Pregledni znanstveni članek
UDK 004.738.5:34

Nezakonite spletne vsebine: ali cenzura na internetu sploh deluje?

BARBARA POVŠE GOLOB
univerzitetna diplomirana matematičarka, vodja Registra.si, Arnes
MAŠA DROFENIK
univerzitetna diplomirana pravnica, Register.si, Arnes

1. Uvod

Razvoj interneta kot svetovnega družbenega fenomena je prispeval k pojavu neverjetne količine vsebin in storitev na tem mediju. Med njimi je seveda tudi cela vrsta takih, ki so nezaželene in potencialno škodljive (kot so lažne novice ali vsebine, škodljive mladoletnikom) ali nezakonite, od prirejanja tujih spletnih iger na srečo, otroške pornografije, spodbujanja sovražnega govora, ksenofobije, nasilja, terorizma do nezakonite objave osebnih podatkov in kršitev pravic intelektualne lastnine. Z znatnim povečanjem števila nezakonitih vsebin, ki jih je mogoče naložiti in do njih dostopati na spletu, so posledično blokade spletnih mest postale naraščajoč trend, za katerega ni mogoče pričakovati, da bi v prihodnje popustil. Evropska unija (EU) se je na izziv, ki ga prinašajo nezakonite spletne vsebine, pred kratkim odzvala s smernicami za hitro in proaktivno odkrivanje, odstranjevanje in preprečevanje ponovnega pojava nezakonite vsebine. Sporočilu o boju proti nezakonitim spletnim vsebinam,[1] s katerim je Evropska komisija opozorila, da bodo morda potrebni dodatni ukrepi za odstranjevanje nezakonitih vsebin s spleta, vključno z zakonodajnimi ukrepi, je sledil še predlog sklopa operativnih ukrepov, ki naj bi jih sprejela podjetja (spletne platforme) v državah članicah EU, s čimer bi se okrepila prizadevanja za internet brez nezakonitih vsebin.[2]

---

[1] Sporočilo COM(2017) 555 z dne 28. 9. 2017 o boju proti nezakonitim spletnim vsebinam in povečanju odgovornosti spletnih platform.

[2] Priporočilo C(2018) 1177 z dne 1. 3. 2018 o ukrepih za učinkovito preprečevanje nezakonitih spletnih vsebin.

V EU trenutno ni harmoniziranega in celostnega pristopa k odstranjevanju nezakonitih spletnih vsebin,[3] temveč soobstajajo različni pristopi, odvisni od države članice in kategorije vsebin. Države članice EU želijo z ukrepom blokade spletnega mesta zlasti preprečiti ali vsaj omejiti dostop in širjenje vsebin, ki spodbujajo sovraštvo, nasilje in terorizem, omogočajo prodajo ponarejenega blaga ali kako drugače kršijo norme nacionalnega prava.[4] V praksi se za tovrstne ukrepe uporablja različna terminologija, kot na primer filtriranje, blokiranje, cenzura interneta, pa tudi zapečatenje ali omejitev dostopa do spletnih strani. Ne glede na rabo izraza je z vidika internetnega uporabnika posledica vedno enaka. Del interneta z blokado spletnega mesta za njegove uporabnike postane (navidezno) nedostopen.[5]

Za uresničitev takšnega cilja so na voljo različne tehnične metode, vendar nobena, ki bi bila ustavno sprejemljiva, ni povsem učinkovita.[6] Z vidika varstva ustavnih svoboščin so blokade spletnih mest še posebno občutljivi ukrepi, povezani z omejevanjem svobode interneta in s tem svobode izražanja.[7] Zato je odrejanje tovrstnih ukrepov sprejemljivo samo kot *ultima ratio*, če je to res nujno za zaščito drugih, pomembnejših ustavnih vrednot javnega interesa[8] in če o odreditvi tovrstnih ukrepov odloči sodišče, ki je ob vsakokratni presoji primernosti ukrepa blokade vezano na načelo sorazmernosti. Drug pomemben vidik, ki ga je ob presoji primernosti ukrepa treba upoštevati, je vprašanje učinkovitosti blokiranja spletnih mest.

Cilj tega prispevka je predvsem podati tehnično oceno učinkovitosti posegov v internetno infrastrukturo z blokiranjem spletnih mest. Po uvodu so v drugem delu predstavljene posamezne tehnične metode blokiranja internetnih vsebin, in sicer na kakšen način omejijo dostopnost ter katere so prednosti pa tudi pasti in njihove omejitve. V tretjem delu so podani osnovni principi delovanja sistema domenskih imen (angl. *domain name system* – DNS),[9] medtem ko četrti del analizira blokade spletnih mest v slovenskem pravnem redu. Petemu

---

[3] Na ravni EU je splošni zakonodajni okvir za odstranjevanje nezakonitih vsebin Direktiva 2000/31/ES o elektronskem poslovanju z dne 8. junija 2000.

[4] Pravni okvir EU ne opredeljuje, še manj pa harmonizira pojmovanje tega, kaj je »nezakonita« vsebina. Evropska komisija nezakonito vsebino opredeljuje kot »kakršnekoli informacije, ki niso v skladu s pravom Unije ali zakonodajo zadevne države članice«. Razen glede spolne zlorabe otrok na spletu in otroške pornografije si države članice EU niso enotne glede tega, katera vsebina je javno sprejemljiva in katera ne. Spletna vsebina, ki je v eni od držav članic EU povsem zakonita, je lahko v drugi državi članici nezakonita.

[5] *Perspectives in Internet Content Blocking: an Overview* 2017.

[6] Glej mednarodne študije o tem: *A Comparative Study on Blocking, Filtering and Take-down of Illegal Internet Content* 2017; Callanan in dr. 2009 ; Poort in dr. 2014.

[7] Glej Damjan, str. 330–332; Klemenčič in dr., str. 361–363.

[8] Damjan, str. 330.

[9] Osnovna funkcija sistema domenskih imen je pretvorba IP-naslovov, kot je na primer 193.2.1.87, v besedne, domenske naslove, kot je na primer www.register.si. Različni zapisi DNS tako omogočajo usmerjanje prometa na internetu.

delu s priporočili, kako pristopiti k reševanju problematike omejitve dostopa do nezakonitih ali neželenih spletnih vsebin, sledi sklepni del.

2. Metode blokiranja spletnih mest

Obstajajo različni tehnični ukrepi, ki jih je mogoče uporabiti za blokiranje spletnega mesta. Največkrat se navajajo: (1) blokade na ravni internetnega protokola (IP-naslova) (na primer 193.2.1.87), (2) blokade na ravni DNS (domene) (primer.si), (3) blokade na ravni URL-naslova (https://www.primer.si/) in (4) metoda globokega pregleda paketov (angl. *deep packet inspection* – DPI-blokade),[10] ki temelji na vpogledu v vsebino, samodejnem pregledovanju celotnega prometa in iskanju vzorca v njem.[11]

Izvedba teh ukrepov prinaša različne stroške, učinke in tveganja. Ocena primernosti uporabljenih tehničnih ukrepov je običajno odvisna od sedmih ključnih dejavnikov: hitrosti in stroškov izvedbe, učinkovitosti blokiranja, enostavnosti obvoda, združljivosti s sodnim postopkom, celovitosti delovanja omrežja in vpliva na zakonite storitve.[12]

2.1. Blokada internetnega protokola (IP-naslova)

Z blokado internetnega protokola se prepreči dostop do določenega IP-naslova (tistega, ki ga ima spletno mesto in je predmet blokade). Prednost te metode je v enostavnosti izvedbe in posledično nizkih stroških. Obenem ima ta tehnični ukrep vsaj dve pomembni pomanjkljivosti, in sicer nevarnost čezmernega blokiranja in enostavnost obvoda blokade.

Ker se en sam IP-naslov pogosto uporablja za gostovanje več (včasih na stotine) spletnih strani, se z blokado IP-naslova blokirajo tudi morebitne druge spletne vsebine, ki so lahko povsem nepovezane s ciljem blokade oziroma so popolnoma zakonite. Običajno ni mogoče, da bi kdorkoli drug, razen ponudnika storitve gostiteljstva (angl. *web hosting provider*), lahko z gotovostjo ugotovil, ali se IP-naslov uporablja za več spletnih strani.[13] Takšna čezmerna blokada pomeni nesorazmeren poseg, s katerim se omejuje pravica do svobodnega izražanja.[14] Ponudnikom zakonite vsebine pa lahko ob izvršitvi ukrepa nastane celo poslovna škoda.

Poleg tega je mogoče takšno blokado razmeroma enostavno zaobiti. Ponudnik vsebine, ki objavlja, administrira in ureja spletno mesto, se blokadi izogne tako, da svojega ponudnika

---

10 Fangfei Wang 2014.

11 Božič, str. 57.

12 *"Site Blocking" to reduce online copyright infringement* 2010.

13 Feiler, str. 9–10.

14 Lodder, Polter, str. 6.

storitve gostiteljstva zaprosi za nov IP-naslov in znova konfigurira svojo domeno, tako da se ta razreši v novi IP-naslov. Internetni uporabniki lahko blokado IP-naslova zaobidejo na primer z uporabo omrežja Tor, ki je namenjeno anonimnemu brskanju,[15] ali z uporabo posredovalnih storitev anonimnih posredniških strežnikov (angl. *proxy server*), podobno kot ponudnik vsebine z uporabo obratnega posredniškega strežnika (angl. *reverse proxy*) in CDN-omrežja (angl. *content delivery network*). Ob tem je pomembno poudariti, da tako ponudnik vsebine kot tudi internetni uporabnik za tovrstne »podvige« ne potrebuje posebnega tehničnega znanja. Navodila za uporabo obvodov so lahko dostopna (na spletu samem).

2.2. Blokada domene (blokada na ravni DNS)

Najpogosteje uporabljeni način blokade temelji na DNS, pri katerem gre dejansko za poseg v DNS-infrastrukturo. Tudi ta metoda je precej enostavna za izvajanje in ne povzroča bistvenih dodatnih stroškov. Pomanjkljivost, podobno kot pri blokadi IP-naslova, zadeva učinkovitost ukrepa, saj je tudi to vrsto blokade razmeroma enostavno zaobiti.

Ponudniki vsebin so zaradi pogostnosti uporabe tega ukrepa nanj največkrat pripravljeni že vnaprej in isto vsebino ponujajo na spletnih straneh pod različnimi domenskimi naslovi.[16] Tudi internetni uporabniki imajo na voljo precej enostavnih rešitev. Do želene vsebine lahko dostopajo neposredno prek IP-naslova. Z blokado domene se namreč onemogoči le dostop prek domene, medtem ko je do spletne vsebine še vedno mogoče dostopati prek IP-naslova. Poleg tega lahko uporabniki prek navideznega zasebnega omrežja (VPN-kanalov)[17] prikrijejo svojo lokacijo in tako obidejo nacionalno zakonodajo ali pa uporabijo DNS-razreševalnike (angl. *DNS resolver*) v tujini, ki ne podležejo nacionalni zakonodaji.[18] Na svojem računalniku si lahko namesto standardnega sistema DNS nastavijo javno DNS-storitev, kot so na primer OpenDNS, Google DNS in Cloudflare DNS. Če se ukrep blokade odredi konkretnemu ponudniku internetnih storitev, pa bo že menjava tega uporabniku znova omogočila dostop do sporne vsebine.

2.3. Blokada URL-naslova

Blokiranje URL-jev se lahko opravi s tako imenovanim globokim pregledom paketov ali (tudi) z uporabo posredniškega strežnika, ki so ga vsi uporabniki prisiljeni uporabljati za nadalj-

---

15 Božič, str. 57.

16 Postopek registracije domen je avtomatiziran, enostaven in hiter, stroški registracije pa so razmeroma nizki.

17 Navodila za uporabo VPN so na voljo v slovenskem jeziku (<https://siol.net/digisvet/nasveti/vpn-kaj-je-zakaj-ga-potrebujete-in-kateri-je-najboljsi-443626>, 12. 4. 2018).

18 Povše Golob, Zwittnig, str. 27.

nji dostop do spleta. Ta način blokiranja je v osnovi problematičen že zato, ker je v nasprotju z arhitekturnimi načeli interneta. Predvsem pa je ta metoda cenovno izjemno neugodna, saj je zanjo treba imeti drago strojno opremo.[19]

Njena prednost je v tem, da predstavlja najmanjše tveganje za čezmerno blokiranje, tako da je poseg v pravico do svobodnega izražanja vsaj do neke mere omejen.[20] Preostali problemi in načini obvodov so povsem isti kot pri prejšnjih metodah blokiranja (blokadi IP-naslova in blokadi domene).

2.4. Deep packet inspection – DPI-blokade

Kot že omenjeno, gre pri tej metodi za tako imenovani globok pregled paketov. Izmed vseh naštetih metod sicer velja za najbolj kompleksno in edino učinkovito obliko filtriranja internetnega prometa. Ker pa temelji na vpogledu v vsebino spletne komunikacije, je zaradi čezmernih in nedopustnih posegov v zasebnost z ustavnega vidika nesprejemljiva.

V splošnem velja, da so stroški prve in druge metode (blokada IP-naslova in blokada domene) zaradi enostavnosti izvedbe podobno nizki, medtem ko je blokiranje URL-jev, ki se uporablja kot varnostni ukrep v zaprtih krogih podjetij in državnih ustanov, lahko precej dražje. Blokiranje internetnega prometa na ravni IP-naslova zaradi možnosti čezmernega blokiranja (tudi povsem zakonite vsebine) predstavlja še dodatno tveganje, medtem ko lahko blokiranje URL-jev zaradi sprememb internetne infrastrukture povzroči neučinkovito delovanje večjega dela omrežja. Ponudniki spletnih vsebin in internetni uporabniki lahko vsakega od zgornjih ukrepov tehnično gledano v celoti in razmeroma enostavno zaobidejo (ne glede na to, za kakšno vrsto blokade gre). V nadaljevanju prispevka se osredotočamo predvsem na blokade na ravni DNS, ki so najpogosteje uporabljena metoda blokiranja tudi pri nas.

3. Sistem domenskih imen (DNS)

Blokade na ravni DNS niso nove. Digitalni posredniki, zlasti ponudniki internetnih storitev (angl. *internet service provider* – ISP), se z zahtevami po blokadah domen srečujejo že vrsto let, kljub temu pa je sistem domenskih imen šele pred kratkim dobil mesto v nacionalni zakonodaji. Direktiva 2016/1148/EU o ukrepih za visoko skupno raven varnosti omrežij in informacijskih sistemov v Uniji in Zakon o informacijski varnosti (ZInfV)[21] sistem domenskih imen definirata kot »hierarhično porazdeljen sistem dodeljevanja imen v omrežju, ki

---

[19] Lodder, Polter, str. 7.

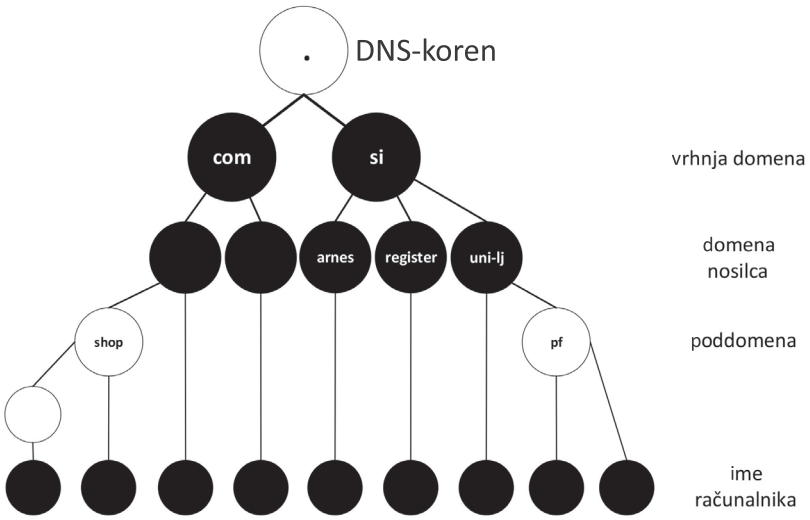
[20] Feiler, str. 10–11.

[21] Uradni list RS, št. 30/18.

posreduje poizvedbe za domenska imena«.[22] V praksi se zahteve po blokadah domen pogosto izkažejo za problematične, saj zaradi nepoznavanja osnovnih principov delovanja tehnologije sistema DNS prinesejo širše in neželene posledice (kot na primer blokiranje povsem zakonite vsebine) ali pa se tehnični posegi v DNS izkažejo za neučinkovite in nesorazmerne (nezakonita vsebina kljub blokadi ostane dostopna na spletu).

Delovanje interneta je v grobem odvisno prav od fizične infrastrukture in sistema DNS. Ta je v ozadju večine internetnih storitev in aplikacij. Njegova osnovna funkcija je omogočanje internetnim uporabnikom, da prek naprav, povezanih v internet (osebnega računalnika, pametnega telefona, tabličnega računalnika, pametne ure in številnih drugih), na enostaven način dostopajo do spletnih strani, elektronske pošte, instantnih sporočil, internetne telefonije in podobno. Vsaka naprava, povezana v internet, ima edinstven naslov, ki je sestavljen iz niza števil, tj. IP-naslova (na primer 193.2.1.87), z uporabo katerega se je mogoče povezati z napravo in dostopati do vsebin in storitev na tej napravi. Da pa si uporabniku ni treba zapomniti zapletenega zaporedja števil, DNS olajša uporabo interneta tako, da IP-naslovu dodeli besedne naslove, tako imenovane domene, pri katerih so različne ravni med seboj ločene s piko (na primer pf.uni-lj.si). Namesto da uporabnik v brskalnik vnese številčni IP-naslov, lahko vnese domeno. Tako različni zapisi DNS omogočajo usmerjanje prometa na internetu.

Slika 1: Struktura DNS (vir: *Register.si*)



[22] Glej 14. točko 4. člena NIS Direktive in 28. točko 4. člena ZInfV.

DNS deluje hierarhično (Slika 1). Na vrhu drevesne strukture je tako imenovani DNS-koren (angl. *DNS root*). Raven neposredno pod DNS-korenom predstavljajo vrhnje domene, ki jih v grobem delimo v dve skupini. V prvo skupino se uvrščajo nacionalne vrhnje domene (angl. *country code top level domains* – ccTLD), kot so na primer .si za Slovenijo, .de za Nemčijo ali .ca za Kanado, medtem ko se v drugo skupino uvrščajo generične vrhnje domene (angl. *generic top level domains* – gTLD), kot so .com, .org, .net in številne druge (.xyz, .berlin, .club, .win, .loan idr.).[23] Na naslednji ravni drevesne DNS-strukture so tako imenovane drugotne ali sekundarne domene (angl. *second level domains* – SLD). Te imamo največkrat v mislih, ko govorimo o internetnih domenah. Ker je sistem DNS hierarhičen, je število poddomen neomejeno in prepuščeno izbiri nosilcev domen (na primer www.register.si ali www.pf.uni-lj.si).

Skladno z drevesno strukturo DNS so različni subjekti odgovorni za posamezno podvejo na ustreznih ravneh. Posameznik ali organizacija lahko vpliva le na podvejo neposredno pod svojo ravnijo v hierarhiji. To pomeni, da register domen,[24] ki upravlja določeno nacionalno vrhnjo domeno, ne more vplivati na drugo nacionalno domeno ali pa na generično domeno niti na domene, ki so registrirane pod temi domenami.[25] Ali povedano drugače, register za nacionalno domeno .si ne more vplivati na nemško nacionalno domeno .de ali na domeno .com. Obenem pa vsak ukrep registra za .si vpliva na celotno podvejo, ki jo nadzoruje.

---

[23] Predpisi, ki urejajo generične vrhnje domene, so za razliko od predpisov, ki urejajo nacionalne vrhnje domene, pripravljeni na globalni ravni. Vrhovna institucija, ki danes upravlja in nadzira dodeljevanje naslovov IP v svetu, je ICANN (Internet Corporation for Assigned Names and Numbers).

[24] Register domenskih imen najvišje ravni je subjekt, ki upravlja in izvaja registracijo imen internetnih domen v okviru določene domene najvišje ravni. Za slovensko nacionalno domeno .si vlogo registra domenskih imen najvišje ravni opravlja Register.si, ki deluje pod okriljem javnega zavoda Akademska in raziskovalna mreža Slovenije (Arnes). Ena od osnovnih funkcij Registra.si je zagotavljanja registracije domen pod .si, v okviru katere:

- oblikuje pravila za registracijo domen v skladu z lokalno zakonodajo, mednarodnimi priporočili in v skupno dobro lokalne internetne skupnosti (prebivalcev Slovenije);
- zagotavlja varno, stabilno in neprekinjeno delovanje vseh servisov;
- skrbi za razvoj, vzdrževanje in nadzor tehničnega sistema za registracijo domen (EPP-strežnika, portala za registrarje, odjemalca in aplikacije za registrarje);
- zastopa .si v mednarodnih organizacijah;
- spremlja razvoj in novosti na področju registracije domen;
- administrira postopek alternativnega reševanje domenskih sporov (postopek ARDS);
- promovira uporabo nacionalne vrhnje domene .si;
- skrbi za nenehno posodabljanje in razvoj storitev in infrastrukture v skladu s potrebami uporabnikov;
- vzpostavlja poslovne odnose z registrarji, nosilci in drugimi poslovnimi partnerji, ki temeljijo na vzajemnem zaupanju;
- z akcijami ozaveščanja javnosti o prednostih nacionalne domene skrbi za rast števila registriranih domen pod .si;
- z aktivnim vključevanjem v projekte lokalne skupnosti prispeva k razvoju uporabe interneta v Sloveniji;
- se aktivno vključuje v upravljanje interneta v Sloveniji.

[25] Povzeto po CENTR: *Domain conflicts and the legal system* 2012.

Ob normalnem delovanju sistema DNS, tj. brez nepredvidenih tehničnih posegov vanj, so posamezne spletne strani dostopne na podlagi domene oziroma njej odgovarjajočega IP-naslova, ki ju internetni uporabnik vtipka v ukazno vrstico spletnega brskalnika. Z blokado domene pa se uporabniku onemogoči dostop do spletnega mesta prek domene (ne pa tudi prek IP-naslova). Posledično namesto pričakovane spletne vsebine internetni uporabnik dobi odgovor »stran ni dosegljiva« ali pa naleti na drugo spletno stran, na kateri je obvestilo o onemogočenem dostopu do spletne strani z nezakonito vsebino in o razlogih za preusmeritev. V drugem primeru gre dejansko za preusmeritev domene na ravni DNS.[26]

Primer obvestila o blokirani spletni strani:

OBVESTILO – SPLETNA STRAN JE NEDOSEGLJIVA

Spoštovani!

Poskusili ste dostopiti do spletne strani, do katere je Finančna uprava Republike Slovenije onemogočila dostop zaradi kršitve predpisov, izvajanje katerih nadzoruje.

Spletne strani, do katerih se dostopa prek določene domene, resda lahko vsebujejo nezakonito vsebino (na primer otroško pornografijo, spodbujanje k nasilju, rasizmu, terorizmu), lahko ponujajo škodljive oziroma neprimerne storitve, pred katerimi je treba zaščititi najbolj ranljive skupine internetnih uporabnikov, zlasti mladoletne osebe, ali pa se uporabljajo za nezakonite namene, kot je na primer poskus goljufije. Ob tem je pomembno poudariti, da je v primeru kršitve zakona in nezaželene aktivnosti na internetu spletna vsebina tista, ki predstavlja težavo, in ne ime domene. Domena je v tem primeru le naslov oziroma eden od naslovov, prek katerih je (med drugim!) dostopna določena spletna vsebina, medtem ko s samo vsebino ni povezana. V praksi organi, ki izdajajo zahteve po blokadah in preusmeritvah domen, v nasprotju z navedenim (tudi zaradi nepoznavanja delovanja DNS in tehnologije) samo domeno pogosto enačijo s spletno stranjo.[27]

---

[26] Povše Golob, Drofenik, str. 18.

[27] Prav tam, str. 19.

4. Blokade spletnih mest v slovenskem pravnem redu

V Sloveniji se je prvi poskus blokade spletne strani zgodil leta 2003, ko je takratni Inšpektorat RS za varstvo osebnih podatkov[28] slovenskim ponudnikom internetnih storitev odredil omejitev dostopa do spletne strani www.udba.net.[29] Drugi, v javnosti odmevnejši primer blokade je sledil leta 2010 s predlogom Urada za nadzor nad prirejanjem iger na srečo (UNPIS),[30] da se omeji dostop do spletnih strani bwin.com, bet-at-home.com in expekt.com zaradi nezakonitega prirejanja spletnih iger na srečo, tj. brez koncesije Vlade Republike Slovenije. Od takrat so bili pred domačimi sodišči predstavljeni številni argumenti za sprejetje in zavrnitev zahtev po omejevanju dostopa do spletnih strani,[31] željá po sistematičnem filtriranju interneta pa je, podobno kot v tujini, tudi pri nas še vedno vse več.

Pristojnost odrejanja ukrepov, s katerimi se posega v omejevanje svobode interneta, je v slovenskem pravnem redu pridržana izključno sodiščem. Glede na možnost tretjega odstavka 12. člena Direktive o elektronskem poslovanju[32] bi takšno odločitev lahko sprejeli upravni organi ali sodišča. Vendar se je slovenski zakonodajalec zaradi teže ukrepa odločil pristojnost prenesti zgolj na civilna in kazenska sodišča. Pravno relevantna zakonodaja, Zakon o elektronskem poslovanju na trgu (ZEPT),[33] le sodišču dovoljuje, da lahko odredi onemogočanje dostopa do nezakonitih vsebin zaradi odkrivanja in preprečevanja kaznivih dejanj, varstva zasebnosti, varovanja tajnih podatkov in poslovne tajnosti. Takšen predlog lahko sodišču v javnem interesu posredujejo tudi za nadzor pristojni upravni organi, skladno s področno zakonodajo, vendar pa sami takega ukrepa ne morejo odrediti.[34]

---

[28] Inšpektorat za varstvo osebnih podatkov je bil kot organ v sestavi Ministrstva za pravosodje pristojen za varstvo osebnih podatkov. Kasneje se je na podlagi Zakona o informacijskem pooblaščencu (ZInfP), ki je začel veljati 31. 12. 2005, združil s Pooblaščencem za dostop do informacij javnega značaja v samostojen državni organ – Informacijski pooblaščenec RS.

[29] Strokovno združenje ponudnikov internetnih storitev (SISPA) je izrazilo nasprotovanje ukrepu, saj da gre za nevaren precedens. Zaradi možnosti enostavnega obvoda blokade je glavni inšpektor priznal nemogoče izvajanje in odločitev o blokadi preklical.

[30] Prirejanje iger na srečo je do 1. 1. 2013 nadzoroval Urad za nadzor prirejanja iger na srečo (UNPIS), z Zakonom o spremembah in dopolnitvah Zakona o igrah na srečo (ZIS-E, Uradni list RS, št. 108/12) pa je bil nadzor prenesen na Davčno upravo RS (DURS), ki se je 1. 8. 2014 s Carinskim uradom RS (CURS) združila v Finančno upravo RS.

[31] Zlasti pred Upravnim in Vrhovnim sodiščem RS zaradi omejevanja dostopa do spletnih igralnic. Sodišče je v veliki večini zadev tem zahtevam ugodilo, čeprav argumenti, ki se uporabljajo za utemeljitev sodnih zahtevkov, niso vedno prepričljivi.

[32] Direktiva 2000/31/ES Evropskega parlamenta in Sveta z dne 8. junija 2000 o nekaterih pravnih vidikih storitev informacijske družbe, zlasti elektronskega poslovanja na notranjem trgu, UL L 178, 17. 7. 2000, str. 1–16.

[33] Uradni list RS, št. 61/06 s spremembami.

[34] Določba 9. člena ZEPT.

Skladno z navedenim se v Sloveniji omejuje dostop do nezakonitih spletnih igralnic po 107.a členu Zakona o igrah na srečo (ZIS),[35] ki ureja nadzor nad nezakonitim prirejanjem iger na srečo prek spleta. Poleg tega se onemogočanje dostopa do spletnih strani omenja tudi v podzakonskem aktu, Pravilniku o načinu izvrševanja pooblastil uradnih oseb Finančne uprave RS in označitvi službenih vozil Finančne uprave RS (Pravilnik).[36] Ta v 8. členu omogoča ukrep »zapečatenja spletnih strani« zaradi preprečevanja kršitev davčne zakonodaje, ki ga Finančna uprava RS odreja samostojno, brez odredbe sodišča.

4.1. Blokade (tujih) spletnih igralnic po Zakonu o igrah na srečo

Določba 107.a člena ZIS omogoča, da v primeru, če ponudnik spletnih iger na srečo brez koncesije prostovoljno ne izvrši prepovedne odločbe nadzornega organa, Upravno sodišče na predlog Finančne uprave RS ponudniku storitev informacijske družbe (ponudniku internetnih storitev) odredi omejitev dostopa do spletnih strani, prek katerih se take igre prirejajo.[37] Omejevanje dostopa do nezakonitih spletnih igralnic je torej v pristojnosti Upravnega sodišča RS, ki o tem odloča na predlog predlagatelja (tj. Finančne uprave RS kot nadzornega organa).[38] O predlogu sodišče odloči v sedmih dneh od njegovega prejema,[39] znotraj tega roka pa da ponudniku storitev informacijske družbe tudi možnost, da se izreče o predlogu. Poleg tega ima ponudnik možnost pritožbe zoper odločitev Upravnega sodišča na Vrhovno sodišče RS.

Sodišče je pri izrekanju vrste ukrepa oziroma načina izvedbe ukrepa vezano na zakon in predlog predlagatelja. S sklepom običajno odredi tehnično definiran in jasen ukrep preusmeritve nedovoljenega spletnega mesta na drugo spletno mesto na podlagi domene. Ponudnik storitev informacijske družbe glede tehnične izvedbe ni v dvomu. Zmedo pri ponudniku bi lahko povzročilo v odredbi napačno navedeno ime spletnega mesta, ki je predmet blokade, če bi predlagatelj na primer predlagal omejitev dostopa do spletne strani, za katero bi se izkazalo, da ne vsebuje spletne igralnice, ampak neko drugo (povsem zakonito) vsebino. Takšne očitne

---

35 Uradni list RS, št. 14/11 s spremembami.

36 Uradni list RS, št. 57/15.

37 ZIS predpisuje tudi načela, ki jih mora Finančna uprava RS upoštevati v svojem predlogu (sorazmernost, upoštevanje tehničnih možnosti), in sestavine, ki jih mora vsebovati predlog (obseg omejitve, način izvršitve).

38 Zakonodajalec je takšno ureditev utemeljil s pojasnilom, da gre pri vsakem omejevanju dostopa do spletnih strani za ukrepe, ki so povezani z omejevanjem svobode interneta in s tem svobode izražanja kot ustavno zagotovljene pravice, zato je primerno, da tudi o omejitvi dostopa do spletnih strani, prek katerih se prirejajo spletne igre na srečo brez koncesije, odloči sodišče (Predlog zakona o spremembah in dopolnitvah Zakona o igrah na srečo (ZIS-D), EVA 2010-1611-0084 z dne 28. 10. 2010).

39 Po petem odstavku 107.a člena lahko ponudnik storitve informacijske družbe zoper odločbo Upravnega sodišča v treh dneh vloži pritožbo, o kateri Vrhovno sodišče RS odloči najpozneje v 15 dneh po prejemu pritožbe.

pomote predlagatelja, ki so se v praksi že zgodile,[40] je sodišče po opozorilu ponudnika storitev informacijske družbe pravočasno odpravilo s sklepom, s katerim je odredilo omejitev dostopa do pravilno navedene spletne strani.

Podobno kot sodišče odpravlja očitne pisne pomote predlagatelja, pazi tudi na ustreznost roka za izvršitev naloženega ukrepa. Predlagatelj od ponudnika storitev informacijske družbe navadno zahteva izvedbo ukrepa naslednji dan po pravnomočnosti odločbe sodišča. Z vidika ponudnika storitev informacijske družbe je izvršitev ukrepa na točno določen dan lahko otežena ali celo neizvedljiva.[41] Zato sodišče - upoštevajoč, da se po zakonu omejitev dostopa do spletnih strani lahko odredi le na način, ki je najmanj obremenjujoč za ponudnika storitev informacijske družbe -, v takih primerih rok za izvršitev ukrepa s sklepom o omejitvi dostopa do spletne strani ustrezno podaljša.[42]

V praksi se izkaže, da se prireditelji spletnih iger na srečo izvršenim ukrepom hitro prilagodijo oziroma jih enostavno izničijo, saj so jim poznani možni načini obvodov blokade, na morebitno omejitev dostopa do njihovega spletnega mesta pa so že vnaprej pripravljeni. Ker vsebino spletne igralnice ponujajo na več zamenljivo podobnih spletnih naslovih, lahko ob izvršitvi ukrepa blokade nemudoma omogočijo dostop do spletne igralnice prek (drugega) delujočega spletnega mesta,[43] pri tem pa celo v večji meri ohranijo ime igralnice, zaradi česar internetni uporabnik nima nikakršnih težav z dostopom do blokirane spletne igralnice. Do nje lahko še naprej dostopa enostavno, z vpisom imena igralnice v brskalnik. Kljub temu vprašanje (ne)učinkovitosti v obstoječi sodni praksi ni razlog, ki bi lahko bil podlaga za neugoditev ukrepu omejitve dostopa do spletne strani. Vrhovno sodišče RS je namreč zavzelo stališče, da se z izvršitvijo ukrepa doseže to, da je večina uporabnikov ob vsakodnevni uporabi interneta

---

40 Sklep Upravnega sodišča RS I U 586/2018 z dne 27. 3. 2018.

41 Za ponudnike storitev informacijske družbe ni nujno, da zagotavljajo štiriindvajseturno dežurstvo. Izvršitev naloženega ukrepa v nesorazmerno kratkem enodnevnem roku ponudnikom storitev informacijske družbe povzroča nesorazmerne dodatne stroške, saj morajo praktično za vsak delovni dan zagotoviti, da je na delovnem mestu ali v pripravljenosti oseba, ki ima ustrezna znanja in notranja pooblastila za izvedbo ukrepa. Krog teh oseb je pri vseh ponudnikih storitev informacijske družbe nujno omejen že zaradi notranjih varnostnih politik upravljanja informacijskih sistemov pri ponudnikih. S tem ko se od ponudnikov storitev informacijske družbe zahteva, da naloženi ukrep izvršijo naslednji dan po vročitvi odločbe, se jih dejansko sili, da notranjo organizacijo prilagodijo tako, da je vselej na delovnem mestu ali vsaj v pripravljenosti pristojna oseba.

42 Sklep Upravnega sodišča RS I U 597/2018 z dne 27. 3. 2018, I U 586/2018 z dne 27. 3. 2018, I U 185/2018 z dne 30. 1. 2018 in dr.

43 Na primer na drugi internetni domeni s podobno zamenljivimi znaki. Pravila registracije domen namreč nudijo praktično neomejene možnosti registracije zamenljivo podobnih domen, tako da prireditelji lahko izbirajo med številnimi (nacionalnimi in generičnimi) vrhnjimi domenami in pri tem niso geografsko omejeni. To pomeni, da lahko ponudnik vsebine (prireditelj spletnih iger na srečo) že takoj po izvršitvi ukrepa ponudi dostop do iste vsebine prek domene, ki se sintaktično le nebistveno razlikuje od prejšnje.

pri poskusu dostopa do spletne strani nezakonitega prireditelja iger na srečo preusmerjena na drugo spletno stran, na kateri bo obveščena o neuspešnem poskusu dostopa do spletne strani z nezakonito ponudbo iger na srečo in o razlogih za preusmeritev. Po mnenju Vrhovnega sodišča RS se s tem doseže osnovni namen ukrepa, saj prvi odstavek 107.a člena določa, da se ponudniku storitev informacijske družbe odredi omejitev dostopa in ne morebiti popolna preprečitev dostopa.[44]

4.2. Zapečatenje spletnih strani zaradi kršitev davčne zakonodaje

Finančna uprava RS blokado domene s preusmeritvijo nedovoljenega spletnega mesta na drugo spletno mesto nalaga ponudnikom internetnih storitev tudi v povezavi s postopkom nadzora nad opravljanjem dela na črno. Z izdajo odločbe po uradni dolžnosti od ponudnikov internetnih storitev zahteva, da se s preusmeritvijo spletnega mesta omeji dostop do tistih spletnih strani, prek katerih davčni zavezanci opravljajo neregistrirane tržne dejavnosti. Odločitev o blokadi posameznega spletnega mesta utemeljuje z Zakonom o finančni upravi (ZFU)[45] in z že omenjenim pravilnikom, ki v 8. členu uradni osebi Finančne uprave RS omogoča, da ponudnikom informacijske družbe naloži ukrep »zapečatenja spletnih strani« in objavo obvestila o zapečatenju.[46] Zadevna določba 8. člena Pravilnika razširja sicer zakonsko določen in predpisan ukrep zapečatenja poslovnih prostorov, dokumentov in predmetov. ZFU v 37. členu namreč ne omenja možnosti »zapečatenja spletnih strani«, niti iz samega besedila ne izhaja, da bi se za spletne strani smiselno uporabljala pravila o zapečatenju, ki veljajo za dokumente, predmete oziroma poslovne prostore.[47]

Aktualna ureditev v podzakonskem pravnem aktu je problematična, saj v nasprotju z veljavno zakonodajno ureditvijo v ZEPT, ki daje pristojnost odrediti odstranitev nezakonitih vsebin ali onemogočanje dostopa do njih le sodišču, ne pa tudi upravnim oziroma inšpekcijskim organom, Finančni upravi RS omogoča samostojno odrejanje blokade spletnega mesta in s tem posege, povezane z omejevanjem svobode interneta in svobode izražanja, brez odredbe sodišča. Navsezadnje to pomeni tudi, da isti organ v vsebinsko enakih primerih, kot je prirejanje spletnih iger na srečo in omejevanje dostopa do spletnih igralnic brez ustreznega dovoljenja, postopa drugače, prvič v vlogi odločevalca in drugič v vlogi predlagatelja. Dodaten problem

---

[44] Sklep Vrhovnega sodišča RS I Up 54/2012 z dne 16. 2. 2012 in I Up 66/2012 z dne 16. 2. 2012.

[45] Uradni list RS, št. 25/14.

[46] Tretji odstavek 8. člena Pravilnika.

[47] Prvi odstavek 37. člena ZFU se glasi: »Če uradna oseba pri opravljanju nalog finančne uprave ugotovi, da je kršen zakon ali drug predpis, katerega izvajanje nadzoruje, lahko, če je to nujno potrebno zaradi preprečitve nadaljnje kršitve, do odprave nepravilnosti z odločbo prepove opravljanje dejavnosti ter hkrati zapečati poslovne prostore, dokumente ali predmete.«

predstavlja neenotna formulacija v zakonodaji. Medtem ko ZIS v primeru iger na srečo dovoljuje omejitev dostopa do spletnih strani, pravilnik opredeljuje zapečatenje spletnih strani, ki se izvede z odredbo ponudniku storitev informacijske družbe. Druge težave, povezane z učinkovitostjo ukrepa blokade in možnimi obvodi, pa so povsem enake ali podobne kot v primeru omejevanja dostopa do spletnih igralnic. Davčni kršitelji lahko kljub »zapečatenju« svoje storitve razmeroma neovirano ponujajo naprej in jih ukrepi zapečatenja pri tem bistveno ne ovirajo.

5. Priporočila

EU se je na izziv, ki ga predstavljajo nezakonite spletne vsebine, odzvala s predlogom operativnih ukrepov, ki bi zagotovili hitrejše odkrivanje in odstranjevanje nezakonitih spletnih vsebin, okrepili sodelovanje med podjetji, zaupanja vrednimi prijavitelji[48] in organi pregona ter povečali preglednost in okrepili zaščitne ukrepe za državljane. S predlaganim sklopom operativnih ukrepov se je Evropska komisija osredotočila na industrijo in dejavnosti spletnih platform, zlasti pa na gostiteljske storitve, ki jih te platforme zagotavljajo,[49] ter nanje prenesla breme tehtanja med nezakonito objavo na spletu in temeljnimi ustavnimi pravicami, kot je na primer svoboda izražanja. Dejavnosti teh podjetij bo Komisija spremljala več mesecev in odločila, ali so potrebni dodatni koraki, po potrebi tudi sprejetje nove zakonodaje na ravni EU.

Praksa in izkušnje kažejo, da je edini učinkoviti ukrep v primeru nezakonitih spletnih vsebin njihova odstranitev in ukrepanje zoper kršitelja. Za vsebino spletne strani namreč v prvi vrsti odgovarja oseba, ki spletno mesto objavlja, administrira in ureja, tj. ponudnik vsebine,[50] umik nezakonite vsebine pa se lahko izvede samo lokalno na napravah (strežnikih), kjer se vsebina ponuja. To pomeni, da je primarno treba sprejeti ukrep, usmerjen neposredno proti ponudniku vsebine. Posamezni primeri se enostavno rešijo tako, da ponudnik vsebine prostovoljno odstrani sporno vsebino. Če pa ta zahteve po umiku ne upošteva, ga k odstranitvi sporne vsebine lahko spodbudijo ustrezni pravni postopki.[51]

---

[48] Evropska komisija v Priporočilu C(2018) 1177 z dne 1. 3. 2018 o ukrepih za učinkovito preprečevanje nezakonitih spletnih vsebin opredeljuje »zaupanja vredne prijavitelje« le na široko kot specializirane subjekte s posebnim strokovnim znanjem v odkrivanju nezakonitih vsebin in namenske strukture za odkrivanje takšnih vsebin na spletu.

[49] Gostiteljska storitev je storitev informacijske družbe, pri kateri se shranjujejo podatki prejemnika storitev. Ta kategorija lahko zajema različne akterje, od spletnih tržnic, platform za izmenjavo posnetkov, družbenih omrežij, blogerskih spletišč ali spletišč za ocene do oddelkov za komentarje bralcev na novičarskih straneh.

[50] Navadno je to nosilec domene, ni pa nujno, lahko gre za različni osebi.

[51] CENTR: *Domain conflicts and the legal system* 2012.

Če s ponudnikom vsebine ni mogoče stopiti v stik (ker je ta iz tujine ali pa je neodziven), je naslednji ustrezni naslovnik zahteve za umik sporne vsebine njegov ponudnik storitev gostiteljstva (angl. *web hosting provider*). Šele če so vsi poskusi odstranitve sporne vsebine neuspešni, so upravičene zahteve po omejitvi dostopa do spletne strani, ki gosti nezakonito vsebino (www.primer.si). Z izvedbo ukrepa cilj odstranitve sporne vsebine sicer ne bo dosežen, bo pa vsebina postala težje dosegljiva in s tem omejeni morebitni škodljivi učinki. Ob zadnjem je treba poudariti, da bi takšne zahteve zakonodaja morala dopuščati le izjemoma, upoštevaje načelo sorazmernosti in učinkovitosti ukrepa.

Da bi se v teh izjemnih primerih odreditve blokad karseda omilili negativni učinki, bi po mnenju avtoric tega prispevka bilo treba v postopkih odrejanja tovrstnih ukrepov upoštevati zlasti naslednja priporočila:

- pred odreditvijo blokade spletnega mesta naj se izključijo možni ukrepi bližje viru (odstranitev vsebine pri ponudniku vsebine ali ponudniku storitev gostiteljstva);
- zagotovljena naj bo transparentnost blokiranih mest, politike in pravila glede odreditve blokad naj bodo vnaprej znani, prav tako naj bo javno objavljena evidenca blokiranih spletnih strani;
- ukrepi morajo imeti ustrezno pravno podlago, ponudniki internetnih storitev in drugi ponudniki storitev informacijske družbe ne smejo biti prisiljeni v vlogo sodnikov in nosilcev bremena presojanja zakonitosti vsebin in storitev;
- pri odrejanju tehničnih ukrepov naj se uporablja enotna, jasna in natančna terminologija, ki ne omogoča različnih interpretacij glede tehnične izvedbe naloženega ukrepa;
- ukrepi naj bodo začasni, ko razlog za blokado spletnega mesta preneha, naj se ukrep blokade spletnega mesta prekliče;
- v pripravo zakonodaje, pravil in postopkov naj bodo vključeni strokovnjaki vseh relevantnih področij, prava, informacijske tehnologije, ekonomije in drugih področij, da se omejijo negativne posledice.

6. Sklep

Blokade so tehnični ukrep, ki na sporno vsebino ne vpliva, pač pa internetnim uporabnikom skuša preprečiti ali otežiti dostop do teh vsebin. Za uresničitev takšnega cilja so na voljo različne tehnične metode. Vsaka deluje na drugačen način in ima določene prednosti v primerjavi z drugimi načini blokiranja. Vendar pa nobena metoda, ki bi bila ustavno sprejemljiva,

ni povsem učinkovita.[52] Sodobna tehnologija tako ponudnikom nezakonitih vsebin kot internetnim uporabnikom namreč ponuja raznovrstne obvode (druge imenike DNS, posredniške strežnike, omrežje Tor, CDN-omrežje, VPN-kanale ipd.), ki so vedno širše dostopni in enostavni za uporabo. Vsaka od metod blokiranja deluje na drugačen način, bolj ali manj učinkovito, ima vpliv le na določene uporabnike, povzroča nehotene oziroma nenamerne posledice pri povsem zakonitih vsebinah, ukrepom pa se je razmeroma preprosto izogniti. Kot se izkaže v praksi, izvršeni ukrepi blokad dejansko dosežejo le majhen delež internetnih uporabnikov, medtem ko ponudnikov spornih vsebin (imetnikov spletnega mesta) bistveno ne omejujejo pri nezakonitem dejanju. Zato je vprašljivo, ali je odreditev take blokade sploh primeren ukrep za dosego zastavljenih ciljev.

Kljub temu se najverjetneje ne moremo izogniti dejstvu, da blokade so in bodo vse pogostejši ukrep tudi v prihodnje.[53] Ob tem se je treba zavedati, da čeprav gre pri blokadah za izrazito tehnične posege v internetno infrastrukturo, se z njimi posega v nekatere temeljne človekove pravice, povezane z uporabo interneta. Zato je nujno in primerno, da je odrejanje tovrstnih ukrepov v pristojnosti sodišč, da se odrejajo upoštevaje načelo sorazmernosti in učinkovitosti, da so tehnične formulacije naloženih ukrepov točne in jasne ter da so postopki in procesna pravila glede ravnanja posameznih akterjev, ki so ključni za izvedbo blokade, vnaprej predvideni in določeni.

DNS je bil razvit pred več kot tridesetimi leti, mnogo preden je bilo mogoče napovedati eksponentno rast uporabe, števila storitev in pomena interneta. V osnovi je bil zasnovan kot enostaven, robusten, zanesljiv in skalabilen sistem, katerega osnovna funkcija je preslikava med domenami in IP-naslovi, zaradi česar ni primerno orodje za preprečevanje dostopa do spletnih vsebin in storitev ter ne bi smel biti uporabljen kot nevtralno orodje za obravnavo nezakonitih spletnih vsebin.

---

[52] Glej mednarodne študije: *A Comparative Study on Blocking, Filtering and Take-down of Illegal Internet Content* 2017; Callanan in dr. 2009; Poort in dr. 2014.

[53] Prizadevanja za odstranitev nezakonite vsebine in razprave v javnosti so bili večinoma osredotočeni na odgovornost digitalnih posrednikov, kot so ponudniki internetnih storitev, ponudniki gostovanja in spletne strani s torrenti. Njihovo pravno vlogo in odgovornost je dobro preučila tuja in domača pravna stroka, medtem ko je sistem domenskih imen v pravni literaturi manj prisoten. Registri domen v preteklosti niso bili predmet vsebinskih razprav o odgovornosti, povezava domen z nezakonito vsebino pa je pojav, ki do pred kratkim ni bil zelo aktualen. O tem glej Schwemer 2018.

Literatura

A Comparative Study on Blocking, Filtering and Take-down of Illegal Internet Content. Swiss Institute of Comparative Law, 2017, <https://edoc.coe.int/en/internet/7289-pdf-comparative-study-on-blocking-filtering-and-take-down-of-illegal-internet-content-.html> (10. 4. 2018).

BOŽIČ, Gorazd. Blokiranje tujih spletnih igralnic. V: Simič, N., in dr., *Telekomunikacije in zasebnost: zbornik referatov*. Ljubljana: Elektrotehniška zveza Slovenije, 2012, str. 56–58.

CALLANAN, Cormac, in dr. *A Study on Internet blocking, balancing cybercrime responses in democratic societies*, 2009, <http://www.aconite.com/sites/default/files/Internet_blocking_and_Democracy.pdf> (10. 4. 2018).

CENTR. *Domain conflicts and the legal system*, 2012, <https://www.centr.org/library/library/policy-document/centr-paper-domain-conflicts-and-the-legal-system.html> (15. 5. 2017).

DAMJAN, Matija. Dostop do interneta kot temeljna pravica. V: Ahtik, Meta, in dr., *Pravo v informacijski družbi*. Ljubljana: IUS Software, GV Založba, 2014, str. 321–332.

FANGFEI WANG, Faye. *Site-blocking Orders in the EU: Justifications and Feasibility*. 14th Annual Intellectual Property Scholars Conference (IPSC), Boalt Hall School of Law, University of California, Berkeley, 7-8 August 2014, <https://www.law.berkeley.edu/files/Wang_Faye_Fangfei_IPSC_paper_2014.pdf > (6. 4. 2018).

FEILER, Lukas. Website Blocking Injunctions under EU and U.S. Copyright Law - Slow Death of the Global Internet or Emergence of the Rule of National Copyright Law?. *TTLF Working Paper*, 2012, št. 13.

KLEMENČIČ, Goran, in dr. Internet in človekove pravice. V: Bogataj Jančič, Maja, in dr., *Pravni vodnik po internetu.* Ljubljana: GV Založba, 2007, str. 361–395.

LODDER, Arno R., POLTER, Puck. ISP blocking and filtering: on the shallow justification in case law regarding effectiveness of measures. *EJLT*, 2017, letn. 8, št. 2, str. 1–16.

Perspectives in Internet Content Blocking: An Overview. Internet Society, 2017, <https://www.internetsociety.org/resources/doc/2017/internet-content-blocking/> (6. 4. 2018).

POORT, Joost, in dr. Baywatch: two Approaches to Measure the Effects of Blocking Access to The Pirate Bay. *Telecommunications Policy*, 2014, letn. 38, št. 4, str. 383–392.

POVŠE GOLOB, Barbara, ZWITTNIG, Benjamin. DNS kot kritična infrastruktura. V: Simič, N., in dr., *Telekomunikacije in zasebnost: zbornik referatov*. Ljubljana: Elektrotehniška zveza Slovenije, 2015, str. 24–27.

POVŠE GOLOB, Barbara, DROFENIK, Maša. Ali sta blokiranje in preusmerjanje domen res primerna ukrepa za preprečevanje dostopa do spletnih vsebin. *Pravna praksa*, 2017, leto 36/1294, št. 22, str. 18–20.

"Site Blocking" to reduce online copyright infringement: a Review of Sections 17 and 18 of the Digital Economy Act. Ofcom, 2010, <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/78095/Ofcom_Site-Blocking-_report_with_redactions_vs2.pdf> (28. 3. 2018).

SCHWEMER, Sebastian Felix. On Domain Registries and Website Content: Shift in Intermediaries' Role in Light of Unlawful Content or just another Brick in the Wall?. *International Journal of Law and Information Technology*, 2018, letn. 26, št. 4, str. 273–293, <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3107547> (19. 10. 2018).

TOMŠIČ, Matic. *VPN: Kaj je, zakaj ga potrebujete in kateri je najboljši*, 2017, <https://siol.net/digisvet/nasveti/vpn-kaj-je-zakaj-ga-potrebujete-in-kateri-je-najboljsi-443626> (28. 3. 2018).