

SVEUČILIŠTE U ZAGREBU
FILOZOFSKI FAKULTET
ODSJEK ZA INFORMACIJSKE I KOMUNIKACIJSKE ZNANOSTI

Ana Perčinlić

Cenzura na internetu

DIPLOMSKI RAD

Mentorica:

dr. sc. Ivana Hebrang Grgić

Zagreb, 2014.

Sadržaj

1.	Uvod.....	4
2.	Cenzura općenito.....	5
3.	Začetci cenzure na internetu.....	7
4.	Razlozi cenzure na internetu	11
5.	Načini cenzure na internetu.....	13
5.1.	Tehnička cenzura.....	15
5.1.1.	Blokiranje IP adrese	15
5.1.2.	DNS filtriranje.....	16
5.1.3.	URL blokiranje.....	16
5.1.4.	Filtriranje HTTP Proxyja.....	17
5.1.5.	Filtriranje paketa.....	17
5.1.6.	Ponovno uspostavljanje internetske veze	17
5.1.7.	Napadi DOS (Denial-of-Service)	18
5.1.8.	Rušenje poslužitelja.....	18
5.1.9.	Nadzor	18
5.2.	Netehnička cenzura	18
5.2.1.	Autocenzura.....	19
5.3.	Točke napada.....	19
6.	Tvrtke u službi cenzure	20
6.1.	Amesyn.....	22
6.2.	Blue Coat.....	22
6.3.	Gamma International.....	23
6.4.	Hacking team.....	23
6.5.	Trovicor.....	24
7.	PRIMJERI CENZURE U SVIJETU	25
7.1.	Cenzura u Narodnoj republici Kini	25
7.2.	Cenzura u zapadnim i razvijenim zemljama	29
7.2.1.	Australija	30
7.2.2.	Francuska	31
7.2.2.1.	Hadopi	32
7.2.2.2.	LCEN (Law for Trust in the Digital Economy)	33
7.2.3.	SAD.....	33
7.2.3.1.	CDA, COPA i CIPA.....	34
7.2.3.2.	PIPA i SOPA.....	35

7.3. Cenzurirano Arapsko proljeće.....	36
8. Pristup internetu u Hrvatskoj i uloga knjižnica.....	40
9. Zaključak.....	44
Literatura.....	45
SAŽETAK.....	49

1. Uvod

„Cenzura sprječava uvoz naše najdragocjenije robe – istine.“¹ Izjava je Johna Milтона u javnoj osudi cenzure koju je provodila engleska vlada još u 17. stoljeću, i iskazuje da je tada već jaka svijest o kobnim posljedicama uskraćivanja informacija i onemogućavanja slobodne kritike i mišljenja. Danas, situacija ne izgleda mnogo bolje, jer Milton je, kako je i sam napomenuo, ipak uspio objaviti svoje mišljenje, a trenutačno stanje nekih zemalja niti ne dopušta svojim građanima da budu razjareni oko uskraćenog znanja. Sloboda tiska, sloboda govora, sloboda pristupu informacijama, tri su cilja za koje se još uvijek treba boriti.

No prodor nove tehnologije daje nadu zapriječenim narodima u uspjeh te borbe. Brzo, lako, sveobuhvatno epiteti su kojima se informacijsko doba opisuje i koje omogućuje korisnicima da vrlo lako pristupaju globalnoj mreži komunikacije i informacije u bilo kojem kutku svijeta. Zastrašujuće prodoran medij kao internet može donijeti revoluciju, a to se trenutačno i događa, jer se mnogobrojni aspekti ljudskog života sele u područje virtualnog, bilo to dobro ili ne. Korisnici interneta su odraz same tehnologije koju koriste: „Politička filozofija interneta, iako još većinski neusustavljena, nije ni u kojem slučaju neartikulirana. Težnje korisnika interneta uvelike odražavaju najbolje karakteristike same tehnologije – otvorena, meritokratska, bez prava vlasništva i transparentna.“² Ipak, ne treba biti pretjerano romantičan bez obzira na potencijalnu snagu medija kao što je internet i zanemariti činjenicu da koliko se korisnici trude maksimalno iskoristiti dano komunikacijsko sredstvo, u istoj mjeri različiti agenti, institucije i vlade rade predano na tome da se taj potencijal suzbije.

Cenzura interneta je glavna tema ovog diplomskog rada te će se u poglavljima koja slijede baviti njom, provođenjem iste i posljedicama koje ostavlja. Rad je podijeljen u dva dijela: u prvom se daje opći pregled cenzure i cenzure na internetu, nakon čega slijede poglavlja o razlozima i načinima provođenja cenzure, završavajući kratkim pregledom tvrtki koje su se posvetile izradi i izvozu tehnologije korištene za cenzuru. Drugi dio rada je posvećen pojedinim slučajevima cenzure interneta i tu su probrane države Kina, kao jedan od najrigoroznijih provoditelja cenzure u svijetu, potom je dan osvrt na razvijene i zapadne demokratske zemlje kao barjaktare slobode riječi kako bi se dao prikaz ne tako lijepe strane

¹Milton, John. Areopagitika. Beograd: „Filip Višnjić“, 1990. str. 63.

²Downes, L. Who Really Stopped SOPA and Why? Forbes. 2012. URL: <http://www.forbes.com/sites/larrydownes/2012/01/25/who-really-stopped-sopa-and-why/> (30.8.2014.)

proklamirane slobode govora u tim zemljama. Treće poglavlje se bavi nedavnim događajima u arapskim zemljama u kojima se moglo svjedočiti o presedanskim slučajevima poteza vlade u pokušaju cenzure, te koja je još uvijek na snazi, i na kraju rad završava kratkim osvrtom na cenzuru u Hrvatskoj.

2. Cenzura općenito

Hrvatska enciklopedija definira cenzuru kao „sustav administrativnih mjera koje poduzimaju državne, vjerske, stranačke i druge vlasti protiv objelodanjivanja, čitanja, širenja i posjedovanja, slušanja i gledanja nepoćudnih i za društvo opasnih tiskanih i rukopisnih knjiga, filmova, videokaseta i slične građe te radijskih i televizijskih emisija, kazališnih predstava i dr.“³ Riječ cenzura je latinskog porijekla, dolazi od riječi *censere* što znači *dati mišljenje, preporučiti*.⁴

Cenzura kao jednostavno definirano uskraćivanje informacija supostoji zajedno s informacijom, kroz povijest u različitim oblicima. Potrebno je naglasiti da je uvijek vezana uz društvo u kojem informacije kolaju, odraz je njegovih mijena i kulturalne tradicije, razlikuje se prema kulturi države u kojoj se provodi, gotovo uvijek je odraz unutarnjih previranja te njezini razmjeri ovise o procjeni vladajućih koliko izgovorena ili tiskana riječ ugrožava više interese.⁵ Cenzura je dugovječna djelatnost, i dio je ljudske povijesti. Uz to, ne čini se da jenjava, štoviše, u nekim zemljama je naočigled sve jača.⁶

Primjeri najstarije prisile na cenzuru kreću od starih civilizacija. Prva zabilježena knjiga kojoj je bila dosuđena sudbina spaljivanja jest Protagorina *O bogovima* iz 5. st. pr. Kr., a razlog uništenja spomenute knjige bilo je dovođenje u sumnju postojanje bogova.⁷ I kao što ovaj primjer pokazuje, prvi sadržaji koji su cenzurirani su oni najopasniji, stoga nije bilo riječi o cenzuriranju opscenih sadržaja, nego je prva cenzura bila isključivo političke prirode.⁸

Povijest cenzure teče dalje kroz stari Rim, potom kasnu antiku gdje je broj zabranjenih knjiga bio relativno malen. Nedugo poslije kad je kršćanstvo postala priznata religija,

³ Cenzura. // Hrvatska enciklopedija. URL: <http://www.enciklopedija.hr/Natuknica.aspx?ID=11246> (30.8.2014.)

⁴ Cenzura. // Hrvatski jezični portal. URL: <http://hjp.novi-liber.hr/index.php?show=search>

⁵ Cenzura. // Hrvatska enciklopedija. URL: <http://www.enciklopedija.hr/Natuknica.aspx?ID=11246> (30.8.2014.)

⁶ Bitso, C. et al. Trends in Transition from Classical Censorship to Internet Censorship. IFLA, str. 4. URL: <http://www.ifla.org/publications/trends-in-transition-from-classical-censorship-to-internet-censorship-selected-country-o> (30.8.2014.)

⁷ Cenzura. // Hrvatska enciklopedija. URL: <http://www.enciklopedija.hr/Natuknica.aspx?ID=11246> (30.8.2014.)

⁸ Gren, J. Encyclopedia of Censorship. New York: Facts on File, Inc., 2005. Str. XVIII

cenzura se okrenula poganskim i heretičkim piscima, a prvi popis zabranjenih knjiga nastao je 496. godine pod imenom *De libris recipiendis et non recipiendis*, uz popis dopuštenih knjiga.⁹ Popis nepoćudnih pisaca i knjiga naglo raste nakon Gutenbergova izuma, jer je sukladno povećanjem brzine širenja informacija i cenzura postala učestalija,¹⁰ i u kratkom su roku tržište preplavile 'opasne' knjige antičkih pisaca kao Ovidija i Boccaccia ili nepoćudne znanstvene ili filozofske knjige, a koje su do tada bile privilegija samostanskih knjižnica. Sljedeći cenzorski val uslijedio je nakon Reformacije Martina Luthera. Godine 1526. engleski kralj Henrik VIII. objavljuje prvi popis zabranjenih knjiga, Crkva svoj *Index librorum prohibitorum* objelodanjuje 1559., a 1571. osniva se posebna Crkvena institucija za nadgledanje tiskarstva i izdavaštva pod imenom Kongregacija za Indeks. Kroz sljedeća stoljeća će, pri opadanju crkvene moći, vladari preuzimati ulogu glavnih cenzora, (primjer je Marije Terezije koja je 1753. osnovala Cenzorsku komisiju) no zajedno s jačanjem građanske svijesti u 18. i 19. stoljeću pojavit će se i mnogi pokreti za slobodu misli i riječi, među njima najpoznatiji francuski enciklopedisti. No, najjaču cenzuru svijet tek čeka u 20. stoljeću pojavom mnogih totalitarnih režima – nacističkog (nacionalsocijalisti su već 1933. objavili *Crni popis* koji je s jačanjem političke stranke neprekidno rastao), fašističkog, komunističkog, od kojih neki još uvijek ne jenjavaju, kao socijalistički režim Narodne republike Kine.¹¹

Pitanje cenzure, uvijek je pitanje moći, „uspostavljanje i zadržavanje kontrole uključuje ograničavanje i nijekanje informacije“,¹² no kao što isti tekst navodi, cenzura predstavlja negativnu stranu moći, proskriptivnu, a ne preskriptivnu.¹³ John Milton se 1644. u govoru u prilog slobodi tiska upućenom engleskom parlamentu, (tzv. *Areopagitika*), osvrnuo na povijest cenzure kako bi upozorio englesku vlast na opasnost cenzure govoreći „No, netko će reći, što ako je izum, makar su njegovi izumitelji loši, dobar? Možda je tako, pa ipak, cenzura nije neki dubokoumni izum, i svatko bi lako mogao posegnuti za njom, pa zašto onda to nisu činile najbolje i najmudrije vlasti republika u svim dobima, već najgori i najopasniji ugnjetavači i tirani, i to upravo zato da bi spriječili reformaciju.“¹⁴

Uz riječ cenzura, usko je vezana i sintagma sloboda govora, kao suprotni pojam. Pravo na slobodu govora je „temeljno ljudsko pravo, koje se temelji na osobnom integritetu i demokraciji. Sloboda govora je blisko povezana sa slobodom misli i preduvjet je za samoizražavanje i samoispunjenje individue. Pravo na izražavanje omogućuje otvorenu

⁹ Stipčević, A. Sudbina knjige. Lokve: Naklada Benja, 2000. Str. 189-210.

¹⁰ Cenzura. // Hrvatska enciklopedija. URL: <http://www.enciklopedija.hr/Natuknica.aspx?ID=11246> (30.8.2014.)

¹¹ Stipčević, A. Sudbina knjige. Lokve: Naklada Benja, 2000. Str. 189-210.

¹² Gren, J. Encyclopedia of Censorship New York: Facts on File, Inc., 2005. Str. XV

¹³ Ibid., str. XVIII

¹⁴ Milton, J. Areopagitika. Beograd : „Filip Višnjić“, 1990. Str. 37

debatu o političkim, društvenim i moralnim vrijednostima i potiče umjetnička i znanstvena nagruća, slobodna od inhibicija.“¹⁵ Sloboda medija i govora je popisana kao temeljno ljudsko pravo u članku 19. u Općoj deklaraciji o ljudskim pravima: „Svatko ima pravo na slobodu mišljenja i izražavanja; to pravo uključuje slobodu zadržavanja mišljenja bez uplitanja i slobodu traženja, primanja i širenja informacija i ideja putem bilo kojeg medija i bez obzira na granice.“¹⁶ Problem cenzure i spriječene slobodne govora je kulturološki, vjerski, politički, ekonomski i temeljno ljudski problem. I ponovno, osvrćući se na Miliona, njegov govor još uvijek stoji značajan i suvremen, primjenjiv na slobodu govora koja nakon gotovo 400 godina, uz svu tehnologiju koju posjedujemo, nije dosegla razinu koja je dostojna ljudskog bića i građanina bilo koje zemlje svijeta.

„Jer knjige nisu sasvim mrtve stvari, one sadrže u sebi životnu snagu, djelotvornu i živu koliko i duša koja ih je stvorila. [...] Tko ubije čovjeka, ubija razumno stvorenje, sliku Boga. Ali onaj tko ubije knjigu, ubija sam razum...“¹⁷

3. Začeci cenzure na internetu

Internet je danas vjerojatno najmoćniji medij. Sve dosadašnje kulturalne uvriježenosti dalekometne komunikacije, kao tiskovine ili televizija su ostale po strani u borbi s velikom mrežom, i iako neće u potpunosti nestati, njihovo značenje je posljednjih desetljeća umanjeno ekonomičnošću, jednostavnošću i propusnosti interneta. „Internet je društveni, kulturni, komercijalni, obrazovni i zabavni globalni komunikacijski sustav čija je pravovaljana svrha donijeti korist i ovlastiti *online* korisnike, rušeći prepreke u stvaranju i raspodjeli sadržaja diljem svijeta.“¹⁸

Nove tehnologije vezane uz računalstvo nazivaju se 'tehnologijom oslobođenja' jer niti jedan komunikacijski model u ljudskoj povijesti nije se širio tolikom brzinom, tolikim prostorom u tako kratkom vremenskom roku, niti je omogućio demokratizaciju korisnika u mjeri kao što je to učinio internet.¹⁹ Mnogobrojni su primjeri umrežavanja kritičnih skupina

¹⁵ Jørgensen, R.F. Internet and Freedom of Expression. Raoul Wallenberg Institute, 2001. Str. 33. URL: <http://www.ifla.org/files/assets/faife/publications/ife03.pdf> (30.8.2014.)

¹⁶ Opća deklaracija o ljudskim pravima. Narodne novine. 2009. URL: http://narodne-novine.nn.hr/clanci/medunarodni/2009_11_12_143.html (9.9.2014.)

¹⁷ Milton, J. Areopagitika. Beograd : „Filip Višnjic“, 1990. Str. 28

¹⁸ Bitso, C. et al. Trends in Transition from Classical Censorship to Internet Censorship. IFLA, str. 6. URL: <http://www.ifla.org/publications/trends-in-transition-from-classical-censorship-to-internet-censorship-selected-country-o> (30.8.2014.)

¹⁹ Deibert, R.; Rohozinski, R. Liberation vs. Control: the Future of Cyberspace. // Journal of Democracy 21, 4(2010.), str. 44.

korisnika interneta, koji su demokratičnost mreže iskoristili u široj društvenoj borbi za specifične ciljeve, i sve više smo svjedoci društvenih revolucija kojima je posrednik vrlo često bila upravo tehnologija. Kako je tehnologija dio društva koje se razvija, a novijim generacijama postaje sastavni dio svakodnevice, sve više i u dijelovima svijeta koji se često promatraju kao periferija razvijenom svijetu, globalizacija je učinila moguće djelovanje na razinama koje su do nedavno bile rezervirane za zemlje izrazito stabilne financijske situacije, da ne kažemo obilja, a time upravo tehnologiju učinila ključnim sustavom za prodor novih ideja i stavova, te brzu diseminaciju istih, vrlo često potkopavajući režime i društvene sustave represivnog nagnuća. Jedan od primjera je protest koji je pokrenuo Oscar Morales, nezaposleni inženjer iz Kolumbije. Organizirao je pokret pod imenom "Un Million Voces Contra Las FARC" protiv nasilnih pobunjenika iz FARC-a kao protest protiv terorizma, te pokrenuo 12 milijuna prosvjednika u 190 gradova. Protest je većinski organiziran preko društvenih mreža, a ujedno je i najveći antiteroristički prosvjed ikad u svjetskoj povijesti.²⁰

No, naravno, ono što omogućuje veliku moć i slobodu sasvim prirodno stvara i antagonizam od strane agenata kojima protežan medij komplicira poslovanje i djelovanje. Ne smije se smetnuti s uma, da iako je internet i tehnologija produkt razvijenog društva - svojevrsni napredak civilizacije, on je neodvojivo vezan uz to društvo koje posjeduje svoje unutarnje strukture i nazore ustanovljivane čak i stoljećima i kojima nije intrinzična brzina mijene kao što bi to bilo kulturi tehnologije. Zastrašujuće velikom broju kultura i zemalja je slobodan protok informacija više prijatna nego pogodnost, a slučaj nije da je taj strah zahvatio samo 'nazadne' zemlje, s tradicionalnijim vrijednostima. Mnogi društveni sustavi nisu bili spremni na ono što im je donijela tehnološka revolucija 20. stoljeća koja rapidno zalazi u sve kutke globaliziranog svijeta. Generacije koje pripadaju tom novom kulturnom nasljeđu počinju se ujedinjavati u neku apstraktnu tehnološku naciju, te dijele saznanja bez obzira na etničke ili druge pripadnosti.

„Ironično, od kada je internet postao na široko popularan i dostupan sredinom 90-ih, dostupnost određenih tipova sadržaja općenito definiranih kao ilegalni ili štetni postali su preokupacija mnogih vlada, regulatornih agencija i međunarodnih organizacija. Posljedično, mnoge države pokušavaju razriješiti problem vezan uz sadržaj na internetu uvodeći nove ili dopunjavajući postojeće zakone.“²¹ Cohen navodi kako je internet kao istinski masovni medij

²⁰ Ross, A. Internet Freedom: Historic Roots and the Road Forward. // SAIS Review of International Affairs 30, 2(2010), str. 3.

²¹ Bitso, C. et al. Trends in Transition from Classical Censorship to Internet Censorship. IFLA, str. 7. URL: <http://www.ifla.org/publications/trends-in-transition-from-classical-censorship-to-intenet-censorship-selected-country-o> (30.8.2014.)

postao prijeteća sila za kontrolu informacija nekim vladama i to u mnogo većoj mjeri nego ijedan drugi medij, stoga se prečesto događa da je reakcija tih vlada i sredstava kontrole toliko postrožena da nadilazi ili odgovara potrebama.²²

Izrazito moćno društveno sredstvo kao što je internet nije sasvim otporno na zloupotrebu. Štoviše, njegova dostupnost i gostoljubivost omogućuje pristup svima bez diskriminacije o njihovoj namjeri, stoga bilo tko tko je tehnološki potkovan, ima moć rasprostirati informacije ili učiniti već postojeće nedostupnima. Takve namjere su osobito opasne ako dolaze s viših instanci, s većom legitimnom moći, kao što su vlade koje djeluju kroz ustave ili zakone. Morozov navodi da uvriježena ideja da nitko ne kontrolira internet i da je internet imun na regulaciju, ne odgovara stvarnosti, te baš suprotno, upravljanje internetom odvija se iz privatnog sektora i ne proizlazi iz javnog dogovora kao što se smatra. Morozov također upozorava da iako je tehnologija smanjila moć nositelja političke moći – „kao što su to učinili barut i tiskarska preša u ranijim razdobljima povijesti – također je i ovlastio one koje ne bismo nužno nazvali 'prijateljima građanskog društva'“²³

A to posljedično vodi do fenomena cenzure, problema koji nije toliko rijedak, a negativne posljedice mogu sezati od loše reputacije neke države zbog filtriranja informacija što je u očima strane diplomacije pričinjava nestabilnom i nedemokračičnom, pa sve do izravnih kršenja ljudskih prava i ugrožavanja pojedinaca ili skupina koji zastupaju određeni (politički, vjerski...) stav. Cenzura osobito pogađa glavni prostor razmjene ideja kao blogove, elektroničku poštu, društvene mreže i time prijeti temeljima strukture interneta. Cenzura interneta je relativno nov fenomen i trenutačno nedovoljno istražen, tvrde Constance Bitso i drugi u svom članku.²⁴ Također se ističe kako cenzurirani sadržaj varira s obzirom na društvo ili kontekst u kojem se cenzura provodi te može sezati od dječje pornografije i kockanja do sadržaja o organiziranju političkih disidenata. Isti izvor navodi kako su mnoge zemlje već od ranih 1990-ih i proliferacije interneta počele sastavljati zakone o internetskoj cenzuri.²⁵ Ako se problem ne čini osobito bitnim, treba svrnuti pozornost na podatke *Reportera bez granica* koji su u svom izvješću iz 2013. godine naveli da trenutačno dvije milijarde ljudi diljem svijeta ima pristup Internetu, no za trećinu njih, pristup je ograničen nekim oblikom državne

²²Ibid., str. 18

²³ Morozov, E. The Internet : a room of our own? // Dissent 56, 3(2009), str. 81.

²⁴ Bitso, C. et al. Trends in Transition from Classical Censorship to Internet Censorship. IFLA, str. 5. URL: <http://www.ifla.org/publications/trends-in-transition-from-classical-censorship-to-intenet-censorship-selected-country-o> (30.8.2014.)

²⁵Ibid.

cenzure.²⁶ Prema istraživanjima Open Net Initiative organizacije više od četrdesetak zemalja filtrira internet, a među njima su i zemlje koje se smatraju izrazito demokratičnima.²⁷ Cohen 1997. navodi da više od 30 zemalja u tome trenutku ima ili stvara neku zakonsku osnovu za cenzuru interneta, a kao najčešći razlozi su navedeni zaštita djece, javnog morala, javne sigurnosti, političke objektivnosti te utišavanje rasizma i govora mržnje.²⁸

Što je točno cenzura interneta? Iako je ona usko vezana uz razloge i pobude onoga koji cenzuru provodi, postoje neke zajedničke crte u svakoj cenzuri, kako u bilo kojem mediju, tako i cenzuri interneta. O samim razlozima bit će više govora u sljedećem poglavlju, a ovdje će se zadržati na nekim općim definicijama. Zukerman 2010. godine cenzuru interneta definira kao „nemogućnost korisnika u određenoj zemlji da pristupe određenom *online* sadržaju.“²⁹ Leberknight opisuje cenzuru interneta kao „kontrolu ili supresiju objavljivanja ili pristupa informaciji na internetu.“³⁰ Hrvatski Centar informacijske sigurnosti (CIS) cenzuru opće prihvaćeno definira kao „blokiranje pristupa internetskim stranicama za koje se smatra da su nepoželjne.“³¹ Upravo ovaj pojam nepoželjnosti je kritičan, jer unatoč tomu što svaka od ovih definicija stvara dojam zdravorazumske kontrole raspačavanja opasnih i štetnih informacija, granica koja određuje korisnu i nužnu informaciju od one koja je opasna i nepoželjna, čini se nije tako lako određiva. Problem postaje mnogo dublji. Ross tvrdi da je cenzura interneta politički problem zbog ograničavanja slobode govora, te raskol na globalnoj razini razmjeni ideja.³² Ponovno, cenzura je uvijek povezana s društvom u kojem kolaju informacije, stoga je ono i odgovorno za nju. U istom članku dalje se navodi kako stoga nije začuđujuće da različite društvene skupine imaju potrebu nametnuti neku vrstu cenzure, bile te skupine roditelji, učitelji, kler, političari ili druge skupine. Kako god bilo, da bi bila djelotvorno provedena, cenzura mora biti nametnuta zakonskim okvirima.³³

Morozov zadržava negativistički stav i smatra da internet ne uspijeva prenijeti ideje i riječi građanstva, prvenstveno zbog toga što su vlade savladale tehničke mogućnosti provedbe

²⁶ Enemies of the Internet : 2013 report. Reporters without borders. 2013. Str. 44. URL:

http://surveillance.rsf.org/en/wp-content/uploads/sites/2/2013/03/enemies-of-the-internet_2013.pdf (30.8.2014.)

²⁷ Deibert, R.; Rohozinski, R. Liberation vs. Control: the Future of Cyberspace. // Journal of Democracy 21, 4(2010.), str. 45.

²⁸ Bitso, C. et al. Trends in Transition from Classical Censorship to Internet Censorship. IFLA, str. 5. URL: <http://www.ifla.org/publications/trends-in-transition-from-classical-censorship-to-internet-censorship-selected-country-o> (30.8.2014.)

²⁹ Zukerman, E. Intermediary Censorship // Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace. MIT Press, 2010. str. 71.

³⁰ Leberknight, C.S. A Taxonomy of Internet Censorship and Anti-Censorship. Princeton University. 2010. Str.3.

³¹ Cenzura na internetu. Centar za informacijsku sigurnost, 2011. Str. 5. URL:

<http://www.cis.hr/files/dokumenti/CIS-DOC-2011-06-016.pdf> (30.8.2014.)

³² Ross, A. Internet Freedom: Historic Roots and the Road Forward. // SAIS Review of International Affairs 30, 2(2010), str. 5.

³³ Ibid.

cenzure i iskoristile ih za onemogućavanje prodora kritičnih informacija.³⁴ Prema izvješćima *Reportera bez granica* stvari se čine još gorima: uz regularnu vojsku svake države, mnoge sada imaju tzv. *cyber* vojske, koje mogu ili ne moraju biti službene, a najbolji primjeri su kineska, sirijska i iranska *cyber* vojska.³⁵ Tu ne treba zanemariti niti onu vjerojatno najjaču, a to je američka pod imenom U.S. Cyber Command pod nadležnosti NSA-a, tj. National Security Agency³⁶ koja je stekla poraznu reputaciju zbog prekoračenja ovlasti nadzora, unatoč navedenih razloga očuvanja stabilizacije i sigurnosti. Vrlo negativistička slika cenzure jest ona Rossova prema kojoj danas internet u mnogim zemljama sve više izgleda kao Intranet.³⁷ S tom informacijom na umu, u sljedećem poglavlju će biti govora o razlozima koji se učestalo javljaju kao zakonsko objašnjenje provođenja cenzure.

4. Razlozi cenzure na internetu

S obzirom na mogućnosti koje internet pruža, variraju razlozi cenzure. Način na koji se koristi medij, preispitivan je s viših instanci, te ako postoji politički, društveni, ekonomski, vjerski, filozofski, moralni, ideološki, vojni, korporativni ili obrazovni razlog zbog kojeg ljudi osjećaju napad na sebe ili svoje vrijednosti, može doći do cenzure sadržaja.³⁸ Razlozi cenzure spadaju pod diskusiju moralnosti cenzure, jer navedeni razlozi zbog kojih se cenzura provodi, čak i kada su jasno formulirani, mogu biti vrlo labilni i neuvjerljivi u danom kontekstu. Zbog istog razloga može biti cenzuriran sadržaj koji je uistinu štetan, dok u drugom kontekstu, pod istom izlikom može biti uklonjen sadržaj koji je od izrazite važnosti za zajednicu ali remeti uspostavljenu političku ravnotežu. Prvi razlog koji se najčešće navodi kao opravdanje za cenzuru je strah od zločinačke djelatnosti ili terorizma. No, protivnici cenzure tvrde da je razlog zadiranja u strukturu interneta uvijek politički.³⁹ Dihotomija istih razloga je ključan problem u određivanju sadržaja za cenzuru. Bambaour postavlja pitanje kako razlikovati

³⁴ Morozov, E. The Internet: A room of our own? // *Dissent* 56, 3(2009), str. 83.

³⁵ Internet Enemies Report 2012. Reporters Without Borders, 2012. Str. 6. URL: http://en.rsf.org/IMG/pdf/rapport-internet2012_ang.pdf (30.8.2014.)

³⁶ Deibert, R.; Rohozinski, R. Liberation vs. Control: the Future of Cyberspace. // *Journal of Democracy* 21, 4(2010.), str. 49.

³⁷ Ross, A. Internet Freedom: Historic Roots and the Road Forward. // *SAIS Review of International Affairs* 30, 2(2010), str. 5.

³⁸ Bitso, C. et al. Trends in Transition from Classical Censorship to Internet Censorship. IFLA, str. 4. URL: <http://www.ifla.org/publications/trends-in-transition-from-classical-censorship-to-internet-censorship-selected-country-o> (30.8.2014.)

³⁹ Bitso, C. et al. Trends in Transition from Classical Censorship to Internet Censorship. IFLA, str. 10. URL: <http://www.ifla.org/publications/trends-in-transition-from-classical-censorship-to-internet-censorship-selected-country-o> (30.8.2014.)

cenзуru pornografije u Saudijskoj Arabiji, cenзуru političkog govora u Kini ili poteze američke vlade kojima se cenзуrom koriste u borbi protiv piratstva.⁴⁰ Bili razlozi cenzure zaštita djece ili borba protiv kriminala, zaštita autorskih prava ili radikalnih razloga kao zatiranje političkih disidenata, cenзуra u konačnici daje isti rezultat.⁴¹ Morozov upozorava da zakoni koji se temelje na cenзuri određenog sadržaja svejedno mogu davati legitimitet cenзuri interneta primjerice u Kini, Tajlandu, Vijetnamu, Turskoj i Rusiji, gdje se sloboda političkog govora onemogućava pod isprikom cenzuriranja 'online vulgarnosti'.⁴²

Nekoliko autora koji su se bavili cenзуrom interneta, klasificirali su vrste cenзura prema motivima zbog kojih se provodi. Cohen navodi sljedeće:

1. Nacionalna sigurnost (fabrikacija oružja, ilegalni narkotici, zaštita od terorizma)
2. Zaštita maloljetnika (zlostavljanje, marketinška usmjerenost na djecu, nasilje i pornografija)
3. Zaštita ljudskog dostojanstva (poticanje na rasnu netrpeljivost ili diskriminaciju)
4. Ekonomska sigurnost (pronevjere, krađa kreditnih kartica)
5. Informacijska sigurnost (zlonamjerno hakiranje)
6. Zaštita privatnosti (neautorizirano poslovanje osobnim podacima, elektroničko napastovanje, *spam*)
7. Zaštita reputacije (klevete, nezakonito usporedno oglašavanje)
8. Zaštita intelektualnog vlasništva (nezakonita distribucija zaštićenog materijala kao što je glazba, softver, knjige, itd.)⁴³

Deibert navodi nekolicinu razloga. Politički razlozi pri čemu je cenзуra usmjerena na stranice koje izražavaju stajališta opozicije, a usko je povezano i s ljudskim pravima, slobodnom govora, pravima manjima i vjerskim pokretima. Sljedeća je društvena cenзуra koja se bavi cenзуrom tema kao što su seksualnost, kockanje, ilegalne droge, alkohol ili neke druge zabranjene supstance. Treća bi bila sigurnosna cenзуra, tj. cenзуra sadržaja povezanog s vojnim sukobima, graničnim previranjima i militantnim grupama.⁴⁴ Dok politički stabilnije zemlje cenzuriraju pornografiju i sadržaje koji potiču rasizam i ksenofobiju, represivne države najčešće cenzuriraju ono što se u njihovoj kulturi smatra nemoralnim sadržajem, što može

⁴⁰ Ibid., str. 13.

⁴¹ Cenзуra na internetu. Centar za informacijsku sigurnost, 2011. str. 5. URL: <http://www.cis.hr/files/dokumenti/CIS-DOC-2011-06-016.pdf> (30.8.2014.)

⁴² Morozov, E. The Internet: A room of our own? // Dissent 56, 3(2009), str. 82.

⁴³ Bitso, C. et al. Trends in Transition from Classical Censorship to Internet Censorship. IFLA, str. 11. URL: <http://www.ifla.org/publications/trends-in-transition-from-classical-censorship-to-internet-censorship-selected-country-o> (30.8.2014.)

⁴⁴ Ibid., str. 13.

sezati od političkog govora do bilo kojeg sadržaja koji se tiče ljudskih prava kao pitanja o *gay* i lezbijskoj populaciji ili samo ženskim pravima.⁴⁵

No sve vrste cenzure imaju jedno zajedničko: „cenzurom većina zemalja želi da određeni sadržaj nestane s interneta.“⁴⁶

5. Načini cenzure na internetu

Cenzuru mogu provoditi sveučilišta, škole, roditelji, različite interesne strane, pa čak i pojedinci mogu cenzurirati sami sebe kroz autocenzuru, no ipak najbitniji sprovoditelj cenzure je vlada.⁴⁷ Načini cenzure ovise o sadržaju koji se cenzurira, kome je cenzura u interesu te kakvim mogućnostima dotični raspolažu, tko su oni koji informaciju pokušavaju dobiti ili raspačavati i na koji način. Kad se govori o cenzuri na internetu, najčešće se misli na cenzuru u tehničkom smislu, no to nije jedini oblik provođenja cenzura, jer postoje 'klasične' metode cenzure, kao što je prisila na autocenzuru ili neki drugi oblik fizičkog zaprečivanja. Cenzura u autoritarnim državama se provodi najčešće kombinacijom tehnoloških i društveno-političkih mjera.⁴⁸

Prema Leberknightu osnovni kriteriji za odabir prihvatljive metode za cenzorasu:

- Cijena – resursi i mogućnosti cenzora su direktno pogođeni ovom stavkom, jer je presudna za raspoloživost cenzora
- Obuhvat – raspon komunikacijskih sredstava koji su zahvaćeni cenzurom
- Opseg – broj korisnika i uređaja koji mogu istodobno biti cenzurirani
- Brzina – vrijeme reakcije cenzora
- Efikasnost⁴⁹ – djelotvornost na različitim razinama, npr. serverima, ulazima (*ports*), stranicama, korisničkim uređajima...
- Lažni negativni rezultati – preciznost cenzora
- Lažni pozitivni rezultati – previše lažno pozitivnih rezultata iscrpljuje resurse cenzora
- Zaobilaznost⁵⁰ – koliko je jednostavno zaobići cenzorski sustav⁵¹

⁴⁵ Ibid., str. 18.

⁴⁶ Ibid., str. 13.

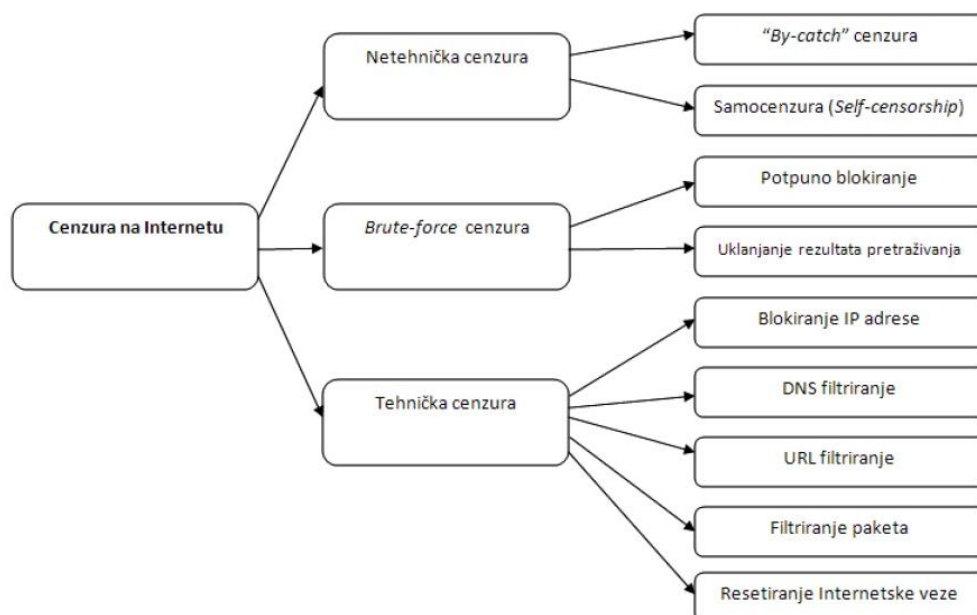
⁴⁷ Ibid., str. 6.

⁴⁸ Morozov, E. Whither Internet Control? // Journal of Democracy 22, 2(2011). Str. 73.

⁴⁹ U izvorniku *granularity*

⁵⁰ U izvorniku *circumvention*

⁵¹ Leberknight, C.S. A Taxonomy of Internet Censorship and Anti-Censorship. Princeton University, 2010. str. 3.



Slika 1. Cenzura na internetu⁵²

Centar informacijske sigurnosti usustavljuje složeniju taksonomiju cenzure, prva je po sredstvima koji se koriste te se dijeli na netehničku, tehničku i *brute-force* cenzuru.⁵³ Sve tri se dalje dijele na podskupine kako je prikazano na slici br. 1. Netehnička cenzura obuhvaća *by-catch* cenzuru i autocenzura, što su uobičajene metode cenzure koje se koriste u drugim medijima, televiziji, na radiju, tiskovinama i općenito slobodi govora, a primjenjive su i na cenzuru interneta. Drugu skupinu čine metode *brute-force* cenzure koja se provodi potpunim blokiranjem ili uklanjanjem rezultata pretraživanja. Treća skupina je tehnička cenzura podijeljena na blokiranje IP adrese, DNS filtriranje, URL filtriranje, filtriranje paketa i resetiranje internetske veze.⁵⁴

Unatoč tomu što cenzura provedena kroz društveno-političke metode može biti rigoroznija od one temeljene samo na tehnološkim mjerama,⁵⁵ ipak su od najvećeg interesa upravo tehničke metode cenzure, jer su specifične samo za medij interneta, te se razvijaju sukladno s razvojem same mreže. Tehnička cenzura se ugrubo može podijeliti prema hardverskoj i softverskoj cenzuri.⁵⁶ Hardverska cenzura koristi sustave kao što su uređaji za Deep Packet Inspection koji klasificiraju mrežni promet i ispituju informacijske pakete.⁵⁷

⁵²Cenzura na internetu. Centar za informacijsku sigurnost, 2011. str. 7. URL: <http://www.cis.hr/files/dokumenti/CIS-DOC-2011-06-016.pdf> (30.8.2014.)

⁵³Ibid.

⁵⁴Ibid.

⁵⁵Morozov, E. Whither Internet Control? // Journal of Democracy 22, 2(2011). Str. 74.

⁵⁶Leberknight, C.S. A Taxonomy of Internet Censorship and Anti-Censorship. Princeton University, 2010. Str.5.

⁵⁷Ibid.

Softver za cenzuru se temelji uglavnom na filtrima i blokiranju sadržaja⁵⁸, a programi koji se bave cenzurom na internetu poznat je pod nazivom *ensorware*.⁵⁹ Centar informacijske sigurnosti navodi pet načina provedbe tehničke cenzure a to su blokiranje IP adrese, DNS filtriranje, URL filtriranje, filtriranje paketa, resetiranje internetske veze.⁶⁰ Slijedi kratak pregled različitih metoda cenzure, tehničkih i netehničkih, te dodatno poglavlje o najčešćim točkama napada unutar infrastrukture interneta.

5.1. Tehnička cenzura

Tehnička cenzure je manipulacija sadržajem i informacijama nekom od tehničkih metoda. U ovom poglavlju bit će objašnjenemetode blokiranja IP adrese, DNS filtriranja, URL blokiranja, filtriranja HTTP Proxyja, filtriranja paketa, rušenje poslužitelja, DOS napadi, ponovno uspostavljanje internetske veze i nadzor.

5.1.1. Blokiranje IP adrese

Filtriranje preko IP adrese se koristi za blokiranje nepoželjnog sadržaja onemogućavanjem pristupa pojedinim IP adresama.⁶¹ Blokiranjem IP adrese blokira se povezivanje web stranice tj. poslužitelja te određene IP adrese ili više njih.⁶² Blokiranje IP adrese je najraniji oblik internetske cenzure koji se javio u Kini već 1990-ih godina.⁶³ Osim što je jedan od najučestalijih oblika cenzure, ista metoda se može koristiti i kao sprečavanje nepoželjne veze između korisnika i web stranice ili nekog poslužitelja, a također se na forumima i stranicama može koristiti u službi onemogućavanja pristupa određenim korisnicima. Blokiranje IP-a je najjeftiniji oblik cenzure, no ne omogućava visoku preciznost u operaciji. Jednostavno je i jeftino za inkorporiranje u sustav, no najveći je problem nenamjerno blokiranje i korisnog sadržaja.⁶⁴

⁵⁸Ibid.

⁵⁹ Cenzura na internetu. Centar za informacijsku sigurnost, 2011. str. 5. URL: <http://www.cis.hr/files/dokumenti/CIS-DOC-2011-06-016.pdf> (30.8.2014.)

⁶⁰ Ibid., str. 7.

⁶¹ Leberknight, C.S. A Taxonomy of Internet Censorship and Anti-Censorship. Princeton University, 2010. str.4.

⁶² Cenzura na internetu. Centar za informacijsku sigurnost, 2011. str. 7-8 URL: <http://www.cis.hr/files/dokumenti/CIS-DOC-2011-06-016.pdf> (30.8.2014.)

⁶³ Defeat Internet Censorship: Overview of Advanced Technologies and Products. Global Internet Freedom Consortium, 2007. Str. 5. URL:

http://www.internetfreedom.org/archive/Defeat_Internet_Censorship_White_Paper.pdf (30.8.2014.)

⁶⁴ Leberknight, C.S. A Taxonomy of Internet Censorship and Anti-Censorship. Princeton University, 2010. str.4.

Murdoch i Anderson govore o načinima na koji se odabiru nepoželjne IP adrese. Prva je filtriranje zaglavlja (*TCP/IP header filtering*) pri čemu cenzorski usmjernik (engl. *router*) pregledava IP adresu i broj pristupne točke (engl. *port number*), te ako je odredište nađeno na crnoj listi, veza se ne uspostavlja ili preusmjerava na stranicu koja upozorava da je pristup zabranjen. Drugi način je filtriranje sadržaja, samo što usmjernik umjesto naslova ispituje sadržajne pakete u potrazi za riječima i pojmovima koji su na crnoj listi, no pažnja nije toliko usmjerena na sadržaj, već na ishodište ili odredište na koje paketi putuju.⁶⁵

5.1.2. DNS filtriranje

DNS ili *Domain Name Server* služi kao posrednik između internetskog pretraživača u koji korisnik upisuje slovanu adresu (URL – *Uniform Resource Locator*) neke stranice, te pronalazi brojčanu adresu (IP adresu) dotične stranice kojom se koriste računala. Kad je neka stranica blokirana kroz DNS filtar, više ju nije moguće pronaći. Nepoželjna stranica još uvijek postoji na Webu, no nije ju moguće locirati.⁶⁶ Kad korisnik zatraži određenu URL adresu, u slučaju DNS filtriranja pretraživač vraća zahtjev bez IP adrese ili u slučaju DNS preusmjeravanja, vraća zahtjev s različitom adresom. Tražena stranica još uvijek postoji ali je pristup onemogućen izmijenjenim informacijama na poslužitelju.⁶⁷ DNS filtriranje nije vrlo učinkovita metoda cenzure, jer je umjesto URL adrese moguće upisati izravno IP adresu i pristupiti željenom sadržaju,⁶⁸ koristeći upute koje su dostupne na internetu. CIS spominje još jednu metodu zaobilaženja ovog tipa cenzure a to je korištenje alata kao što su JAP, Freenet i drugi koji omogućuju korištenje poslužitelja koji nisu koruptirani, npr. korisnik u Kini može koristiti DNS poslužitelj u SAD-u koji ima pristup traženoj stranici.⁶⁹

5.1.3. URL blokiranje

⁶⁵ Bitso, C. et al. Trends in Transition from Classical Censorship to Internet Censorship. IFLA, str. 15-16. URL: <http://www.ifla.org/publications/trends-in-transition-from-classical-censorship-to-internet-censorship-selected-country-o> (30.8.2014.)

⁶⁶ DNS Filtering to Fight Internet Piracy Violates the First Amendment. Jurist. 2012. URL: <http://jurist.org/datetime/2012/01/lauren-mack-dns-filtering.php> (30.8.2014.)

⁶⁷ Cenzura na internetu. Centar za informacijsku sigurnost, 2011. str. 8. URL: <http://www.cis.hr/files/dokumenti/CIS-DOC-2011-06-016.pdf> (30.8.2014.)

⁶⁸ DNS Filtering to Fight Internet Piracy Violates the First Amendment. Jurist. 2012. URL: <http://jurist.org/datetime/2012/01/lauren-mack-dns-filtering.php> (30.8.2014.)

⁶⁹ Cenzura na internetu. Centar za informacijsku sigurnost, 2011. str. 8. URL: <http://www.cis.hr/files/dokumenti/CIS-DOC-2011-06-016.pdf> (30.8.2014.)

Na sličnom principu kao i DNS filtriranje, funkcionira i URL blokiranje. Određene stranice su identificirane i uključene u svojevrsnu bazu stranica kojima se ne može pristupiti. Ova metoda je vrlo jednostavna, neprilagodljiva, te se vrlo lako može zaobići jednostavnim upisivanjem IP adrese u pretraživač umjesto URL adrese.⁷⁰

5.1.4. Filtriranje HTTP Proxyja

Vrlo često korisnici su primorani koristiti HTTP Proxyje, posredničke poslužitelje između web-preglednika i interneta, kako bi se uopće spojili na internet. HTTP Proxy je najlakši način kontrole cjelokupnog protoka informacija čime se lako blokira i filtrira zlonamjerna sadržaj i štetni programi,⁷¹ no time je filtriranje tog poslužitelja u svrhu cenzure mnogo uspješnije od DNS filtriranja. S obzirom da je ta metoda i zahtjevnija, obično se kombinira s drugim oblicima filtriranja.⁷²

5.1.5. Filtriranje paketa

Filtriranje paketa se odvija unutar vatrozida na dolaznim paketima informacija koji su potom filtrirani prema postavljenim kriterijima filtra. Paket je potom ili prihvaćen ili odbijen. Filtar se može konfigurirati da prihvaća pakete koji se smatraju sigurnim i potpunim nepropuštanjem svih ostalih ili odbijanjem neodgovarajućih paketa i prihvaćanjem ostalih, te treći način konfiguracije omogućuje spremanje paketa u karantenu a korisnik sam odlučuje hoće li ga prihvatiti ili ne. Prva metoda je najsigurnija no blokira veliku količinu podataka.⁷³ Jedan od najučinkovitijih načina cenzure jest kombinacija URL blokiranja i paketnog filtriranja.⁷⁴

5.1.6. Ponovno uspostavljanje internetske veze

Metoda cenzure koja se rjeđe koristi jer je poprilično radikalna, temelji se na potpunom blokiranju TCP veze (engl. *Transmission Control Protocol*) pri pokušaju spajanja

⁷⁰ Ibid., str. 9

⁷¹ Što je Proxy poslužitelj? Windows Microsoft. URL: <http://windows.microsoft.com/hr-hr/windows-vista/what-is-a-proxy-server> (9.9.2014.)

⁷² Bitso, C. et al. Trends in Transition from Classical Censorship to Internet Censorship. IFLA, str. 16. URL: <http://www.ifla.org/publications/trends-in-transition-from-classical-censorship-to-internet-censorship-selected-country-o> (30.8.2014.)

⁷³ Cenzura na internetu. Centar za informacijsku sigurnost, 2011. str. 10-11. URL: <http://www.cis.hr/files/dokumenti/CIS-DOC-2011-06-016.pdf> (30.8.2014.)

⁷⁴ Ibid.

na istu. Pokušaj spajanja s korisničke strane ili sa strane poslužitelja će biti blokirani u vremenskom periodu od 30 minuta, a ako se komunikacija odvijala posrednički, stranica može biti blokirana i drugim korisnicima ili web stranicama.⁷⁵

5.1.7. Napadi DOS (Denial-of-Service)

Puno ime metode je *Dedicated Denial of Service Attacks* (DDoS), a postiže se prekomjernim brojem zahtjeva korisnika ili kompjutera upućen poslužitelju što rezultira zagušenjem poslužitelja, čime se veza prekida. Freedom House ovu metodu naziva 'tehničkim nasiljem' jer hakeri mogu paralizirati ili sasvim srušiti stranicu.⁷⁶

5.1.8. Rušenje poslužitelja

Kompanija koja posluje kao domaćin nekom poslužitelju, može ga u potpunosti ugasiti i odspojiti s interneta. Mogućnost za vlasnika poslužitelja, ipak, jest da prenese sadržaj poslužitelja u neku drugu kompaniju ako posjeduje sigurnosnu kopiju.⁷⁷

5.1.9. Nadzor

Nadzor je konstantno tehničko praćenje razmjene paketa podataka između korisnika i računala-domaćina. U slučaju da je sadržaj koji protiče zabranjen, neka od metoda cenzure može biti primijenjena. Vrlo često je smisao konstantnog nadzora prouzrokovati strah, više nego cenzurirati – korisnici koji su svjesni da su nadzirani, ne odlučuju se tako lako na objavljivanje ili pretraživanje zabranjenog sadržaja.⁷⁸

5.2. Netehnička cenzura

⁷⁵ Ibid.

⁷⁶ Ross, A. Internet Freedom: Historic Roots and the Road Forward. // SAIS Review of International Affairs 30, 2(2010), str. 10.

⁷⁷ Bitso, C. et al. Trends in Transition from Classical Censorship to Internet Censorship. IFLA, str. 16. URL: <http://www.ifla.org/publications/trends-in-transition-from-classical-censorship-to-internet-censorship-selected-country-o> (30.8.2014.)

⁷⁸ Ibid., str. 16.

Netehnička cenzura je ona koja ne pripada domeni tehničke organizacije interneta, te se ne svodi isključivo na medij interneta, nego se bazira na prokušanim metodama korištenim ponekad i stoljećima u procesu cenzure. Cenzura je vrlo često zakonski potpomognuta, čime nakladnici, autori ili ISP-ovi (engl. *ISP – Internet service providers*) mogu zaprimati službene zahtjeve za uklanjanjem, izmjenom ili blokiranjem stranica ili sadržaja ili u drastičnijim oblicima mogu biti zatočeni ili pod prijetnjom zatvaranja, otkaza, fizičkog zlostavljanja, čak i smaknuća. Cenzori mogu raditi na propagandi plaćajući pojedincima da pišu članke i komentare u korist određene ideje ili protiv opozicije, stvarati svoje stranice i publikacije kao dio samopromocije. Još jedan od vrlo djelotvornih načina cenzure je ograničenost pristupu internetu zbog visokih cijena izdavanja dozvole ili ograničenje općeg pristupa internetu zbog manjkave infrastrukture što može biti namjerno ili ne.⁷⁹

5.2.1. Autocenzura

Samocenzura ili autocenzura jest „cenzuriranje samoga sebe; javno djelovanje (npr. novinara, književnika) pri kojem se po vlastitoj volji izbjegavaju teme koje bi mogle biti nepoćudne vlasti, iako sama vlast ne provodi cenzuru.“⁸⁰ Autocenzuru provode privatne ili pravne osobe kao odgovor na prijetnju zbog kršenja zakona o govoru na internetu.⁸¹

Što se tiče interneta, autocenzura se provodi samonadzorom u izboru ključnih riječi pri pretraživanju interneta i izborom sadržaja koji korisnik sam odabire objaviti. Autocenzura je reakcija na mogućnost zakonske prijetnje, promocijama određenih društvenih normi, ili neslužbenim metodama zastrašivanja. U većini slučajeva, autocenzura nije problem o kojem se govori ili piše. Također, sumnja da država sudjeluje u nadzoru korisnika, bio to slučaj ili ne, je snažan poticaj na oprez pri objavi sadržaja ili posjećivanju stranica koje bi mogle privući pozornost autoriteta.⁸²

5.3. Točke napada

⁷⁹Internet Censorship. // Wikipedia. URL: http://en.wikipedia.org/wiki/Internet_censorship#Non-technical_censorship (30.8.2014.)

⁸⁰Cenzura. // Hrvatska enciklopedija. URL: <http://www.enciklopedija.hr/Natuknica.aspx?ID=11246> (30.8.2014.)

⁸¹Ross, A. Internet Freedom: Historic Roots and the Road Forward. // SAIS Review of International Affairs 30, 2(2010), str. 10.

⁸²About Filtering. Open Net Initiative. URL: <https://opennet.net/about-filtering> (30.8.2014.)

Open Net Initiative navodi najčešće točke napada cenzure, a pojedine države provode cenzuru na svim navedenim razinama:

- Mreža s magistralnom osnovom (*Internet backbone*) – cenzura na državnoj razini može biti efikasno provedena filtriranjem sadržaja i tehnologijom za blokiranje na razini magistrale, time utječući na pristup informacijama u cijeloj državi.
- Pružatelji internetskih usluga – državna cenzura se najčešće provodi na ovoj razini; ISP-ovi koriste ili su prisiljeni koristiti neku od metoda filtriranja.
- Institucije – filtriranje na institucionalnoj razini korištenjem tehničkog blokiranja ili nametnute autocenzure odvija se u tvrtkama, državnim organizacijama, školama i *cyber* kafićima. U nekim zemljama, cenzura na toj razini se vrši pod pritiskom države, no čest je slučaj i zabrana unutar institucija kako bi se povećala produktivnost na radnim mjestima.
- Osobna računala– kućna i osobna računala mogu biti cenzurirana ugradnjom softvera za filtriranje koje onemogućava pristup određenim stranicama.⁸³

6. Tvrtkeu službi cenzure

Problem cenzure u autoritarnim državama ne proizlazi samo iz djelatnosti restriktivne države, uz tehnologiju vlastite izrade i rada vlastitih institucija, već postoji dublja problematika. Unatoč tomu što glavina aktivističke energije usmjerene kroz nove tehnologije dolazi sa Zapada, činjenica je da nemaju svi jednako mišljenje o slobodi govora čak i u liberalnim državama koje se ponose slobodom pristupa informacijama. Uočeno je da je najnaprednija tehnologija korištena u cenzuriranim zemljama zapravo zapadnjačkog podrijetla, te da mnoge zapadnjačke tvrtke rade predano na tome da osmisle i implementiraju sustave primjereno skrojene za potrebe, primjerice, diktature. To dodatno komplicira globalnu borbu za slobodom informacija jer se postavlja pitanje kako spriječiti cenzuru u društvu i političkom ustroju koje tome nije sklono, ako i ono koje podržava određene ideje nije spremno raditi za isti cilj. Pobrojavanje tvrtki koje se koriste kršenjem ljudskih prava u svrhu zarade daje dojam uzaludnosti borbi i aktivističkim stavovima. Reporter bez granica navode nekoliko tvrtki koje se bave izradom alata za cenzuru i izvozom istih u države kritičnog stanja, te će o tim tvrtkama kasnije biti govora. Proizvodi koje ove tvrtke izvoze koriste se za

⁸³Ibid.

kršenje ljudskih prava, špijuniranje novinara, disidenata, političkih aktivista, stoga tvrtke moraju biti svjesne odgovornosti i posljedica koje ima primjena te tehnologije u autoritarnim režimima, a svaki propust u izvozu njihovog softvera je očit znak nemara u poslovanju.⁸⁴

Morozov navodi nekoliko slučajeva u kojima je cenzura potpomognuta zapadnjačkom tehnologijom: aktivisti za ljudska prava u Libiji su prijavili da su se pojavili transkripti njihovih SMS poruka, što je njihovoj vladi bilo omogućeno kroz proizvode njemačke tvrtke Siemens, a koje održavaju Nokia Siemens Networks (sa sjedištem u Finskoj) i Trovicor, također njemačka kompanija. Egipatski aktivisti su otkrili da je Mubarakov režim koristio alate razvijene u britanskoj tvrtci Gamma International, a koji su im omogućili prisluškivanje razgovora na Skypeu.⁸⁵ Reporteri bez granica tvrde da je zapadnjačka tehnologija u službi cenzure pronađena u Bahreinu, Iranu, Siriji, Jemenu, Kual Lumpur i Maleziji, među njima su američka tvrtka BlueCoat s djelovanjem u Siriji, francuska kompanija Amesyn u Libiji u službi Gadaffija, te Vodafone u Egiptu. Talijanska kompanija AreaSpa se povukla iz Sirije i suradnje s Assadovim režimom zbog kampanja koje su se vodile protiv nje.⁸⁶ Open Net Initiative je objavio da je Netsweeper (sa sjedištem u Kanadi) i američke tvrtke Websense i McAfee (u vlasništvu Intel) proizvode programe za potrebe cenzure u većini državnih ustroja Srednjeg Istoka i Sjeverne Afrike, a što je još dubioznije, Websense to čini unatoč samoobvezi da neće opskrbljivati represivne vlade svojom tehnologijom.⁸⁷

Morozov navodi da je cijeli problem dvojbjen i naoko nerješiv jer tvrtke koje proizvode i izvoze tehnologiju za cenzuru razvile su je u skladu s zapadnjačkim zakonima i unutar obavještajnih agencija, dok s druge strane argument da se dotična tehnologija koristi samo za nadzor ekstremističkih djelatnosti ima sve manju težinu te je sve teže povjerovati u njega.⁸⁸ „Ponuda će uvijek naći svoj put kako bi ispunila potrebu,“ i sve dok tehnologija nalazi svoju primjenu u zapadnim zemljama, sankcije neće polučiti učinak. Morozov opet navodi primjer elektroničkog špijuniranja u Egiptu za vrijeme Mubarakovog režima koje je najvjerojatnije izvedeno uz pomoć američkih saveznika.⁸⁹ Reporteri smatraju da je jedino

⁸⁴ Enemies of the Internet : 2013 report. Reporters without borders, 2013. Str. 3. URL: http://surveillance.rsf.org/en/wp-content/uploads/sites/2/2013/03/enemies-of-the-internet_2013.pdf (30.8.2014.)

⁸⁵ Morozov, E. Political Repression 2.0. The New York Times.2011. URL: <http://www.nytimes.com/2011/09/02/opinion/political-repression-2-0.html> (30.8.2014.)

⁸⁶ Internet Enemies Report 2012. Reporters Without Borders.2012. Str. 6. URL: http://en.rsf.org/IMG/pdf/rapport-internet2012_ang.pdf (30.8.2014.)

⁸⁷ Morozov, E. Political Repression 2.0. The New York Times.2011. URL: <http://www.nytimes.com/2011/09/02/opinion/political-repression-2-0.html> (30.8.2014.)

⁸⁸ Ibid.

⁸⁹ Morozov, E. Political Repression 2.0. The New York Times.2011. URL: <http://www.nytimes.com/2011/09/02/opinion/political-repression-2-0.html> (30.8.2014.)

rješenje uvođenje kontrole izvoza softvera i hardvera za nadzor na razini zakonodavstva. Nadati se da će se privatni sektor sam moralno osvijestiti bi bilo previše za očekivati.⁹⁰

Slijedi kratki pregled pet tvrtki koje su Reporteri označili kao korporativni neprijatelji interneta i plaćenici digitalnog doba, a to su Amesyn, BlueCoat, Gamma International, Hacking Team i Trovicor.⁹¹

6.1. Amesyn

Amesyn je francuska tvrtka koja je trenutačno pod tužbom FIDH-a (Federation International des Droits Humains) zbog prodavanja vlastitog softvera za špijuniranje nazvanog EAGLE, a kojeg je prodala Libiji za vrijeme Gadaffijeve vlade i koji je iskorišten za špijuniranje novinara i aktivista za ljudska prava. Tvrtka je tužena zbog sudjelovanja u mučenju. Sustav EAGLE omogućuje vladi analizu prometa na internetu, čuvanje podataka za kasniju policijsku ili obavještajnu istragu. EAGLE se temelji na Deep Packet Inspection tehnologiji. Podaci iz Amesyna ukazuju da su bili upleteni u analizu podataka dobivenih iz različitih izvora (SMTP, POP, IMAP, Webmail, VOP, chat protokoli, internetski promet, te pretraživači).⁹²

6.2. Blue Coat

Blue Coat je vjerojatno najpoznatija tvrtka za *online* sigurnost, no i za cenzorsku opremu, američkog podrijetla, a njezina prisutnost je uočena u zemljama kao što su Sirija i Burma. Također koriste Deep Packet Inspection koji im omogućuje nadzor, cenzuru interneta, te uvid u svaki informacijski paket bilo kojeg internetskog protokola, te su u mogućnosti ispitati ga prema sadržaju (cenzurirani ili zabranjeni pojmovi) ili prema tipu (elektronička poruka, VoIP, BitTorrent Protocol).

Blue Coat nudi također takozvane *Intelligence Centres*, koji tvrtkama ili vladama omogućuje nadzor protoka informacija i identificiranje problema u performansama. U opsežnom istraživanju koje je proveo Citizen Lab na Sveučilištu u Torontu koje se temeljilo na skeniranju internetu u potrazi za uređajima Blue Coat tvrtke izvijestili su da su uređaji pronađeni u Egiptu, Kuvajtu, državi Katar, Saudijskoj Arabiji i Ujedinjenim Arapskim Emiratima, te da je također vrlo vjerojatno da su isti korišteni i u Bahreinu, Kini, Indiji,

⁹⁰ Enemies of the Internet : 2013 report. Reporters without borders, 2013. Str. 4. URL: http://surveillance.rsf.org/en/wp-content/uploads/sites/2/2013/03/enemies-of-the-internet_2013.pdf (30.8.2014.)

⁹¹ Ibid.

⁹² Ibid.

Indoneziji, Iraku, Keniji, Libanonu, Maleziji, Nigeriji, Rusiji, Južnoj Koreji, Singapuru, Tajlandu, Turskoj i Venezueli.⁹³

6.3. Gamma International

Gamma International je tvrtka koja proizvodi Finfisher tehnologiju za napredno špijuniranje (engl. *spyware*), a koja je pronađena u zemljama koje su poznate po zlostavljanju novinara, npr. Bahrein i Ujedinjeni Arapski Emirati. Finfisher omogućuje čitanje kriptiranih datoteka, elektroničkih poruka i preslušavanje glasa pri pozivima.

Gamma International je tvrtka njemačkog podrijetla no danas je dio Gamma Group smještene u Ujedinjenom Kraljevstvu te je specijalizirana za opremu za nadzor i praćenje. Svoje podružnice također ima i u Južno-istočnoj Aziji i Bliskom Istoku. Njihova tehnologija se smatra jednom od najnaprednijih u svom području proizvodnje. Svoje proizvode isključivo prodaju vladama i agencijama koje izvršavaju zakone.

Njihova tehnologija funkcionira pomoću virusa Trojan koji zarazi računalo ili pametni telefon te je uređaj potom pod kontrolom vladinih organizacija. Njihovom tehnologijom također je moguće zaraziti cijeli internet kafić kako bi se mogle pratiti sve mušterije. Jednom kad je instaliran, virus je gotovo nemoguće ukloniti, a uređaj se njima zarazi lažnim obavijestima o *updateima*, elektroničkom porukom ili fizičkim pristupom uređaju.

Rapid7 je u svojoj studiji identificirao kontrolni softver FinFishera u aktivnoj upotrebi u Australiji, Češkoj, Estoniji, Etiopiji, Indoneziji, Latviji, Mongoliji, Državi Katar, Ujedinjenim Arapskim Emiratima i SAD-u. Nekoliko njihovih servera je pronađeno na Brunejima, Turkmenistanu, Singapuru, Nizozemskoj, Indoneziji i Bahreinu.⁹⁴

6.4. Hacking team

Zemlja podrijetla ove tvrtke je Italija, a sumnja se da je izvozila svoju tehnologiju u Ujedinjene Arapske Emirate i Maroko. Njihov DaVinci sustav za udaljeno upravljanje (engl. Remote control system) može se probiti kroz kriptirane elektroničke poruke, datoteke i telefonske protokole na internetu. Također može na daljinu aktivirati mikrofone i kamere na kompjuteru, a Hacking Team tvrdi da je moguće nadzirati više stotina tisuća računala

⁹³ Ibid., str. 8.

⁹⁴ Ibid.

istodobno. Virus Trojan je dostupan za različite operativne sustave kao Windows, Linux, Mac, Android, Symbian i Blackberry.

Iako kompanija tvrdi da ne prodaju svoj softver zemljama koje su poznate po kršenju ljudskih prava, neka medijska izvješća i istraživanja stručnjaka ukazuju da je softver Hacking Teama pronađen u zemljama s lošom reputacijom kad se radi o ljudskim pravim i demokraciji.⁹⁵

6.5. Trovicor

Trovicor, tvrtka njemačkog podrijetla, s podružnicama u Švicarskoj, Dubaiju, Pakistanu, Kuala Lumpuru i Češkoj, nastala je unutar tvrtke Siemens pod nazivom Department for Voice and Data Recording te djeluje od 1993. Trovicor je jedan od najvećih dobavljača opreme za prisluškivanje, te navodno opskrbljava više od 100 zemalja. Trovicor omogućuje prisluškivanje telefonskih poziva, SMS poruka, VoIP-a, te internetskog prometa. Ne omogućuje praćenje tvrdog diska. Kompanija nudi tzv. Lifecycle management Technology što znači da nude procjenu mreža i internetske strukture u državi, omogućujući rješenja za primjerena svakom slučaju, kao i osposobljavanje državnih službenika za rad na njihovoj tehnologiji.⁹⁶

⁹⁵ Ibid., str. 11.

⁹⁶ Ibid., str. 13.

7. PRIMJERI CENZURE U SVIJETU

„Cenzura je međunarodna, konstantna i prožimajuća... Brige koje su primarne jednoj naciji besmislene su drugoj. Ali politička i moralna/kulturalna cenzura može se promatrati kao prepoznatljiv, čak predvidiv geografski obrazac. Vrsta kulturalne cenzure koja prevladava u Americi, Britaniji i u manjoj mjeri Europi i drugim zapadnjačkim nacijama kao Australiji, je vrlo često nebitna drugdje. Za najsiromašnije nacije cijeli koncept je besmislen... Ovdje je neprimjerena izgladnjelost djece, a ne dječja pornografija. Temelji cenzure u zemljama trećeg svijeta su politički, ukorijenjeni u želji da vladajuća stranka održi privilegirani status. Sudski postupci vezani uz cenzuru koji dopijaju na naslovnici tiču se pobunjenih, ne nepristojnih.“⁹⁷

7.1. Cenzura u Narodnoj republici Kini

Narodna republika Kina je zemlja s najvećim brojem internetskih korisnika na svijetu a taj broj se konstantno povećava, trenutačno ih je više od 500 milijuna prema Reporterima bez granica.⁹⁸ Unatoč tomu, Kina je ujedno i zemlja s najsloženijim cenzorskim sustavom na svijetu, te se mnoge autoritarne države ugledaju na izgrađeni kineski sustav kao uzor za ograničavanje nepoćudnog sadržaja unutar vlastitih granica.

Kao i većina infrastrukture izgrađene u Kini, razvoj arhitekture i infrastrukture interneta je povezan s državnim ustrojem, stoga je i posljedično izrazito centraliziran. Država izdaje licencu kompanijama za davanje pristupa internetu (Internet Access Providers) i omogućavanje internetskih usluga, te sve moraju biti najmanje 51% u državnom vlasništvu. Trenutačno je u Kini devet takvih kompanija koje su zadovoljile uvjete i sve imaju pristup barem jednoj inozemnoj internetskoj magistrali.⁹⁹ S obzirom na dane propise, legitimno se može tvrditi da je kineski internet u vlasništvu države, to jest vladajuće stranke. Četiri velike državne kompanije čine okosnicu interneta u Kini - CTNET, Chinanet, Cernet i CHINAGBN. Od restrukture mreže 2008. godine istaknula su se tri nacionalna davatelja usluga - China

⁹⁷ Gren, J. Encyclopedia of Censorship New York: Facts on File, Inc., 2005. str. XX

⁹⁸ Enemies of the Internet : 2013 report. Reporters without borders, 2013. Str. 19. URL: http://surveillance.rsf.org/en/wp-content/uploads/sites/2/2013/03/enemies-of-the-internet_2013.pdf (30.8.2014.)

⁹⁹ Zheng, H. Regulating the Internet: China's Law and Practice // Beijing Law Review 4, 1(2013). str 1.

Telecom, China Unicom i China Mobile, a pristup internetu se potom delegira na mjesne kompanije.¹⁰⁰

Nove tehnologije prodiru sve dublje u niže slojeve, te postaju dostupne radničkoj klasi putem mobitela i mobilnog interneta, a pristup informacijama i komunikaciji stvara „društvo umrežene radničke klase“ kako ju naziva Rebecca MacKinnon, no upozorava da se time otvara i put autoritarnoj vladi ka organizaciji i indoktrinaciji te kreiranju radne snage koju je lako „programirati“.¹⁰¹ Nove tehnologije omogućuju široj javnosti pogodnosti kakve su koje desetljeće unatrag bile nezamislive, no u Kini je još uvijek dalek put od brzog, sveprodirućeg i slobodnog interneta. Ekonomski razvitak Kine je vrlo nejednak, a pristup internetu je u potpunosti manipuliran. Kako navodi Freedom House, infrastruktura je poprilično siromašna, centralizirana, vrlo često je pristup usporen ili sasvim zapriječen. Pristup inozemnim stranicama je usporen zbog blokiranja, filtriranja i nadzora na nacionalnoj razini.¹⁰²

Godine 1996. u Kini je proglašen popis zabranjenog sadržaja koji kola informacijskim mrežama, a taj sadržaj je svrstan u četiri skupine: informacije koje ugrožavaju nacionalnu sigurnost, razotkrivaju državne tajne, prijete društvenoj stabilnosti i seksualno sugestivan sadržaj.¹⁰³ Danas je taj popis nešto duži i precizniji izravno zabranjujući kršenje Ustava, potkopavanje režima, širenje glasine koje potiču na rastroj društvenog poretka, poticanje nezakonitog okupljanja, udruživanja, marširanja i prosvjeda te ostalog.¹⁰⁴ No većina zabilježenih slučajeva ukazuje da su tabu teme kineske vlade one vezane uz građanske pokrete oko problema kao što su zagađenje okoliša, zagađenost hrane, policijsko nasilje, te da se najčešće cenzurira ne kritički govor nego informacije koje bi mogle voditi do građanskih akcija.¹⁰⁵

Kineska vlada provodi cenzuru na nekoliko razina, tehničkim metodama, *cyber* policijom, zakonodavstvom, nadzorom i prisilom na autocenzuru.¹⁰⁶ Freedom House navodi

¹⁰⁰ Enemies of the Internet : 2013 report. Reporters without borders, 2013. Str. 19. URL: http://surveillance.rsf.org/en/wp-content/uploads/sites/2/2013/03/enemies-of-the-internet_2013.pdf (30.8.2014.)

¹⁰¹ MacKinnon, R. China's "Networked Authoritarianism" // Journal of Democracy 22, 2(2011). Str. 34-35.

¹⁰² Freedom on the Net 2013: A Global Assessment of Internet and Digital Media. Freedom House, 2013. str. 186.

¹⁰³ Zheng, H. Regulating the Internet: China's Law and Practice // Beijing Law Review 4, 1(2013). Str. 2.

¹⁰⁴ Chung, J. Comparing Online Activities in China and South Korea: The Internet and the Political Regime // Asian Survey 48, 5(2008). Str. 736.

¹⁰⁵ Freedom on the Net 2013: A Global Assessment of Internet and Digital Media. Freedom House, 2013. Str. 193.

¹⁰⁶ Chung, J. Comparing Online Activities in China and South Korea: The Internet and the Political Regime // Asian Survey 48, 5(2008). Str. 734.

tri vrste cenzure koja se provodi u Kini: automatsko tehničko filtriranje, prisilna autocenzura i proaktivna manipulacija, te ćemo se na sve tri osvrnuti u daljnjem tekstu.¹⁰⁷

Najveći projekt za cenzuru i nadzor kineske vlade pod imenom Golden Shield Project postao je kolokvijalno poznat kao Veliki kineski vatrozid. Projekt je sačinjen od standardnih vatrozida i proxy servera na izlaznim točkama (engl. *Internet gateways*) koji omogućuju blokiranje sadržaja preusmjeravanjem IP adresa.¹⁰⁸ Također se koristi tehnologijom DPI (Deep Packet Inspection) kako bi automatski blokirao sadržaj na temelju detekcije ključnim riječima. DPI tehnologija ispituje korisnički zahtjev kao i rezultat pretraživanja u potrazi zabranjenih riječi. Godine 2012. projekt je nadograđen te sada ima mogućnost blokiranja kriptiranih veza, stoga jedan od glavnih državnih davatelja usluga China Unicom trenutačno prekida vezu u pokušaju prodora kriptiranog sadržaja.¹⁰⁹

Stranice koje kineska vlada redovito blokira su stranice koje se teško mogu nadzirati, a to su najčešće inozemne obavijesne stranice (kao BBC) ili stranice koje se često kritički osvrću na kineski režim a to su Amnesty International, Human Rights Watch, te društvene stranice i blogovi. Te stranice su konstantno blokirane jer ne žele surađivati s kineskom vladom.¹¹⁰ Ono što se najčešće filtrira je 'osjetljivi' sadržaj, kao protest na trgu Tiananmen 1989., nezavisnost Tibeta i Tajvana, te mnogi drugi.¹¹¹ No, kako navodi Freedom House „filtriranje je heterogeno i vrlo često nekonzistentno, ovisi o trenutku, tehnologiji i geografskoj regiji.“¹¹² Govoreći i Velikom kineskom vatrozidu, neki naglašavaju da nije nužno da sav sadržaj treba biti filtriran i ispitan, jer uvijek treba imati na umu da vatrozid djeluje kao panoptikum, jer korisnici znajući za njega, sami se spontanu odlučuju za autocenzuru, što nas dovodi do drugog tipa cenzure prema Freedom Houseu.¹¹³

Cenzura interneta je sveprisutna i provodi se na različitim razinama i metodama, prisiljavajući pasivno korisnike na autocenzuru, uznemiravanjem putem elektroničke komunikacije ili osobno, a korisnici koji su pritvoreni ili trajno zatočeni, služe kao opomena ostalima o provedbi nadzora.¹¹⁴ Isti strah dijele i korisnici i različiti davatelji usluga i privatni entiteti. Pritisak je toliko jak da primjerice forumi imaju svoje vlastite filtre kako bi na

¹⁰⁷ Freedom on the Net 2013: A Global Assessment of Internet and Digital Media. Freedom House, 2013. Str. 194.

¹⁰⁸ Golden Shield Project. // Wikipedia. URL: http://en.wikipedia.org/wiki/Golden_Shield_Project (30.8.2014.)

¹⁰⁹ Enemies of the Internet : 2013 report. Reporters without borders, 2013. Str. 20. URL:

http://surveillance.rsf.org/en/wp-content/uploads/sites/2/2013/03/enemies-of-the-internet_2013.pdf (30.8.2014.)

¹¹⁰ Zheng, H. Regulating the Internet: China's Law and Practice // Beijing Law Review 4, 1(2013). Str. 2.

¹¹¹ Ibid.

¹¹² Freedom on the Net 2013: A Global Assessment of Internet and Digital Media. Freedom House, 2013. Str. 194-195

¹¹³ Ibid., str. 195.

¹¹⁴ MacKinnon, R. China's "Networked Authoritarianism" // Journal of Democracy 22, 2(2011). Str. 40-41.

vrijeme detektirali neprimjerene riječi kako bi što prije maknuli ili izmijenili objavljenu poruku, a korisnik pri tome dobiva poruku da njegova izjava nije mogla biti objavljena zbog neprikladnog sadržaja.¹¹⁵ Privatni entiteti također zapošljavaju administratore koji uočavaju i potom brišu protupropisne komentar, pri čemu se korisnici također potiču da prijave takav sadržaj ako ga primijete prije administratora.¹¹⁶ Nadzor je povećan donošenjem zakona da se svi korisnici stranica za mikroblogiranje moraju registrirati pravim imenom i telefonskim brojem. Stranica Sina Weibo, koja broji više stotina milijuna korisnika i pretpostavlja se da 30% internetskih korisnika na svijetu ima izrađen račun,¹¹⁷ dodjeljuje svakom korisniku 80 bodova koje gubi kršenjem uvjeta. Ako korisnik izgubi sve bodove, njegov račun se trajno briše. Izgubljeni bodovi se mogu nadoknaditi ako u određenom periodu ne naprave nikakav prekršaj ili nekom promotivnom aktivnošću.¹¹⁸

Inozemni davatelji usluga se moraju prisiliti na autocenzuru ako žele dospjeti na kinesko tržište. Primjer je Apple koji je cenzurirao svoj glasovno navodeći sustav Siri i onemogućio mu da odgovara na pitanja vezana za masakr na trgu Tiananmen.¹¹⁹ U slučaju tvrtke TOM-Skype, kineske verzije Skype-a, mnoge poruke su presretane automatskim filterom, a poruke se čak i pohranjuju.¹²⁰ Google je jedna od kompanija koja je izrazito bila pogođena cenzorskim sustavom u Kini, stoga se 2010. povukla s kineskog tržišta, i počela preusmjeravati korisnike na necenzurirani pretraživač u Hong Kongu.¹²¹

Treća metoda kontrole sadržaja u Kini jest 'proaktivna manipulacija'. Ideja takve manipulacije je zauzimanje virtualnog prostora kao polja ideološke borbe. Kineska vlada to čini pomoću zaposlenih komentatora koji su plaćeni da objavljuju provladine komentare i uz to prijavljuju korisnike koji su suprotnog stajališta. Procjenjuje se da je u takvoj vrsti propagande zaposleno više stotina tisuća radnika.¹²² Tu se možemo osvrnuti i na sintagmu 'autoritarno oslobođenje' koju su skovali Baogang He i Mark Warren 2008. godine a vrlo je bliska sintagmi proaktivne manipulacije. Dok se smatra da bi nove tehnologije mogle donijeti oslobođenje kineskom narodu i pozvati ga na borbu, He i Warren svojim pojmom daju do

¹¹⁵ Zheng, H. Regulating the Internet: China's Law and Practice // Beijing Law Review 4, 1(2013). Str. 3.

¹¹⁶ Ibid.

¹¹⁷ Sina Weibo. // Wikipedia. URL: http://en.wikipedia.org/wiki/Sina_Weibo (30.8.2014.)

¹¹⁸ Enemies of the Internet : 2013 report. Reporters without borders, 2013. Str. 21. URL:

http://surveillance.rsf.org/en/wp-content/uploads/sites/2/2013/03/enemies-of-the-internet_2013.pdf (30.8.2014.)

¹¹⁹ Freedom on the Net 2013: A Global Assessment of Internet and Digital Media. Freedom House, 2013. Str. 199.

¹²⁰ Enemies of the Internet : 2013 report. Reporters without borders, 2013. Str. 21. URL:

http://surveillance.rsf.org/en/wp-content/uploads/sites/2/2013/03/enemies-of-the-internet_2013.pdf (30.8.2014.)

¹²¹ Freedom on the Net 2013: A Global Assessment of Internet and Digital Media. Freedom House, 2013. Str. 198-199.

¹²² Ibid., str. 199.

znanja da postoji mogućnost da se kroz nove tehnologije postigne suprotan, mračniji učinak, a to je da se autoritarni režim stabilizira time kroz konstantnu propagandu.¹²³

Unatoč crnim prognozama i statusu interneta u Kini, postoje i mnoge pozitivne strane umrežavanja kineskog naroda. „Unatoč tehničkom filtriranju, nametnutoj autocenzuri i manipulaciji, internet je primarni izvor novosti i foruma za raspravu, osobito za mlađu generaciju. Kineski *cyberspace* je prepun *online* aukcija, društvenih mrežam, kućnih video uradaka, velike populacijegamera, te srčanih rasprava o društvenim i političkim problemima. Isključivo političke organizacije, etničke manjine i progonjene vjerske grupe ostaju nezastupljene iako jesu koristili internet za diseminaciju zabranjenog sadržaja, te prekooceanski mediji i grupacije za ljudska prava potvrđuju da su slali pretplatnicima u Kini elektroničke poruke s vijestima, uputama za tehnologiju za probijanje cenzure ili kopije zabranjenih publikacija.“¹²⁴ Te informacije o saznanju da broj korisnika koji se opire cenzuri raste je obećavajuća.

7.2. Cenzura u zapadnim i razvijenim zemljama

Iako se uskraćena sloboda informacija povezuje sa zemljama koje nisu uspjele uspostaviti demokratsko društvo, određeni slučajevi u zapadnim zemljama pokazali su da razvijene zemlje nisu imune na kršenje prava na slobodan pristup informacijama. Ovo poglavlje će se baviti trima zemljama razvijenog svijeta – Francuskom, Australijom i SAD-om i recentnim događajima u navedenim zemljama koji su izazvali oštre kritike javnosti i aktivista. Iako je Freedom House u svom izvješću iz 2013. sve tri zemlje proglasio zemljama slobodnog interneta, Reporteri bez granica su ipak u svom izvješću iz iste godine Francusku i Australiju stavili u kategoriju zemalja pod nadzorom, tj. zemalja koje se služe zabrinjavajućim postupcima u ograničavanju pristupa određenim sadržajima bez obzira na objašnjenje, a koji djeluju intruzivno ili bi mogli imati drastičnije ili kobnije posljedice. Francuska i Australija su time dospjele u kategoriju zemalja u kojima se nalaze Egipat, Eritreja, Indija, Kazahstan, Malezija, Rusija, Južna Koreja, Šri Lanka, Tajland, Tunis, Turska i Ujedinjeni Arapski Emirati.¹²⁵

¹²³ MacKinnon, R. China's "Networked Authoritarianism" // Journal of Democracy 22, 2(2011). Str. 36.

¹²⁴ Freedom on the Net 2013: A Global Assessment of Internet and Digital Media. Freedom House, 2013. Str. 200.

¹²⁵ Internet Enemies Report 2012. Reporters Without Borders, 2012. Str. 40, str. 46. URL: http://en.rsf.org/IMG/pdf/rapport-internet2012_ang.pdf (30.8.2014.)

SAD je i prema izvješću Reportera bez granica slobodna zona barem što se tiče interneta, no nedavni incidenti koji su eskalirali ne idu u prilog zemlji koja se smatra primjerom demokratskog društava. Govorit će se o prvim spornim zakonima sa svrhom zaštite djece, te nedavnim prijedlozima uvođenja zakona u SAD-u koji su prema stavu aktivista prijetili slobodi pristupa informacijama u SAD-u, što bi na posljetku rezultiralo narušenom pristupu informacija na globalnoj razini.

7.2.1. Australija

U Australiji je omogućen brz, visokokvalitetan pristup internetu i drugim digitalnim medijima.¹²⁶ No, kao što je spomenuto, Reporteri bez granica upozoravaju na „spremnost vlade da stvori represivni sustav filtriranja interneta koji bi bio rukovođen na netransparentan način od vladinih agencija i temeljen na vrlo širokim kriterijima.“¹²⁷ Freedom House navodi nedavne prijedloge za uvođenje cenzure putem propisa davateljima internetskih usluga i iako trenutno ne postoji zakon, u zadnjih par godina pojavila se nekolicina prijedloga koji se tiču prikupljanja i zadržavanja podataka, nadzora i filtriranja.

2012. Australija se priključila Vijeću europske konvencije o *cyber*-kriminalu (Council of Europe Convention on Cybercrime). Konvencija nalaže da je ISP dužan nadzirati, presretati i zadržavati podatke kad mu je uručen nalog i samo u slučaju kriminalne istrage vezane uz određena područja navedena u Konvenciji, a to su dječja pornografija, intelektualno vlasništvo, *online* prijevare i krivotvorenje, te računalni prekršaji.¹²⁸ No, Australija je otišla i korak dalje i nije se ograničila samo na zločine navedene u konvenciji, već za bilo koji zločin koji se istražuje. Konvencija nalaže da ISP u slučaju istrage sačuva podatke o računalnim *logovima* maksimalno 90 dana, dok australsko zakonodavstvo nalaže 180 dana.

Od 2010. australska vlada je radila na tome da se cenzurira sav sadržaj označen oznakom RC (Refused Classification). Prema ACMA-i (Australian Communication and Media Authority) vlasnik „zabranjenog“ sadržaja će primiti obavijest o ukidanju stranice. ISP stranice je obaviješten od ACMA-e da sadrži ilegalan ili uvredljiv materijal i potom će stranica biti blokirana. Broadcasting Service Act propisuje koji su to sadržaji zabranjeni, a to su sadržaji koji su prema klasifikacijskom odboru zadobili oznake RC (Refused

¹²⁶ Freedom on the Net 2013: A Global Assessment of Internet and Digital Media. Freedom House, 2013. str. 75

¹²⁷ Internet Enemies Report 2012. Reporters Without Borders, 2012. Str. 41 URL: http://en.rsf.org/IMG/pdf/rapport-internet2012_ang.pdf (30.8.2014.)

¹²⁸ Freedom on the Net 2013: A Global Assessment of Internet and Digital Media. Freedom House, 2013. str 83-84

Classification), R18+, te MA15+. ¹²⁹ Problem je nastao kada su 2013. godine razotkriveni slučajevi blokiranja brojnih legalnih stranica koje nisu sadržavale ikakav ilegalan sadržaj, s vrlo nejasnim opravdanjem. Aktivisti tvrde da klasifikacija ilegalnog sadržaja nije dovoljno transparentna, da cilj zaštite djece nije opravdanje za cenzuriranje sadržaja koji je dopušten odraslim korisnicima, te je također problematično što ACMA ne obavještava korisnike kad je u procesu blokiranja stranice, niti vlasnici sadržaja imaju priliku za obranu sadržaja koji je klasificiran kao RC. ¹³⁰ Australijski ogranak nevladine organizacije Electronic Frontier Foundation zatražio je od vlade da bude jasnija kako URL-ovi i web stranice dopijevaju na crnu listu. ¹³¹

7.2.2. Francuska

Reporteri bez granica uvrstili su Francusku na popis zemalja Neprijatelji interneta, u skupinu zemalja pod nadzorom. Reporteristi ističu kako je vlada krenula u sasvim krivom smjeru svojim nedavnim zakonima o filtriranju interneta i odsijecanjem veze i onemogućavanju pristupa internetu, najčešće pod paskom zaštite intelektualnog vlasništva i sigurnosti. ¹³²

Prema Europskom sudu, „filtriranje interneta je prekršaj nad slobodom informacija“. ¹³³ Nadalje, filtriranje interneta je kršenje temeljnih prava europskih građana i prava na slobodan protok *online* informacija. Sud također tvrdi da su sve mjere koje nalažu nadzor protoka informacija protivne europskom zakonu i krše temeljna prava. ¹³⁴

Francuska je, unatoč tomu sve do nedavno prakticirala zakone koji su se ogriješili o izjavu suda a to su prijeporni zakoni HADOPI i LCEN. ¹³⁵ Iako je Freedom House klasificirao internet u Francuskoj kao slobodan, nekoliko ekscesa pokazuje zabrinjavajuće tendencije francuske vlade. Političari su u zadnjih par godina predlagali vrlo restriktivne mjere poput zatvaranja korisnika koji često posjećuju ekstremističke stranice ili kaznenog gonjenja Twittera zbog govora mržnje koji se učestalo objavljuje na njihovoj stranici. ¹³⁶ Predmeti

¹²⁹ Ibid., str. 79.

¹³⁰ Freedom on the Net 2013: A Global Assessment of Internet and Digital Media. Freedom House, 2013. Str.80.

¹³¹ Internet Enemies Report 2012. Reporters Without Borders, 2012. Str. 41. URL: http://en.rsf.org/IMG/pdf/rapport-internet2012_ang.pdf (30.8.2014.)

¹³² Ibid., str. 47

¹³³ Ibid., str. 48.

¹³⁴ Ibid.

¹³⁵ Freedom on the Net 2013: A Global Assessment of Internet and Digital Media. Freedom House, 2013. Str. 285.

¹³⁶ Ibid., str. 282.

cenzure ili potencijalne cenzure su najčešće vezani uz frekventne socijalne probleme u Francuskoj kao govor mržnje, kleveta, autorsko pravo, poricanje Holokausta, dječja pornografija.¹³⁷

Godine 2011. dodatak zakonu LCEN predlaže da različite vladine organizacije mogu prisiliti vlasnike sadržaja da ih uklone ili prisiliti ISP-a da blokira stranicu. Zakon navodi da bi se taj postupak mogao provoditi u slučaju kršenja zakona, radi očuvanja javnog reda, zaštite maloljetnika, javnog dobra, u interesu očuvanja nacionalne odbrane ili zaštite fizičkih osoba.¹³⁸ Taj zakon je odmah iskritiziran zbog nejasne i vrlo obuhvatne formulacije koja bi bila primjenjiva na gotovo sve web stranice, stoga je na kraju i odbijen 2013.¹³⁹ Google Transparency Report je objavio da su u periodu od siječnja do lipnja 2012. zahtjevi francuske vlade za odstranjenje sadržaja porasli za 128% u usporedbi s prethodnim šestomjesečnim periodom.¹⁴⁰ Francuska vlada je stoga kritizirana da je „Web 1.0“ vlada.¹⁴¹

7.2.2.1. Hadopi

U svrhu zaštite intelektualnog vlasništva na internetu, francuska vlada je 2009. godine uvela HADOPI zakon. Najkontroverznije je tako zvano *three strikes* pravilo koje onemogućava pristup internetu korisniku koji tri puta prekrši zakon o intelektualnom vlasništvu.¹⁴² Proces kažnjavanja slijedio je tri koraka.

1. Kad bi korisnik skinuo ilegalan sadržaj s interneta, dobio bi upozorenje elektroničkom poštom da je prekršaj počinjen.¹⁴³ Korisniku bi se pristupilo preko njegove IP adrese, te bi nakon prekršaja bilo zatraženo od ISP-a da nadzire korisnikovo spajanje na internet.¹⁴⁴
2. U slučaju da se korisnik u narednih šest mjeseci ogлуši na upozorenje te nastavi s ilegalnom aktivnošću, pismo upozorenja bi se potom slalo korisniku i korisnikovom ISP-u.¹⁴⁵

¹³⁷ Ibid., str. 287.

¹³⁸ Freedom on the Net 2013: A Global Assessment of Internet and Digital Media. Freedom House, 2013. Str. 286.

¹³⁹ Ibid.

¹⁴⁰ Ibid.

¹⁴¹ Ibid., str. 287.

¹⁴² Ibid., str. 290.

¹⁴³ Ibid.

¹⁴⁴ HADOPI law. // Wikipedia. URL: http://en.wikipedia.org/wiki/HADOPI_law (12.9.2014.)

¹⁴⁵ Freedom on the Net 2013: A Global Assessment of Internet and Digital Media. Freedom House, 2013. str. 290.

3. Ako bi korisnik u sljedećih godinu dana počinio i treći prekršaj, njegov bi slučaj bio proslijeđen javnom tužitelju, te bi korisnik bio kažnjen novčanom kaznom od 1500 € i uskraćivanjem pristupu internetu.¹⁴⁶

Upozoravajuća elektronička poruka u prvom koraku zaprimilo je 1,5 milijuna korisnika, fizičko pismo upozorenje pri počinjenom drugom koraku dobilo je 10000 korisnika, dok je u četrnaest slučajeva tužba dospjela javnom tužitelju, no samo su dva korisnika uistinu kažnjeno gonjena. Na kraju, pretplatnik je stavljen na crnu listu a drugim davateljima internetskih usluga je zabranjeno pružati im usluge.

Osnovna kritika HADOPI zakona je kršenje temeljnih prava pri uskraćivanju pristupa internetu, jer korisniku onemogućuje pristup informacijama, ne samo u svrhu učenja i obavijesti već i osobnih informacija koje je korisnik pohranio. HADOPI je stoga povučen kao zakon 2013. godine.

7.2.2.2. LCEN (Law for Trust in the Digital Economy)

LCEN je dekret kojim se određuje da nekolicina francuskih vladinih agencija ima mogućnost zahtijevati da se sadržaj koji smatraju štetnim ukloni s interneta. Kritično je što je cenzuru moglo zatražiti više ministarstava koji nemaju izravne veze s medijima i regulacijom interneta kao ministarstvo obrane, pravde, unutarnjih poslova, ekonomije, komunikacija, zdravlja, digitalne ekonomije, te ANSSI (L'Agence nationale de la sécurité des systèmes d'information).¹⁴⁷

Također je bilo naloženo da nekoliko kompanija, internetskih stranica i e-trgovina mora u periodu od dvije godine pohranjivati korisničke podatke kao brojeve telefona, podatke o transakcijama, povijest pretraživanja weba što znači da je time omogućena legalna ugradnja administrativnog sustava za filtriranje interneta. Neke od tih kompanija su eBay, Facebook, Google, Microsoft, Yahoo.¹⁴⁸

7.2.3. SAD

¹⁴⁶ Ibid.

¹⁴⁷ French Government Plans to Extend Internet Censorship. Open Net Initiative. 2011. URL: <https://opennet.net/blog/2011/06/french-government-plans-extend-internet-censorship> (30.8.2014.)

¹⁴⁸ Freedom on the Net 2013: A Global Assessment of Internet and Digital Media. Freedom House, 2013. Str. 292.

Spomenut će se nekoliko zakona i prijedloga koji su pokušali regulirati internet u SAD-u. Enciklopedija cenzure navodi tri zakona - The Communications Decency Act (CDA), The Child Online Protection Act (COPA) i Children's Internet Protection Act (CIPA),¹⁴⁹ sva tri su povećana zaštiti osjetljive skupine djece i maloljetnika od štetnog sadržaja, doneseni krajem 90-ih godina 20. st., za vrijeme predsjedništva Billa Clintona. No zakoni koji su ipak najkontroverzniji su nedavni prijedlozi zakona za zaštitu intelektualnog vlasništva, PIPA i SOPA koji će biti obrađeni u zasebnom poglavlju.

7.2.3.1.CDA, COPA i CIPA

Communications Decency Act (CDA) je dodatak zakonu o telekomunikacijama (Telecommunications Act) potpisan 1996. Njegova prvotna svrha je zaštita djece pod pretpostavkom da je internet sličan medij kao televizija i telefonija te da se može regulirati na sličan način, no da se cenzura može provoditi lakše nego na pisanoj riječi. Ipak, 1997. Vrhovni sud je presudio da CDA krši prvi amandman, te da se internet mora tretirati jednako kao i pisana riječ, stoga podilazi istim pravilima o slobodi govora.¹⁵⁰

Sljedeći zakon koji je donesen je COPA - Child Online Protection Act donešen 1998. u svrhu da nadopuni propuste prijašnjeg zakona CDA-a, te da zaštiti maloljetnike i djecu bez kršenja prvog amandmana i slobode govora,¹⁵¹ no presuda je bila da COPA nije uspjela popraviti nedostatke prijašnjeg zakona navodeći da COPA još uvijek nije isključivo konstruirana kako bi zaštitila maloljetnike a da svejedno krši prava odraslih korisnika. Termin 'štetno za maloljetnike', kako navodi enciklopedija, ne razlikuje spolni odgoj namijenjen desetogodišnjacima i ono što je primjereno šesnaestogodišnjacima, verifikacija identiteta za odrasle krši prvi amandman te mnogi drugi razlozi.¹⁵²

Sljedeći u nizu je CIPA - Children's Internet Protection Act, zakon koji je stupio na snagu 2000. godine. CIPA je nalažala, a po tome se i ovaj zakon razlikovao od prethodnog CDA-a i COPA-e, da se škole i knjižnice opreme tehnologijom koja će onemogućavati pristup pornografiji i ostalom sadržaju koji je štetan za maloljetnike, a u slučaju da to ne učine u zadanom roku prestali bi biti državno financirani.¹⁵³ U jednom apelu na zakon rečeno je da s obzirom na veličinu, brzinu rasta i arhitekturu interneta nije moguće s danim sredstvima

¹⁴⁹ Gren, J. Encyclopedia of Censorship. New York : Facts on File, Inc., 2005. Str. 282.

¹⁵⁰ Ibid.

¹⁵¹ Ibid.

¹⁵² Ibid., str. 283.

¹⁵³ Ibid., str. 284.

razviti sustav filtriranja koji dovoljno blokira kako bi zaštitio maloljetnike ali ne toliko da bi uskratio pristup odraslim korisnicima.¹⁵⁴ I ovaj posljednji zakon je kao i dva prethodna bio preispitan zbog određenih sudskih slučajeva jer je njime prekršen prvi amandman.

7.2.3.2. PIPA i SOPA

U SAD-u su bila predložena dva prijedloga zakona o regulaciji protoka ilegalnog sadržaja u svrhu zaštite autorskog prava. Godine 2011. predloženi su Protect IP Act (PIPA) i Stop Online Piracy Act (SOPA) usmjereni na web stranice izvan SAD-a koje su kršile američke zakone o autorskom pravu. Ti zakoni bi omogućili da ISP-i blokiraju pristup stranicama neadekvatnog sadržaja čak i ako bi stranice sadržavale istodobno legalan sadržaj. Predloženi od američkog Kongresa, prijedlozi su dobili potporu filmske i glazbene industrije jer je zakon „naoko cilja na mnoštvo inozemnih web stranica koje prodaju nelicencirana ili krivotvorena američka dobra potrošačima SAD-a izvan legalnog dosega...“¹⁵⁵

„Prijedlog zakona za promicanje napretka, kreativnosti, poduzetnosti i inovativnosti borbom protiv krađe vlasništva SAD-a, te za druge svrhe“¹⁵⁶ stoji u zaglavlju prijedloga zakona pod imenom SOPA. No, samo prijedlozi su izazvali žestoki otpor javnosti, od velikih kompanija do običnih korisnika interneta. Electronic Frontier Foundation je popisao niz točaka po kojima se prijedlozi smatraju neučinkovitim i opasnim.¹⁵⁷ Razlozi protivljenju su skupoća provedbe zakona (procijenjeno je da bi porezne obveznike provedba zakona stajala 47 milijuna dolara u 5 godina, privatni sektor i više puta isti iznos, a troškove bi najviše snosile tehnološke kompanije time gušeći razvoj), onemogućavanja slobode govora (stranice mogu biti ukinute s neke više instance pod izlikom kršenja zakona, a bez pravog pravnog procesa koji bi to i utvrdio), narušavanje infrastrukture interneta, neučinkovitosti zakona u sprečavanju piratstva.¹⁵⁸

Otpor je izazvao već prvi zakon PIPA, a SOPA je trebala biti unaprijeđena verzija prethodnog prijedloga, no „sedamdeset stranica nacrta je bilo gore, mnogo gore od PIPA-e, nudeći božićni popis legalnih mogućnosti i tehničkih sredstava za vlasnike prava i robnih žigova, od kojih niti jedan ne bi mogao učiniti mnogo da spriječi kršenje zakona čak i kad su

¹⁵⁴ Ibid.

¹⁵⁵ Downes, L. Who Really Stopped SOPA and Why? Forbes. 2012. URL:

<http://www.forbes.com/sites/larrydownes/2012/01/25/who-really-stopped-sopa-and-why/> (30.8.2014.)

¹⁵⁶ A BILL To promote prosperity, creativity, entrepreneurship, and innovation by combating the theft of U.S. property, and for other purposes. (SOPA Bill)

¹⁵⁷ What is SOPA? SOPA Blackout. URL: <http://sopablackout.org/learnmore/> (30.8.2014.)

¹⁵⁸ Ibid.

preispisali osnovna pravila digitalnog života.¹⁵⁹ SOPA bi time omogućila da državne i privatne stranke mogu prisiliti američke ISP-ove da preusmjere korisničke zahtjeve, pretraživače da uklone valjane poveznice te zahtijevati da se prekinu veze s 'ozloglašanim' stranicama.¹⁶⁰

Borba protiv prijedloga dosegla je neviđene razmjere, mnogi internetski portali su se zavili u crno u znak protesta, *online* peticija je brojala 10 milijuna potpisa, a članovi Kongresa su zaprimili 3 milijuna elektroničkih poruka i nepoznat broj telefonskih poziva. Zajedničko pismo Kongresu su poslale neke od najvećih tehnoloških kompanija kao Google, Yahoo, Facebook, Twitter, LinkedIn i eBay. Prijedlozi su konačno odbačeni 2013., čime je izvojevana najveća bitka za internet do sada.

7.3. Cenzurirano Arapsko proljeće

Arapsko proljeće je krenulo kao val prosvjeda nakon samospaljivanja Muhameda Bouazizija u prosincu 2010. u Tunisu. Uslijedili su protesti diljem zemlje unutar nekoliko sati nakon Bouazizijeve smrti, što je prerاسlo u revoluciju koja će zahvatiti šire područje Sjeverne Afrike i Bliskog Istoka, te se ta regija, vrlo brzo se našla u plamenu političke borbe. Egipat, Libija, Sirija, Tunis, Bahrein, Saudijska Arabija su se suočile s građanskim pobunama na ulicama protiv trenutne političke situacije. Ono što je zabilježeno, a što je od posebnog značaja za temu cenzure, je jačanje opće cenzure na cijelom tom području. Sada je poznato da tehnologija možda nije bila presudna (Morozov¹⁶¹ i Gladwell¹⁶² su se posebno osvrnuli na fenomen preuveličavanja uloge tehnologije u nedavnim revolucijama), no njihova uloga nije nebitna, što se retrogradno može interpretirati kroz političke mjere provedene da se uspori, onemogućući i suzbije organiziranje putem interneta.

Rasprave na internetu o prosvjedima, okupljanju i otporu, objavljivanje video snimaka nasilja vršenog nad prosvjednicima na YouTube-u dovelo je do toga da se arapska revolucija

¹⁵⁹ Downes, L. Who Really Stopped SOPA and Why? Forbes. 2012. URL: <http://www.forbes.com/sites/larrydownes/2012/01/25/who-really-stopped-sopa-and-why/> (30.8.2014.)

¹⁶⁰ Ibid.

¹⁶¹ Morozov, E. Facebook and Twitter are Just Places Revolutionaries Go. The Guardian. 2011. URL: <http://www.theguardian.com/commentisfree/2011/mar/07/facebook-twitter-revolutionaries-cyber-utopians> (30.8.2014.)

¹⁶² Gladwell, M. Small Change. The New Yorker. 2010. URL: <http://www.newyorker.com/magazine/2010/10/04/small-change-3?printable=true> (30.8.2014.)

počela nazivati „Twitter revolucijom“ i „Facebook revolucijom“. ¹⁶³ No, analizom događaja koji su doveli do proplamsaja borbe i daljnjeg razvitka događaja, utvrđeno je da bi se „arapska revolucija [...] najvjerojatnije dogodila i bez interneta.“ ¹⁶⁴ Ipak, ovdje ćemo dati kratki prikaz poteza navedenih vlada u cenzuri interneta.

Glavni problem koji se navodi jest da internetska komunikacija nije dostupna samo prosvjednicima, već i vladi i institucijama i pobornicima te vlade, a koji mogu raditi protiv pobunjenih pojedinaca i grupa. Problem postaje dublji kad se prisjetimo da je infrastruktura interneta najčešće u većinskom vlasništvu vlade koju prosvjednici žele srušiti ili promijeniti. ¹⁶⁵ Markus Sabadello navodi četiri mjere koje vlada može provesti *online* kao protuudar aktivistima: cenzura pojedinih stranica i servisa, gašenje cjelokupnog pristupa internetu, *online* propaganda režima, te identifikacija i uhođenje aktivista i simpatizera. ¹⁶⁶ Čak i prije revolucije 2010. i 2011. različite metode cenzure su bile primjenjivane u sjevernoafričkoj regiji: cenzura političkih stranica, nadzor, praćenje, filtriranje elektroničkih poruka itd. ¹⁶⁷ no s novim društvenim događajima situacija je postala mnogo drastičnija.

U Tunisu je internet dostupan od 1996. godine, što ga čini jednom od prvih zemalja u sjevernoafričkoj regiji koja je imala pristup. Na žalost već od samog početka, internet je bio podložan kontroli, te se smatra da su korisnici interneta u Tunisu zapravo bili pokusni kunići za globalnu industriju tehnologije za cenzuru i nadzor. ¹⁶⁸ Struktura interneta u Tunisu je planski građena, namjerno centralizirana sve s ciljom da se održi kontrola nad protokom informacija. ¹⁶⁹ Tijekom revolucije 2011. mnogi internetski servisi su cenzurirani kao YouTube, Wikileaks, stranice za ljudska prava, aktivistički blogovi, a najdalji korak je vlada poduzela krađom lozinki za račune na društvenim mrežama. Mnogi aktivistički bloggери su identificirani, vrlo često i zatočeni. ¹⁷⁰

¹⁶³ Sabadello, M. The Role of New Media for the Democratization Processes in the Arab World. Project Danube.2012. Str. 1. URL: <http://projectdanube.org/wp-content/uploads/2011/10/The-Role-of-New-Media-for-the-Democratization-Processes-in-the-Arab-World.pdf> (30.8.2014.)

¹⁶⁴ Ibid.

¹⁶⁵ Ibid., str. 4.

¹⁶⁶ Sabadello, M. The Role of New Media for the Democratization Processes in the Arab World. Project Danube, 2012. str. 6 URL: <http://projectdanube.org/wp-content/uploads/2011/10/The-Role-of-New-Media-for-the-Democratization-Processes-in-the-Arab-World.pdf> (30.8.2014.)

¹⁶⁷ After the Arab Spring: New Paths for Human Rights and the Internet in European Foreign Policy. Directorate-General for External Policies of the Union, 2012. Str. 5. URL: [http://www.europarl.europa.eu/RegData/etudes/note/join/2012/457102/EXPO-DROI_NT\(2012\)457102_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/note/join/2012/457102/EXPO-DROI_NT(2012)457102_EN.pdf) (30.8.2014.)

¹⁶⁸ Ibid., str. 5.

¹⁶⁹ Ibid., str. 9.

¹⁷⁰ Sabadello, M. The Role of New Media for the Democratization Processes in the Arab World. Project Danube. 2012. Str. 5. URL: <http://projectdanube.org/wp-content/uploads/2011/10/The-Role-of-New-Media-for-the-Democratization-Processes-in-the-Arab-World.pdf> (30.8.2014.)

Za razliku od Tunisa, egipatski internet nije bio u tolikoj mjeri cenzuriran, koliko se vlada fokusirala na opći nadzor i praćenje – kad bi neki od blogera ili novinara svojim djelovanjem ugrozio režim, bio bi uhićen, vrlo često i zatočen. Tehnologija za nadzor je izgrađena u suradnji s američkim partnerima.¹⁷¹ Tek je nakon prosvjeda 2011. vlada poduzela oštrije mjere cenzure koje su na kraju rezultirale možda najdrakonskijom mjerom do tada kad se radi o cenzuri interneta. Naime, egipatska vlada je naredila četirima velikom kompanijama koje kontroliraju internetsku vezu, da je u potpunosti prekinu, što je učinjeno u roku od 15 minuta¹⁷² Mnogi su pratili situaciju nakon isključenja Egipta iz internetske veze, spekulirajući koliko dugo bi taj potez egipatske vlade mogao trajati i koliko dugo će 80 milijuna korisnika biti odvojeno od globale komunikacijske mreže. „Ovo je sasvim drugačija situacija od skromne manipulacije internetom koja se odvijala u Tunisu, gdje su određene rute bile blokirane, ili u Iranu, gdje je internet bio ograničenog protoka kako bi internetske veze postale mučno usporene. Potez egipatske vlade večeras je u biti izbrisao svoju zemlju s karte svijeta.“¹⁷³ Potpuno gašenje interneta potrajalo je od 25. siječnja do 2. veljače 2011. Istodobno je bio onemogućen SMS servis.¹⁷⁴

Sirija se od svojih susjeda razlikuje po tome što je vrlo tehnološki nerazvijena, u usporedbi s Tunisom npr., te je potom ta vrlo loša komunikacijska veza dodatno usporena cenzurom i kontrolom. Sirija se uglavnom fokusirala na nadzor i praćenje potencijalno opasnih pojedinca, kao boraca za ljudska prava i političkih aktivista.¹⁷⁵ S vremenom, sirijska vlada je uložila dodatna sredstva za povećanje nadzora koristeći se tehnologijom iz Europske Unije (Italije, Francuske, Njemačke) i Sjeverne Amerike. Istraživanja koja su potvrdila prisutnost te tehnologije u Siriji izazvala su javnu osudu, stoga je Vijeće Europske Unije zabranilo izvoz opreme i softvera sa svrhom nadzora interneta i telefonske komunikacije.¹⁷⁶

¹⁷¹After the Arab Spring: New Paths for Human Rights and the Internet in European Foreign Policy. Directorate-General for External Policies of the Union, 2012. Str. 5. URL: [http://www.europarl.europa.eu/RegData/etudes/note/join/2012/457102/EXPO-DROI_NT\(2012\)457102_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/note/join/2012/457102/EXPO-DROI_NT(2012)457102_EN.pdf) (30.8.2014.), str. 9.

¹⁷²Ibid., str. 10.

¹⁷³Cowie, J. Egypt Leaves the Internet. Renesys. 2011. URL: <http://www.renesys.com/2011/01/egypt-leaves-the-internet/> (30.8.2014.)

¹⁷⁴Internet censorship in the Arab Spring. // Wikipedia. URL: http://en.wikipedia.org/wiki/Internet_censorship_in_the_Arab_Spring (30.8.2014.)

¹⁷⁵After the Arab Spring: New Paths for Human Rights and the Internet in European Foreign Policy. Directorate-General for External Policies of the Union, 2012. Str. 10. URL: [http://www.europarl.europa.eu/RegData/etudes/note/join/2012/457102/EXPO-DROI_NT\(2012\)457102_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/note/join/2012/457102/EXPO-DROI_NT(2012)457102_EN.pdf) (30.8.2014.)

¹⁷⁶Ibid., str. 11.

Od 2000. godine i početka vladavine predsjednika Bashar al-Assada pristup stranicama kao što su Facebook nije bio moguć, no 2011. pristup je ponovno omogućen.¹⁷⁷ Ta informacija je dočekana sa sumnjom. U zemlji u kojoj je potrebna identifikacija i otisak prsta da bi se kupila SIM kartica, korisnici interneta sumnjaju u dobre namjere svoje vlade, što potvrđuje izjava anonimne aktivistice: „Vlada je ponovno omogućila pristup internetu jer su shvatili da im je korisnije dopustiti aktivistima da komuniciraju na stranici i potom nas identificirati s njihovim timom lojalista koji pretražuju internet.“¹⁷⁸

Libija je još jedna zemlja koja se odlučila na krajnji potez isključivanja cjelokupnog interneta u kritičnom trenutku. Po uzoru na egipatski slučaj, u veljači 2011. serveri su isključeni, no pretpostavlja se da taj slučaj nije toliko drastičan kao u Egiptu s obzirom da je infrastruktura interneta u Libiji znatno slabija od one u Egiptu – samo 6% stanovništva ima pristup internetu od kuće, dok je u Egiptu ta brojka 24%. Ipak, tih 6% uglavnom čine najobrazovaniji, time i politički najsvjesniji građani.¹⁷⁹ Također, utvrđeno je da ipak cjelokupni internet nije ugašen, već je pristup nekim vladinim stranicama ostao dostupan.¹⁸⁰

Odjek arapske revolucije imao je utjecaj na režime drugih totalitarnih zemalja, naime kineska vlada je osjetila bojazan zbog mogućnosti širenja prosvjeda u Sjevernoj Africi jer su ti događaji izrazito podsjećali na prosvjed 1989. na trgu Tiananmen koji su pokrenuli studenti. Za vrijeme arapskog proljeća ili 'revolucije jasminka' kako se često u medijima navodilo, aktivisti su pozivali kineske građane na slične prosvjede¹⁸¹ što je rezultiralo cenzurom određenih pojmova na internetu, kao 'Egipat' i 'jasmin' jer su direktno upućivali na članke o političkom preokretu u arapskom svijetu.¹⁸² Neki članci navode kako je kineska vlada imala osobitih problema s cenzurom potonjeg pojma, jer je jasmin također ime kineske narodne pjesme, koju je, ironično, tadašnji glavni sekretar Partije Hu Jintao pjevao na putu u Afriku što je bilo zabilježeno u medijima i video snimkama, što su aktivisti iskoristili u borbi protiv

¹⁷⁷ Social Media: a double-edged sword in Syria. Reuters. 2011. URL: <http://www.reuters.com/article/2011/07/13/us-syria-social-media-idUSTRE76C3DB20110713>(30.8.2014.)

¹⁷⁸ Ibid.

¹⁷⁹ Internet censorship in the Arab Spring. // Wikipedia. URL: http://en.wikipedia.org/wiki/Internet_censorship_in_the_Arab_Spring (30.8.2014.)

¹⁸⁰ After the Arab Spring: New Paths for Human Rights and the Internet in European Foreign Policy. Directorate-General for External Policies of the Union, 2012. Str. 12. URL: [http://www.europarl.europa.eu/RegData/etudes/note/join/2012/457102/EXPO-DROI_NT\(2012\)457102_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/note/join/2012/457102/EXPO-DROI_NT(2012)457102_EN.pdf) (30.8.2014.)

¹⁸¹ Johnson, I. Calls for a 'Jasmine Revolution' in China Persist. The New York Times. 2011. URL: http://www.nytimes.com/2011/02/24/world/asia/24china.html?_r=0 (30.8.2014.)

¹⁸² Tong, B. Jasmine Revolution and Censorship in China. The East Asia Gazette. 2011. URL: <http://www.asia-gazette.com/news/china/2011/03/03/jasmine-revolution-and-censorship-china> (30.8.2014.)

cenzure objavljujući masovno tu snimku i dovodeći cenzore u dvojbu hoće li cenzurirati ili ne dvojbeni sadržaj.¹⁸³

8. Pristup internetu u Hrvatskoj i uloga knjižnica

Cenzura u Hrvatskoj u obliku koji postoji u Kini, Rusiji, Iranu, pa čak SAD-u ili Francuskoj ne postoji. Reporterima bez granica su u svom izvještaju o slobodi tiska smjestili Hrvatsku na 65. mjesto 2014. godine, što je napredak od prethodne godine kad se nalazila na 68. mjestu.¹⁸⁴ U članku 38. Ustava Republike Hrvatske navodi se zabrana cenzure i objavljuje sloboda govora: „Jamči se sloboda mišljenja i izražavanja misli. Sloboda izražavanja misli obuhvaća osobito slobodu tiska i drugih sredstava priopćavanja, slobodu govora i javnog nastupa i slobodno osnivanje svih ustanova javnog priopćavanja. Zabranjuje se cenzura. Novinari imaju pravo na slobodu izvještavanja i pristupa informaciji. Jamči se pravo na pristup informacijama koje posjeduju tijela javne vlasti. Ograničenja prava na pristup informacijama moraju biti razmjerna naravi potrebe za ograničenjem u svakom pojedinom slučaju te nužna u slobodnom i demokratskom društvu, a propisuju se zakonom.“¹⁸⁵ Unatoč tomu, zašto je Hrvatska smještena dosta nisko na ljestvici Reportera? Reporterima uglavnom izvještavaju o kršenju ljudskih prava pri fizičkom i pravnom maltretiranju novinara, kao što je bilo u slučaju Dušana Miljuša¹⁸⁶, Željka Peratovića¹⁸⁷ i ubojstva Ive Pukanića. „Cenzura je u Hrvatskoj formalno zabranjena (Ustav čl. 38). Zbog toga se u Hrvatskoj povremeno pribjegava rafiniranim i kompliciranim (teže uočljivim) oblicima kontroliranja medija i novinara.“¹⁸⁸

No nikakva istraživanja nisu provedena u slučaju cenzure na internetu i, barem naoko, čini se da se ta vrsta cenzure u Hrvatskoj ne provodi. Ustav dopušta provjeru sadržaja na internetu ali bez narušavanja prava na slobodan pristup informacijama. Centar za

¹⁸³ Johnson, I. Calls for a 'Jasmine Revolution' in China Persist. The New York Times. 2011. URL: http://www.nytimes.com/2011/02/24/world/asia/24china.html?_r=0 (30.8.2014.)

¹⁸⁴ World Press Freedom Index 2014. Reporters Without Borders. 2014. URL: <http://rsf.org/index2014/en-index2014.php#> (30.8.2014.)

¹⁸⁵ Ustav Republike Hrvatske. Wikisource. URL: http://hr.wikisource.org/wiki/Ustav_Republike_Hrvatske (30.8.2014.)

¹⁸⁶ Zagreb Daily's Crime Correspondent Beaten with Baseball Bat. Reporters Without Borders. 2008. URL: <http://en.rsf.org/croatia-zagreb-daily-s-crime-correspondent-03-06-2008,27290.html> (30.8.2014.)

¹⁸⁷ Judicial Harassment of Zeljko Peratovic Must Stop. Reporters Without Borders. 2010. URL: <http://en.rsf.org/croatia-judicial-harassment-of-zeljko-26-11-2010,38909.html> (30.8.2014.)

¹⁸⁸ Grčar, I. Dirigirano novinarstvo u Hrvatskoj. Zarez. 2013. URL: <http://www.zarez.hr/clanci/dirigirano-novinarstvo-u-hrvatskoj> (30.8.2014.)

informacijsku sigurnost stoga zaključuje da u Hrvatskoj ne postoje zakoni koji bi dopuštali filtriranje interneta jer je trenutačno nemoguće provoditi kvalitetnu provjeru sadržaja. Pristup internetu zakonski operateri mogu uskratiti poradi sigurnosti rada ili održavanja telekomunikacijske mreže, te zaštite podataka. Privatne mreže (kao CARNet) mogu ograničiti pristup prema pravilniku vlastitog poslovanja.¹⁸⁹

Stoga sve upućuje da je pristup internetu u Hrvatskoj neometan, neograničen i necenzuriran, što bi je svrstalo u jednu od rijetkih zemalja kojoj se cenzura ekonomski, politički i kulturalno trenutačno ne isplati, a u upravo u isplativosti možda leži razlog zašto hrvatski korisnici uživaju blagodati slobodnog interneta.

Jedno od najbitnijih mjesta osiguravanja javnog pristupa internetu u svim demokratskim državama, pa tako i u Hrvatskoj, je knjižnica. Knjižnica je konstantna točka kad se govori o slobodi govora i slobodi pristupu informacijama, dostupnost informacije je temelj njezinog postojanja i poslovanja. No na knjižničarima je i teška zadaća posredovanja između korisnika kojoj knjižnica stoji na raspolaganju i vanjskih pritisaka. Informacija koju korisnik dobiva putem interneta, jednako je vrijedna kao i informacija doseguta bilo kojim drugim medijem, stoga je IFLA prepoznala važnost pristupa internetu iz knjižnice kako bi se omogućio ravnopravno dostupan izvor znanja. *Manifest o internetu* nalaže slobodan pristup svima bez obzira na dob, rasu, nacionalnost, vjeru, kulturu, političko određenje, itd., te se pristup ne smije ograničavati ideološkom, političko ili vjerskom cenzurom. IFLA također upozorava na izvore koji su „netočni, izazivaju zabunu ili su čak uvredljivi,“ no podupire se slobodan protok informacija. Prema manifestu, cenzure ne bi trebalo biti, a izbjegavanje nepoćudnog sadržaja se može postići edukacijom korisnika i poticanjem na kvalitetne izvore.¹⁹⁰

Hrvatske knjižnice su rano počele uvoditi računala kao moguće sredstvo educiranja i informiranja što je bilo navedeno i u strategiji kulturnog razvitka Republike Hrvatske već sredinom 90-ih godina prošlog stoljeća. Gradska knjižnica u Rijeci je prva knjižnica koja je imala pristup internetu i omogućila ga korisnicima knjižnice, a knjižnica Medveščak (godine 2001.) je prva omogućila korištenje interneta svim građanima kroz projekt „Besplatni internet za sve“, bili oni članovi ili ne.¹⁹¹ „Hrvatske su knjižnice u 21. stoljeću, kao uostalom i sve svjetske knjižnice, mjesto gdje odrasli napreduju u pismenosti ili informatičkoj pismenosti,

¹⁸⁹ Cenzura na internetu. Centar za informacijsku sigurnost, 2011. Str. 17. URL: <http://www.cis.hr/files/dokumenti/CIS-DOC-2011-06-016.pdf> (30.8.2014.)

¹⁹⁰ IFLA-in manifest o internetu. IFLA. URL: <http://www.ifla.org/files/assets/faife/publications/policy-documents/internet-manifesto-hr.pdf> (9.9.2014.), str. 2

¹⁹¹ Matovina, J.; Pavlaković, S.; Srtičević, I. Besplatni Internet za sve : Internet u narodnoj knjižnici. // Vjesnik bibliotekara Hrvatske 45, 3/4(2002), str. 187.

mjesto gdje obitelji imaju pristup zdravstvenim i financijskim informacijama, gdje stanovnici mogu učiti o svom lokalnom i globalnom okruženju, gdje građani mogu naučiti kako doći do informacija o javnoj politici i stvarima koje se tiču zajednice, gdje starije osobe mogu naučiti kako da budu u kontaktu s djecom i unucima, mjesto gdje postoje mrežne službe i izvori.¹⁹²

Istraživanje iz 2012. godine u narodnim knjižnicama istočne Hrvatske, pokazalo je da 90% knjižnica omogućava pristup internetu korisnicima ili svim građanima, no trećina ih tu uslugu naplaćuje što se izravno kosi s postavkama IFLA-inog *Manifesta*. Ipak, korisnici su vrlo svjesni svog prava na besplatan pristup internetu, stoga se za njega zalažu čak i ako ga plaćaju u međuvremenu. To je osobito bitno za socijalno ugrožene skupine građana kojima pristup internetu može biti presudan u pokušaju nalaženja zaposlenja ili informiranju kako poboljšati svoju životnu situaciju. Možda najbolji od programa koji se provodi u knjižnicama, a koji je na tom tragu je program Knjižnica grada Zagreba *Knjigom do krova*, projekt s ciljem podrške beskućnicima u pokušaju da ih se aktivira i uključi u društvo i tržište rada. Projekt omogućuje informatičko opismenjavanje beskućnika, ali im u suradnji s drugim institucijama nudi i psihološku pomoć.¹⁹³

Mnoge knjižnice imaju već spomenute programe informacijskog opismenjavanja različitih društvenih skupina, npr. program Knjižnice grada Zagreba koje su se posvetile informatičkom educiranju osoba treće dobi,¹⁹⁴ a slične radionice provodi i gradska knjižnica Marka Marulića u Splitu,¹⁹⁵ dok je knjižnica u Rijeci na želju korisnika organizirala 'tehno info pult' za edukaciju o korištenju tablet računala gdje su knjižničari korisnike uglavnom treće dobi podučavali kako napraviti račune na Facebooku, Skypeu i nekim ostalim servisima.¹⁹⁶

No skupina korisnika kojoj knjižničari moraju pristupati s osobitom pažnjom su dakako djeca i mladi. S obzirom na znatiželju i revnost kojom djeca često prilaze mnogočemu, a s druge strane neiskustvo i bezazlenost koje ih čini ih ranjivima u konzumaciji informacija koje su možda nepodobne za njihovu dob, odgovornost knjižničara je velika jer je na njima da odluče koju od metoda će primijeniti za zaštitu najmlađih korisnika. Od 1991. Hrvatska je potpisnica Konvencije o pravima djece koja propisuje da svako dijete ima pravo

¹⁹²Sviben, Z. Mrežne službe i izvori za građane u narodnim knjižnicama. //Slobodan pristup informacijama u službi kulturnog razvitka / uredile Alemka Belan-Simić i Aleksandra Horvat. Zagreb : Hrvatsko knjižničarsko društvo, 2002. Str. 105.

¹⁹³Knjigom do krova. Knjižnice grada Zagreba. URL: <http://beskucnik.kgz.hr/> (9.9.2014.)

¹⁹⁴65 plus. Knjižnice grada Zagreba. URL: <http://www.kgz.hr/default.aspx?id=1296> (9.9.2014.)

¹⁹⁵Informatička radionica za umirovljenike. Gradska knjižnica Marka Marulića. URL: http://www.gkmm.hr/tecaj_informatike_za_umirovljenike.htm (9.9.2014.)

¹⁹⁶Tehno info pult u Narodnoj čitaonici. Gradska knjižnica Rijeka. 2013. URL: <http://gkr.hr/O-nama/Novosti/Tehno-info-pult-u-Narodnoj-citaonici> (9.9.2014.)

na pristup informacijama, no također propisuje da bude zaštićeno od štetnog sadržaja i materijala.¹⁹⁷ IFLA je 2007. izdala izjavu o internetu i knjižničnim uslugama za djecu u kojoj izjavljuje da se zalaže za zaštitu djece, ali se izrazito protivi cenzuri i filtriranju, no istodobno knjižnica treba zauzeti oštar stav o nepoćudnom sadržaju te informirati korisnike, osobito roditelje i staratelje najmlađih korisnika.¹⁹⁸ Iako istraživanja koja propituju korištenje filtara u hrvatskim narodnim knjižnicama nisu brojna, podatak iz već spomenutog istraživanja o internetu i računalima u narodnim knjižnicama istočne Hrvatske govori da postoje knjižnice koje filtriraju internet, i taj broj je činila čak trećina knjižnica koje su ispitane, unatoč tomu što je uzorak činio geografski ograničen i razmjerno mali broj knjižnica,¹⁹⁹ no to ukazuje da je odgovornost koju knjižničari osjećaju u zaštiti maloljetnika prevagnula nad smjericama IFLA-e.

¹⁹⁷Stričević, I. Slobodan pristup informacijama za djecu i mladež – granice odgovornosti. // Slobodan pristup informacijama u službi kulturnog razvitka / uredile Alemka Belan-Simić i Aleksandra Horvat. Zagreb : Hrvatsko knjižničarsko društvo, 2002. Str. 141.

¹⁹⁸Internet and Children's Library Services. IFLA. URL: <http://www.ifla.org/publications/internet-and-children-s-library-services> (9.9.2014.)

¹⁹⁹Internet i računala u narodnim knjižnicama: pilot istraživanje u Istočnoj Hrvatskoj. Knjižničarstvo, 2012. Str. 42. URL: http://www.knjiznicarstvo.com.hr/wpcontent/uploads/2013/06/208_Faletar_Lacovic_Cadovska_Horvat_2013_1.pdf (9.9.2014.)

9. Zaključak

Nakon cjelokupnog rada, općeg pregleda cenzure na internetu, popisa mnogobrojnih metoda provođenja cenzure, brojnih primjera provođenja cenzure te statistike koja nikako ne ide u prilog slobodi govora, štoviše upućuje na masovno kršenje temeljnih prava kao ljudskih bića i građana, globalna situacija izgleda poprilično mučno. Ipak, nema razloga za posustajanje, jer predanost kojom se informacije uskraćuju nije manja od predanosti korisnika i 'malih' ljudi u marljivom radu da se tih informacija dokopaju. „Sofisticiranost metoda koje koriste cenzori i obavještajne službe testiraju dovitljivost novih davatelja usluga i aktivista koji su im spremni pomoći. Ali budućnost slobode informacija ovisi o ishodima ove bitke. Ovo je bitka bez bombi, zatvorskih rešetki te praznih redaka u novinama...“²⁰⁰ Ovaj rad je pokušao dati uvid u povijest i sadašnjost cenzure na internetu, načine i razloge zbog kojih se provodi, te dajući primjer na nekim državama kao Kini, SAD-u, Francuskoj, Australiji i Hrvatskoj ili nekim nedavnim političkim odvijanjima kao Arapskom proljeću. Opsežnost informacija o ovoj temi mogu biti pripisani mnogim organizacijama koje rade na osvještavanju o problemu cenzure kao što su Reporteri bez granica, Open Net Initiative, Freedom House, IFLA i čije su publikacije neizbježne kao literatura na ovu temu, te određenim pojedincima koji konstantno i prodorno komentiraju trenutačne društvene prilike i njihov odnos prema slobodi govora, kao najznačajnijeg među mnogima navodim Evgenija Morozova.

Na niti jedan medij korisnici nisu polagali takvo pravo kao što polažu na internet, vjerojatno jer je svatko od njih dinamični i idejni sudionik u izgradnji globalne informacijske mreže. Stoga, najprirodnije se čini završiti rad citatom iz Deklaracije o nezavisnosti *cyberspacea*: „Mi nemamo izabranu vladu, niti je izgledno da ćemo je imati, tako da vam se obraćam ne s većim autoritetom od onog s kojim se sloboda sama uvijek obraća. Proglašavam globalni društveni prostor koji gradimo da bude prirodno neovisan od tiranija koju nam težite nametnuti. Nemate nikakvo moralno pravo vladati nad nama niti posjedujete ijednu metodu prisile koje bi smo se s razlogom trebali bojati.“²⁰¹

²⁰⁰Enemies of the Internet : 2013 report. Reporters without borders. 2013. Str. 5. URL: http://surveillance.rsf.org/en/wp-content/uploads/sites/2/2013/03/enemies-of-the-internet_2013.pdf (30.8.2014.)

²⁰¹Barlow, J.P. A Declaration of the Independence of Cyberspace. 1996. URL: <https://projects.eff.org/~barlow/Declaration-Final.html> (30.8.2014.)

Literatura

1. 65 plus. Knjižnice grada Zagreba. URL: <http://www.kgz.hr/default.aspx?id=1296> (9.9.2014.)
2. About Filtering. Open Net Initiative. URL: <https://opennet.net/about-filtering> (30.8.2014.)
3. After the Arab Spring : New Paths for Human Rights and the Internet in European Foreign Policy. Directorate-General for External Policies of the Union. 2012. URL: [http://www.europarl.europa.eu/RegData/etudes/note/join/2012/457102/EXPO-DROI_NT\(2012\)457102_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/note/join/2012/457102/EXPO-DROI_NT(2012)457102_EN.pdf) (30.8.2014.)
4. Badurina, B.; Dragija, M.; Golub, K. Akcija „Internet u knjižnice“ i „Knjižnice na Internet“ komisije za automatizaciju anketa o stupnju informatizacije narodnih knjižnica. // Vjesnik bibliotekara Hrvatske 43, 2(2000), str. 185-188.
5. Barlow, J. P. A Declaration of the Independence of Cyberspace. 1996. URL: <https://projects.eff.org/~barlow/Declaration-Final.html> (30.8.2014.)
6. Bitso, C. et al. Trends in Transition from Classical Censorship to Internet Censorship. IFLA, str. 4. URL: <http://www.ifla.org/publications/trends-in-transition-from-classical-censorship-to-intenet-censorship-selected-country-o> (30.8.2014.)
7. Cenzura na internetu. Centar za informacijsku sigurnost. 2011. URL: <http://www.cis.hr/files/dokumenti/CIS-DOC-2011-06-016.pdf> (30.8.2014.)
8. Cowie, J. Egypt Leaves the Internet. Renesys. 2011. URL: <http://www.renesity.com/2011/01/egypt-leaves-the-internet/> (30.8.2014.)
9. Defeat Internet Censorship : Overview of Advanced Technologies and Products. Global Internet Freedom Consortium. 2007. URL: http://www.internetfreedom.org/archive/Defeat_Internet_Censorship_White_Paper.pdf (30.8.2014.)
10. Deibert, R.; Rohozinski, R. Liberation vs. Control : the Future of Cyberspace. // Journal of Democracy 21, 4(2010).
11. DNS Filtering to Fight Internet Piracy Violates the First Amendment. Jurist. 2012. URL: <http://jurist.org/datetime/2012/01/lauren-mack-DNS-filtering.php> (30.8.2014.)
12. Downes, L. Who Really Stopped SOPA and Why? Forbes. 2012. URL: <http://www.forbes.com/sites/larrydownes/2012/01/25/who-really-stopped-sopa-and-why/> (30.8.2014.)

13. Enemies of the Internet : 2013 report. Reporters without borders. 2013. URL:
http://surveillance.rsf.org/en/wp-content/uploads/sites/2/2013/03/enemies-of-the-internet_2013.pdf (30.8.2014.)
14. Freedom on the Net 2013 : A Global Assessment of Internet and Digital Media. Freedom House, 2013.
15. French Government Plans to Extend Internet Censorship. Open Net Initiative. 2011. URL:
<https://opennet.net/blog/2011/06/french-government-plans-extend-internet-censorship> (30.8.2014.)
16. Gladwell, M. Small Change. The New Yorker. 2010. URL:
<http://www.newyorker.com/magazine/2010/10/04/small-change-3?printable=true> (30.8.2014.)
17. Golden Shield Project. // Wikipedia. URL:
http://en.wikipedia.org/wiki/Golden_Shield_Project (30.8.2014.)
18. Grčar, I. Dirigirano novinarstvo u Hrvatskoj. Zarez. 2013. URL:
<http://www.zarez.hr/clanci/dirigirano-novinarstvo-u-hrvatskoj> (30.8.2014.)
19. Gren, J. Encyclopedia of Censorship New York: Facts on File, Inc., 2005. str. XVIII
20. Hrvatska enciklopedija URL: <http://www.enciklopedija.hr/> (30.8.2014.)
21. Hrvatski jezični portal URL: <http://hjp.novi-liber.hr/>
22. IFLA-in manifest o internetu. IFLA. URL:
<http://www.ifla.org/files/assets/faife/publications/policy-documents/internet-manifesto-hr.pdf> (9.9.2014.)
23. Informatička radionica za umirovljenike. Gradska knjižnica Marka Marulića. URL:
http://www.gkmm.hr/tecaj_informatike_za_umirovljenike.htm (9.9.2014.)
24. Internet and Children's Library Services. IFLA. URL:
<http://www.ifla.org/publications/internet-and-children-s-library-services> (9.9.2014.)
25. Internet censorship in the Arab Spring. // Wikipedia. URL:
http://en.wikipedia.org/wiki/Internet_censorship_in_the_Arab_Spring (30.8.2014.)
26. Internet Censorship. // Wikipedia. URL:
http://en.wikipedia.org/wiki/Internet_censorship#Non-technical_censorship (30.8.2014.)
27. Internet Enemies Report 2012. Reporters Without Borders, 2012. URL:
http://en.rsf.org/IMG/pdf/rapport-internet2012_ang.pdf (30.8.2014.)
28. Internet i računala u narodnim knjižnicama : pilot istraživanje u Istočnoj hrvatskoj. Knjižničarstvo. 2012. URL:

- http://www.knjiznicarstvo.com.hr/wpcontent/uploads/2013/06/208_Faletar_Lacovic_Cadovska_Horvat_2013_1.pdf (9.9.2014.)
29. Johnson, I. Calls for a 'Jasmine Revolution' in China Persist. *The New York Times*. 2011. URL: http://www.nytimes.com/2011/02/24/world/asia/24china.html?_r=0 (30.8.2014.)
 30. Jørgensen, R.F. *Internet and Freedom of Expression*. Raoul Wallenberg Institute, 2001. URL: <http://www.ifla.org/files/assets/faife/publications/ife03.pdf> (30.8.2014.)
 31. *Judicial Harassment of Zeljko Peratovic Must Stop*. Reporters Without Borders. 2010. URL: <http://en.rsf.org/croatia-judicial-harassment-of-zeljko-26-11-2010,38909.html> (30.8.2014.)
 32. *Knjigom do krova*. Knjižnica grada Zagreba. URL: <http://beskucnik.kgz.hr/> (9.9.2014.)
 33. Leberknight, C. S. *A Taxonomy of Internet Censorship and Anti-Censorship*. Princeton University, 2010.
 34. MacKinnon, R. China's "Networked Authoritarianism" // *Journal of Democracy* 22, 2(2011).
 35. Matovina, J.; Pavlaković, S.; Srtičević, I. *Besplatni Internet za sve : Internet u narodnoj knjižnici*. // *Vjesnik bibliotekara Hrvatske* 45, 3/4(2002), str. 184-194.
 36. Milton, J. *Areopagitika i drugi spisi o građanskim slobodama*. Beograd : Filip Višnjić, 1990.
 37. Morozov, E. Facebook and Twitter are Just Places Revolutionaries Go. *The Guardian*. 2011. URL: <http://www.theguardian.com/commentisfree/2011/mar/07/facebook-twitter-revolutionaries-cyber-utopians> (30.8.2014.)
 38. Morozov, E. *Political Repression 2.0*. *The New York Times*. 2011. URL: <http://www.nytimes.com/2011/09/02/opinion/political-repression-2-0.html> (30.8.2014.)
 39. Morozov, E. *The Internet: A room of our own?* // *Dissent* 56, 3(2009).
 40. Morozov, E. *The Net Delusion: The Dark Side of Internet Freedom*. New York: Public Affairs, 2011.
 41. Morozov, E. *Whither Internet Control?* // *Journal of Democracy* 22, 2(2011).
 42. *Opća deklaracija o ljudskim pravima*. *Narodne novine*. 2009. URL: http://narodne-novine.nn.hr/clanci/medunarodni/2009_11_12_143.html (9.9.2014.)
 43. Ross, A. *Internet Freedom: Historic Roots and the Road Forward*. // *SAIS Review of International Affairs* 30, 2(2010).
 44. Sabadello, M. *The Role of New Media for the Democratization Processes in the Arab World*. Project Danube. 2012. URL: <http://projectdanube.org/wp->

content/uploads/2011/10/The-Role-of-New-Media-for-the-Democratization-Processes-in-the-Arab-World.pdf (30.8.2014.)

45. Sina Weibo. // Wikipedia. URL: http://en.wikipedia.org/wiki/Sina_Weibo (30.8.2014.)
46. Social Media: a double-edged sword in Syria. Reuters. 2011. URL: <http://www.reuters.com/article/2011/07/13/us-syria-social-media-idUSTRE76C3DB20110713>(30.8.2014.)
47. Stipčević, A. Sudbina knjige. Lokve: Naklada Benja, 2000.
48. Stričević, I. Slobodan pristup informacijama za djecu i mladež – granice odgovornosti. // Slobodan pristup informacijama u službi kulturnog razvitka / uredile Alemka Belan-Simić i Aleksandra Horvat. Zagreb : Hrvatsko knjižničarsko društvo, 2002. Str. 141-155.
49. Sviben, Z. Mrežne službe i izvori za građane u narodnim knjižnicama. //Slobodan pristup informacijama u službi kulturnog razvitka / uredile Alemka Belan-Simić i Aleksandra Horvat. Zagreb : Hrvatsko knjižničarsko društvo, 2002. Str. 96-106.
50. Što je Proxy poslužitelj? Windows Microsoft. URL: <http://windows.microsoft.com/hr-hr/windows-vista/what-is-a-proxy-server> (9.9.2014.)
51. Tehno info pult u Narodnoj čitaonici. Gradska knjižnica Rijeka, 2013. URL: <http://gkr.hr/O-nama/Novosti/Tehno-info-pult-u-Narodnoj-citaonici> (9.9.2014.)
52. Tong, B. Jasmine Revolution and Censorship in China. The East Asia Gazette. 2011. URL: <http://www.asia-gazette.com/news/china/2011/03/03/jasmine-revolution-and-censorship-china> (30.8.2014.)
53. Ustav Republike Hrvatske. Wikisource. URL: http://hr.wikisource.org/wiki/Ustav_Republike_Hrvatske (30.8.2014.)
54. What is SOPA? SOPA Blackout. URL: <http://sopablackout.org/learnmore/> (30.8.2014.)
55. World Press Freedom Index 2014. Reporters Without Borders. 2014. URL: <http://rsf.org/index2014/en-index2014.php#> (30.8.2014.)
56. Zagreb Daily's Crime Correspondent Beaten with Baseball Bat. Reporters Without Borders. 2008. URL: <http://en.rsf.org/croatia-zagreb-daily-s-crime-correspondent-03-06-2008,27290.html> (30.8.2014.)
57. Zheng, H. Regulating the Internet: China's Law and Practice // Beijing Law Review 4, 1(2013).
58. Zukerman, E. Intermediary Censorship // Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace. MIT Press, 2010.

CENZURA NA INTERNETU

SAŽETAK

Internet je trenutačno najrasprostanjeniji medij, sredstvo komunikacije koje dostupnošću i jednostavnošću sve više zauzima revolucionarnu ulogu u društvu, sličnu onoj koju je imao tiskarski stroj pet stoljeća ranije. I kao i pet stoljeća ranije, brza diseminacija informacija omogućava nove načine usvajanja znanja i protoka ideja, i to na vrlo demokratičan i lako dostupan način, no kao i tada, mnogim autoritarnim državama ili institucijama osvještavanje građana i korisnika ugrožava stabilnost režima. Cilj ovog rada je bio definirati cenzuru na internetu, upozoriti na njezine negativne posljedice, pozvati na oprez u vrlo diskutabilnim situacijama cenzuriranja u svrhu zaštite, sigurnosti i borbe protiv kriminalnih aktivnosti i terorizma. Prezentirane su metode cenzure uz primjere provođenja istih u različitim zemljama svijeta.

Ključne riječi: internet, cenzura, informacija, sloboda govora, pristup

ABSTRACT

The Internet is currently the most prevailing medium in the world, mode of communication that by its accessibility and simplicity now takes a revolutionary part in society, similar to the one that printing press had five centuries ago. And as five centuries ago, fast dissemination of information democratically enables new ways of learning and flow of ideas, but also, for many authoritarian states or institutions enlightenment of citizens and users endangers the stability of regime. The intention of this paper was to define Internet censorship, point out the negative consequences and to forewarn about the disputable situations of censoring with pretext of protection, safety and fight against crime and terrorism. The paper also reviews different methods of Internet censorship with examples of implementation of the aforementioned in several world states.

Key words: Internet, censorship, information, free speech, access

Ana Perčinlić rođena je 1989. u Travniku. Nakon završene srednje škole u Zagrebu, upisuje studij komparativne književnosti i portugalskog jezika na Filozofskom fakultetu. Godine 2011. upisuje diplomski studij komparativne književnosti i informacijskih i komunikacijskih znanosti, smjer bibliotekarstvo. Paralelno uz studij na Filozofskom fakultetu, studira dramaturgiju na Akademiji dramske umjetnosti.