežu, a među glavnim igračima su ITU, UNESKO i UNDP (Razvojni program UN).

Drugi učesnici

Osim formalnih učesnika WSIS-a, drugi igrači – internetska zajednica i ICANN – koji nisu bili zvanično priznati kao akteri, učestvovali su u ovom procesu uglavnom preko civilnog društva i poslovnog sektora.

Internetska zajednica

Terminologija

Drugi termini koriste se naizmenično sa 'internetskom zajednicom', kao što su očevi interneta i tehnolozi. Mi koristimo termin 'internetska zajednica' zato što ona podrazumeva visok nivo zajedničkih vrednosti njenih pripadnika. Ovaj niz zajedničkih vrednosti jedna je od izrazitih karakteristika zajednice.

Internetska zajednica uključuje institucije i pojedince koji razvijaju i propagiraju internet od njegovog početka. Istorijski posmatrano, pripadnici internetske zajednice bili su povezani sa univerzitetima, gde su radili prvenstveno na razvijanju tehničkih standarda i na uspostavljanju osnovne funkcionalnosti interneta. Internetska zajednica je takođe stvorila onaj početni duh interneta koji se zasniva na principima deljenja resursa, otvorenog pristupa i protivljenja mešanju vlade u regulisanje interneta. Od samog početka njeni pripadnici štitili su početni koncept interneta od snažne komercijalizacije i jakog uticaja vlade.

U kontekstu međunarodnih odnosa, internetska zajednica predstavlja naučnu zajednicu.[12] Ranu internetsku zajednicu vodilo je nekoliko, uglavnom prećutnih, pravila i jedna glavna formalna procedura – Zahtev za komentare (RFC). Svi glavni i osnovni standardi interneta opisani su preko RFC. Iako ti zahtevi nisu imali strogu regulativnu ili formalnu strukturu, rane internetske zajednice rukovodile su se snažnim običajem i pritiskom na sebi slične. Većina učesnika u ovom procesu delila je slične vrednosti, sisteme ocenjivanja i stavove.

Rano rukovođenje internetom od strane internetske zajednice osporeno je sredinom devedesetih godina pošto je internet postao deo globalnog društvenog i privrednog života. Razvoj interneta uveo je grupu novih aktera, kao što je poslovni sektor, koji su došliiz različitih profesionalnih kultura i shvatanja interneta i njegovog upravljanja, što je dovelo do povećane tenzije. Na primer, devedesetih godina, internetske zajednice i Network Solutions,[13] ušli su u tzv. DNS rat, sukob u vezi sa kontrolom glavnih servera i Sistema imena domena.

Danas, internetsku zajednicu predstavljaju ISOC i IETF. ISOC je odigrao bitnu ulogu u standardizaciji interneta i promovisanju suštinskih vrednosti interneta, kao što je otvorenost. On je takođe aktivno uključenn u izgradnju kapaciteta i pružanje pomoći zemljama u razvoju, uglavnom u Africi, da razviju osnovnu internetsku infrastrukturu.

Internetska zaednica bila je važan akter i u procesu osnivanja i rukovođenja ICANN-om. Jedan od 'očeva interneta', Vint Serf, bio je predsednik Borda ICANN-a od 2000. do 2007. godine. Pripadnici internetske zajednice drže važne položaje u raznim organima odlučivanja u ICANN-u.

Druga vrsta kritike fokusira se na činjenicu da je, sa 2 milijarde korisnika, internet prevazišao politički okvir baziran na ICANN-u koji se fokusira na internetsku zajednicu kao na glavno biračko telo. Sledeći ovaj argument, kako se linija između građana i korisnika interneta zamagljuje, zahteva se veće angažovanje vlada i drugih struktura koje predstavljaju građane pre nego onih koje predstavljaju samo korisnike interneta, a koji se često opisuju kao 'internetska zajednica'. Oni koji su se zalagali za veće angažovanje vlada u upravljanju internetom koristili su ovaj pristup predstavljanja građana pre nego korisnika interneta i zajednica.

Internetska zajednica obično opravdava svoju specijalnu poziciju u upravljanju internetom tehničkom stručnošću. Ona tvrdi da je ICANN tehnička organizacija i da zato treba da je vode stručnjaci za tehniku koristeći stručna znanja. Sa sve većim poteškoćama održavanja ICANN-a kao isključivo tehničke organizacije, opravdavanje specijalne uloge internetske zajednice suočava se sa čestim izazovima. Vrlo je verovatno da će se pripadnici internetske zajednice postepeno integrisati u glavna akterske grupe, uglavnom civilno društvo i poslovni sektor, ali i u vlade. Iako internetska zajednica može nestati kao zasebna grupa zainteresova-

nih učesnika, biće značajno da se sačuvaju vrednosti koje ona promoviše: otvorenost, učestvovanje u znanju i zaštita interesa korisnika interneta.

Internetska korporacija za dodeljena imena i brojeve (ICANN)

ICANN je glavna institucija upravljanja internetom. Odgovoran je za rukovođenje glavnom strukturom interneta, koja se sastoji od adresa Internetskog protokola (IP), imena domena i glavnih servera. Sve veće interesovanje za ulogu ICANN-a odvijalo se paralelno s razvojem interneta početkom milenijuma i ICANN je privukao pažnju globalnih političkih krugova tokom procesa WSIS-a (2002-2005).

Iako je WSIS glavni akter u oblasti upravljanja internetom, on ne upravlja svim aspektima interneta. Ponekad ga, iako pogrešno, opisuju kao 'internetsku vladu'. ICANN rukovodi strukturom interneta, ali nema ovlašćenja nad drugim aspektima upravljanja internetom, kao što su sajber-bezebdnost, politika sadržaja, zaštita autorskih prava, zaštita privatnosti, održavanje kulturne raznolikosti ili premošćivanje digitalnog jaza.

ICANN je neprofitna korporacija registrovana u Kaliforniji. Njena funkcionalna ovlašćenja počivala su na Memorandumu o razumevanju (MoU) sa Ministarstvom trgovine SAD, koji je inicijalno potpisan 1998. i dva puta produžavan, drugi put od septembra 2006. do septembra 2009. Od 1. oktobra 2009, formalni osnov za funkciju ICANN-a predstavlja Izjava o obavezama koju su potpisali ICANN i Ministarstvo trgovine SAD. Ovaj dokument trasira put za ICANN kao nezavisnu instituciju.

ICANN je multiakterska institucija koja uključuje mnoštvo aktera s različitim mogućnostima i ulogama. Oni spadaju u četiri glavne grupe:

1. Akteri koji su uključeni od samog osnivanja ICANN-a, uključujući internetsku zajednicu, poslovnu zajednicu i Vladu SAD.
2. Međunarodne organizacije, s najznačajnijom ulogom ITU i Svetske organizacije za intelektualnu svojinu (WIPO).
3. Nacionalne vlade čije je povećano interesovanje za preuzimanje veće uloge u ICANN-u počelo s procesom WSIS-a.
4. Korisnici interneta (zajednica uopšte).

ICANN je eksperimentisao raznim pristupima da bi uključio korisnike interneta. U početnim danima, prvi pokušaj bio je da se korisnici interneta uključe preko neposrednih izbora svojih predstavnika u rukovodeća tela ICANN-a. Bio je to i pokušaj da se ICANN-u obezbedi legitimna baza. Sa slabim odzivom i zloupotrebom postupka, neposredno glasanje je propalo zato što nije obezbedilo stvarno predstavljanje internet korisnika. U novije vreme, ICANN pokušava da uključi korisnike interneta preko upravljačke strukture 'kao celine'. Ovaj organizacioni ekepsriment još traje.

Na proces donošenja odluka u ICANN-u uticali su rani procesi upravljanja internetom zasnovani na transparentnim, otvorenim i obuhvatnim pristupima koji idu odozdo. Jedna od glavnih razlika između prve internetske zajednice iz osamdesetih godina i sadašnjeg konteksta odlučivanja u ICANN-u jeste nivo 'društvenog kapitala'. U prošlosti, internetska zajednica je imala visok nivo međusobnog poverenja i solidarnosti koji je mnogo pojednostavljivao proces donošenja odluka i rešavanja sporova u donosu na sadašnju situaciju. Razvoj interneta uključio je druge aktere, pa bi shodno tome bilo teško identifikovati bilo kakav društveni kapital među sadašnjim korisnicima interneta. Tako je zahtev internetske zajednice da zadrži neke od predašnjih procedura donošenja odluka uveliko utopijski. Bez društvenog kapitala, jedini način da se obezbedi potpuno funkcionalan proces donošenja odluka jeste da se on formalizuje i da se razviju razni kontrolni mehanizmi.

Neke korekcije procedura odlučivanja već su urađene da bi odrazile ovu promenljivu realnost. Najvažnija je bila reforma ICANN-a iz 2002, koja je uključila jačanje Upravnog savetodavnog komiteta (GAC) i napuštanje sistema neposrednog glasanja.

Pitanja

Tehničko nasuprot političkom rukovodstvu

Dihotomija između tehničkog i političkog rukovodstva dovela je do stalne tenzije u aktivnostima ICANN-a. ICANN prikazuje sebe kao 'tehničko koordinativno telo za internet' koje se bavi samo tehničkim pitanjima i ostaje po strani od aspekata javne politike interneta. Funkcioneri ICANN-a smatarli su ovaj specifičan tehnički karakter glavnim konceptualnim argumentom za odbranu jedinstvenog statusa i roganizacione strukture ove institucije. Prva predsedavajuća ICANN-a, Ester Dajson, istakla je:

> *ICANN ne 'teži da se bavi' bilo kakvim pitanjima upravljanja internetom; on, u stvari, upravlja instalacijama, ne ljudima. Ima veoma ograničen mandat da upravlja nekim (uglavnom tehničkim) aspektima internetske strukture uopšte i DNS-om posebno.*[14]

Kritičari ove izjave obično ukazuju na činjenicu da ne postoji nikakva tehnički neutralna rešenja. Na kraju krajeva, svako tehničko rešenje ili odluka promoviše određene interese, ovlašćuje neke grupe i utiče na društveni, ekonomski i politički život. Odluke o pitanjima kao što su .xxx (materijali za odrasle) jasno ilustruju da će ICANN morati da se bavi aspektima javne politike tehničkih pitanja.

Međunarodni status ICANN-a

Specijalne veze između ICANN-a i Vlade SAD odavno se nalaze na udaru kritike, koja poprima dva glavna oblika. Prvi počiva na principijelnim obzirima, naglašavajući da se vitalni element globalne strukture interneta, koji bi mogao uticati na sve države, nalazi pod kontrolom samo jedne zemlje. Ova kritika bila je očita tokom procesa WSIS-a i bila je pojačana opštom sumnjom u spoljnu politiku SAD posle vojne intervencije u Iraku. Na ovom nivou rasprave, uobičajen kontraargument glasi da je internet stvoren u SAD uz finansijsku pomoć vlade. Ovo daje Vladi SAD moralni osnov za odlučivanje o formi i tempu internacionalizacije upravljanja internetom. Ovaj argument je naročito moćan u američkom Kongresu, koji se snažno protivi bilo kakvoj internacionalizaciji.

Drugi oblik počiva na praktičnim i pravnim obzirima. Na primer, neki kritičari tvrde da ukoliko sudstvo SAD vrši svoju ulogu i pravilno primenjuje režim sankcija protiv Irana i Kube, onda bi moglo da prisili ICANN – kao američki privatni pravni subjekt – da skine sa interneta državne domene ove dve zemlje. Prema ovom argumentu, zadržavanjem iranskih i kubanskih imena domena, ICANN krši američki zakon o sankcijama. Iako nikad do sada nije došlo do skidanja državnih imena domena, to ostaje mogućnost koja je data važećem pravnom statusu ICANN-a.

Signal za novi momenat u raspravi o statusu ICANN-a dolazi potpisivanjem Izjave o obavezama. Ona pruža osnov za nezavisni ICANN i otvara novi niz pitanja o budućem nadzoru, izveštavanju, odnosima s vladama, itd.

Oba ključna pitanja – bavljenje stvarima javne politike i internacionalizacijom – mogla bi da se reše promenom statusa ICANN-a, koja bi smanjila nedoumice i popravila jasnoću njegove misije. Budući razvoj ICANN-a zahtevaće inovativna rešenja. Moguće kompromisno rešenje mogla bi biti transformacija ICANN-a u međunarodnu organizaciju *sui generis,* koja bi sačuvala sve prednosti sadašnje strukture ICANN-a i istovremeno se bavila nedostacima, naročito problemom svog međunarodnog legitimiteta.

Fusnote

1 Izuzetak je bila Vlada SAD i nekoliko razvijenih zemalja (Australija, Novi Zeland i, tada, Evropska komisija).

2 Proces WSIS-a započeo je prvim pripremnim sastankom koji je održan jula 2002. u Ženevi. Prvi samit održan je u Ženevi (decembar 2003) a drugi u Tunisu (novembar 2005).

3 Izbor članova WGIG-a izvršen je kombinacijom predstavničkog i stručnog kriterijuma. Predstavnička struktura rukovodila se principom po jedna trećina učesnika iz vlada, civilnog društva i poslovnog sektora. Predstavnici vlada birani su prema uobičajenim kriterijumima regionalnih grupa UN. Iako je poštovan predstavnički aspekt, od izabranih članova se očekivalo da budu upoznati s materijom da bi mogli dati doprinos raspravi unutar WGIG-a.

4 Deklaracija o principima WSIS-a, WSIS-03/GENEVA/DOC/4-E, 12. decembar 2003, član 49. Dostupno na: **http://www.itu.int/wsis/docs/geneva/official/dop.html**

5 Brazilski model rukovođenja državnim imenom domena obično se uzima kao uspešan primer multiakterskog pristupa. Nacionalno telo zaduženo za brazilske domene otvoreno je svim korisnicima, uključujući vlasti, poslovni sektor i civilno društvo. Brazil je postepeno proširio ovaj model na druga područja upravljanja internetom, naročito na proces pripremanja za IGF 2007, koji je zasedao u Rio de Žaneiru.

6 Lesage C (1991) *La rivalite franco-britannique. Les cables sous-marins allemands* (Pariz, 1915) str.257-258; citirano u Headrick DR, *The Invisible Weapon: Telecommunications and International Politics 1851-1945*. Oxford Univesity Press: Oxford, UK, str. 110.

7 Cukier KN (2005) The WSIS wars: an analysis of the politicization of the Internet, u *The World Summit on the Information Society: Moving from the past into the future*. Stauffacher D, Kleinwächter W (izd.). United Nations ICT Task Force: New York, NY, USA, str. 176.

8 Vlada SAD kritikovala je uključivanje ITU u osnivanje CORE u jednom telegramu: *bez odobrenja vlada članica da se održi globalni susret koji bi uključivao neovlašćeno trošenje resursa i zaključivanje 'međunarodnih sporazuma'*.

9 Pogodnost da se sve obavlja na jednom mestu bila je jedan od argumenata za osnivanje ITU kao centralnog igrača u upravljanju internetom.

10 Dragocene komentare dala je Ajša Hasan.

11 Uspostavljanje Jednoobrazne politike rešavanja sporova u vezi sa imeniam domena (UDRP).

[12] Internetska zajednica ispunjava sve kriterijume iz definicije naučne zajednice koju daje Piter Has: *proefsionalna grupa koja veruje u iste odnose uzroka i posledice, testove istine da ih prihvati, i deli zajdničke vrednosti; njeni članovi dele zajdničko shvatanje problema i njegovih rešenja*. Haas P (1999) *Saving the Mediterranean: the politics of international environemantal co-operation*. Columbia Universtity Press: New York, NY, USA, str. 55.

[13] Network Solutions je tehnološka kompanija osnovana 1979. Posao registracije imena domena postao je najvažniji deo ove kompanije. Od januara 2009, Network Solutions je uredila preko 6,6 miliona imena domena. (Izvor: Vikipedija).

[14] Berkmanov centar za internet i društvo (The Berkman Center for Internet and Society), *The debate over Internet: a snapshot in the year 2000*. Dostupno na: **http://cyber.law.harvard.edu/is99/governance/introduction.html#_ftn10**

Osmi deo

Proces upravljanja internetom

Proces upravljanja internetom

Ovaj deo opisuje iskustva političkog procesa Foruma upravljanja internetom (IGF), koji iako nije naročito vidljiv na globalnoj političkoj sceni, predstavlja veoma značajan eksperiment u globalnom upravljanju. U vremenu kada postoji potreba za popravljanjem uspešnosti u globalnom upravljanju, IGF može da ponudi neke korisne lekcije.

Šta tvorci politika mogu da nauče od IGF-a

Debata o reformi globalnog upravljanja, ubrzana je posle neuspeha Kopenhagenskog samita 2009. o klimatskim promenama, sa fokusom na dva suštinska pitanja:

1. Kako dovoljno proširiti globalno upravljanje da uključi sve relevantne igrače.
2. Kako dovoljno produbiti globalno upravljanje da usvoji efikasan i operativan proces odlučivanja.

Recepti su različiti. Mnogi pokušavaju da smanje složenost uvodeći 'globalni upravni odbor' po uzoru na G20, ili fokusirajući se na podatke regionalnih/interesnih grupa, ili smanjujući 'buku' vezanu za učešće nedržavnih aktera.[1] Drugi smatraju da UN mogu/treba da se reformišu da bi postale jedno od glavnih mesta za rukovođenje globalnim pitanjima. Još više je onih koji tragaju za novim i inovativnim formatima koji će proširiti i produbiti globalno upravljanje da bi moglo da se bavi složenim političkim pitanjima, kao što su klimatske promene, migracije i globalno zdravlje.

Šta je Forum o upravljanju internetom?

IGF je glavno globalno telo za bavljenje pitanjima javne politike interneta. Stvoreno je na Svetskom samitu informacionog društva (WSIS) u Tunisu 2005. godine, kao rezultat kompromisa između vladinog i nevladinog rukovođenja internetom.[2] Kao rezultat ovog kompromisa, IGF nije bio ni predmet velikih očekivanja ni rezultat nekog velikog plana. Korak po korak, bez velikih reči ili gromoglasnih proglasa, razvio se *modus operandi* IGF-a. Ovaj forum je do sada imao četiri godišnja susreta: Atina (2006), Rio de Žaneiro (2007), Hajderabad (2008), Šarm el Šeik (2009). Ima mali sekretarijat sa sedištem u Ženevi. Podstakao je stvaranje niza regionalnih i nacionalnih foruma za upravljanje internetom, akademskih mreža (GIGANet) i drugih pratećih aktivnosti.

Kada raspravljamo o tome kako druge globalne oblasti upravljanja mogu da izvuku korist od iskustva IGF-a, važno je imati na umu dve razlike između upravljanja internetom i tradicionalnog multilateralizma. Prvo, ovo drugo, kao što je pitanje klimatskih promena, postepeno se otvaralo za nevladine igrače. U slučaju upravljanja internetom, vlade su morale da prime već postojeće nevladine organizacije kojima su rukovodili ICANN, IETF i drugi pravni subjekti. Drugo, IGF nije organ odlučivanja. On nema mandat da usvaja međunarodne ugovore ili druga pravna dokumenta. On je forum za 'oblikovanje odluka', koji svojim savetovanjem stvara bazu za odluke koje usvajaju druge institucije, kao što su ICANN, ITU i WIPO, da navedemo samo neke.

Iskustvo i naučene lekcije IGF-a organizovani su u četiri glavne grupe:

1. Pristupi za bavljenje pitanjima globalne politike.
2. Rukovođenje političkim procesima.
3. Bavljenje naučnim i tehničkim aspektima političkih pitanja.
4. Povećanje uključenosti i učestvovanja.

Pristupi za bavljenje pitanjima globalne politike

Globalni izazovi ne moraju nužno da iziskuju globalna rešenja

Jedna od mantri globalnog upravljanja glasi da su nam za globalne probleme potrebna globalna rešenja. Klimatske promene ne poštuju nacionalne granice. Komunikacija internetom lako zaobilazi tradicionalna ograničenja vezana za suverenitet. Argument glasi da, ukoliko politika nije globalna, postoji opasnost da nacionalna i regionalna praksa može da podrije global-

nu stvar. Na primer, neke zemlje, povećavanjem emitovanja CO_2, mogu da podriju nastojanja drugih zemalja da smanje emitovanje ugljen-dioskida. Tako, koristeći ovu liniju argumentacije, jedini način bavljenja globalnim problemima ide preko globalnih rešenja.

Problem je u tome što je pri pokšaju da se dođe do nekog globalnog dogovora, moguće propustiti mnogo drugih lokalnih, nacionalnih i regionalnih političkih mogućnosti. Kopenhagenski pregovori o klimatskim promenama pokazali su da nije lako doći do globalnog dogovora. Teško je uklopiti raznolikost interesa i profesionalnih/nacionalnih pristupa u jednom dokumentu koji će svi potpisati. U oblasti klimatskih promena, postoje mnoge neglobalne inicijative, uključujući inicijative privatnog sektora, lokalnih vlasti i poslovng sektora. U tom smislu, IGF predstavlja ogledni model.

IGF nije formiran zato da bi sačinio globalni, pravno obavezujući dogovor. Umesto toga, obezbedio je prostor za promovisanje različitih regionalnih i nacionalnih inicijativa za upravljanje internetom, kao i za stvaranje veza i sinergije između njih.(plavo) Brazil raspolaže izvanrednim načinom vođenja nacionalne politike IGF-a. Egipat je lider u bezbednosti dece. Latinska Amerika ima izvrstan program za koordinaciju vođenja internet imena i brojeva. Indija neprestano napreduje u dovođenju interneta u najsiromašnije zajednice. Spisak je dug. Ovi primeri su predočeni IGF-u, o njima se raspravljalo, i u mnogim slučajevima doveli su do oponašanja (npr. brazilsko državno rukovođenje). Globalni ideal razvijanja interneta pospešuje se bez nekog globalnog, pravno obavezujućeg aranžmana.

Povećavajte političku doslednost kroz multiakterstvo

Jedan od glavnih izazova za svaki globalni politički proces danas predstavlja postizanje političke doslednosti u bavljenju multidisciplinarnim pitanjima. IGF služi kao kišobran pod kojim različiti postojeći režimi, uključujući informacionu tehnologiju, ljudska prava, trgovinu i intelektualnu svojinu, mogu da idu skupa. Kroz proces IGF-a, razne političke zajednice otkrivaju da su njihove prethodno izolovane političke oblasti zaista deo šireg procesa upravljanja internetom. U nekim spornim oblastima, kao što je multijezičnost, IGF pomaže sasvim različitim organizacijama, uključujući vlade, ICANN, UNESKO i ITU, da koordiniraju usredsređenost na neku temu. Neobično široko multiaktersko učešće razvodnilo je oštru borbu između raznih organizacija i obezbedilo prostor za povezivanje inače različitih inicijativa unutar koherentnog političkog procesa. Ono je takođe umanjilo problem kopiranja kod bavljenja političkim pitanjima.

Olakšajte koordinaciju između nacionalnih, regionalnih i globalnih političkih nivoa

U sve integrisanijem svetu, trenutna komunikacija i sve veći uticaj nedržavnih aktera zamagljuju liniju između nacionalnog, regionalnog i globalnog političkog prostora. Neke nevladine organizacije koriste 'forum shoping' za ubacivanje svojih političkih inicijativa na najpovoljnijem političkom nivou. Neke vlade u EU, na primer, koriste tzv. pranje politike: ako neka inicijativa ne bude usvojena na državnom nivou, ona se protura preko regionalnog nivoa i ponovo uvodi kao 'međunarodna obaveza' zemlje.

U oblasti upravljanja internetom, mreža političkih foruma kompleksna je i postojala je mnogo pre stvaranja IGF-a (međunarodne organizacije, ICANN, ISOC – internetsko društvo, i razna standardizaciona tela). Osim toga, akteri politike upravljanja internetom vrlo su agilni, lako se kreću sa jednog političkog sloja i foruma na drugi, koristeći savremenu komunikacionu tehnologiju. IGF je pokušao da maksimalno poveća korist i smanji opasnosti od političkih procesa koji se vode na više nivoa. Koordinira globalne, regionalne i nacionalne aktivnosti i odozdo (kod pripremanja za IGF) i odozgo (širenje znanja sa IGF-a). Transparentnost IGF-a čini ovaj proces zatvorenijim za 'forum shoping'.

Rukovođenje političkim procesima

Efikasno i uspešno vođstvo: mudrac na sceni, vodič van scene
Jedan od glavnih razloga za uspeh IGF-a jeste vođstvo Nitina Desaja, predsedavajućeg, i Markusa Kumera, izvršnog koordinatora Sekretarijata. Oba imaju veliko i dodatno diplomatsko iskustvo. Desaj je bio odgovoran za pripremu nekoliko velikih samita UN; Kumer je imao uspešnu karijeru u švajcarskoj diplomatskoj službi. Dok Desaj rukovodi 'scenom' glavnih događaja IGF-a, Kumer izgrađuje razumevanje i uključivanje preko blagovremene onlajn komunikacije van scene i preko učešća u glavnim događajima raznih profesionalnih zajednica okupljenih oko IGF-a. Njihovo temeljno poznavanje propisa, procedura i prakse UN pomoglo im je da pronalaze kreativna rešenja i da primenjuju efikasan, iako nenapisan, *modus operandi* IGF-a.

Gradite poverenja pravilnim tajmingom i rasporedom

IGF je okupio učesnike iz različitog profesionalnog i kulturnog miljea oko istog stola. Oni nisu u prošlosti radili za iste institucije, nisu pohađali iste univerzitete, nisu se kretali u istim društvenim krugovima, niti su gradili

poverenje na neke druge načine. Poverenje je moralo da se gradi u atmosferi u kojoj su sumnje već bile prisutne zbog sporova u prošlosti (npr. između ITU i ICANN-a), ili zbog opšteg osećanja 'geosumnji' uzrokovanih iračkim ratom, ili zbog uobičajenog etiketiranja 'mi protiv njih'.

Izgradnja poverenja zahteva strpljenje i pažljiv redosled aktivnosti. Svaka faza u procesu IGF-a imala je za cilj povećanje uzajamnog razumevanja i donošenja novog znanja i informacija na sto. Rezultat toga bila je postepena izgradnja poverenja, kao i vrlo bogata debata. Neki predlozi, kao što je rani poziv na usvajanje Okvirne konvencije o internetu, bili su odbijeni: vreme nije bilo zrelo za dalju formalizaciju oblasti upravljanja internetom. Pre pet godina, to je moglo da dovede do tenzija i da eventualno prekine proces upravljanja internetom. Danas, vode se rasprave o globalnom ugovoru o sajber-bezbednosti. Pravilno rukovođenje vremenom bilo je bitno za krajnje sporno pitanje centralne uloge ICANN-a, institucije sa sedištem u SAD, u rukovođenju internetskim imenima i brojevima, jezgrom globalne strukture interneta. Pre pet godina, to je bilo uzrok velikih neslaganja. Danas, otkako je Vlada SAD započela internacionalizaciju uloge i strukture ICANN-a, stvari nisu sporne kao što su bile. Ovo je dobar primer da se sporna politička pitanja mogu vremenom poboljšavati, ako se radi pažljivo i ne dozvoli prerastanje u političku krizu. IGF je veoma uspešan u tom smislu. Diplomate i tvorci politike mogu da uče od IGF-a kako se efikasno gradi poverenje pravilnim tajmingom aktivnosti i pažljivim redosledom. Vreme je bitno, iako nedovoljno, za izgradnju poverenja.

Za dodatnu raspravu o ICANN-u videti Sedmi deo

Neka se odvija politički proces

U savremenom društvu, postoji fokusiranost na logično postavljanje doslednih planova i merenje njihovih doprinosa/ishoda. Globalno upravljanja i diplomatija nisu nikakav izuzetak u tome. Globalna kriza iz 2008. daje nam primer kako jedan sistem, zasnovan u velikoj meri na matematičkom modelovanju, može da dovede do kolapsa ukoliko ne uzme u obzir složenost društvenih uslova.

U istoriji diplomatije, rizik koji je povezan sa prekomernim rukovođenjem političkim procesima lepo ilustruje uspeh Bečkog kongresa (1814) i neuspeh Versajskog ugovora (1919). Bečki kongres je stvorio osnov za jedan od najmirnijih perioda u evropskoj istoriji: gotovo 100 godina bez nekog velikog rata. Versajski ugovor, s druge strane, propao je samo nekoliko godina po potpisivanju. U Beču su pregovarači, polako, bez unapred određenog velikog

plana i sa mnogo socijalne interakcije, ostvarili uspešan mirovni dogovor. Tome je doprineo diplomatski genij Meterniha i Taljerana. U Versaju su se, međutim, diplomate angažovale u krajnje organizovanom procesu, u kojem sarađivalo na stotine naučnika, statističara i kartografa, da bi stvorile 'naučno sazdan mir'. Pokušali su da izmere pravdu i na kraju su stvorili političke uslove koji su doveli do Drugog svetskog rata. Oštre razlike između u samom načinu vođenja pregovora u Beču i Versaju daju nam ubedljiv argument protiv prekomernog rukovođenja diplomatskim procesima.

Iako se IGF ne može upoređivati sa ovim velikim diplomatskim događajima, njegova praksa bliža je pristupu Bečkog kongresa. IGF podrazumeva minimum potrebnog planiranja i struktuiranja. Procesi IGF-a razvili su i poprimili optimalan oblik preko kolektivnog modelovanja angažovanih učesnika, uključujući i one sa suprotnim stavovima.

Prihvatite da tekst ostaje najvažniji u diplomatiji

Uprkos svim nadama u virtuelno održavanje konferencija i u druge tehnologije, danas – još više nego u prošlosti – tekst ostaje glavno oruđe diplomatije.[3] Tekst je glavni za proces IGF-a, iako IGF nije doveo ni do jednog završnog dokumenta (tj. konvencije, ugovora, deklaracije). Većina razmena između pripremnih sesija vrši se preko mejling lista ili mejlova. Sajtovi su prepuni teksta, sa vrlo malo fotografija ili slika. IGF ima vrlo aktivnu podršku društvenih medija, koji koriste tekstualno oruđe kao što su blogovi i Tviter.

Novi značaj teksta izbio je u prvi plan preko doslovnog izveštavanja na susretima IGF-a, što je moglo imati bitan uticaj na multilateralnu diplomatiju i pregovore. Doslovno izveštavanje predstavlja istovremeno transkribovanje i prikazivanje svake usmene intervencije na sastanku dok se predstavlja. Učeći iz prakse ICANN-a, Sekretarijat Radne grupe za upravljanje internetom (WGIG) uveo je doslovno izveštavanje u aprilu 2005. IGF je nastavio s ovom praksom. Sve verbalne intervencije istovremeno transkribuju specijalni stenografi i one se odmah prikazuju na velikom ekranu u konferencijskoj sali, i prenose se preko interneta. Dok delegati govore, transkripti njihovih govora pojavljuju se na ekranu.

Doslovno izveštavanje izvršilo je veliki uticaj na diplomatski *modus operandi*. Svest o tome da će ono što se kaže biti sačuvano u štampanoj formi tera mnoge učesnike da budu pažljiviji pri izboru nivoa i dužine verbalnih intervencija. Doslovno izveštavanje takođe povećava transparentnost sastanaka.

Prihvatite da neformalnost na međunarodnim konferencijama može uzrokovati nejednakost u učestvovanju

Jedan od izazova s kojima se suočava IGF predstavlja balansiranje formalne kulture diplomatije UN i neformalne kulture internetske zajednice. Posle četiri godišnja sastanka IGF-a, čini se da je prevladala neformalna kultura. Iako ova kultura stvara ogućnosti za uključivanje u procese i olakšava učestvovanje omladine i širih zajednica širom sveta, ona takođe postavlja nekoliko izazova. Učesnici iz nacionalnih kultura sa snažnim poštovanjem društvene hijerarhije mogu se osećati neprijatno, nerado se uključujući u razgovore, u vrlo neformalnoj radnoj atmosferi. Štaviše, u diplomatskim, pravnim i nekim drugim profesionalnim kulturama, učestvovanje u debatama ustrojeno je profesionalnim protokolima.

Paradoksalno, neformalnost u proceduri i raspravama može sputati učestvovanje nekih delegata i stvoriti potencijalnu nejednakost. IGF se bavio ovom opasnošću nastojeći da pronađe načine za prilagođavanje raznih nivoa formalnosti, nudeći ambijente u kojima različiti akteri mogu opušteno učestvovati. Povećao je, na primer, nivo protokola nekih, uglavnom plenarnih, sednica, dodajući više tipično diplomatskih proceduralnih pravila (npr. formalno predstavljanje) i organizovao je specijalne sednice za parlamentarce.

Bavljenje naučnim i tehničkim aspektima političkih pitanja

Priznajte da su nauka i tehnologija retko politički neutralne

Proces IGF-a je još jednom potvrdio da pitanja nauke i tehnologije (S&T) imaju uticaja na kreiranje politike, dajući ovlašćenja raznim grupama i interesima. U nekom trenutku, pitanja S&T prerastaju u politička; politička pitanja, sa svoje strane, zahtevaju odluke o vrednostima i intetresima koji su stavljeni na kocku.

U ovom kontekstu, opasno je prikazivati pitanja vezana za nauku i tehnologiju kao politički neutralna. Ako se naučni i tehnološki argumenti promovišu kao 'krajnja istina', ovaj pristup može da ima suprotno dejstvo. Na primer, kod pregovora o klimatskim promenama, takav pristup doprineo je krajnjoj ranjivosti naučnih argumenata. Sa Univerziteta Ist Anglija curili su mejlovi, a lažni podaci o himalajskim lednicima bacali su sumnju na, inače čvrste, naučne argumente o klimatskim promenama.

Pitanje međuigre između nauke i politike takođe je važno u drugim oblastima, kao što je zdravstvena bezbednost i bezbednost hrane. Naučnici moraju povećati svoje prisustvo u diplomatskoj areni, a diplomate će morati da uče kako da se bave naučnim pitanjima.

U procesu IGF-a, nauka i tehnologija su doprinele obaveštenom kreiranju politike. O tehničkim pitanjima raspravlja se u širem društvenom i ekonomskom kontekstu. Multiakterski sastav IGF-a, koji obuhvata naučnike, informatičare, diplomate, ekonomiste i ostale stvorio je povoljan kontekst za uspešnu međuigru između nauke i tehnologije i kreiranja politike.

Poboljšajte komunikaciju među različitim profesionalnim i organizacionim kulturama

Napisan je značajan broj knjiga o temi međukulturne komunikacije: kako razgovarati sa Arapima, Kinezima, Amerikancima, itd. Međutim, iskustvo IGF-a pokazuje da je u jednom političkom procesu, glavni izazov često kako olakšati razmenu između različitih profesionalnih kultura (npr. advokata, inženjera) i različitih organizacionih kultura (npr. međunarodnih organizacija, vlada, kompanija). U današnjem globalizovanom svetu, sa trenutnom komunikacijom, često je lakše komunicirati unutar istih proefsionalnih krugova, čak i preko nacionalnih granica. Profesije dele isti način oblikovanja problema i pronalaženja rešenja. Na primer, nemačkom programeru može biti lakše da komunicira sa programerom u Kini nego sa, recimo, nemačkim diplomatom.

Kako globalna pitanja sve više postaju tehnička (npr. klimatske promene, trgovina, zdravlje), uspešna međuprofesionalna komunikacija može se postići putem obuke, obrazovanja i izlaganja drugim kulturama. Bolja međuprofesionalna komunikacija može takođe doprineti boljoj političkoj koherentnosti između ministarstava i međunarodnih organizacija. IGF je napravio pozitivne korake u međuprofesionalnoj komunikaciji olakšavanjem delotvorne razmene ideja između specijalista iz raznih profesija, uključujući informatiku, diplomatiju i ekonomiju. Dobar primer za ovo predstavlja široka profesionalna i institucionalna raznolikost diskutanata uključenih u rasprave na IGF-u.

Napravite pravu mešavinu između tehničkog znanja i diplomatskih veština

U većini globalnih političkih procesa, postoji jedna dilema: da li treba da ih vode specijalisti (npr. naučnici kod klimatskih promena) ili diplomate.

Argument u korist specijalista kaže da za bavljenje tehničkim pitanjima, čovek treba da poseduje dubinsko poznavanje tih pitanja. Prema ovom stanovištu, na primer, potrebna je naučna pozadina da bi se razgovaralo o pitanjima klimatskih promena. Diplomate se obično bave političkim, društvenim i drugim netehničkim aspektima pitanja o kojima se vode pregovori.

Uspeh vođstva IGF-a – Desaja i Kumera – osporio je urbanu legendu da tehničkim pitanjima treba da se bave tehnički stručnjaci. Kao novajlije u oblasti upravljanja internetom, Desaj i Kumer su dali nepristrasan doprinos dugotrajnoj debati o pitanjima kao što su pozicija ICANN-a, regulativa imena domena, itd. Ponekad, kao što pokazuje IGF, 'diplomatizacija' bavljenja tehničkim pitanjima može pomoći u prevazilaženju tradicionalnih sporova u tehničkim zajednicama. Iskustvo IGF-a potvrđuje da ne postoji gotov recept za angažovanje specijalista i diplomata. Reč je o dinamičnoj međuigri koja zavisi od specifičnog konteksta i uključenih pojedinaca. Jedini 'savet' je da se razvija svest o opasnosti da specijalisti ili diplomate dobiju isključivu ulogu.

Povećana uključenost i učestvovanje

Pojačajte nacionalne diplomatske uticaje uključivanjem nedržavnih aktera u diplomatske aktivnosti[4]

SSa više igrača i sa više složenih pitanja na stolu, tradicionalni diplomatski pristup ograničen je. Čak ni najefikasnije diplomatske službe ne mogu da obezbede toliko 'diplomatskih kapaciteta' (tj. kvalifikovanih ljudskih resursa) koliko je potrebno. Širi diplomatski kapacitet može se obezbediti uključivanjem aktera iz civilnog društva, poslovnog sektora, lokalnih vlasti i drugih pravnih subjekata uključenih u globalne političke procese.

Neke države, kao što su Kanada, Švajcarska i skandinavske zemlje, prepoznale su ranije ovu evoluciju i već su uklopile nedržavne aktere u svoje spoljnopolitičke aktivnosti. Ova praksa nije uobičajena umnogim zemljama u razvoju, gde su diplomatske službe male, sa ograničenim finansijskim i ljudskim resursima, i gde su se nacionalne multiakterske strukture pojavile tek tokom poslednjih nekoliko godina.

IGF je na praktičan način doprineo podizanju svesti o prednostima multiakterstva u vladinim krugovima, naročito kod zemalja u razvoju. Pored šireg principa uključenosti, multiakterstvo IGF-a pokazalo je praktično re-

šenje koje pomaže zemljama da povećaju svoj diplomatski trag bez dodele dodatnih resursa. Pojavljuju se multiakterska nacionalna tela IGF-a. Vlade više koordiniraju rad poslovnog sektora i civilnog društva. Neke male i zemlje u razvoju, u političkim procesima upravljanja internetom, predstavljaju stručnjaci iz akademskog kruga i nevladinih organizacija.

Ponekad, podsticanje takve uključenosti predstavlja uglavnom stvar koordinacije i stvaranja nacionalnog multiakterskog okvira. Predana izgradnja kapaciteta putem obuke u programima koji uključuju različite zainteresovane strane iz iste države takođe je od pomoći: učesnici u programu obuke teže da razviju uzajamno poverenje i timski duh.

Jačajte učestvovanje na daljinu osnivanjem punktova[5]

Za forum koji raspravlja o upravljanju internetom prirodno je da širi broj učesnika na svojim sastancima na one koji ne mogu da budu fizički prisutni. Danas, pored redovnih internet prenosa sastanaka, glavna inovacija IGF-a je uvođenje 'udaljenih punktova'. Udaljeni punktovi se definišu kao lokalni sastanci koji se održavaju paralelno sa sastancima IGF-a, a domaćini su univerziteti, IKT centri, nevladine organizacije i drugi akteri koji se bave upravljanjem internetom i političkim pitanjima. Sastanci IGF-a se prenose tako da udaljeni učesnici budu informisani o stvarima o kojima se raspravlja. Kao deo udaljenog punkta, učesnici mogu da šalju tekst i video pitanja na koja odgovaraju diskutanti IGF-a u obliku intervencija u stvarnom vremenu. Osim toga, punktovi drže diskusije i okrugle stolove koji su povezani s temama IGF-a iz lokalne perspektive. Putem ovih aktivnosti, lokalni punktovi obogaćuju koordinaciju između globalnih i lokalnih političkih procesa. Na primer, tokom IGF-a 2008, udaljeni punkt u Madridu pratio je sesiju o sajber-bezbednosti i kasnije je nastavio svoju raspravu o sajber-bezbednosti u specifičnom španskom kontekstu. Ukupno osam udaljenih punktova radilo je paralelno sa IGF-om 2008 (Madrid, Lahor, Barselona, Beograd, Buenos Ajres, Sao Paulo, Bogota i Pune). Preko 450 časova ovog događaja prenošeno je za učesnike iz daljine, a ukupno 522 učesnika priključilo se sastanku tokom četvorodnevnog događaja.([6]

Posle uspešne probne implementacije 2008. godine, Sekretarijat IGF-a usvojio je koncept udaljenih punktova. Kao rezultat snažne podrške zemlje domaćina i radnih grupa za učestvovanje na daljinu (RPWG),[7] IGF u Šarm el Šeiku doživeo je podizanje nivoa daljinskog učestvovanja na 12 punktova sa svih kontinenata. Prenos je bio mnogo bolji, a glavnim sesijama i radionicama prisustvovali su, na daljinu, punktovi i pojedinci iz celog sveta. Ispisivanje teksta na ekranu predstavljalo je još

jedno poboljšanje koje je povećalo pristup za one koji slabije čuju, a bilo je i kompenzacija za tehničke (audio) poteškoće za one sa usporenim internetskim vezama.
Iskustvo IGF-a pokazuje da daljinsko učestvovanje značajno povećava uključenost i otvorenost međunarodnih susreta. Ono stvara direktnu vezu između globalnog i lokalnog, što često nedostaje u multilateralnoj diplomatiji.

Prikupite mnoštvo informacija preko 'dugog repa' politike

Koncept 'dugog repa' politike inspirisan je virusnim marketingom i odnosi se na veoma raznolike političke informacije koje bi se inačei izgubile u tradicionalnim međuvladinim procesima. Pojedinci i grupe mogu da izraze svoja mišljenja direktno IGF-u preko lične uključenosti u događaje, internetske komunikacije i daljisnkog učestvovanja. Ove nove ideje i uvidi, koji ne bi stigli do najviših globalnih foruma u većini političkih procesa, znatno su obogatili proces IGF-a. Jedna od lekcija koju IGF može da prenese jeste da je prvi korak ka uključnijem političkom procesu olakšavanje otvorenog učešća. Potpuna korist od otvorenog i uključnog učestvovanja postiže se samo ako se prikupi i razmotri mnoštvo priloga i, kad god je to moguće, uključe u savetovanja o politici. Uključenost povećava legitimnost procesa i osećanje vlasništva kod široke lepeze aktera.

Obezbedite značajno učešće iz zemalja u razvoju: prelazak sa formalne na funkcionalnu jednakost

U svetu UN, male i zemlje u razvoju obično obezbeđuju ravnopravan status insistirajući na formalnom predstavljanju i procedurama. Za razliku od razvijenih i velikih zemalja, njima nedostaje organizovana mreža paralelnog predstavljanja interesa šireg društva preko poslovnog sektora, civilnog društva i akademskih zajednica.Zato nije iznenađujuće da one prilaze s rezervama prema multiakterskom učešću. Na velikim susretima, koji okupljaju na hiljade učesnika na ravnopravnoj osnovi, mala i nerazvijena zemlja gubi zaštitu procedura UN, gde je ona jedna od 194 predstavnika sa ravnopravnim fromalnim ststusom, bez obzira na veličinu i moć.

Na početku procesa WSIS-a 2002. godine, mnoge male i zemlje u razvoju snažno su se suprotstavljale inicijativi uvođenja ravnopravnog učešća predstavnika poslovnog sveta i civilnog društva. Neke od ovih država zalagale su se za pristup upravljanju internetom iz jedne institucije, što bi im obezbedilo jednu, po mogućnosti međuvladinu 'adresu', gde bi mogle da raspravljaju o svim odgovarajućim pitanjima.[8]

Od 2002. godine, WSIS, WGIG i naročito IGF postigli su značajan napredak u jačanju prorazvojnih aspekata multiakterskog procesa, uključujući bavljenje opasnošću od nedovoljnog predstavljanja malih i zemalja u razvoju.

Na formalnom planu, IGF obezbeđuje da sve sesije i panel-diskusije imaju odgovarajuće učešće raznih aktera iz zemalja u razvoju. Sve veći nivo učestvovanja ljudi iz zemalja u razvoju bio je vidljiv na forumima upravljanjan internetom u Riju i Hajderabadu.

Proces IGF-a pomogao je mnogim malim i zemljama u razvoju da bolje koriste raspoložive ljudske resurse. Ne moraju to biti diplomate, već ljudi sa poznavanjem upravljanja internetom, koji rade u internetskim organizacijama ili na univerzitetima po svetu. Korišćenje stručnjaka koji rade u inostranstvu bitno je, naročito za male zemlje.

Fizičko učestvovanje – tj. prisustvo sastancima – ne mora nužno da se izjednačava sa ravnopravnim učešćem. Ravnopravno učestvovanje zahteva odgovarajuće znanje, veštine i samopouzdanje svakog delegata da se uključi u politički proces. IGF pokušava da obezbedi ravnopravno učešće preko aktivnosti izgradnje kapaciteta. Od 2002. godine, preko 850 funkcionera i profesionalaca iz malih i zemalja u razvoju

Formalna nasuprot funkcionalnoj ravnopravnosti u pregovorima o klimatskim promenama

uključeno je u obuku i druge aktivnosti za izgradnju kapaciteta koje se nalaze van tradicionalnih kurseva, putem obezbeđivanja jedinstvene mešavine predavanja, istraživanja i dubinskog uranjanja u politiku, s ciljem da se učesnicima pomogne da shvate dinamiku IGF-a i da dobiju potrebno samopouzdanje za potpuno i sadržajno učestvovanje u političkim procesima. Angažovanje različitih aktera (diplomata, funkcionera, specijalista) u procesu obuke napaja učesnike svešću o prednostima multiakterskog pristupa i daje im samopouzdanje za učestvovanje na sastancima sa drugim profesionalnim zajednicama.

Proces IGF-a takođe podstiče razvoj zajednica za upravljanje internetom na globalnom jugu, kako na regionalnom (npr. zapadna Afrika, istočna Afrika i Latinska Amerika) tako i na nacionalnom nivou (npr. Kenija, Brazil, Senegal). Ove zajednice pomogle su malim i zemljama u razvoju da organizuju sopstvena multiakterska predstavništva identifikujući nevladine stručnjake koji su već uključeni u akademska istraživanja i u politički proces upravljanja internetom.

Na IGF-u, povećanjem nivoa učestvovanja, podsticanjem izgradnje kapaciteta i stimulisanjem razvoja mreža i zajednica, mnoge zemlje u razvoju napredovale su od formalnog/pasivnog do funkcionalnog/aktivnog učestvovanja u upravljanju internetom.

Fusnote

1 Norveški ministar spoljnih poslova, Johan Gare Store, snažno kritikuje nedostatak legitimnosti G20 u članku *One of the greatest setbacks since World War II*. Dostupno na: **http://www.spiegel.de/international/europe/0,1518,702104,00.html**

2 Postignut je kompromis između dva politička pristupa. Vladocentrični pristup, koji su uglavnom zastupale zemlje u razvoju, smatrao je da internetom treba da upravljaju međunarodne organizacije, kao što je ITU. Nevladin pristup, koji su favorizovale razvijene zemlje, naročito SAD, zalagao se da u upravljanju internetom značajno učestvuje poslovni sektor i civilno društvo. One su se suprotstavljale isključivoj ulozi organizacija kao što je ITU. Svaka strana dobila je ponešto svaranjem IGF-a kao kompromisnog rešenja. Vladocentrični pristup dobio je uklapanjem IGF-a u sistem međunarodnih organizacija. IGF saziva generalni sekretar UN. Nevladin pristup dobio je multiakterski karakter IGF-a uključivanjem poslovnog sektora i civilnog društva. Neki smatraju da su ovim kompromisom oni dobili i zahvaljujući povezivanju IGF-a sa generalnim sekretarom UN da bi se sprečila istaknutija uloga ITU u upravljanju internetom.

3 Zanimljiva paralela je korišćenje SMS usluga na mobilnim telefonima, zahvaljujući kojima tekst ostaje bitan za ljudsku komunikaciju uprkos moćnim oruđima zasnovanim na glasu i video sredstvima.

4 Multiakterstvo se najbolje definiše kao pristup upravljanju koji je opisan kao: *Zbir mnogo načina na koje pojedinci i institucije, javne i privatne, vode zajedničke poslove. Reč je o stalnom procesu kroz koji se sukobljeni ili različiti interesi mogu prilagoditi i iz kojih se mogu preduzeti kooperativne akcije. Ono uključuje formalne institucije i režime koji su ovlašćeni da nameću saglasnost, kao i neformalne aranžmane na koje su ljudi i institucije pristali ili su shvatili da su u njihovom interesu* (Komisija o globalnom upravljanju, 1995).

5 Videti **www.igfremote.com** zbog sadržajnih i suštinskih komentara Džindžer Pak i Marilije Marsel, koje su takođe pogonska snaga iza RPWG.

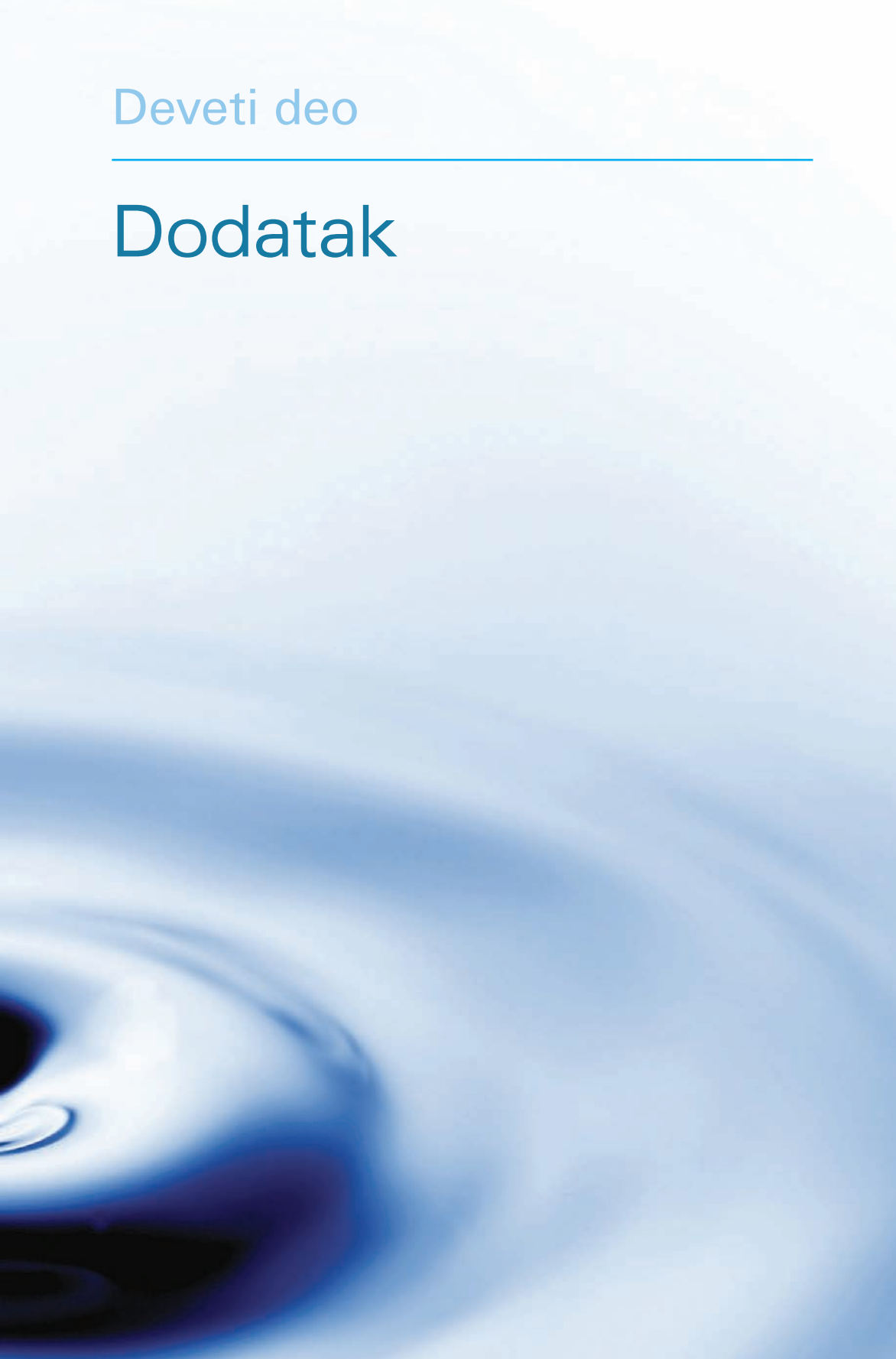
6 Detaljan izveštaj o daljinskom učestvovanju na IGF-u 2008 dostupan je na: **http://www.igfremote.com/ReportRPIGF-final.pdf**

7 **http://www.igfremote.info**

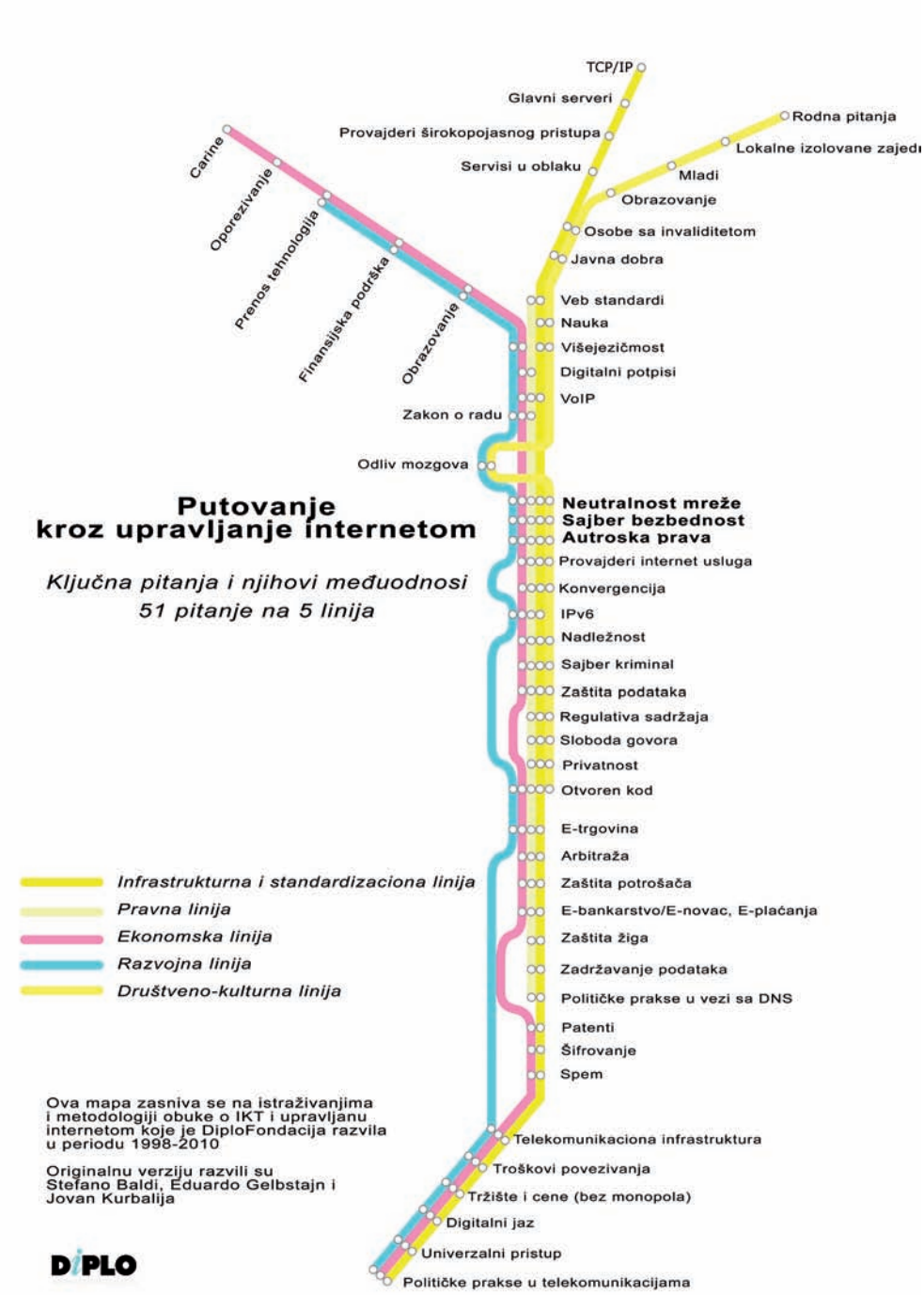
8 Preliminarni uvidi pokazuju da 80-100 međunarodnih organizacija, standarsdizacionih tela, foruma i drugih pravnih subjekata pokriva različite aspekte upravljanja internetom. Čak i za velike, razvijene zemlje, ovo široko polje gotovo je nemoguće pokriti. IGF pokušava da smanji i obuzda složenost izdvajanjem aspekata koji se odnose na upravljanje internetom od drugih političkih procesa (privatnost, intelektualna svojina, ljudska prava, razvoj, elektronska trgovina, itd).

Deveti deo

Dodatak



Dodatak


TCP/IP
Glavni serveri
Provajderi širokopojasnog pristupa
Servisi u oblaku
Rodna pitanja
Lokalne izolovane zajedn
Mladi
Obrazovanje
Osobe sa invaliditetom
Javna dobra
Carine
Oporezivanje
Prenos tehnologija
Finansijska podrška
Obrazovanje
Veb standardi
Nauka
Višejezičmost
Digitalni potpisi
VoIP
Zakon o radu
Odliv mozgova
Putovanje
kroz upravljanje internetom
Ključna pitanja i njihovi međuodnosi
51 pitanje na 5 linija
Neutralnost mreže
Sajber bezbednost
Autroska prava
Provajderi internet usluga
Konvergencija
IPv6
Nadležnost
Sajber kriminal
Zaštita podataka
Regulativa sadržaja
Sloboda govora
Privatnost
Otvoren kod
E-trgovina
Arbitraža
Zaštita potrošača
E-bankarstvo/E-novac, E-plaćanja
Zaštita žiga
Zadržavanje podataka
Političke prakse u vezi sa DNS
Patenti
Šifrovanje
Spem
Infrastrukturna i standardizaciona linija
Pravna linija
Ekonomska linija
Razvojna linija
Društveno-kulturna linija
Ova mapa zasniva se na istraživanjima i metodologiji obuke o IKT i upravljanu internetom koje je DiploFondacija razvila u periodu 1998-2010
Originalnu verziju razvili su Stefano Baldi, Eduardo Gelbstajn i Jovan Kurbalija
DIPLO
Telekomunikaciona infrastruktura
Troškovi povezivanja
Tržište i cene (bez monopola)
Digitalni jaz
Univerzalni pristup
Političke prakse u telekomunikacijama

Kocka upravljanja internetom

Osa ŠTA odnosi se na PITANJA upravljanja internetom (npr. infrastruktura, autorska prava, privatnost). Ona govori o **multidisciplinarnom** aspektu ovog pristupa.

Osa KO kocke fokusira se na glavne AKTERE (države, međunarodne organizacije, civilno društvo, privatni sektor). Ovo je **multiakterska** strana.

Osa GDE kocke bavi se OKVIROM u kojem bi trebalo da se bavimo pitanjima interneta (samoregulativni, lokalni, nacionalni, regionalni i globalni). Ovo je **multislojni** pristup upravljanju internetom.

Kada pomerimo delove IG kocke dobijemo tačku preseka – KAKO. Ovo je deo kocke koji nam može pomoći da vidmo kako bi trebalo da neka pitanja budu regulisana, kako u smislu kognitivnih, pravnih tehnika (npr. analogija) tako i u smislu instrumenata (npr. meko pravo, ugovori, deklaracije). Na primer, jedna specifična tačka preseca - nja može nam pomoći da uočimo KAKO pitanjima privatnosti (što) treba da se bavi civilno društvo (ko) na nacionalnom nivou (gde).

Odvojeno od kocke upravljanaj internetom nalazi se peta komponenta – KADA

Pregled evolucije upravljanja internetom

Akter / Period	Sjedinjene Države	Čuvari interneta	Međunarodne organizacije	Privatni sektor	Zemlje	Civilno društvo
	Ministarstvo odbrane rukovodi DNS-om					
1986	Nacionalna naučna fondacija (NSF) preuzima vođenje od Min. odbrane					
1994				Network Solutions Inc. potpisuje ugovor sa NSF da rukovodi DNS-om u periodu 1994-1998		

Početak DNS rata
Posle predaje DNS-a na upravljanje NSI (privatnoj kompaniji) internetska zajdenica (uglavnom ISOC – Internetsko društvo) godinama pokušava da vrati rukovođenje DNS-om u javni domen. Uspeva u tome posle četiri godine. Ovaj proces je podrazumevao nekoliko diplomatskih tehnika, kao što su: pregovori, izgradnja savezništva, izgradnja konsenzusa, itd.

Jun 1996		IANA/ISOC planiraju da preuzmu od NCI kad istekne rok ugovora; uvode se dodatni domeni; sektor zaštitnih znakova snažno se protivi novim domenima najvišeg nivoa, kao što čini i MTU				
Proleće 1997		Predlog Međunarodnog ad hok komiteta (IAHC). Učesnici u IAHC: dva predstavnika interesnih grupa zaštitnih znakova, WIPO, MTU i NSF; i pet predstavnika IETF-a. Zaključivanje Memoranduma o razumevanju generičkog domena najvišeg nivoa (gTLD) koji precizira da je DNS 'javni resurs'; sedam novih domena; i snažna zaštita za zaštitne znakove. Osnivanje CORE (Saveta registara – ceremonija potpisivanja u martu 1997 u ITU, Ženeva); CORE se odmah raspao. Snažno protivljenje Vlade SAD, NSI i EU				

Akter / Period	Sjedinjene Države	Čuvari interneta	Međunarodne organizacije	Privatni sektor	Zemlje	Civilno društvo
1997	Vlada SAD prenosi upravu DNS-om na Ministarstvo trgovine (DOC)					
Jun 1998	Bela knjiga DOC poziva glavne igrače da predlažu svoja rešenja	Predlozi stižu od IFWP (Međ. foruma o Beloj knjizi), ORSC (Konfederacije otvorenog centralnog servera) i od BWG (Bostonske radne grupe)				
		Umesto da izradi novi nacrt, ISOC se fokusira na: • stvaranje široke koalicije u kojoj se nalaze međunarodne organizacije (iz IAHC inicijative), privatni sektor (IBM) i ključne zemlje (Japan, Australija) i EU. • Stvaranje nove organizacije.				
Drugi deo 1998		September 1998 – Zajednički nacrt ugovora ISOC-NSI Oktobar 1998 – ISOC napušta sporazume i stvara ICANN Internetsku korporaciju (za dodeljena imena i brojeve)				
15 nov. 1998	DOC prenosi vlast na ICANN	ICANN stiče dve ključne nove funkcije: 1 Ovlašćenje da vrši akreditaciju registara za gTLD 2 Rukovodeću menadžersku ulogu (politički aspekt zadržava DOC).				
April 1999		Sporazum DOC – ICANN – NSI i uvođenje zajedničkog sistema registara; NSI gubi monopol ali dobija povoljan prelazni aranžman (rukovođenje sa četiri domena, itd)				
STRUKTURA I FUNKCIONISANJE ICANN-A						
Jun 1998		Formiranje PSO (Organizacije za podršku protokolu) koja se sastoji od IETF-a, WC3 i drugih pionira interneta	Početak procesa domena imena WIPO	Stvorena ASO (Organizacija za podršku adresama) da bi predstavljala registre DNS-a (ARN, RIPE, NCC) Osnovana DNSO (Org. za podršku imenima domena) da bi štitila interese zaštitnih znakova i trgovine	Trideset zemalja osniva GAC da bi stekle više uticaja kod vođenja nacionalnih domena. ICANN reaguje osnivanjem potkomiteta DNSO – ccTLD	

Kraj DNS rata

Ovaj rat se završio kompromisom. ISOC je uspeo da dobije više javne kontrole u rukovođenju DNS-om iako su komercijalni interesi ostali veoma jaki. Tako su bili dobro zaštićeni i interesi privatnog biznisa i zajednica čuvara. To nije bio slučaj sa pozicijom nacionalnih država i opšte internetske zajednice. One su dva najslabija aspekta upravljanja ICANN-om.

Akter / Period	Sjedinjene Države	Čuvari interneta	Međunarodne organizacije	Privatni sektor	Zemlje	Civilno društvo
2000-2003			Pojava veće fokusiranosti MTU, WIPO, UNESKA, OECD-a, Saveta Evrope i Svetske banke na internet	Snažni zahtevi privatnog sektora za regulisanje interneta	Razvoj zakono-davstva u vezi sa intetrnetom	Uključivanje NVO u digitalnu vododelnicu, ljudska prava, pitanja polova na internetu
			Multisektorske i globalne inicijative fokusiraju se na razvoj interneta, upravljanje internetom, itd: G8 DOT Force, Svetski ekonomski forum, Radna grupa UN za IKT, Svetki samit o informacionom društvu (WSIS), Globalno partnerstvo u znanju			
Jun 2002-nov. 2003	Prvi pripremni komitet za WSIS održan je juna 2002; upravljanje internetom pojavilo se kao pitanje tokom zasedanja regionalnog pripremnog komiteta za zapadnu Aziju u Bajrutu (februar 2003) Na prvom samitu u Ženevi (2003) doneta je odluka o osnivanju Radne grupe za upravljanje internetom (WGIG). Multisektorske i globalne inicijative fokusiraju se na razvoj interneta, upravljanje internetom, itd: G8 Dot Force, Svetski ekonomski forum, Radna grupa UN za IKT.					
2004-2005	Radna grupa za upravljanje internetom (WGIG), u ovom periodu je profilisala je raspravu o upravljanju internetom. WGIG je bila multiakcionarsko telo koje se sastojalo od predstavnika vlada, poslovne zajednice i civilnog društva. WGIG je održala četiri pripremna sastanka i sastavila Izveštaj koji je bio osnov za donošenje odluke o upravljanju internetom na WSIS-u – Tunis (2005). U Tunisu je Forum za upravljanje internetom (IGF) predstavljao kompromis između onih koji su se suprotstavljali bilo kakvim promenama u centralizovanom režimu ICANN-a i onih koji su se zalagali za to da se upravljanje internetom vrši putem međuvladinog režima.					
2006-2009	Posle završetka WSIS-a u Tunisu (2005), osnovan je IGF da nastavi politički proces upravljanja internetom. Do sada su održana četiri IGF-a: Atina (2006), Rio de Žaneiro (2007), Hajderabad (2008) i Šarm el Šeik (2009). Dana 30. septembra 2009, Vlada SAD i ICANN potpisali su Izjavu o obavezama kojom je okončan nadzor nad ICANN-om od strane SAD, što je bilo jedno od najspornijih pitanja upravljanja internetom. ICANN je ušao u novu fazu kao nezavisna organizacija sa više pitanja nego odgovora u vezi sa svojom budućom pozicijom i ulogom.					
2010	Peti IGF biće održan u Viljnusu (Litvanija). Na osnovu uvida u prvih pet godina, Ujedinjene nacije će doneti odluku u jesen 2010. o budućnosti IGF-a.					

PREDLOG ZA STANDARDIZACIJU STRUČNIH TERMINA

Svaka revolucionarna promena u nauci i tehnologiji neminovno osniva i postepeno standardizuje svoju posebnu stručnu terminologiju. Svoj specifični jezik stvara i internet. Veoma je važno da se prevod tih stručnih termina na srpski jezik što pre standardizuje i u praksi uniformno pimenjuje radi lakše komunikacije.

U nastavku su iz teksta knjige izvučeni važniji pojmovi vezani za njeno razumevanje i za teme upravljanja internetom, kako bi čitalac imao lakši pregled engleskih i srpskih termina.

Engleski	Srpski
Backbone	Okosnica
Business to business – B2B	Firma firmi
Business to customer – B2C	Firma potrošaču
Business to government – B2G	Firma vladinim službama
Carrier	Telekomunikaciona kompanija
Child safety on the internet	Bezbednost deteta na internetu
Cloud Computing	Servisi u oblaku / Računarstvo u oblaku
Cognitive Toolkit	Kognitivni alati
Content policy	Politika razvoja sadržaja
Core rooters in the Internet	Osnovni ruteri na internetu
Country Code TLD (ccTLD)	Državni domeni najvišeg nivoa
Customer to customer – C2C	Potrošač potrošaču
Cybercrime	Sajber kriminal/on-line kriminal
Cybersquatting	Sajber-skvoting
Digital Divide	Digitalni jaz
Diplomatic footprint	Širinia diplomatskog uticaja
Domain name companies	Kompanije koje trguju imenima domena
Domain Name System	Sistem imena domena
Dot com companies	Kompanije orijentisane na internet poslovanje

Download (speed)	Dolazna brzina
Dual use technologies	Tehnologije koje se mogu zloupotrebiti
E-banking	Elektronsko bankarstvo
E-mail	Elektronska pošta
eXtensible Markup Language	Jezik sa neograničenim i nepredefinisanim oznakama
Fiber-optics cables	Optički kablovi
Generic TLD (gTLD)	Opšti domeni najvišeg nivoa
HyperText Markup Language	Hipertekstualni markirni jezik
Internet Bandwidth Providers	Operatori za pružanje širokopojasnih internet usluga
Internet eXchange Point	Tačka razmene Internet saobraćaja
Internet Governance	Upravljanje internetom
Internet root zone file	Fajl sa osnovnim Internet adresama smešten u zoni glavnih servera
Internet Service Providers	Operatori za pružanje Internet usluga
Multistakeholder approach	Multiakterski pristup
Network neutrality	Neutralnost mreže
Online word processor	Onlajn tekst procesor
Open source software	Softver otvorenog koda
Peer-to-peer sharing files	Međukorisnička razmena fajlova
Policy	Političke prakse / politike
Powerline technology	Korišćenje strujnih kablova
Remote hub	Udaljeni punkt
Root server	Glavni server
Spam	Spem – neželjena poruka reklamne prirode
Sponsored TLD (sTLD)	Sponzorisani domeni najvišeg nivoa
SSL – Secure Sockets Layer	Dodatni nivo zaštite
Stakeholders	Akteri/učesnici/Zainteresovane strane
Taxation	Porezi i takse
Top Level Domains (TLD)	Domeni najvišeg nivoa
Trademark	Zaštitni žig
Transport control protocol/ internet protocol	Protokol kontrole prenosa/ internet protokol
Universal Access	Univerzalni pristup
Voice over IP	Prenos glasa preko internet protokola

Autor ovog rečnika je Nikola Božić, dugogodišnji saradnik DiploFoundation.

Uprava za digitalnu agendu Republike Srbije (digitalagenda.gov.rs) obrazovana je u martu 2011. sa ciljem primene Digitalne agende za Srbiju, koja se sastoji od Nacionalne strategije za informativno društvo i Nacionalne strategije za elektronske komunikacije.

Uprava za digitalnu agendu nastavlja rad prethodnog Ministarstva za telekomunikacije i informativno društvo, koje je u poslednje tri godine sprovelo mnoge inicijative i projekte koji su obuhvatali:

- Usvajanje savremenog pravnog okvira za elektronske komunikacije, kojim je otvoreno tržište elektronskih komunikacija u svim segmentima, uveden određen broj zaštita konkurencije i ojačan institucionalni okvir u sektoru.
- Sprovođenje elektronskog portala vlade (e-Government Portal) (euprava.gov.rs) koji trenutno pruža više od 250 usluga koje građani mogu da poručuju, potpisuju i plaćaju direktno onlajn.
- Sprovođenje nacionalnog projekta "Digitalne škole" koji je opremio svih 2.910 osnovnih škola u Srbiji računarskim laboratorijama (~30.000 radnih stanica)
- Uspostavljanje Javne institucije "Nacionalne akademske, istraživačke i obrazovne mreže" i njeno jačanje kroz regionalni SEELight projekat, što obuhvata polaganje i dugoročnu podršku za preko 3.000 km optičkih vlakana i koji povezuje sve univerzitetske i školske centre u Srbiji sa susednim zemljama i ostatkom Evropske Unije.
- Stvaranje globalne mreže „Žene na ICT“ u okviru ITU, i promocija osnaživanja žena i devojaka kroz i pomoću ICT, kao i ohrabrivanje mladih žena i devojaka da razmotre karijeru u ICT-u preko globalnog „Dana devojaka u ICT-u".
- Sprovođenje nacionalne kampanje „Click Safely“ (Bezbedno klikni) za poboljšanje bezbednosti deteta onlajn, u kojoj učestvuju deca u osnovnim i srednjim školama, nastavnici i roditelji.
- Potpisivanje Protokola o sporazumu sa Srpskim nacionalnim registrom imena u internet domenu koje podržava lokalna internet zajednica na uvođenju nove IDN ccTLD na ćiriličnom pismu . –srb.
- Podrška i direktno angažovanje kod lokalne Internet zajednica preko Web, društvenih mreža, redovnih sastanak uživo ('TweetUps“) i zajedničke organizacije raznih radionica i drugih događaja.

Registar nacionalnog internet domena Srbije (RNIDS) je ekspertska, nevladina i neprofitna organizacija.

Osnovni zadatak RNIDS-a je da upravlja internet domenima najvišeg nivoa (country code Top-Level Domains) .rs i .срб koji predstavljaju Republiku Srbiju na Internetu, poštujući principe kvaliteta, efikasnosti, nezavisnosti i transparentnosti, tako da se realizuju interesi Internet zajednice Srbije.

Upravljanje .rs i .срб domenima ICANN (Internet korporacija za dodeljena imena i brojeve) je poverila RNIDS-u rezolucijama svog Upravnog odbora:

- .rs domen - rezolucija br. 07.76, od 11. septembra 2007.
- .срб domen - rezolucija br. 2011.04.21.18, od 21. aprila 2011.

Upravljanje internet domenima najvišeg nivoa podrazumeva sledeće osnovne aktivnosti:

- .tehničko i administrativno upravljanje Centralnim registrom za .rs i .срб
- .propisivanje, objavljivanje i sporvođenje pravila koja se odnose na registraciju internet domena i poddomena
- .održavanje osnovnih DNS servera za .rs i .срб domene
- .održavanje javno dostupnog WHOIS servera za .rs i .срб domene

- .razvoj i primena pravila za rad oblašćenih registara u skladu sa najboljom praksom koristeći i iskustva drugih nacionalnih registara
- .razvoj i primena pravila koja omogućavaju rešavanje sporova povodom korišćenja domenskih imena, uz primenu procedura medijacije, arbitraže i pruženje saveta koji se odnose na internet domene
- .saradnja sa sličnim regionalnim i međunarodnim organizacijama
- .promocija .rs i .срб domena
- .sakupljanje, obrada i objavljivanje infoermacija o razvoju nacionalnog internet okruženja

RNIDS u potpunosti podržava koncept na kojem je zasnovan EuroDIG, a posebno onaj koji prodrazumeva angažovanje svih zainteresovanih strana u pripremi evropskog doprinosa Međunarodnom forumu o upravljanju Internetom.

Kontakt
RNIDS
Žorža Klemansoa 18a/I
11000 Beograd, Srbija
PAK 101147
Tel. ++381 (0)11 7281-281 i 7281-282
E-pošta: kancelarija@rnids.rs
www.rnids.rs

DiploFoundation je neprofitna organizacija koja radi na jačanju sadržajnog učešća svih aktera u diplomatskoj praksi i međunarodnim odnosima. Naše aktivnosti se vrte oko i dovode u žižu obrazovanje, obuku i izgradnju kapaciteta:

- **Kursevi:** Mi nudimo postdiplomski nivo kurseva i radionice u vezi sa mnoštvom diplomatskih tema za diplomate, državne službenike, osoblje međunarodnih organizacija i NVO, i za studente međunarodnih odnosa. Naši kursevi se odvijaju onlajn i kombinovano.
- **Izgradnja kapaciteta:** Uz pomoć donatorskih i partnerskih agencija, nudimo programem izgradnje kapaciteta za učesnike iz zemalja u razvoju iz više oblasti, uključujući upravljanje internetom, ljudska prava, diplomatiju i advokaturu i diplomatiju zdarvstva.
- **Istraživanja:** Putem istraživanja i konferencija, istražujemo teme koje se odnose na diplomatiju, međunarodne odnose i onlajn učenje.
- **Publikacije:** Naše publikacije kreću se u dijapazonu od razmatranja savremenih tokova u diplomatiji do novih analiza tradicionalnih aspekata diplomatije.
- **Razvoj softvera:** Kreirali smo niz softverskih aplikacija za diplomate i ostale koji rade u međunarodnim odnosima. Takođe se ističemo u razvijanju onlajn programa.

Diplo ima sedište na Malti, sa kancelarijama u Ženevi i Beogradu. Diplo je nastala iz projekta za uvođenje oruđa informacione i komunikacione tehnologije (IKT) u diplomatsku praksu, koji je započet 1993. na Mediteranskoj akademiji diplomatskih studija na Malti. U novembru 2002, Diplo je osnovana kao nezavisna neprofitna fondacija od strane vlada Malte i Švajcarske. Naše interesovanje proširilo se sa primene informacione tehnologije u diplomatiji na druge nove i tradicionalne aspekte obučavanja i prakse iz diplomatije i međunarodnih odnosa.

Beleška o autoru

Jovan Kurbalija je osnivački direktor DiploFondacije. Bivši je diplomata sa profesionalnim akademskim iskustvom u međunarodnom pravu, diplomatiji i informacionoj tehnologiji. Godine 1992, osnovao je Odeljenje za informacionu tehnologiju i diplomatiju na Mediteranskoj akademiji diplomatskih studija na Malti. Posle više od deset godina obučavanja, istraživanja i objavljivanja, ovo odeljenje je 2002. preraslo u DiploFondaciju.

Od 1994. godine, dr Kurbalija drži kurseve o uticaju IKT/internetskog upravljanja. Predaje na Mediteranskoj akademiji diplomatskih studija na Malti, Bečkoj diplomatskoj akademiji, Holandskom institutu za međunarodne odnose (Klingendel), Institutu za postdiplomske međunarodne i razvojne studije u Ženevi, na Koledžu za osoblje UN i na Univezitetu Južna Kalifornia. Dr Kurblalija je gostujući professor Evropskog koledža u Brižu. Glavna istraživačka interesovanja dr Kurbalije uključuju razvoj međunarodnog režima za internet, korišćenje interneta u diplomatiji i modernim pregovorima, te uticaj interneta na savremene međunarodne odnose.

Dr Kurbalija objavio je i uredio brojne knjige, članke i poglavlja, uključujući: *Internetski vodič za diplomate, Znanje i diplomatija, Uticaj IT na diplomatsku praksu, Informaciona tehnologija i diplomatske službe zemalja u razvoju, Moderna diplomatija i Jezik i diplomatija.* Sa Stefanom Baldijem i Eduardom Gelbstajnom, koautor je *Biblioteke informacionog društva,* niza od osam knjižica koje pokrivaju široku lepezu programa povezanih s internetom.

Sa suprugom Aleksandrom i ćerkom Zoë, dr Kurbalija živi u Ženevi.

Jovan Kurbalija
UVOD U
UPRAVLJANJE INTERNETOM

Naslov originala:
Jovan Kurbalija
AN INTRODUCTION TO
INTERNET GOVERNANCE

Izdavač:

Prevod:
Lazar Macura

Stručna redaktura:
Nikola Božić

Štampa:
AS design, Beograd

Tiraž:
600 primeraka

ISBN 978-86-6081-066-5

CIP - Каталогизација у публикацији
Народна библиотека Србије, Београд

005:004.738.5

КУРБАЛИЈА, Јован, 1963-
Uvod u upravljanje internetom / Jovan Kurbalija. - 2. izd. - Beograd : Albatros Plus, 2011 (Beograd : AS design). - 208 str. : ilustr. ; 24 cm. - (#Bioblioteka #Posebna izdanja / Albatros Plus)

Prevod dela: An Introduction to Internet Governance. - Autorova slika. - Tiraž 600. - Beleška o autoru: str. 208. - Napomene i bibliografske reference uz svako poglavlje.

ISBN 978-86-6081-066-5

a) Интернет - Управљање
COBISS.SR-ID 185350156

Spisak često korišćenih skraćenica

APEK	Azijsko-pacifička ekonomska kooperacija
ccTLD	Državni kod domena najvišeg nivoa
DMCA	Zakon o digitalnim milenijumskim autorskim pravima
DNS	Sistem imena domena
DRM	Rukovođenje digitalnim pravima
GAC	Vladin savetodavni komitet pri ICANN
gTLD	Generički Domen najvišeg nivoa
HTML	hipertekstualni markirni jezik
IANA	Internetska uprava za dodeljene brojeve
ICANN	Internetska korporacija za dodeljena imena i brojeve
ICC	Međunarodna trgovinska komora
ICT	Informaciona i komunikaciona tehnologija
IDN	Internacionalizovano ime domena
IETF	Radna grupa inženjera za razvoj interneta
IGF	Forum upravljanja internetom
IP	Internet protokol
IPR	Prava na intelektualnu svojinu
ISOC	Internetsko društvo
ISP	Provajderi internet usluga
IXP	Tačka razmene internet saobraćaja
MTU	Međunarodna telekomunikaciona unija
MoU	Memorandum o razumevanju
OECD	Organizacija za ekonomsku saradnju i razvoj
PKI	Javna šifarska infrastruktura
S&T	Nauka i tehnologija
SGML	Standardni opšti markirni jezik
sTLD	Zaštićeni domen najvišeg nivoa
TCP/IP	Protokol kontrole prenosa/internet protokol
TLD	Domen najvišeg nivoa
TRIPS	Aspekti prava na intelektualnu svojinu koji se odnose na trgovinu
UDHR	Univerzalna deklaracija o ljudskim pravima
UDRP	Jednoobrazna politika rešavanja sporova u vezi sa imenima domena
UNECOSOC	Ekonomski i društveni savet Ujedinjenih nacija
UNCITRAL	Komisija UN za Zakon o međunarodnoj trgovini
UNESKO	Obrazovna, naučna i kulturna organizacija UN
VoIP	Prenos glasa preko internet protokola
W3C	WWW konzorcijum
WGIG	Radna grupa za upravljanje internetom
WIPO	Svetska organizacija za intelektualnu svojinu
WSIS	Svetski samit o informacionom društvu
XML	Jezik sa neograničenim i nepredefinisanim oznakama

Uvod u upravljanje internetom daje obuhvatan pregled glavnih pitanja i aktera u ovoj oblasti. Knjiga je pisana na jasan i pristupačan način, propraćena brojnim slikama i ilustracijama. Bavi se tehničkim, pravnim, ekonomskim, razvojnim, društveno-kulturnim aspektima upravljanja internetom, dajući kratak uvod, rezime glavnih pitanja i rasprava, te pregled raznih stavova i pristupa svakom pitanju. Ova knjiga nudi praktičan okvir za analizu i raspravu o upravljanju internetom.

Od 1997. godine, preko 1000 diplomata, informatičkih stručnjaka, aktivista civilnog društva i studenata pohađalo je kurseve zasnovane na tekstu i pristupu koji su predstavljeni u ovoj knjizi. Sa svakim novim ciklusom kursa, gradivo se osvežava i popravlja. Ovo redovno osvežavanje čini kjnigu naročito korisnom kao nastavni priručnik za uvodne studije upravljanja internetom.

DiPLO
www.diplomacy.edu
Digitalna agenda
RNIDS
Registar nacionalnog internet domena Srbije
9 788660 810665