Sigurnosna mjera - zabrana pristupa internetu

Dražen Škrtić

Namen prispevka:
Prikaz pravnih okvira za izricanje sigurnosne mjere zabrane pristupa Internetu i načina provođenja sigurnosne mjere

Metodologija:
Deskriptivnom metodom obuhvaćene su odredbe Kaznenog zakona kojima su definirani okviri za izricanje sigurnosne mjere i provedbeni propis za izvršavanje sigurnosne mjere.

Ugotovitve:
Sigurnosna mjera zabrane pristupa Internetu uvedena je u Kazneni zakon prema uzoru na poredbeno pravo i izriče se počiniteljima koji kriminalnu aktivnost ostvaruju uporabom Interneta. Neubrojivoj osobi, koja je kazneno djelo počinila putem Interneta ako postoji opasnost da će zlouporabom Interneta ponovno počiniti kazneno djelo, može se izreći sigurnosna mjera zabrane pristupa Internetu u trajanju od šest mjeseci do dvije godine računajući od izvršnosti sudske odluke. O pravomoćno izrečenoj mjeri sud obavještava Hrvatsku agenciju za poštu i elektroničke komunikacije na čiji zahtjev operatori elektroničkih komunikacijskih usluga koji pružaju uslugu pristupa Internetu ili putem koje je moguć pristup Internetu obustavljaju pružanje usluge pristupa Internetu, raskidaju postojeći i provode zabranu sklapanja novog ugovora uključujući i unaprijed plaćene usluge s osobom kojoj je izrečena sigurnosna mjera za vrijeme trajanja izrečene sigurnosne mjere.

Omejitve/uporabnost raziskave:
Ograničenje predstavlja nedostatak izrečenih sigurnosnih mjera zabrane pristupa Internetu i praktičnog izvršenja te sigurnosne mjere.
Praktična uporabnost:
U preglednom članku daje se prikaz odredbi Kaznenog zakona, poredbenog prava i provedbenog propisa za izvršavanje izrečene sigurnosne mjere zabrane pristupa Internetu.

Izvirnost/pomembnost prispevka:
Predstavljene su odredbe Kaznenog zakona kojima su definirani pravni okviri za izricanje sigurnosne mjere zabrane pristupa Internetu

Ključne besede: Kazneni zakon, Internet, sigurnosne mjere

1 Uvod

Promjene zakonodavstva koje se odnosi na pravo na pristup Internetu, uvjetovane brzim razvojem informatičke tehnologije su dinamične. Istraživanjem zakonodavstava dvadeset država članica VE (Austrija, Azerbejdžan, Belgija, Češka, Estonija, Finska, Francuska, Njemačka, Irska, Italija, Litva, Nizozemska, Poljska, Portugal, Rumunjska, Rusija, Slovenija, Španjolska, Švicarska i Velika Britanija) koje je proveo Europski sud za ljudska prava utvrđeno je da je

pravo na pristup Internetu u teoriji zaštićeno ustavnim jamstvima koje se odnose na slobodu izražavanja i slobodu primanja ideja i informacije. Pravo na pristup Internetu smatra se inherentnim pravu na pristup informacijama i komunikacijama zaštićenog nacionalnim ustavima, a obuhvaća pravo za svakog pojedinca na sudjelovanje u informacijskom društvu i obvezu za države da svojim građanima jamči pristup Internetu.

Legislativna ograničenja uporabe i pristupa Internetu radi prevencije kriminaliteta i nacionalne sigurnosti koja obuhvaćaju cenzuru pristupa Internetu (website shut down by authorities), zabrane pristupa određenim uslugama na Internetu, blokiranja internet stranica određenog sadržaja, ograničenja anonimnog pristupa Internetu, ograničenja korištenja određenih programa (torrent) i uporaba računalnih programa radi blokiranja i filtriranja određene vrste sadržaja. Zabrana pristupa određenim uslugama na Internetu odnosno blokiranja internet stranica određenog sadržaja ne predstavlja potpunu zabranu pristupa Internetu već samo ograničenja pristupa Internetu.

U članku analiziramo međunarodne pravne okvire za izricanje zabrane pristupa Internetu, komparativno pravo, praksu Europskog suda za ljudska prava (ESLJP), odredbe Kaznenog zakona kojima je definirana sigurnosna mjera kao i provedbeni propis kojim je definiran način provedbe sigurnosne mjere.

2 Međunarodni pravni okviri

Direktiva Europskog parlamenta i Vijeća jedan je od međunarodnih pravnih izvora koji obvezuju države članice na propisivanje i provođenje učinkovitih mjera za blokiranje pristupa internet stranicama koje sadrže dječju pornografiju.

Direktiva Europskog parlamenta i Vijeća za borbu protiv spolnog iskorištavanja djece i dječje pornografije propisuje mjere protiv internet stranica koje sadrže ili raspačavaju dječju pornografiju i obvezuje države članice da poduzmu potrebne mjere kako bi se osiguralo brzo uklanjanje internet stranica koje sadrže ili šire dječju pornografiju na njihovom teritoriju i nastojanje da se osiguraju uklanjanje takvih stranica izvan svog teritorija. Države članice mogu poduzeti mjere kako bi blokirale pristup internet stranicama koje sadrže dječju pornografiju ili šire dječju pornografiju prema korisnicima Interneta unutar svog teritorija. Te mjere moraju biti provedene u transparentnim postupcima i pružiti odgovarajuća osiguranja, a osobito kako bi se osiguralo da su ograničenja nužna i razmjerna, te da su korisnici informirani o razlogu ograničenja. Mjere zaštite uključuju mogućnost sudske pomoći.[1]

3 Poredbeno pravo

U odnosu na ograničenja u slučajevima nezakonitog sadržaja na Internetu, europske zemlje usvojile su razne pristupe i zakonske mjere, u rasponu od suspenzije pojedinačnih prava pristupa Internetu, uklanjanja nezakonitih sadržaja ili blokiranje pristupa određenim internet stranicama. U većini europskih zemalja, zaštita prava maloljetnika i napori u borbi protiv seksualnog iskorištavanje maloljetnika, predstavljaju temelj odgovarajućih mjera ograničavanja

[1] Članak 25. DIRECTIVE 2011/92/EU OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL, of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA, Official Journal of the European Union L 335/1.

pristupa tim internet stranicama (Francuska, Njemačka, Švicarska i Velika Britanija). Kada je riječ o običnom kriminalitetu, mjere kojima se ograničava pristup su različite i manje restriktivne u šest zemalja (Austrija, Estonija, Finska, Italija, Litva i Nizozemska).[2]

Opseg ograničenja je različit, a razlika je uglavnom u skladu s prirodom počinjenog djela, odnosno između djela protiv prava intelektualnog vlasništva i drugih kaznenih djela. Prema izvještaju OESS-a pod nazivom "Sloboda izražavanja na Internetu: Studija o zakonskim propisima i praksi vezanih uz slobodu izražavanja, slobodan protok informacija i medijskog pluralizma na Internetu u zemljama sudionicama OSCE",[3] ne postoje opće zakonske odredbe o blokiranje pristupa Internetu u Austriji, Češkoj, Njemačkoj i Poljskoj. Pet zemalja (Estonija, Finska, Nizozemska, Rusija i Velika Britanija) nemaju zakonodavstvo kojim se osigurava za potpuna blokada bez obzira na vrstu kaznenog djela, ali su donesene konkretne zakonske odredbe kojima se dopušta blokiranje pristupa u slučaju određenih vrsta kaznenih djela. To uključuje dječju pornografiju, rasizam, govor mržnje, poticanje na terorizam i uvredu.[4]

U Rusiji potpuna zabrana pristupa Internetu nije moguća, ograničenja pristupa mogu se izreći pod saveznim zakonima o određenim osnovama, primjerice za zaštitu temelja ustavnog poretka, morala, zdravlja ili legitimnih prava i interesa drugih, ili u interesu nacionalne sigurnosti i obrane (Savezni zakon br. 149-FZ).[5]

U onim zemljama koje nemaju opće ili specifične zakonodavne okvire koji propisuje blokiranja internet stranice i/ili blokiranje pristupa, nalog za blokiranje može izdati sud ili se blokada može provesti na osnovu suglasnosti.[6]

Filtriranje sadržaja uporabom računalnih programa je manje invazivna odnosno nametljiva tehnika ograničenja pristupa internet stranicama. Prilikom pretrage Interneta uporabom tražilica

računalni program blokira ili filtrira određene sadržaje i uklanja određene rezultate pretraživanja iz indeksa pretrage.

Računalni program za filtriranje koristi se uglavnom u školama, knjižnicama i/ili Internet kafićima U većini slučajeva, ne postoje zakonski uvjeti za njihovo korištenje, ali zakoni nekih države članice, poput Bjelorusije, Hrvatske, Litve, Poljske i Turske, propisuju uporabu računalnih programa za filtriranje u akademskim ustanovama, bibliotekama i Internet kafićima. U drugima državama, poput Kanade, Češke, Mađarske i Norveške, korištenje računalnih programa za filtriranje je dobrovoljno i ne podliježe nikakvim zakonima ili zakonskim odredbama.[7]

---

[2] CASE OF YILDIRIM v. TURKEY *(Application no. 3111/10)* JUDGMENT, STRASBOURG, 18 December 2012 , FINAL 18/03/2013, točka 33.

[3] Freedom of Expression on the Internet, Study of legal provisions and practices related to freedom of expression,the free flow of information and media pluralism on the Internet in OSCE participating States, dostupno na http://www.osce.org/fom/80723 18.09.2013.

[4] CASE OF YILDIRIM v. TURKEY *(Application no. 3111/10)* JUDGMENT, STRASBOURG, 18 December 2012 , FINAL 18/03/2013, točka 34.

[5] Ibid. točka 35.

[6] Ibid. točka 36.

[7] Freedom of Expression on the Internet, Study of legal provisions and practices related to freedom of expression,the free flow of information and media pluralism on the Internet in OSCE participating States, str. 26, str. 180, dostupno na http://www.osce.org/fom/80723 18.09.2013.

U Hrvatskoj je, korištenje Interneta u školama, knjižnicama i Internet kafićima regulirano aktima koji moraju biti u skladu sa zakonom, a filteri se koriste za blokiranje nepoželjnih sadržaja. Računalni programi za filtriranje implementiraju ISP (davatelji usluga, operatori) kao što su Hrvatska Akademska i istraživačka mreža (CARNet), a mogu spriječiti prikaz internet stranica koje sadrže neprimjeren sadržaj na računalima u hrvatskim osnovnim i srednjim školama. U tom smislu, pristup se prati po temama kao što su droga, kockanje, nasilje, govor mržnje, hacking i internet stranice koje sadrže pornografiju i druge neprimjerene sadržaje. Motiv za ovaj pristup je prije svega zaštita djece.[8]

Mogućnost žalbe protiv mjera zabrane pristupa Internetu usko je povezana s općim jamstvima prava na informaciju i izražavanja mišljenja stavova. U Azerbejdžanu, Belgiji, Češkoj, Litvi, Španjolskoj i Velikoj Britaniji, nema posebne odredbe koje propisuju postupak podnošenja žalbe protiv odluka kojima se ograničava pristup internetskim stranicama. Navode se opće ustavne odredbe o slobodi izražavanja i informiranja ili u slučaju Velike Britanije, na mogućnost sudskog nadzora, ako korisnik može dokazati da ima dovoljan interes za pobijanje izrečenih mjera.[9]

4 Praksa europskog suda za ljudska prava

Europski sud za ljudska prava donio je prvu presudu o pravu na slobodan pristup Internetu u slučaju YILDIRIM v. TURKEY (Landmark European Court Decision). Sud zaključuje da je došlo do povrede članka 10. Konvencije. Okolnosti slučaja utvrđene su kako slijedi.

Podnositelj zahtjeva rođen 1983. godine i živi u Istambulu. Posjeduje i vodi web stranicu http://sites.google.com/a/ahmetyildirim.com.tr/academic/ na kojoj objavljuje svoj akademski rad i svoje stavove o raznim temama. Web stranica stvorena pomoću Google Sites - website creation and hosting service (http://sites.google.com/).

Dana 23. lipnja 2009 Denizli Prvostupanjski Kazneni sud , naredio je na temelju članka 8 (1) (b) Zakona br. 5651 o reguliranju internetskih publikacija i borbi protiv kaznenih djela na Internetu blokiranje http://sites.google.com/site/kemalizminkarinagrisi/benimhikayem/atatuerk-koessi/at internet stranice (u daljnjem tekstu "uvredljive internet stranice“), kao preventivnu mjeru u kontekstu kaznenog postupka protiv vlasnika internet stranice koji je optužen za vrijeđanje uspomena na Atatürka. Istog dana , na temelju članka 8 (3) Zakona br. 5651, kopija naloga za blokiranje dostavljena je Upravi telekomunikacija i informatičke tehnologije ("TIB") na izvršenje. Dana 24. lipnja 2009. godine, na zahtjev TIB , Denizli Prvostupanjski Kazneni sud promijenio je svoju naredbu od 23. lipnja 2009. godine i naložio blokadu svih pristupa Googleovim stranicama na temelju članka 8. Zakona br . 5651. TIB je naveo da je to jedini način da blokira uvredljive internet stranice, a obzirom da vlasnik stranice nije imao certifikat poslužitelja i da živi u inozemstvu. TIB je 24. lipnja 2009. godine blokirao pristup Google Sites i podnositelj zahtjeva nije bio u mogućnosti pristupiti vlastitoj internet stranici. Dana 01. srpnja 2009. godine podnio je zahtjev za deblokadu internet stranice. U zahtjevu je istakao da je redovito koristio internet stranice za objavljivanje svog akademskog rada i iznošenje mišljenja o raznim temama, a mjera zabrane pristupa provedena je prema internet stranicama koje nisu bile povezane s internet stranicom koja je blokirana zbog nezakonitog sadržaja. Tvrdio je da je radi blokade internet stranice s nezakonitim sadržajem trebalo izabrati metodu kojom bi bila

[8] Ibid. str. 174-175.
[9] CASE OF YILDIRIM v. TURKEY *(Application no. 3111/10)* JUDGMENT, STRASBOURG, 18 December 2012 , FINAL 18/03/2013., točka 37.

blokirana samo stranica s nezakonitim sadržajem, a kojom ne bi bile blokirane i ostale internet stranice i naveo primjer blokiranje URL-a internet stranice.

U prilogu svog zahtjeva, dostavio je sudu presliku upozorenja koje se pojavilo kada je pokušao pristupiti svojoj internet stranici (http://sites.google.com/a/ahmetyildirim.com.tr/academic/): "The Telecommunications and Information Technology Directorate has applied the order issued by the Denizli Criminal Court of First Instance on 24 June 2009 in respect of this website (sites.google.com) as a preventive measure."

Dana 13. srpnja 2009. godine Denizli Kazneni Sud odbio je zahtjev podnositelja, pozivajući se na preporuku TIB, koji smatra da je jedino sredstvo za blokiranje pristupa počiniteljevoj internet stranici u skladu s nalogom za blokiranje, bilo blokiranje pristupa stranicama http://sites.google.com, na kojoj je bio pohranjen sadržaj podnositelja prigovora. Podnositelj zahtjeva napisao je 25. travnja 2012. godine Sudu informaciju da je još uvijek nije u mogućnosti pristupiti svojoj internet stranici, iako, koliko je shvatio, kazneni postupak protiv vlasnika uvredljive internet stranice prekinut 25. ožujka 2011. godine zbog nemogućnost utvrđivanja identiteta i adrese optuženog, koji živi u inozemstvu.[10]

U odnosu na ograničenja prava na slobodu izražavanja, ograničenje će predstavljati kršenje članka 10., osim ako je "propisano zakonom", radi provedbe jednog ili više od legitimnih ciljeva navedenih u članku 10. stavak 2. Konvencije te da je "nužna u demokratskom društvu" za postizanje tih ciljeva. Sud na početku ponavlja da izraz "propisano zakonom" u smislu članka 10. stavka 2. zahtijeva prvo, da bi osporena mjera trebala imati neku osnovu u domaćem pravu, međutim, to se odnosi i na kvalitetu zakona u konkretnom pitanju, koja bi trebao biti dostupna dotičnoj osobi, koja mora biti u stanju sagledati njegove posljedicu, te da bi trebao biti u skladu s vladavinom prava. Prema utvrđenoj sudskoj praksi, pravilo je "predvidivo" ako je formulirano dovoljno jasno da svaki pojedinac - ako treba i uz odgovarajući savjet - regulira svoje ponašanje.[11]

U ovom predmetu Sud primjećuje da je blokiranje pristupa internetskim stranicama koja je predmet sudskog postupka imalo zakonsku osnovu u odredbama članka 8 (1) Zakona br. 5651. Odredba članka 8. (1) Zakona br. 5651 je također zadovoljava zahtjev dostupnosti i predvidljivosti, iako podnositelj zahtjeva tvrdi da bi to pitanje trebalo biti odgovoreno negativno jer je odredba neodređena.[12]

Sud dosljedno smatra da domaće pravo za ispunjavanje tog zahtjeva, mora pružiti mjeru pravne zaštite od proizvoljnog miješanja javnih vlasti u prava zajamčena Konvencijom. Prema tome, zakon mora navesti dovoljno jasno opseg takve diskrecije i način njene primjene.[13]

Sud također primjećuje da članak 8, stavak (3) i (4), Zakona br. 5651. daje široke ovlasti tijelima uprave (TIB) u provedbi blokiranja temeljem prvotno izdanog u odnosu na navedenu stranicu. Činjenično stanje predmeta pokazuju da je TIB mogao zatražiti proširenje opsega blokiranja iako nikakav postupak nije bio vođen protiv internet stranice ili domene i bez stvarne potrebe za uspostavu potpune blokade.[14]

[10] CASE OF YILDIRIM v. TURKEY *(Application no. 3111/10)* JUDGMENT, STRASBOURG, 18 December 2012 , FINAL 18/03/2013., točke 1.-14.
[11] Ibid. točka 57.
[12] Ibid. točka 58.
[13] Ibid. točka 59.
[14] Ibid. točka 63.

Kao što je navedeno, Sud smatra da takva ograničenja nisu nužno nespojiva s Konvencijom. Međutim, potreban pravni okvir osigurava djelotvornu kontrolu nad opsegom zabrane i djelotvorni sudski nadzor kako bi se spriječila bilo kakva zlouporabe vlasti. U tom smislu, sudska kontrola zakonitosti takve odluke, na temelju suprotstavljenih interesa i postizanja ravnoteže između njih, nezamisliva je bez okvira koji se zasnivanju preciznim i posebnim pravilima u vezi s primjenom preventivnih ograničenja slobode izražavanja. Sud primjećuje da je, kada Denizli Kazneni Prvostupanjski sud odlučio blokirati potpuni pristup Google Sites prema Zakonu br. 5651, i to samo na preporuku TIB, bez utvrđivanja da li se manje dalekosežna mjera mogla poduzeti radi blokiranja pristupa samo uvredljivim internet stranicama.[15]

Ipak, nema naznaka da je sud s obzirom na primjenu, nastojao sagledati različite interese, posebno procijeniti potrebu da se potpuno blokira pristup Google Sites. Prema mišljenju Suda, taj je nedostatak jednostavno posljedica izričaja članka 8. Zakona br. 5651, koja nije dao nikakvu obvezu domaćim sudovima ispitati je li potpuno blokiranje Google Sites potrebno, uzimajući u obzir kriterije koje je Sud utvrdio i koje primjenjuje na temelju članka 10. Konvencije. Takva obveza, međutim, proizlazi izravno iz Konvencije i sudske praksi institucija Konvencije. Pri donošenju svoje odluke, sud je jednostavno pronašao utvrđenim da je jedino sredstvo za blokiranje pristupa internet stranici počinitelja u skladu s nalogom, potpuno blokiranje pristupa Google Sites. Međutim, prema mišljenju Suda, trebalo je uzeti u obzir, između ostalih elemenata, činjenicu da je takva mjera, činjenjem nedostupnim velike količine informacija, znatno ograničava prava korisnika Interneta i imala je značajan kolateralni utjecaj.[16]

U svjetlu ovih razmatranja i preispitivanja primijenjenog zakonodavstva ovome predmetu, Sud zaključuje da odluka koja proizlazi iz primjene odredbi članka 8. Zakona br. 5651, ne zadovoljava zahtjev predvidljivosti u skladu s Konvencijom i ne dopušta podnositelju stupanj zaštite koji bi bio u skladu s vladavinom prava u demokratskom društvu. Nadalje, čini se da je odredba u izravnom sukobu sa stvarnom formulacijom članka 10. stavka 1. Konvencije, prema kojem su prava koja su navedena u tom članku osigurana "bez obzira na granice".[17]

Sud nadalje primjećuje da je mjera o kojoj je riječ proizvodi proizvoljne učinke i ne može se reći da je bila usmjerena isključivo na blokiranje pristupa uvredljivoj internet stranici, budući da se sastoji u blokiranju pristupa svim stranicama Google Sites. Nadalje, nadzor sudskih postupaka koji se odnose na blokiranje internetskih stranica je nedovoljan da zadovolji kriterije za izbjegavanje zlouporabe jer domaći zakon ne predviđa bilo kakve zaštitne mjere kojima bi se osiguralo da se blokiranje određene stranice se ne koristi kao sredstvo za blokiranje pristupa u cjelini.[18]

Dakle, Sud zaključuje da je ograničenje na pristup izvoru informacija odnosno Internetu kompatibilan s Konvencijom: ako je zabrana definirana strogim zakonskim okvirom, ako zakonski okvir propisuje opseg zabrane, ako postoji jamstvo sudske kontrole.

Ovom presudom Europski sud za ljudska prava (ECHR) u presudi protiv potpunog blokiranja online sadržaja ojačao je pravo pojedinca na pristup Internetu, tvrdeći da je Internet "sada postao jedno od glavnih sredstava za ostvarivanje prava na slobodu izražavanja i informiranja."

---

[15] CASE OF YILDIRIM v. TURKEY *(Application no. 3111/10)* JUDGMENT, STRASBOURG, 18 December 2012 , FINAL 18/03/2013. točka 64.
[16] Ibid. točka 66.
[17] Ibid. točka 67.
[18] Ibid. točka 68.

5 Sigurnosna mjera zabrane pristupa internetu

Kazneni zakon reformirao je sustav sigurnosnih mjera, izbacivanjem sigurnosnih mjera koje su definirane drugim zakonima i sigurnosnih mjera koje su u Kaznenom zakonu propisane kao kaznenopravne mjere *sui generis* ali i propisivanjem novih sigurnosnih mjera. Svrha sigurnosnih mjera je otklanjanje okolnosti koje omogućavaju ili poticajno djeluju na počinjenje novog kaznenog djela.[19] Potpuno nova odredba uvodi načelo razmjernosti u funkciji ograničenja primjene sigurnosnih mjera. Sigurnosna mjera mora biti u razmjeru s težinom počinjenog kaznenog djela i kaznenih djela koja se mogu očekivati, kao i sa stupnjem počiniteljeve opasnosti.[20]

Ukinute su sigurnosne mjere oduzimanje predmeta i protjerivanje stranaca. Sigurnosna mjera oduzimanja predmeta tretira se kao posebna kaznenopravna mjera.[21] Sigurnosna mjera protjerivanja stranca uređena je Zakonom o strancima.

Pored sigurnosnih mjera zabrane obavljanja određene dužnosti ili djelatnosti i zabrana upravljanja motornim vozilom uvode se pet novih sigurnosnih mjera sigurnosnog karaktera: zabrana približavanja, udaljenje iz zajedničkog kućanstva, zabrana pristupa Internetu i zaštitni nadzor po punom izvršenju kazne zatvora. Sigurnosne mjere terapeutskog karaktera, obvezno psihijatrijsko liječenje i obvezno liječenje od ovisnosti dopunjene su novom sigurnosnom mjerom obveznog psihosocijalnog tretmana.

Sigurnosna mjera zabrane pristupa Internetu specijalno je preventivnog karaktera i propisuje zabranu pristupa Internetu osuđeniku za kazneno djelo počinjeno uporabom Interneta, a uvedena je kako bi se osuđeniku onemogućilo ponovno počinjenje kaznenog djela uporabom Interneta.

Sigurnosna mjera zabrane pristupa Internetu, za razliku od legislativnih ograničenja uporabe i pristupa Internetu radi prevencije kriminaliteta i nacionalne sigurnosti koja obuhvaćaju cenzuru pristupa Internetu (website shut down by authorities), zabrane pristupa određenim uslugama na Internetu, blokiranja internet stranica određenog sadržaja, ograničenja anonimnog pristupa Internetu i ograničenja korištenja određenih programa, osuđeniku propisuje apsolutnu (potpunu) zabranu pristupa Internetu. Mjere ograničenja uporabe i pristupa Internetu usmjerene su na uskarćivanje dostupnosti sadržaja određene internet stranice potencijalno neodredivom broju korisnika i u tom segmentu ograničavaju im pristup svim sadržajima dostupnim na Internetu. Nauprot tome, sigurnosna mjera zabrane pristupa Internetu, osuđeniku, točno određenom pojedincu, uskraćuje pristup bilo kojoj informaciji objavljenoj na Internetu i izražavanja svojih pogleda i stavova na Internetu, dakle, prava na slobodu izražavanja i informiranja.

Za izricanje sigurnosne mjere moraju biti kumulativno ispunjena dva uvjeta: osuđenik mora biti osuđen za kazneno djelo počinjeno putem Interneta i mora postojati opasnost da će osuđenik ponovno počiniti kazneno djelo zlouporabom Interneta.

Odredbom nije određeno za koja se kaznena djela počinjena putem Interneta može izreći sigurnosna mjera zabrane pristupa Internetu. Ovako široka odredba primjenjiva je za sva kaznena djela počinjena uporabom Interneta. Odredbu bi ipak trebalo definirati na način da se propišu kaznena djela propisana kaznenim ili drugim zakonom, za koja je moguće izreći kaznu

[19] Članak 66. Kaznenog zakona.
[20] Članak 67. Kaznenog zakona
[21] Članak 79. Kaznenog zakona

kao što su kaznena djela vezana uz zlouporabu droga, kaznena djela povezana s spolnim iskorištavanjem djeteta, zdravljem ljudi, prostitucijom, kockanjem ili klađenjem, terorizmom ili barem glave kaznenog zakona u kojima su propisana kaznena djela kaznenopravne zaštite određenog pravnog dobra kao što su kaznena djela protiv spolnog zlostavljanja i iskorištavanja djeteta, kaznena djela protiv čovječnosti i ljudskog dostojanstva ili kaznena djela protiv zdravlja ljudi. Prva sigurnosna mjera zabrane pristupa Internetu izrečena je zbog opasnosti ponovnog počinjenja kaznenog djela vezanog uz terorizam.[22]

Isto tako nije određeno koji stupanj opasnosti mora postojati da bi se osuđeniku izrekla sigurnosna mjera zabrane pristupa Internetu. Vjerojatnost da će osuđenik ponovno počiniti isto ili drugo kazneno djelo zlouporabom Interneta mora se temeljiti na objektivnim i provjerljivim činjenicama određene razine koje ukazuju da će osuđenik ponovno počiniti istovrsno kazneno djelo ili drugo kazneno djelo zlouporabom Interneta. Stupanj opasnosti trebalo bi propisivati na razini postojanja dovoljno osnova za sumnju ili osnovane sumnje.

Izricanjem i provedbom sigurnosne mjere osuđeniku se zabranjuje bilo kakav pristup Internetu. Zabrana je apsolutna. Nije propisana mogućnost izricanja selektivne zabrane pristupa Internetu u opsegu koji će onemogućiti korištenja nekih servisa i pristup određenim sadržajima i istovremeno zabraniti pristup sadržajima i servisima koji omogućavaju ili poticajno djeluju na počinjenje novog kaznenog djela.

Ako ne postoje tehničke mogućnosti selektivnog razdvajanja pojedinih usluga pristupa Internetu od usluga internet TV ili nekog od oblika elektroničke komunikacije, osuđeniku za kazneno djelo počinjeno uporabom Interneta kojem je izrečena sigurnosna mjera, zabranjen je bilo kakav pristup Internetu, i ograničava mu se pravo na pristup informacijama jer mu onemogućuje mu pristup informativnim sadržajima na Internetu uključujući i internet TV (IPTV), pravo na komunikaciju odnosno elektroničku komunikaciju koja uključuje pisanu elektroničku komunikaciju (e-mail) i govornu elektroničku komunikaciju (VOIP), korištenje servisa elektroničke trgovine (e-Buy), komunikaciju s državnim tijelima (i drugim javnopravnim tijelima) u svrhu dostavljanja podnesaka odnosno primanja pismena i internet bankarstvo.

Izricanjem sigurnosne mjere zabrane pristupa Internetu postiže se svrha njenog izricanja, osuđeniku je zabranjen pristup Internetu i time je eliminirana opasnost da će zlouporabom Interneta ponovno počiniti kazneno djelo, ali mu je zabranjen i pristup sadržajima i servisima koji su dostupni na Internetu, a pristup kojima ne predstavlja opasnost da će osuđenik zlouporabom Interneta ponovno počiniti kazneno djelo.

Osuđeniku koji ne izvršava sigurnosnu mjeru zabrane pristupa Internetu sudac izvršenja može ukinuti uvjetnu osudu i odrediti izvršenje izrečene kazne[23] ili zamjenu rada za opće dobro prvotno izrečenom kaznom,[24] ili opozivanje uvjetnog otpusta.[25]

---

[22] "Komandir Šamil" iz Trogira pušten na slobodu - ne smije koristiti Internet. Splitska je policija u nedjelju kasno navečer uhitila osobu koja je sebe nazvala Komandir Šamil. On je u osmominutnom videozapisu preko YouTubea pozvao takozvane članove otpora na nove eksplozivne napade u Zagrebu. ... U govoru, u kojem posebno ističe kako treba izbjeći civilne žrtve, "Komandir Šamil" kaže: "Drugovi i drugarice, pozdrav! Obraćam se članovima grupe povodom akcija pokreta otpora noćas i prije dva dana u rajonu Zagreba. Ključno je da se pri napadu na neprijateljske ciljeve izbjegnu civilne žrtve. ..... Nužno je da se vrše napadi na kasarne, policijske stanice i pogotovo baze specijalne policije, kao najljućih pasa kerbera vladajuće kaste u Zagrebu .... " http://www.slobodnadalmacija.hr/Crna-kronika/tabid/70/articleType/ArticleView/articleId/199441/Default.aspx dostupno 04.06.2013. (Slobodna dalmacija, objavljeno 15. siječnja 2013. godine).

[23] Članak 58. stavak 5. Kaznenog zakona

[24] Članak 55. stavak 8. Kaznenog zakona

[25] Članak 61. stavak 3. Kaznenog zakona

Trajanje sigurnosne mjere je ograničeno. Osuđeniku za kazneno djelo počinjeno putem Interneta moguće je izreći sigurnosnu mjeru zabrane pristupa Internetu u trajanju od šest mjeseci do dvije godine, računajući od dana **izvršnosti** sudske odluke. Vrijeme provedeno u zatvoru, kaznionici ili ustanovi ne uračunava se u trajanje izrečene sigurnosne mjere. Dakle, trajanje sigurnosne mjere računa se, od dana izvršnosti za osuđenike osuđena na novčanu kaznenu i kojima je umjesto kazne zatvora izrečena novčana kazne ili je kazna zatvora odnosno novčana kazna zamijenjena radom za opće dobro ili uvjetnom osudom odnosno osuđeniku kojem je izrečena zatvorska kazna od dana otpuštanja osuđenika iz zatvora, kaznionice ili ustanove.

Uvođenje sigurnosne mjere potpune odnosno apsolutne zabrane pristupa Internetu predstavlja krajnju mjeru ograničenja pristupa Internetu sa svrhom sprečavanja osuđenika u ponovnom počinjenju kaznenog djela zlouporabom Interneta. Kod izricanje sigurnosne mjere zabrane pristupa Internetu trebalo bi posebno voditi računa o načelu razmjernosti kako u pogledu odluke o izricanju sigurnosne mjere tako i u pogledu njena trajanja.

Prema stajalištu Suda ograničenja prava na slobodu izražavanja će predstavljati kršenje članka 10., osim ako je "propisano zakonom", radi provedbe jednog ili više od legitimnih ciljeva navedenih u članku 10. stavak 2. Konvencije te da je "nužna u demokratskom društvu" za postizanje tih ciljeva. Zakonska odredba kojom je propisana sigurnosna mjera zadovoljava uvjet Konvencije da ograničenje prava na slobodu izražavanja i informiranja bude propisana zakonom. No pitanje da li je ta mjera nužna u demokratskom društvu. Izricanjem te mjere, osuđeniku radi prevencije recidiva, ne ograničava se, nego u potponosti uskračuje (zabranjuje) pravo na slobodu izražavanja i informiranja na Internetu da bi ga se spriječilo u pristupu bilo kojem sadržaju na Internetu koji je „sada postao jedno od glavnih sredstava za ostvarivanje prava na slobodu izražavanja i informiranja“, koji sadržaji omogućavaju ili poticajno djeluju na počinjenje novog kaznenog djela.

Potpuna, apsolutna zabrana pristupa Internetu (Blanket Internet Access Ban) ne zadovoljava zahtjev da „zakonski okvir propisuje opseg zabrane“, jer se opseg zabrane u uvjetima apsolutne zabrane ne može definirati.[26]

Odredbu sigurnosne mjere zabrane pristupa Internetu, treba preispitati u svjetlu presude u slučaju YILDIRIM v. TURKEY i uskladiti je sa stajalištem Europskog suda za ljudska prava u pogledu strogog zakonskog okvira i nužnosti u demokratskom društvu.

6 Izvršenje sudske odluke

Sud će o pravomoćno izrečenoj mjeri obavijestiti regulatorno tijelo nadležno za elektroničke komunikacije koje će osigurati njeno provođenje. Sukladno Zakonu o elektroničkim komunikacijama[27] regulatorno tijelo za provođenje sigurnosne mjere je Hrvatska agencija za poštu i elektroničke komunikacije. Međutim, ukoliko je osuđeniku izrečena zatvorska kazna, regulatorno tijelo bi trebalo biti izvješteno i o izvršnosti sudske odluke kao i o vremenu koje je osuđenik proveo u zatvoru. Pravomoćnost i izvršnost sudske odluke se ne moraju poklapati, obzirom da vrijeme izlaska iz zatvora ne mora biti određeno vremenskim trajanjem zatvorske

[26] U presudi YILDIRIM v. TURKEY Europski sud blokiranje jedne domene na internetu definira kao poptupunu zabranu prisupa internetu (Blanket Internet Access Ban). Poptpuna zabrana pristupa internetu ne ne definira zabranu jednoj od neodredivog broja domena na internetu već svim postojećim domenama i domenama koje će naknadno biti dostupne ne internetu.

[27] Zakon o elektroničkim komunikacijama, NN 73/08, 90/11 i 133/12.

kazne, a vrijeme provedeno u zatvoru, kaznionici ili ustanovi se ne uračunava u trajanje sigurnosne mjere.

Pravilnikom o izvršavanju sigurnosne mjere zabrane pristupa Internetu propisuje se način na koji Hrvatska agencija za poštu i elektroničke komunikacije provodi sigurnosnu mjeru zabrane pristupa Internetu, te obveze operatora elektroničkih komunikacijskih usluga koji pružaju uslugu pristupa Internetu.[28]

Odmah po zaprimanju pravomoćne i izvršne sudske odluke, kojom je počinitelju izrečena sigurnosna mjera zabrane pristupa Internetu, Agencija će o izrečenoj sigurnosnoj mjeri obavijestiti sve operatore te im narediti obustavu pružanja usluge pristupa Internetu, kao i zabranu sklapanja novoga pretplatničkog ugovora za tu uslugu, za vrijeme trajanja izrečene sigurnosne mjere.[29]

Operator koji je s počiniteljem sklopio ugovor za samostalnu uslugu pristupa Internetu, ili bilo koju drugu elektroničku komunikacijsku uslugu koja uključuje uslugu pristupa Internetu, ili putem koje je moguć pristup Internetu, neovisno o načinu pristupa, mora odmah po zaprimanju obavijesti Agencije o izrečenoj sigurnosnoj mjeri obustaviti pružanje te usluge počinitelju.

Operator će u roku od 24 sata od provedene obustave pružanja usluge obavijestiti počinitelja o razlozima zbog kojih mu je obustavljena usluga pristupa Internetu.[30]

Operator koji je s počiniteljem sklopio ugovor za samostalnu uslugu pristupa Internetu, ili bilo koju drugu, neovisno o načinu pristupa, mora raskinuti pretplatnički ugovor s počiniteljem u roku od tri dana od dana zaprimanja obavijesti o izrečenoj sigurnosnoj mjeri.

Ako je pretplatnički ugovor sklopljen s minimalnim obveznim razdobljem trajanja ugovora, operator ima pravo od počinitelja tražiti isplatu mjesečne naknade za ostatak razdoblja obveznog trajanja ugovora, ili naknadu u visini popusta na proizvode i usluge koje je počinitelj ostvario, ako je plaćanje te naknade povoljnije za počinitelja.[31]

Obveza obustave pružanja usluge pristupa Internetu i raskida pretplatničkog ugovora jednako se primjenjuje i na korisnike unaprijed plaćenih usluga.[32]

Izvršenje izrečene sigurnosne mjere svodi se dakle, na zabranu sklapanja pretplatničkog ugovora ili ugovora o unaprijed plaćenim uslugama samostalnog pristupa Internetu ili usluge putem koje je moguć pristup Internetu.

Učinak izricanja sigurnosne mjere zabrane pristupa Internetu iscrpljuje su dakle u zabrani sklapanja pretplatničkog ugovora ili unaprijed plaćene elektroničke komunikacijske usluge ili raskidanju postojećih ugovora za osuđenika kojem je mjera izrečena. Provedbeni propis, pravilnik derogira primanu namjeru zakonodavca da se osuđeniku kojem je izrečena sigurnosna mjera, apsolutno zabrani svaki pristup Internetu i svodi je na puku zabranu sklapanja pretplatničkog ugovora ili unaprijed plaćene usluge s davateljem elektroničkih komunikacija pristupa Internetu komunikacijsku uslugu koja uključuje uslugu pristupa

[28] Članak 1. Pravilnika o izvršavanju zaštitne mjere zabrane pristupa internetu, NN 34/13.
[29] Članak 3. Pravilnika o izvršavanju zaštitne mjere zabrane pristupa internetu, NN 34/13.
[30] Članak 4. Pravilnika o izvršavanju zaštitne mjere zabrane pristupa internetu, NN 34/13.
[31] Članak 5. Pravilnika o izvršavanju zaštitne mjere zabrane pristupa internetu, NN 34/13.
[32] Članak 6. Pravilnika o izvršavanju zaštitne mjere zabrane pristupa internetu, NN 34/13.

Internetu ili usluge putem koje je moguć pristup Internetu. Dakle, osuđenik kojem je izrečena sigurnosna mjera i koja se provodi prema odredbama Pravilnika ne može sklopiti pretplatnički ugovor ili ugovor za korištenje unaprijed plaćene elektroničke komunikacijske usluge s operatorom i biti registrirani korisnik, ali može koristiti internetske usluge temeljem ugovora koji je sa operatorom sklopio član obitelji, njemu bliska osoba, anonimne unaprijed plaćene usluge elektroničkih komunikacija, pristup Internetu u javnim ustanovama (knjižnice), na radnom mjestu, ili korištenjem „*hot spot*“ bežične mreže.

7 Neizvršenje sudske odluke

Neizvršenje sudske odluke kojom je izrečena sigurnosna mjera zabrane pristupa Internetu, propisano je kao kazneno djelo *sui generis*.

Neizvršenje sudske odluke, prema odredbama Pravilnika, odnosi se na službenu ili odgovornu osobu, koja ne raskine postojeći pretplatnički ugovor ili ugovor o unaprijed plaćenim uslugama s osuđenikom kojem je izrečena sigurnosna mjera ili s osuđenikom kojem je izrečena sigurnosna mjera sklopi novi ugovor o pružanju usluga samostalnog pristupa Internetu ili usluge putem koje je moguć pristup Internetu. [33]

Iz odredbi Pravilnika proizlazi dužnost službene ili odgovorne osobe da raskine postojeći pretplatnički ugovor i o tome obavijesti osuđenika kojem je izrečena sigurnosna mjera. Osuđenik nije dužan raskinuti postojeći ugovor, ne može imati odlučujući utjecaj na raskidanje ugovora niti može biti odgovoran za neraskidanje postojećeg ugovora. Odgovornost leži na operatoru odnosno odgovornoj osobi operatora.

Međutim, pristup Internetu ne ostvaruje se samo sklapanjem pretplatničkog ugovora. Pristup Internetu proizlazi i iz obavljanja profesije ili službe. Naime, velik broj zatvorenih mreža elektroničkih komunikacija, pored ovlasti pristupa **Intranetu** uključuje i ovlast pristupa Internetu, na temelju jedinstvenog korisničkog računa i predstavlja jedan od načina na koji zaposlenik ili službenik, ostvaruje pravo pristupa elektroničkim komunikacijskim mrežama koje proizlazi iz pretplatničkog ugovora kojeg je s operatorom sklopila pravna osoba ili državno tijelo. Mogućnost pristupa Internetu, a koja se povezuje s obavljanjem posla ili vršenjem službe, također bi trebala biti ograničena izricanjem i provođenjem sigurnosne mjere zabrane pristupa Internetu. U tom slučaju administrator sustava, bi zaposleniku ili službenoj osobi ostavio mogućnost korištenja korisničkog računa pristupa **intranetu** ali ne i Internetu.

Odgovorna osoba operatora ne smije zaključiti pretplatnički ugovor s osuđenikom kojem je izrečena sigurnosna mjera zabrane pristupa Internetu. Prilikom odbijanja zahtjeva za sklapanjem ugovora, odgovorna osoba operatora dužna je o razlozima na primjeren način obavijestiti podnositelja zahtjeva kojem je izrečena sigurnosna mjera.

Dakle, za kršenje izrečene sigurnosne mjere zabrane pristupa Internetu neraskidanjem postojećeg pretplatničkog ugovora odgovara odgovorna osoba operatera, a za sklapanje pretplatničkog ugovora odgovaraju i odgovorna osoba operatera i osuđenik kojem je izrečena sigurnosna mjera.

[33] Članak 311. stavak 1. Kaznenog zakona.

Kazneno djelo neizvršenja sudske odluke čini i osuđenik kojemu je pravomoćnom presudom izrečena sigurnosna mjera, a koji uporabom identifikacijskih podataka druge osobe ili prikrivanjem identiteta sklopi pretplatnički ugovor s davateljem usluga pristupa Internetu.[34]

Ako osuđenik ne izvršava sigurnosnu mjeru zabrane pristupa Internetu i dođe do opoziva uvjetne osude i određivanja izvršenja izrečene kazne[35] ili zamjene rada za opće dobro prvotno izrečenom kaznom,[36] radi izbjegavanja dvostrukog kažnjavanja, osuđenik neće odgovarati za kršenje sigurnosne mjere koja mu je određena pravomoćnom presudom. U tom smislu, odredbe o kažnjavanju kršenja sigurnosne mjere su supsidijarnog karaktera u odnosu na odredbe o radu za opće dobro i opozivu uvjetne osude. Izričaj „nema kaznenog djela“ isključuje biće kaznenog djela.

8 Zaključak

Mjere cenzure pristupa Internetu (website shut down by authorities), zabrane pristupa određenim uslugama na Internetu, blokiranja internet stranica određenog sadržaja, ograničenja anonimnog pristupa Internetu, ograničenja korištenja određenih programa (torrent) i uporabe računalnih programa radi blokiranja i filtriranja određene vrste sadržaja internet stranica, neodredivom broju korisnika Interneta (pojedinaca) blokira pristup internet stranicama određenog sadržaja. Nasuprot tome sigurnosna mjera zabrane pristupa Internetu, osuđeniku kojem je izrečena, u potpunosti zabranjuje pristup Internetu.

Apsolutna zabrana pristupa Internetu derogirana je podzakonskim propisom (pravilnikom) i stvarnu zabranu pristupa Internetu svodi na zabranu sklapanja pretplatničkog ugovora i registrane unaprijed plaćene elektroničke komunikacijske usluge koja uključuje uslugu pristupa Internetu, ili putem koje je moguć pristup Internetu odnosno raskidanja postojećeg ugovora. Dakle, apsolutna zabrana pristupa kao jednom od glavnih sredstava za ostvarivanje prava na slobodu izražavanja i informiranja, ograničena je podzakonskim propisom. Time nije zadovoljen jedan od glavnih uvjeta članka 10. Konvencije, ograničenje nije propisano propisom ranga zakona. Promjenom odredaba pravilnika, mijenja se opseg primjene zakonske apsolutne zabrane pristupa Internetu.

Dakle, krajnji učinak sigurnosne mjere apsolutne zabrane prisutpa Internetu (Blanket Internet Access Ban) svedena je na zabranu sklapanja pretplatničkog ugovora i registrirane unaprijed plaćene usluge pristupa Internetu odnosno raskidanje postojećeg, a osuđenik istovremeno može neograničeno pristupati svim dostupnim sadržajima na Internetu.

Osim što apsolutna zabrana pristupa Internetu propisana zakonom nije u skladu s odredbom članka 10. Konvencije, ona nije niti tehnički provediva niti je moguće vršiti nadzor provedbe sigurnosne mjere.

Izricanje sigurnosne mjere apsolutne zabrane pristupa Internetu, na način propisan pravilnikom, u uvjetima neograničene mogućnosti pristupa Internetu anonimnim korištenjem unaprijed plaćene usluge pristupa Internetu, elektroničke komunikacijske usluge koja uključuje uslugu pristup Internetu, ili putem koje je moguć pristup Internetu, mogućnosti anonimnog pristupa Internetu kroz hot spot WI-FI pristup Internetu, pristup Internetu na temelju

[34] Članak 311. stavak 2. Kaznenog zakona
[35] Članak 58. stavak 5. Kaznenog zakona
[36] Članak 55. stavak 8. Kaznenog zakona

pretplatničkog ugovora koje je sklopila druga osoba, pristup Internetu na radnom mjestu i javnim ustanovama, nema nikakvog stvarnog učinka.

Dakle, propisivanje, izricanje i provođenje sigurnosne mjere zabrane pristupa Internetu nije svrhovito, niti će se izriacanjem i izvršavanjem sigurnosne mjere postići njena svrha, otklanjanje okolnosti koje omogućavaju ili poticajno djeluju na počinjenje novog kaznenog djela.

Literatura

CASE OF YILDIRIM v. TURKEY *(Application no. 3111/10)* JUDGMENT, STRASBOURG, 18 December 2012 , FINAL 18/03/2013.

DIRECTIVE 2011/92/EU OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL, of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA, Official Journal of the European Union L 335/1.

Freedom of Expression on the Internet Study of legal provisions and practices related to freedom of expression,the free flow of information and media pluralism on the Internet in OSCE participating States, dostupno http://www.osce.org/fom/80723 18.09.2013.

Kazneni zakon NN 125/11 i 144/12.

Pravilnik o izvršavanju zaštitne mjere zabrane pristupa internetu, NN 34/13.

Zakon o elektroničkim komunikacijama, NN 73/08, 90/11 i 133/12,

Zakon o potvrđivanju Konvencije za zaštitu ljudskih prava i temeljnih sloboda i protokola br. 1., 4., 6., 7. i 11. uz konvenciju za zaštitu ljudskih prava i temeljnih sloboda NN-MU 18/97,