Registri domenskih imen in spletne vsebine

Združenje evropskih nacionalnih registrov vrhnjih domenskih imen

Vsebina

Povzetek

Člani združenja CENTR so nacionalni registri vrhnjih domen (ccTLD), ki upravljajo domene najvišje ravni. Njihove odgovornosti segajo od zagotavljanja in upravljanja s tehnično infrastrukturo sistema domenskih imen (DNS) za njihovo vrhnjo domeno (TLD), organiziranja postopka registracije domenskega imena, pa vse do vzdrževanja podatkovne baze registra, da je mogoče z uporabo domenskih imen navigirati po internetu.

Zlonamerne in nezakonite vsebine zmanjšujejo zaupanje v internet kot platformo za inovacije, ustvarjalnost in gospodarske priložnosti. Nacionalni registri vrhnjih domen (ccTLD) si prizadevajo za celovit in učinkovit pristop v boju proti nezakonitim spletnim vsebinam.

Internet je globalna zbirka medsebojno povezanih računalniških omrežij, ki omogoča komunikacijo z uporabo edinstvenih številskih IP-naslovov. Sistem domenskih imen (DNS) deluje kot vrhnji sloj IP-infrastrukture. Domenska imena ljudem lajšajo navigacijo po internetu. Na primer, ko uporabnik vpiše domensko ime spletnega mesta, bo sistem DNS uporabnikovi napravi sporočil, kakšen je ustrezni IP-naslov, na katerem je mogoče najti vsebino spletnega mesta.

Da je vsebina dosegljiva prek interneta, mora biti shranjena na vsaj enem računalniku ali strežniku, ki je povezan z internetom. Če želite učinkovito odstraniti vsebino z interneta, jo je treba izbrisati iz naprave, na kateri gostuje, ali pa je treba prekiniti povezavo te naprave z internetom.

Označitev vsebine kot "nezakonite" je odvisna od nacionalnega pravnega okvirja in se lahko celo razlikuje glede na kontekst. Na nacionalni ravni je določeno, kdo je pristojen za presojanje o tem.

Odstranjevanje nezakonitih vsebin z interneta je edini učinkovit način za preprečevanje dostopa in ogleda vsebine. Dve strani imata neposreden dostop do vsebine ali naprave, na kateri je shranjena vsebina: ponudnik vsebine in ponudnik gostovanja. Najprej je treba vzpostaviti stik z njima.

Kadar se domensko ime uporablja za omogočanje dostopa do vsebine, je lahko nosilec domene ponudnik vsebine in ponudnik gostovanja ali pa lahko nosilec domene ponudnika vsaj identificira. Podatkovna zbirka registra z informacijami o vseh domenskih imenih, registriranih pod vrhnjo domeno, lahko pomaga identificirati nosilca domene in vzpostaviti stik z njim.

Kadar nezakonite vsebine ni mogoče odstraniti z interneta, kar je edina učinkovita rešitev, lahko poskusimo uporabnikom otežiti iskanje ali dostopanje do vsebine. Obstajajo različni načini "blokiranja" internetnih vsebin na različnih ravneh in vključujoč različne akterje. Vsem pa je skupno to, da vsebina ostaja dosegljiva in da lahko dejanje povzroči nenamerno postransko škodo. Zato jih je treba obravnavati kot začasni ukrep v nujnih primerih, ko so bili vsi drugi načini že preizkušeni in so se izkazali za neuspešne. Blokiranje ali izbris domenskega imena je eden od tovrstnih ukrepov.

Nacionalni pravni okviri določajo, katera vsebina je nezakonita, kdo je pooblaščen za njeno obravnavo in kateri postopki so dovoljeni v skladu s pravno ureditvijo. Pri tem lahko prihaja do razhajanj od države do države. Nacionalni registri vrhnjih domen (ccTLD) imajo namreč različne zahteve glede tega, kdo lahko registrira domene in katere so njihove dolžnosti. Kombinacija teh zahtev in nacionalnega pravnega okvirja vpliva na to, kakšne politike in pobude lahko razvije register, ko pristopi k reševanju vprašanja nezakonitih spletnih vsebin.

Običajno so te politike izvirajo iz lokalne skupnosti in so skladne z nacionalnimi zakoni ter naslavljajo nacionalne potrebe, pri čemer so pogosto plod posvetovanja in sodelovanja z drugimi lokalnimi zainteresiranimi stranmi. Uspešne politike in prakse enega nacionalnega registra so lahko navdih tujim. Vendar pa zaradi lokalnega izvora in posebnosti ni nobenega zagotovila, da bo kopiranje projekta ali politike privedlo do enakega pozitivnega rezultata ali da bo sploh zakonito v sklopu drugega nacionalnega registra.

Kot pristop k nezakonitim vsebinam se nacionalni registri vrhnjih domen (ccTLD) med drugim osredotočajo na:

- Izobraževanje in osveščanje na ravni celotne skupnosti.
- Izobraževanje in tesno sodelovanje z organi in s službami kazenskega pregona.
- Vzdrževanje podatkovne baze registra za izboljšanje kakovosti registracijskih podatkov WHOIS ima lahko posredno pozitiven vpliv, saj je malo verjetno, da bi osebe s slabimi nameni registrirale domensko ime z uporabo resničnih osebnih podatkov.
- Vzpostavitev postopkov za izmenjavo registracijskih podatkov s tretjimi osebami v mejah nacionalnih predpisov o varovanju zasebnosti.
- Razvijanje procesov in postopkov za odzivanje na poročila o sumljivih vsebinah. Ti postopki imajo običajno skupno to, da se uporabljajo v omejenih in natančno opredeljenih primerih ter da je vanje vključen zunanji svetovalec s strokovnim znanjem na področju presojanja tovrstnih vsebin.

Uvod

Člani združenja CENTR upravljajo register za eno ali več nacionalnih vrhnjih domen (ccTLD). Njihove odgovornosti segajo od zagotavljanja in upravljanja tehnične infrastrukture sistema DNS za njihovo vrhnjo domeno, organiziranja postopka registracije domenskega imena pa vse do proaktivnega vzdrževanja podatkovne baze registra, da je mogoče z uporabo domenskih imen navigirati po internetu.

Člani združenja CENTR menijo, da sta zaupanje in varnost na spletu bistvenega pomena za ohranjanje interneta kot platforme za inovacije, ustvarjalnost in iskanje gospodarskih priložnosti. Zlonamerne in nezakonite vsebine načenjajo to zaupanje. Registri so zavezani, da skupaj z drugimi akterji prispevajo k celovitemu in učinkovitemu pristopu pri boju proti nezakonitim vsebinam na internetu.

Cilj prispevka

Skupna prizadevanja in uspešno sodelovanje zahtevajo, da zainteresirane strani razumejo in spoštujejo funkcijo, vlogo in omejitve drugih. Cilj tega prispevka je osvetliti vlogo upravljavca nacionalnega registra vrhnje domene (ccTLD), razložiti njegov odnos do spletnih vsebin, raziskati možnosti in omejitve ukrepov ter določiti pričakovanja glede tega, kaj register lahko in česa ne more narediti na področju nezakonitih spletnih vsebin.

Opis prispevka

Prvi del prispevka ponuja vpogled v delovanje interneta, vsebuje razlago o tem, kje se nahaja spletna vsebina in kako do nje dostopamo, ter pojasni vlogo sistema domenskih imen (DNS).

Drugi del prispevka obravnava problematiko nezakonitih vsebin na internetu in preučuje, kako bi lahko upravljavci registrov ccTLD prispevali pri odstranjevanju nezakonitih vsebin.

Tretji del je posvečen sedanjim politikam in praksam registra. Prikazuje, kako različni nacionalni registri razvijajo politike in sprejemajo ukrepe, ki najbolje služijo potrebam lokalnih skupnosti, in tako prispevajo k skupnemu boju proti nezakonitim spletnim vsebinam.

Internet, sistem domenskih imen in spletna vsebina

DNS kot del internetne infrastrukture

Internet in IP-infrastruktura

Internet je zbirka računalniških omrežij, ki so medsebojno povezana, kot celota pa tvorijo globalni komunikacijski sistem. Internetni protokol (IP) je metoda ali niz pravil, v skladu s katerimi se podatki prek interneta pošiljajo iz ene naprave v drugo. Za uspešen prenos je pomembno, da je mogoče pošiljatelja in prejemnika identificirati in locirati v večmilijonski množici računalnikov, pametnih telefonov, strežnikov, internet stvari in drugih naprav, ki so povezane z internetom. Zato ima vsaka povezana naprava vsaj en IP-naslov, ki omogoča njeno prepoznavo v množici drugih naprav. IP-naslov je lahko predstavljen kot številčna oznaka[1]: na primer IP-naslov 2001:db8:85a3::8a2e:370:7334[2] lahko prepozna vmesnik strežnika, na katerem je shranjena vsebina spletnega mesta.

Sistem domenskih imen

Ljudje le s težavo beremo in si zapomnimo številčne IP-naslove. Sistem domenskih imen (DNS) zadevo reši tako, da omogoča uporabo domenskih imen za sklicevanje na IP-naslove. DNS deluje kot vrhnji sloj IP-infrastrukture. Ko uporabnik v brskalnik vpiše domensko ime ali klikne na povezavo z domenskim imenom, bo naprava poiskala ustrezen IP-naslov v sistemu DNS. Ko se ime domene razreši - "razreši" pomeni, da sistem DNS vrne IP-naslov - uporabnikova naprava ve, kje na internetu je mogoče najti vsebino spletnega mesta ali nabiralnik, povezan z e-poštnim naslovom.

Za sistem DNS je značilna hierarhična struktura, sestavljena iz različnih vrhnjih domen (TLD) pod enim samim korenom. Razširitev domenskega imena, torej dela, ki sledi zadnji piki, nakazuje, pod katero vrhnjo domeno (TLD) je ime registrirano (na primer .de, .com, .fr). Hierarhična struktura je pomembna za delovanje sistema DNS in iterativni način iskanja domenskih imen.[3]

Register domenskih imen je odgovoren za upravljanje ene ali več vrhnjih domen (TLD). Vsi registri morajo spoštovati tehnična pravila in zahteve sistema DNS, kar pa zadeva politike delovanja, je vsaka vrhnja domena odgovorna za določitev svojih pravil. Medtem ko morajo generične vrhnje domene (gTLD) upoštevati splošne politike in procese, ki jih je razvila skupnost ICANN, pa nacionalne vrhnje domene (ccTLD) določajo svojo politiko v skladu s potrebami lokalnih internetnih skupnosti.

1 Naslovi IPv6 so dolgi 128 bitov in prikazani v šestnajstiškem nizu, starejša različica IPv4 je dolga 32 bitov in zapisana v skupinah decimalnih števil, ločenih s pikami.

2 Ta IP-naslov služi zgolj za namene dokumentiranja in ni usmerjen v javni internet (RFC 3849, dokumentacijska predpona IPv6).

3 Za več informacij o delovanju sistema DNS obiščite: https://www.centr.org/education/the-dns.html.

Spletne vsebine

Vsebino je treba ustvariti, shraniti in omogočiti dostop do nje, še preden jo je mogoče najti na internetu. Ta postopek je opisan v naslednjem razdelku z opredelitvijo različnih vlog in odgovornosti[4].

Omogočanje dostopa do vsebin na spletu

Ponudnik vsebin

Ponudnik vsebin oskrbuje internet z besedili, zvokovnim gradivom, s slikami, z video posnetki, animacijami in drugimi oblikami vsebin, ki so naložene na spletno mesto, objavljene na blogu, deljene na družbenih platformah itd. Ponudnik vsebin je lahko izvirni ustvarjalec vsebin, vendar to ni nujno.

Da je določena vsebina dosegljiva prek interneta, mora biti shranjena na vsaj enem računalniku ali strežniku, ki je povezan z internetom. Ponudnik vsebin lahko uporablja svoj računalnik ali strežnik ali, bolj verjetno, uporablja storitve in infrastrukturo ponudnika gostovanja.

Ponudnik gostovanja

Ponudnik gostovanja omogoča shranjevanje in povezljivost, ima tehnično znanje in, kar je še pomembneje, potrebno infrastrukturo, zmogljivost in pasovno širino za spoprijemanje s prometom, ki lahko kadar koli pride od koder koli na internetu. Ponudniki gostovanja zagotavljajo platformo za gostovanje vsebin, vendar pa ne odločajo, kaj je objavljeno ali kaj ni - to počnejo njihove stranke (ponudniki vsebin). Z nekaj izjemami, običajno velike organizacije z lastno infrastrukturo in omrežji, ponudniki vsebin uporabljajo storitve ponudnika gostovanja. Ponudniki gostovanja imajo velika podatkovna središča s strežniki, na katerih je shranjena vsebina njihovih strank. Ti strežniki so povezani z internetom in jih je mogoče prepoznati po edinstvenem IP-naslovu. Obstajajo različne vrste gostovanja; najpogostejši sta spletno gostovanje in gostovanje e-pošte. Gostovanje družbenih medijev (npr. videoposnetki, ki jih ustvarjajo uporabniki) lahko obravnavamo kot poseben primer med objavo in gostovanjem.

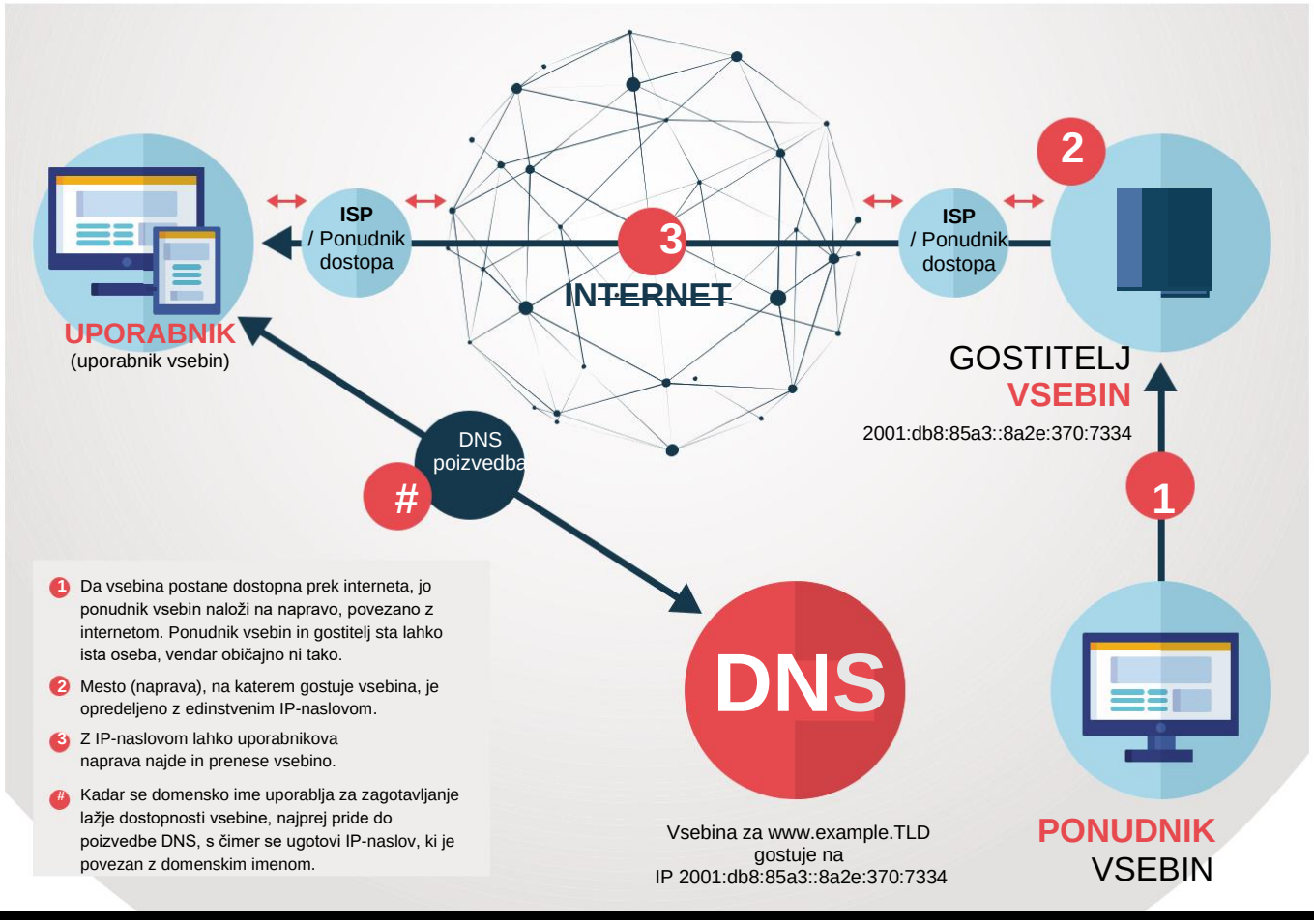
Ponudnik internetnih storitev/Ponudnik dostopa

Ponudnik internetnih storitev (ISP) zagotavlja dostop do interneta. Njegovi odjemalci lahko prek omrežja in infrastrukture ponudnika dostopajo do interneta. Ponudnik internetnih storitev bo dodeli IP-naslove napravam, ki so povezane v njegovo omrežje, na primer strežnikom ponudnika gostovanja, modemom internetnega uporabnika itd. Ponudnik internetnih storitev kot ponudnik dostopa ne shranjuje nobene vsebine, čeprav vsebina potuje prek njegove infrastrukture.

Obstajajo drugi akterji, ki zagotavljajo prenos in izmenjavo podatkov med omrežji, na primer stičišča omrežij (IXP), operaterji (krajših ali daljših) omrežnih infrastruktur ali omrežja za dostavo vsebin (CDN)[5], ki gostijo kopije vsebin svojih strank na strežnikih na različnih geografskih lokacijah, s čimer optimizirajo izkušnjo končnega uporabnika (na primer Cloudflare). Njihovega odnosa do vsebin v nadaljevanju ne bomo več obravnavali.

4 Akterji lahko združujejo eno ali več vlog, opisanih v tem razdelku, na primer ponudnik internetnih storitev lahko ponuja tudi storitve gostovanja.

5 https://en.wikipedia.org/wiki/Content_delivery_network



Uporaba DNS kot orodja za iskanje vsebine

Sistem domenskih imen (DNS) zagotavlja funkcijo, ki pomaga "krmariti" po internetu in omogoča iskanje IP- naslova, povezanega z domenskim imenom. Prav zato nekateri primerjajo sistem DNS s telefonskim imenikom ali z registrom nepremičnin ali podjetij[6].

Imetnik domenskega imena/nosilec domene

Ponudnik vsebine lahko registrira domensko ime, da internetnim uporabnikom olajša dostop do vsebine, ki jo je ponudil prek spleta. Domensko ime deluje kot oznaka IP-naslova, pri čemer si ga je lažje zapomniti kot številčni IP-naslov in lahko vsebuje koristne informacije, na primer ime podjetja v e-poštnem naslovu ali pa se domensko ime nanaša na vsebino spletne strani.

Imetnik domenskega imena ni nujno ponudnik vsebine (ali edini ponudnik vsebine), objavljene pod domenskim imenom. Na primer spletne strani univerz, spletne strani z blogi ali spletne strani družbenih omrežij omogočajo drugim, da objavijo vsebino na spletni strani, ki je prepoznavna po enem samem domenskem imenu.

Imetnik domenskega imena ali nosilec domene ima pravico do uporabe določenega domenskega imena. Za pridobitev te pravice posameznik ali pravna oseba registrira ime pri nacionalnem registru, bodisi neposredno ali prek registrarja. Nosilec domene je odgovoren za uporabo imena.

6 https://en.wikipedia.org/wiki/Domain_Name_System

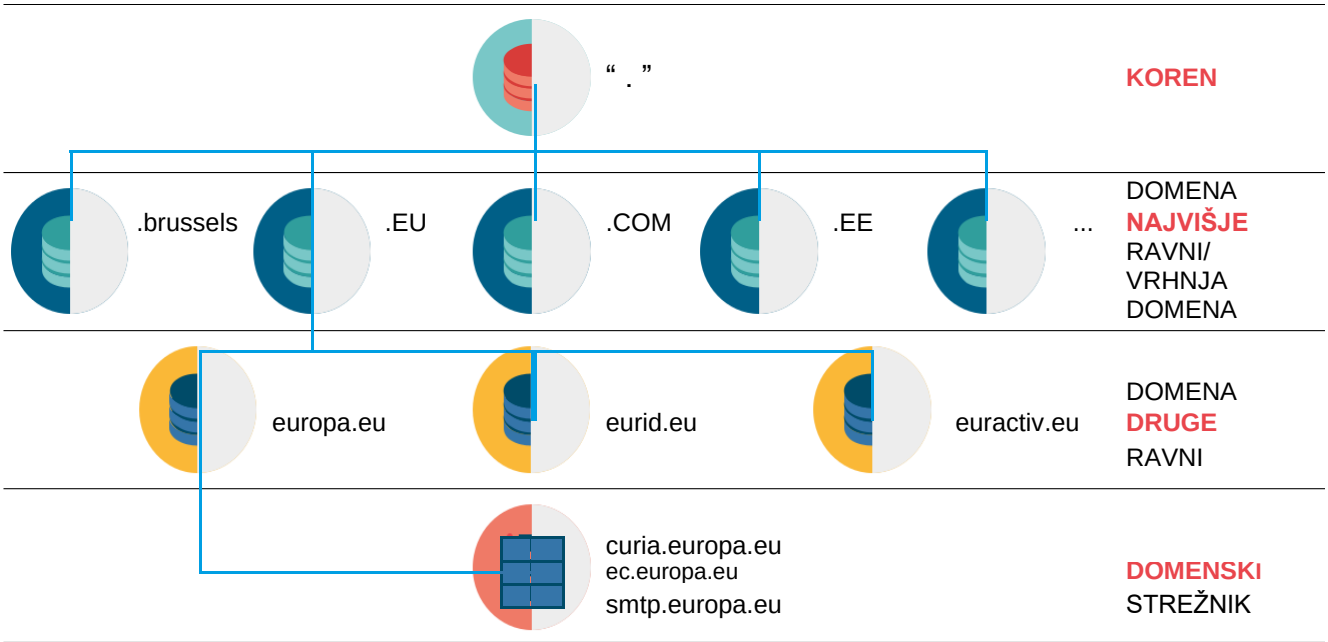
Registrar

Registrar je podjetje, ki pravnim osebam in posameznikom neposredno ali prek mreže preprodajalcev ponuja storitve registracije domen. Registrar je akreditiran s strani enega ali večih registrov za ponujanje domenskih imen pod določeno vrhnjo domeno (TLD). Registrar bo preveril razpoložljivost domenskega imena in vodil postopek registracije, medtem ko register upravlja vrhnjo domeno (TLD) zahtevanega imena. V okviru postopka registracije bo registrar predložil kontaktne podatke imetnika domene in tehnične podatke, povezane z domenskim imenom (na primer kateri imenski strežniki vsebujejo zapise DNS, ki bodo spletnim brskalnikom in e-poštnim odjemalcem povedali, kje naj najdejo spletni strežnik z vsebino spletnega mesta ali e-poštni strežnik, ki obdeluje e-pošto). Registrar ne gosti vsebine in nobena vsebina ne prehaja prek njegove infrastrukture. V praksi pa številni registrarji svojim strankam nudijo tudi gostovanje in druge storitve.

Register vrhnje domene

Register upravlja eno in edino verodostojno bazo domenskih imen, registriranih pod vrhnjo domeno (TLD), in te podatke objavlja v sistemu DNS. Strežniki registra domen vsebujejo podatke o imetniku domene, registraciji domene (na primer datum poteka), IP-naslove, povezane z domenskim imenom, in druge tehnične podrobnosti. Register večkrat na dan objavi posodobljeno območno DNS datoteko, pri čemer gre za besedilno datoteko, ki vsebuje povezave med domenskim imenom in lastnimi imenskimi strežniki za vsako registrirano ime ter druge vire. Ta datoteka vsebuje informacije o tem, kako najti IP-naslove in druge podatke, ki so potrebni za navigacijo po internetu. Registri ne hranijo vsebin in jih ne spreminjajo.

> Opomba: Večina ponudnikov internetnih storitev predpomnilniško shranjuje DNS-podatke o nedavnih poizvedbah po domenskih imenih iz različnih vrhnjih domen v tako imenovanih neavtoritativnih imenskih strežnikih, da pospešijo brskanje za svoje stranke. DNS-poizvedba bo opravljena, če strežnik ponudnika internetnih storitev ne bo ponudil nedavnega odgovora. Posledično lahko traja nekaj časa, preden spremembe v sistemu DNS (na primer, ko register odstrani domensko ime iz sistema DNS) obveljajo povsod na internetu.



Drevesna struktura sistema domenskih imen (DNS)

Ukrepanje proti nezakonitim vsebinam na internetu

Kaj je nezakonita vsebina?

Definicija znotraj nacionalnih pravnih okvirjev

Izraz "nezakonita vsebina" se uporablja za opis vsebine, ki je prepovedana v nacionalnem okviru iz kakršnega koli razloga. Evropska komisija, na primer, nezakonito vsebino opredeljuje kot "vse informacije, ki niso skladne s pravom Unije ali zakonodajo zadevne države članice."[7] Z izjemo vprašanj, povezanih s spolno zlorabo otrok, ni splošnega mednarodnega soglasja o tem, kaj je ustrezna vsebina z vidika javnega reda. Kar je dovoljeno znotraj ene jurisdikcije, je lahko prepovedano znotraj druge. Dopustnost vsebine je lahko odvisna tudi od konteksta: vsebina, ki se v nekem kontekstu presodi kot nezakonita (na primer nespodobna komedija, ki jo gledajo otroci), je lahko sprejemljiva v drugem (ko jo gledajo odrasli), in to celo znotraj enejurisdikcije.[8]

Nekatere države so vzpostavile ciljno usmerjen pravni okvir za spletne vsebine, medtem ko v drugih jurisdikcijah vprašanja o spletnih vsebinah obravnavajo na podlagi obstoječih splošnih okvirov, ki niso specifični za internet. S primerjalno študijo v 47 državah članicah Sveta Evrope so izluščili štiri široke kategorije pravnih podlag za presojanje zakonitosti spletnih vsebin:

- varovanje zdravja in morale (vključno s spolno zlorabo otrok ali nezakonitimi igrami na srečo);
- zaščita nacionalne varnosti, ozemeljske celovitosti ali javne varnosti (vključno s protiterorizmom);
- varstvo pravic intelektualne lastnine; in
- zaščita pred obrekovanjem in nezakonitim ravnanjem z osebnimi podatki.[9]

Kdo lahko presoja o zakonitosti vsebine?

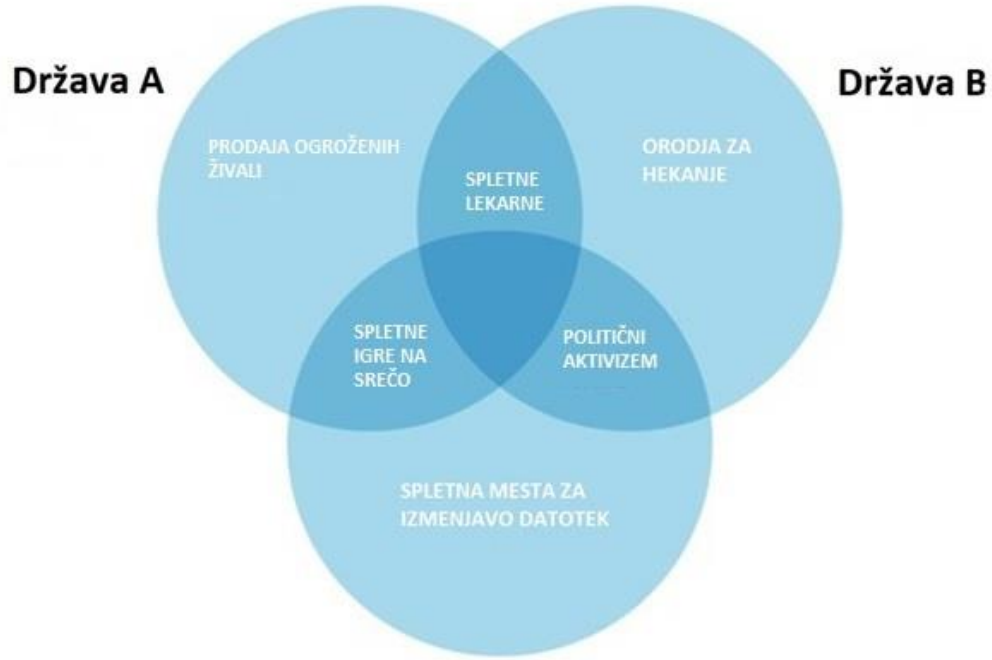
Označitev vsebine kot "nezakonite" je odvisna od nacionalnega pravnega okvirja in se lahko celo razlikuje glede na kontekst. Ali je vsebina nezakonita ali ne, je odločitev nacionalnih sodišč ali pristojnih organov. Poleg tega se lahko postopek razlikuje celo znotraj iste jurisdikcije. Nekateri organi so lahko pooblaščeni za presojo zakonitosti vsebine in neposredno ukrepanje na podlagi te presoje, medtem ko morajo drugi organi pridobiti sodno odločbo, na podlagi katere lahko ukrepajo glede vsebine.

---

7 *Commission Recommendation of 1.3.2018 on measures to effectively tackle illegal content online*, C(2018)1177, European Commission, March 2018, https://ec.europa.eu/digital-single-market/sl/news/commission-recommendation-measures-effectively-tackle-illegal-content-online

8 *Internet Society Perspectives on Internet Content Blocking: An Overview,* Internet Society, March 2017, https://www.internetsociety. org/wp-content/uploads/2017/03/ContentBlockingOverview.pdf

9 *Comparative study on blocking, filtering and take-down of illegal Internet content,* CEO, December 2015, https://www.coe.int/en/web/freedom-expression/study-filtering-blocking-and-take-down-of-illegal-content-on-the-internet (dostop 7. junija 2018).



Vennov diagram, ki prikazuje, da je v določenih državah nekaj zakonito, v drugih pa ne

Ponudnik vsebin je odgovoren za vsebine, ki so dostopne drugim uporabnikom interneta. Nosilec domene je dolžan poskrbeti, da se njegovo oz. njeno domensko ime ne uporablja za lažje iskanje nezakonitih vsebin na internetu. Kar še dodatno zaplete zadevo je, dani nujno, da sta ponudnik in uporabnik vsebine znotraj iste jurisdikcije. Poleg tega bi lahko vsebina gostovala še v nekem tretjem geografskem območju z lastnimi zakoni, moralo in definicijami, kaj je zakonito in kaj ne.

Nacionalni register vrhnje domene (ccTLD) je glede spletnih vsebin v istem položaju kot katera koli organizacija ali celo posameznik. Poda lahko oceno in oblikuje mnenje o tem, kaj je znotraj in kaj zunaj zakonskih omejitev. Nima pa posebnega pooblastila za učinkovito presojo o zakonitosti vsebine, ki je objavljena na spletu. Ko register dostopa do spletnih vsebin, to naredi enako kot kateri koli posameznik, ki med brskanjem po internetu dostopi do spletnega mesta in naloži vsebino na svoj računalnik. Ni bližnjice, ki bi registru omogočala vpogled v vsebine, ki jih objavijo imetniki domene. Registri ne gostijo nobenih vsebin in te ne prehajajo prek njihove infrastrukture.

Nekateri registri predvidijo možnost ukrepanja v očitnih primerih nezakonitih vsebin, kjer ni posebnega dvoma, tveganje v povezavi z odgovornostjo pa je glede na njihove splošne pogoje minimalno. Na splošno registri nimajo ustreznih sredstev in osebja ter kot taki niso v položaju, ki bi omogočal proaktivno brskanje po internetu z namenom iskanja nezakonitih vsebin.

Kje se nahajajo spletne vsebine?

Lokacija na internetu

Da je vsebina dosegljiva prek interneta, mora biti shranjena na vsaj enem računalniku ali strežniku, ki je povezan z internetom. Lokacija vsebine je določena z edinstvenimi IP-naslovi v napravah,[10] na katerih je shranjena.

10 S tehničnega vidika IP-naslov identificira vmesnik, prek katerega naprava izmenjuje informacije, ne pa naprave same kot take.

Fizična lokacija

Naprave, ki vsebujejo vsebino, je mogoče geografsko izslediti v katerem koli delu sveta, ki je oskrbovan z elektriko in ima povezavo z internetom. Sicer pa ni nobenih drugih strogih pravil ali zahtev glede tega, kje naj bi vsebina gostovala s tehničnega vidika, čeprav lahko fizična lokacija vpliva na hitrost in kakovost povezave.

Vsebino je mogoče shraniti na enem samem strežniku ali pa gostuje na različnih strežnikih (na primer gostovanje v oblaku, gostovanje v gručah). Vsebina je lahko na enem ali več strežnikih v isti državi kot ponudnik vsebin in uporabnik vsebin. Ti strežniki so lahko tudi kjer koli drugje na svetu in so podvrženi pravilom različnih jurisdikcij.

Odstranjevanje nezakonitih vsebin

Odstranjevanje nezakonitih vsebin z interneta je edina učinkovita rešitev, ki preprečuje dostop do vsebin in njihovo uporabo. To se lahko doseže tako, da se izbriše vsebine z naprave, na kateri so shranjene, ali pa se prekine povezavo te naprave z internetom.

Vzpostavitev stika s ponudnikom vsebin ali s ponudnikom gostovanja

Dve strani imata neposreden dostop do vsebine ali naprave, na kateri je shranjena vsebina: ponudnik vsebin in ponudnik gostovanja. Ponudnik vsebin ima orodja in dostopna gesla za spreminjanje ali odstranjevanje vsebine, ki jih je postavil na spletno mesto, objavil na platformi družbenih medijev ali drugje. Ponudnik gostovanja lahko odstrani vsebine s svojih strežnikov ali znotraj same infrastrukture učinkovito prepreči dostop do vsebin.

Treba je opozoriti, da ponudniki gostovanja običajno shranjujejo vsebine različnih strank na isti fizični napravi, zato lahko odklop ali zaseg strežnika vpliva na različne ponudnike vsebin in prepreči dostop do zakonitih vsebin. Upravljavci družbenih omrežij in blogov lahko imajo možnost odstranitve spornih objav ali nezakonitih vsebin na svojih platformah.

Vzpostavitev stika z nosilcem domenskega imena

Nosilec domene je prvi, na kogar se obrnemo, če se domensko ime uporablja za dostop do nezakonitih vsebin. Nosilec domene je lahko tudi ponudnik vsebine ali pa je s slednjim lahko v tesnem stiku. Nosilec mogoče ni izvirni ustvarjalec nezakonitih vsebin ali pa se ne zaveda, da se njegovo domensko ime uporablja za dostop do nezakonitih vsebin[11]. Vendar pa naj bi bil nosilec v večini primerov sposoben pomagati določiti vir nezakonitih vsebin in tudi ukrepati, da se le-ta odstrani .

Register vzdržuje verodostojno zbirko podatkov z informacijami o vseh domenskih imenih, registriranih pod njegovo vrhnjo internetno domeno (TLD), in lahko pomaga pri prepoznavi nosilca domene ter navezovanju stika z njim. Zbirka podatkov registra med drugim vsebuje, , podatke o nosilcu domene, registraciji domene (npr. datum poteka) in imenskih strežnikih, ki se nanašajo na domensko ime.

Nacionalni registri vrhnjih domen (ccTLD) vlagajo veliko truda v vzdrževanje svojih podatkovnih zbirk in sprejemajo upravičene zahteve po razkritju informacij. Vzpostavitev stika z registrom z namenom pridobitve informacij o nosilcu domene je lahko prvi korak v postopku učinkovite odstranitve nezakonitih vsebin z interneta. Več o tem v razdelku III, v katerem so predstavljene trenutne prakse registrov.

Opomba: Nemara bi bilo smiselno, da organi kazenskega pregona in drugi pristojni nadzorni organi navežejo stik z registrarji, saj bodo slednji mogoče lahko zagotovili dodatne koristne informacije, denimo podatke o računih ali kreditnih karticah, pa tudi podatke o tem, katere druge domene je registrirala ista stranka itd.

11 Na primer ob velikih univerzitetnih omrežjih ali platformah družbenih medijev, kjer veliko uporabnikov objavlja vsebine, ali kadar je strežnik zlorabljen in ga zločinci uporabljajo za gostovanje vsebin.

Omejevanje dostopa do spletnih vsebine

Nadaljnji ukrepi, ko je izbris nezakonitih vsebin neuspešen

Kadar ponudnika vsebin ali ponudnika gostovanja ni mogoče izslediti ali z njim vzpostaviti stika z namenom odstranitve nezakonitih vsebin z interneta, kar je edina učinkovita rešitev, lahko poskusimo uporabnikom otežiti iskanje ali dostop do vsebin. Obstajajo različni načini blokiranja internetnih vsebin na različnih ravneh in z vključevanjem različnih akterjev. Poročilo organizacije Internet Society iz leta 2017[12] opisuje najsodobnejše metode in ocenjuje njihovo učinkovitost. V prispevku je obravnavano blokiranje na podlagi IP-naslova in internetnega protokola, blokiranje na osnovi podrobnega pregleda paketov, blokiranje na podlagi URL-naslova, na osnovi platforme in na osnovi sistema DNS, in sicer na ravni omrežja ali ponudnika internetnih storitev. V zaključku poročila je ugotovljeno, da ne glede na raven in metodo, je "uporaba internetnega blokiranja za nezakonito vsebino na splošno neučinkovita, pogosto povsem neuporabna in nagnjena k povzročitvi nenamerne škode za internetne uporabnike." Blokiranje vsebin ne reši težave: vsebine ostanejo na voljo, zato je treba blokiranje obravnavati kot začasni ukrep v nujnih primerih ali ko so bili vsi drugi načini že preizkušeni in so se izkazali za neuspešne.

V tem prispevku se osredotočamo na dejanja, povezana z registrom domen, na primer, ko register prepreči, da bi domensko ime razrešilo veljaven IP-naslov, tako da začasno blokira domensko ime ali ga izbriše iz sistema DNS.

Tveganje in pomanjkljivosti pri izbrisu domenskega imena na nivoju registra

Blokiranje ali izbris domenskega imena in njegova odstranitev iz sistema DNS pomeni, da uporabnik pri iskanju domenskega imena ne bo več dobil veljavnega IP-naslova. Uporabnik bo namesto nalaganja pričakovanega spletnega mesta prejel sporočilo o napaki z obvestilom, da domensko ime ne obstaja[13].

Izbris ali blokiranje domenskega imena je dokaj enostavna tehnična operacija, ki pa predstavlja drastičen poseg v sistem DNS, zaradi katerega domenskega imena ni več mogoče uporabljati za navigacijo do vsebine (tako nezakonite kot zakonite), ki je objavljena pod domenskim imenom in različnimi poddomenami, pri čemer vse storitve, povezane z domenskim imenom, na primer e-pošta, prenehajo delovati. To se običajno zgodi v nekaj urah, zaradi predpomnjenja pa lahko traja tudi nekaj dni. Pred vsako odločitvijo o izbrisu ali blokiranju je treba pretehtati vse posledice ter upoštevati načeli preudarnosti in sorazmernosti. Uredba EU o sodelovanju na področju varstva potrošnikov (v veljavo je stopila januarja 2020) jasno določa, da se registrom naloži izbris domenskih imen le v primerih, "če ni na voljo nobene druge učinkovite poti, da se doseže prenehanje ali prepoved kršitve iz te uredbe, in da se prepreči nevarnost resnega oškodovanja kolektivnih interesov potrošnikov."[14]

Za izboljšanje zaupanja in varnosti so nekateri nacionalni registri vrhnje domene (ccTLD) na osnovi svojih nacionalnih zakonov in pristojnosti oblikovali postopke hitrega izbrisa ali deaktivacije domenskih imen, ki se uporabljajo v zločinske namene, s čimer so vzpostavili odnose z domačimi organi kazenskega pregona in/ali uglednimi varnostnimi podjetji ali nacionalnimi CERT-i. Za tovrstne odnose je običajno značilno medsebojno razumevanje postopanja in nadzora, saj se tako zagotovi, da so odločitve pravične in odgovorne. Kakšne ukrepe je mogoče sprejeti, je odvisno od nacionalnega okvira registra ter pravnih vprašanj in vprašanj glede odgovornosti v zvezi z obveščanjem tretjih strank.

12 Internet Society Perspectives on Internet Content Blocking: An Overview, Internet Society, March 2017, https://www.internetsociety.org/wp-content/uploads/2017/03/ContentBlockingOverview.pdf

13 Domain Conflicts in the Legal System, Norid, September 2017, https://www.norid.no/sl/domenekonflikter/rettslig-behandling/ veilinger/

14 Uredba (EU) 2017/2394 z dne 12. decembra 2017, ki je stopila v veljavo 17. januarja 2020. Člen 9/IV (g) https://eur-lex.europa.eu/legal-content/SL/TXT/PDF/?uri=CELEX:32017R2394&from=EN

V naslednjih odstavkih so obdelana določena tveganja in vprašanja, povezana z blokiranjem ali izbrisom domenskih imen.

Blokiranje ali izbris domenskega imena lahko oteži iskanje nezakonitih vsebin na internetu, vendar ne reši težave ali kaznivega dejanja, saj vsebina ostane na voljo tistim, ki jo želijo najti. Za povrh obstaja veliko tveganj in pomanjkljivosti. Ta so obravnavana v nadaljevanju.

Vprašljiva učinkovitost in lažni občutek varnosti, saj vsebine ostajajo na voljo

Blokiranje ali izbris domenskega imena ne odstrani nezakonitih vsebin z interneta. Vsebine ostajajo na voljo in do njih lahko dostopate neposredno z uporabo IP-naslova namesto domenskega imena. Tovrstno dejanje ni nobena znanost in že enostavna poizvedba v Googlu ponudi kopico razlag in videoposnetkov, ki prikazujejo, kako lahko do spletnega mesta dostopate prek IP-naslova. Če izbrišete domensko ime, boste zmanjšali verjetnost, da uporabniki po naključju naletijo na nezakonite vsebine, vendar pa ne boste ustavili tistih, ki aktivno iščejo tovrstne vsebine. "Zaradi internetne arhitekture lahko končni uporabniki zlahka zaobidejo blokiranje z domenskim imenom, zato je ukrep dolgoročno najverjetneje v veliki meri neučinkovit, kratkoročno pa prežet z nepričakovanimi posledicami."[15]

Poleg tega lahko ponudniki nezakonitih vsebin predvidijo blokiranje in sprejmejo previdnostne ukrepe za nadaljnje zmanjšanje učinka ukrepa. Ponudnik vsebin lahko na primer registrira več domenskih imen pod isto vrhnjo domeno (TLD) ali pod različnimi vrhnjimi domenami v različnih jurisdikcijah in poskrbi, da vsa vodijo na isti IP-naslov in posledično do istih vsebin. Hiperpovezave, ki se uporabljajo v e-poštnih sporočilih, na platformah ali spletnih straneh, se lahko neposredno povežejo z IP-naslovom brez uporabe sistema DNS.

Nevarnost preobsežnega blokiranja in postranske škode

Ko se domensko ime izbriše ali blokira, to vpliva na vse vsebine, ki so dosegljive pod domenskim imenom in poddomenami, kar vključuje tako domnevno nezakonito vsebino kot tudi vse druge vsebine. Če izbrišete domensko ime družbenega omrežja ali spletnega dnevnika, kjer lahko posamezni uporabniki objavljajo svoeo vsebine ali ustvarijo svoj osebni blog, boste vplivali na vse uporabnike, ne samo na tiste, ki so objavljali nezakonite vsebine, ampak tudi na vse ostale, ki so objavili svoje družinske slike, izrazili politično mnenje, podjetja, ki uporabljajo spletno stran za promocijo in e-poslovanje itd. Ko blokirate domensko ime, vse storitve, povezane z domenskim imenom, na primer e-pošta, takoj prenehajo delovati.

V izmišljeni študiji primera v prispevku "Domenski spori v pravnem sistemu" norveški register opisuje vpliv in posledice blokade domenskega imena Univerze v Oslu, potem ko je študent objavil nezakonite vsebine na spletni strani pod domeno univerze.[16]

Nevarnost izvajanja ukrepa v pretiranem obsegu in pogoste napake

Ker je blokiranje domenskih imen s tehničnega vidika enostavno, obstaja tveganje za prekomerno izvajanje tega ukrepa.[17] Cena napake je z vidika izvršitelja majhna, po drugi strani pa imajo napake lahko dramatičen vpliv na nosilca domene v primeru neupravičenega blokiranja njegove domene18. Na primer podjetje, ki posluje elektronsko, ima lahko blokirano spletno mesto ali pa se zgodi, da cela institucija nenadoma ni več dosegljiva po e-pošti.

> Opomba: obstajajo tudi druge oblike blokiranja ali poseganja v sistem DNS, na primer na ravni ponudnika internetnih storitev (ISP) ali na ravni registrarja. Večina teh ukrepov ima podobne pomanjkljivosti in večinoma jih je mogoče zaobiti. Noben ukrep blokiranja ne zagotavlja celovite rešitve, saj noben ne odstrani vsebin.

15 'SAC 056 - SSAC Advisory on Impacts of Content Blocking via the Domain Name System', SSAC, 9 October 2012.

16 Glej polje na strani 10, *Domenski spori v pravnem sistemu,* Norid, september 2017, https://www.norid.no/sl/domenekonflikter/rettslig-vendling/veileder/

17 'Notice and Takedown in the Domain Name System: ICANN's Ambivalent Drift into Online Content Regulation: (pp. 1379 - 1383) 18 Primer je opisan v naslednji objavi v spletnem dnevniku:
"*Main French Internet Provider Orange blocks traffic to Google',* Alix Guillard, 27.10.2016, https://en.blog.nic.cz/2016/10/27/french-orange-blocks-traffic-to-google/

Trenutna praksa nacionalnih registrov vrhnjih domen

Kot smo že omenili, nacionalni pravni okviri določajo, katera vsebina je nezakonita, kdo je pooblaščen za ukrepanje zoper le-to in kateri postopki so dovoljeni v skladu z vladavino prava. To se lahko razlikuje od države do države. Poleg tega imajo nacionalni registri vrhnjih domen (ccTLD) različne zahteve glede tega, kdo lahko registrira domene in kakšne so njihove dolžnosti. Kombinacija teh zahtev in nacionalnega pravnega okvirja vpliva na to, katere politike in pobude se razvijejo v sklopu registra in se uporabljajo za pristop k vprašanju nezakonitih spletnih vsebin.

Običajno so te politike zakoreninjene v nacionalni skupnosti in skladne z nacionalno zakonodajo ter obravnavajo nacionalne potrebe, pri čemer so pogosto plod posvetovanja in sodelovanja z drugimi nacionalnimi zainteresiranimi stranmi. Uspešne politike in prakse enega nacionalnega registra vrhnje domene (ccTLD) bi lahko navdihnile druge. Vendar pa zaradi nacionalnega izvora in posebnosti ni nobenega zagotovila, da bo kopiranje projekta ali politike privedlo do enakega pozitivnega rezultata ali da bo sploh zakonito v sklopu drugega nacionalnega registra (ccTLD).

Izobraževanje in osveščanje s posebnim poudarkom na odprtem dialogu in sodelovanju z organi ter s službami kazenskega pregona

Uporabniki se na spletu soočajo z različnimi tveganji in nevarnostmi (na področju tehničnih vprašanj, zasebnosti itd.), prepoznavanje in spopadanje z nezakonitimi vsebinami pa je le eno izmed njih. Številni nacionalni registri vrhnjih domen (ccTLD) se čutijo dolžne svojo skupnost opozarjati na nevarnosti interneta, zato izobražujejo in podajajo smernice o tem, kako se lahko uporabniki bolje zaščitijo, kako ublažiti tveganja ali rešiti težave.

Izobraževanje in osveščanje na ravni skupnosti

Nacionalni registri (ccTLD) se ukvarjajo z osveščanjem in izobraževanjem lokalnih spletnih skupnosti z namenom, da bi internet postal varnejši. Registri prevzamejo pobude, da nosilce domen in širšo lokalno skupnost uporabnikov opozarjajo na neželene vsebine in dajejo navodila za ukrepanje. Registri obveščajo svoje skupnosti na različne načine, na primer z organiziranjem srečanj ali udeležbo na delavnicah, s predstavitvami, z razpravami o nezakonitih vsebinah v svojih publikacijah itd.

Številna spletna mesta registrov imajo stran ali razdelek o nezakonitih vsebinah, ki opisuje potencialne težave in nevarnosti, razloži politiko ter vlogo registra in kaj (tehnično) lahko in česa ne more storiti v primeru nezakonitih vsebin.

Register bo vsakega uporabnika, ki se želi pritožiti zaradi morebitne nezakonite spletne vsebine, napotil k organizacijam in vladnim službam, ki so specializirane za ocenjevanje in obravnavo določenih vrst spletnih vsebin (na primer nezakonite igre na srečo, spolna zloraba otrok, ponarejeno blago itd.).

Primeri

Nic.at (.at): spletna stran avstrijskega registra vsebuje podatke o nacionalnem uradu za poročanje in ukrepanje proti otroški pornografiji in nacionalsocializmu na internetu. Glejte tukaj in tukaj.

Nominet (.uk): register za domeno .uk pojasnjuje, kako lahko uporabniki, ki želijo podati ugovor na vsebino spletnega mesta, stopijo v stik z registrarjem ali lastnikom spletnega mesta, ob tem pa zagotavlja povezave do številnih organov s sedežem v Združenem kraljestvu, ki bi jim lahko pomagali. Glejte tukaj.

AFNIC (.fr): francoski register ponuja povezavo do namenske platforme za poročanje pod okriljem Ministrstva za notranje zadeve, prek katere je mogoče podati prijavo "o vsebini spletnega mesta ali o nezakonitem ravnanju ter kršenju javnega reda in miru".

Norid (.no): spletna stran norveškega registra ponuja povezavo do spletnega mesta policije z nasveti, kako obvestiti policijo o nezakonitih dejavnostih na spletu, in povezavo do svetovalne službe slettmeg.no, ki ponuja nasvete, kako odstraniti podatke z interneta.

DNS.PT (.pt): portugalski register je v sodelovanju z drugimi organizacijami, ki se ukvarjajo z nepooblaščenim razširjanjem avtorsko zaščitenih vsebin, razvil in gosti spletni portal, ki omogoča hiter in enostaven dostop do spletnih mest z digitalnimi vsebinami, ki spoštujejo pravice intelektualne lastnine avtorjev in ustvarjalcev.

Registri bodo včasih uporabili svoje komunikacijske kanale za opozarjanje pred zločinci, ki uporabljajo lažna spletna mesta, na primer za pridobitev uporabniških poverilnic za bančništvo ali e-trgovino. Registri uporabljajo svoje komunikacijske kanale tudi za prikazovanje načinov, kako lahko uporabniki preverijo zakonitost spletnega mesta. Običajno je lažno spletno mesto registrirano pod bolj eksotično vrhnjo domeno tuje države, sam register pa nima dostopa ali vpliva na uporabljeno domensko ime.

Primer

SIDN (.nl) je nedavno izdal opozorilo o spletni bančni goljufiji.

Izobraževanje in tesno sodelovanje z organi in službami kazenskega pregona

Številni registri se posebej osredotočajo na osveščanje in vzpostavljanje dobrih odnosov z organi pregona in drugimi organi (na primer z agencijami za varstvo potrošnikov ali igralniškimi komisijami). Pomembno je, da te agencije in organi, ki imajo v mnogih primerih pooblastilo za presojo zakonitosti vsebin, razumejo, kaj register počne, kako jim lahko pomaga v primerih nezakonitih vsebin, in da vzpostavijo dobre komunikacijske kanale. Tako se izognejo izgubi dragocenega časa, ko od registra zahtevajo, da sprejme ukrepe, ki niso v pristojnosti registra, ali ko svojih zahtevkov ne naslovijo na osebo ali storitev, ki se lahko ustrezno odzove. Organi kazenskega pregona imajo pomembno vlogo v boju proti nezakonitim spletnim vsebinam in jih je treba v večini primerov obravnavati kot prvo kontaktno točko za pritožbe.

Pomembno je, da ljudje, ki delajo v službah kazenskega pregona in ustreznih organih, dobro razumejo, kako delujeta internet in sistem DNS, pa tudi vlogo registra ter možnosti in omejitve ukrepov na ravni registra. Nekateri registri razvijajo tudi smernice ali postopke za nemoteno in hitro komunikacijo med določenimi agencijami ali organi in registrom.

Primeri

NORID (.no) je avtor informativnega vodnika za organe kazenskega pregona, policijo in ljudi, ki delujejo v pravosodnem sistemu - "Domenski spori v pravnem sistemu". Register je v sodelovanju z organom za pregon razvil tudi posebne smernice o tem, kako naj organi pregona ravnajo pri zasegu domenskega imena.

SWITCH (.ch): V primerih kazenskih ali upravnih postopkov lahko organi pristopijo k registru z zahtevami za preklic ali blokiranje domenskih imen. Register je v sodelovanju z regulatorjem razvil smernice o tem, kako mora organ postopati v tovrstnih primerih in koliko možnosti za ukrepanje ima register SWITCH pri odzivu na navodila organov.

Nominet (.uk) je v sodelovanju s svojo lokalno internetno skupnostjo razvil postopek sodelovanja z organi pregona Združenega kraljestva. V skladu s tem postopkom lahko organi kazenskega pregona v Združenem kraljestvu Nominetu predložijo uradna potrdila o kriminalnem dejanju ali vsebini v povezavi z domenami .uk, posledično pa so te domene deaktivirane v roku 48 ur po predaji obvestila nosilcu domene in registrarju. Poročilo o ukrepih deaktivacije se objavi vsako leto.

Register kot ponudnik verodostojnih podatkov o domenskih imenih

Kot smo že omenili, je edini učinkovit ukrep v boju proti nezakonitim vsebinam odstranitev vsebin z interneta. Če uporabnik ali organizacija na spletnem mestu zasledi nezakonito vsebino, najprej naveže stik z nosilcem domene, ki lahko vsebino odstrani ali prilagodi.

Register zbira podatke, da lahko določi nosilca domene (stranko) in da lahko v primeru spora, tehničnih težav, spremembe splošnih pogojev, neizvedenih plačil itd. naveže stik z nosilcem. Splošni pogoji registra običajno izrecno zahtevajo, da nosilec domene ob registraciji navede točne osebne in kontaktne podatke ter da dane podatke sproti posodablja. Navedba lažnih ali netočnih podatkov predstavlja kršitev splošnih pogojev in lahko privede do izbrisa domene.

Registri vlagajo veliko časa in truda v vzdrževanje podatkovne baze. Na ta način izboljšujejo kakovost registracijskih podatkov WHOIS, kar ima lahko tudi posredno pozitiven vpliv, saj je malo verjetno, da bi osebe s slabimi nameni registrirale domeno z uporabo resničnih osebnih podatkov. Ukrepi in prakse za vzdrževanje kakovostne podatkovne baze so odvisni od dejavnikov, značilnih za register, kot so nacionalna zakonodaja, velikost registra, količina obdelanih registracij itd., in lahko vključujejo:[19]

- Natančen pregled podatkov, ki so podani ob registraciji, da se izločijo očitno lažni vnosi (na primer nosilec domene z imenom Miki Miška);
- Samodejno preverjanje formata navedenih podatkov (na primer e-poštni naslov, telefonska številka);
- Pregled pravne dokumentacije, ki jo predloži nosilec domene, v državah, kjer obstaja takšna zahteva o predložitvi pravne dokumentacije;
- Naključno preverjanje registracijskih podatkov že registriranih domenskih imen (register naključno izbere in preveri več domen na dan, mesec ali leto);
- Preverjanje podatkov v primeru pritožbe;
- Navzkrižno preverjanje posredovanih podatkov v uradnih podatkovnih bazah (na primer veljavna poštna številka, obstoječa telefonska številka, številka podjetja/organizacije ali nacionalna identifikacijska številka, če so takšni podatki zahtevani ob registraciji).

19 Primeri temeljijo na raziskavi med člani združenja CENTR iz leta 2017.

Pomembno je opozoriti, da mnogi nacionalni registri vrhnjih domen (ccTLD) nimajo neposrednega stika z nosilcem domene.
V tem primeru vsi stiki, vključno z zagotavljanjem in s posodabljanjem podatkov o registraciji, potekajo prek registrarja.

> **Primeri prizadevanja registra za pridobivanje in vzdrževanje točnih podatkov o registraciji:**
>
> Norid (.no) zahteva, da so vsi nosilci domen registrirani v norveškem Centralnem koordinacijskem registru za pravne osebe ali v Nacionalnem registru. Register .no nato redno preverja, ali nosilci še obstajajo glede na Centralni koordinacijski register za pravne osebe. Domene pravnih oseb, ki so bile razpuščene, so samodejno določene za odstranitev.
>
> DK Hostmaster (.dk) zahteva, da se danski nosilci domen identificirajo s pomočjo NemID, rešitve za prijavo, ki jo uporabljajo danske banke, vladna spletna mesta in druga zasebna podjetja. Tuji nosilci so podvrženi oceni tveganja, s katero določijo, ali bodo prejeli zahtevo za predložitev dokazila o istovetnosti pred registracijo visoko tveganje - ali v 30 dneh po registraciji - nizko tveganje (strankam, ki ne predstavljajo nikakršnega tveganja, ni treba predložiti dokazila). Če nosilec domene ne more ali ne želi predložiti dokazila o svoji istovetnosti, se domena izbriše.
>
> Register SIDN (.nl) meni, da lažne spletne trgovine načenjajo ugled domene .nl kot močne in varne vrhnje domene. Razvija sisteme za zgodnje odkrivanje domen, ki se uporabljajo za lažne spletne trgovine, in preučuje poročila žrtev prevar ter informacije, ki jih posreduje Nacionalni urad za poročanje o spletnih goljufijah. Če so podatki o registraciji vpletenih domenskih imen lažni, jih register lahko deaktivira.

Nekateri registri imajo posebne postopke za prijavo ali pritožbo zaradi lažnih registracijskih podatkov:

- Nominet (.uk) podajanje pritožbe zaradi napačnih podatkov WHOIS
- AFNIC (.fr) zahteva za preverjanje podatkov nosilca domene
- DNSBelgium (.be) postopek za preklic domene Prekliči/prekliči+

Izmenjava podatkov o registraciji s tretjimi osebami

Registri morajo pri izmenjavi informacij o nosilcih domen s tretjimi osebami spoštovati nacionalne predpise o varovanju zasebnosti. Pravilnik in postopek pridobivanja kontaktnih podatkov najdete na spletnem mestu registra. Obstajajo različne prakse, saj nekateri registri zahtevajo, da je zahtevek za razkritje podatkov oddan ročno prek spletnega obrazca, drugi registri omogočajo dostop (ki je sicer omejen skladno z uredbo GDPR) do registracijske baze (prek protokola Whois), spet drugi pa imajo vgrajeno orodje, ki omogoča neposredno pošiljanje sporočila registracijskemu zavezancu.

> **Primeri**
>
> AFNIC (.fr) Zahtevek za razkritje osebnih podatkov
>
> AFNIC (.fr) Obrnite se na administrativni kontakt za domensko ime
>
> DomReg.lt (.lt) "Obrnite se na nosilca domene"

Odzivi na poročila o sumljivih vsebinah

Nekateri registri so vzpostavili postopke za odzivanje na poročila o sumljivih vsebinah z blokiranjem ali začasno ukinitvijo domenskega imena v posebnih primerih. Ti postopki imajo običajno skupno to, da se uporabljajo v omejenih in natančno opredeljenih primerih ter da je vanje vključena zunanja stran s strokovnim znanjem na področju presojanja tovrstnih vsebin.

Tovrsten postopek je lahko koristen, ko je sodno odločanje o preklicu domenskega imena dolgotrajno. Ena od nevarnosti je, da se pritožniki ne zavedajo omejenega učinka ukrepa, ki ga je sprejel register, in ne nadaljujejo z ukrepi za odstranjevanje vsebin z interneta.

Primeri

SIDN (.nl) je zasnoval prostovoljni postopek za prijavo in odstranitev (Notice-and-Take-Down procedure) na osnovi nizozemskega nacionalnega kodeksa za prijavo in odstranitev. Postopek za prijavo in odstranitev je mogoče izvajati le v primerih, ko lahko pritožnik dokaže, da so bili sprejeti zadostni ukrepi za navezavo stika s ponudnikom vsebin, z upravljavcem spletnega mesta, nosilcem domene in registrarjem, in sicer zaradi očitnega razloga, da lahko te stranke učinkovito rešijo težavo in odstranijo vsebine. Le v nedvoumno nezakonitih primerih se lahko SIDN odloči za (začasno) odstranitev imenskih strežnikov domene.

Switch (.ch) - 15. člen "Odloka o internetnih domenah" zagotavlja pravno podlago za blokiranje domenskih imen v primeru "upravičenega suma, da se zadevna domena uporablja (1) za dostop do kritičnih podatkov z uporabo nezakonitih postopkov; ali (2) za distribucijo zlonamerne programske opreme"; prošnjo za blokiranje vloži služba za boj proti kibernetski kriminaliteti, ki jo priznava švicarski regulator. Glejte tukaj.

Finska (.fi) - 172. člen Zakona o elektronskih komunikacijskih storitvah daje finski agenciji za transport in komunikacije TRAFICOM pravico, da sprejme potrebne ukrepe za odkrivanje, preprečevanje, preiskovanje in sprožitev kazenske preiskave vseh pomembnih kršitev informacijske varnosti, usmerjenih v javno komunikacijsko omrežje ali storitve z uporabo domenskih imen .fi ali njihovih nosilcev. Ukrepi so lahko dejanja, usmerjena v podatke korenskega imenskega strežnika fi in lahko vključujejo naslednje: 1) preprečevanje in omejitev prometa na domensko ime; 2) preusmeritev prometa z enega domenskega imena na drugega; in 3) vsak drug primerljiv tehnični ukrep v smislu podrazdelkov 1–2.

Nedavno je register EURid (.eu) napovedal sodelovanje z Mednarodno koalicijo za boj proti ponarejanju (IACC), da bi iz podatkovne zbirke registracij za domeni .eu in .ею lažje odstranili lažna domenska imena in vzpostavili varnejši domenski prostor za uporabnike interneta.

Zaključek

Zlonamerne in nezakonite vsebine načenjajo zaupanje v internet. Nacionani pravni okviri določajo, katera vsebina je nezakonita in kdo je pristojen za ukrepanje zoper njo znotraj okvirjev pravne države. To se lahko razlikuje od države do države.

Odstranjevanje nezakonitih vsebin z interneta je edina učinkovita rešitev, s katero preprečimo dostop in uporabo. Ponudnik vsebin in ponudnik gostovanja imata neposreden dostop do vsebin ali naprave, na kateri so vsebine shranjena. Nacionalni registri vrhnjih domen (ccTLD) nimajo dostopa do vsebin, prav tako pa tudi ne gostijo vsebin in jih ne prenašajo prek svoje infrastrukture.

Nacionalni registri vrhnjih domen so zavezani k temu, da prispevajo k celovitemu in učinkovitemu pristopu za boj proti nezakonitim spletnim vsebinam ter razvijajo politike in pobude, na primer:

- osveščanje in izobraževanje svojih skupnosti o nevarnostih interneta,
- olajševanje sodelovanja z organi in s službami kazenskega pregona,
- zagotavljanje podatkov o registraciji sumljivih domenskih imen,
- odgovarjanje na poročila o domenah, ki se uporabljajo za olajševanje dostopa do sumljivih vsebin v okviru nacionalne pristojnosti.

Uspešne politike in prakse, predstavljene v prispevku, bi lahko navdihnile druge nacionalne registre vrhnjih domen (ccTLD). Vendar pa zaradi nacionalnega izvora in posebnosti ni nobenega zagotovila, da bo kopiranje projekta ali politike pripeljalo do enakega pozitivnega rezultata ali da bo enak pristop sploh zakonit v okviru drugega nacionalnega registra vrhnje domen (ccTLD).

CENTR je združenje evropskih nacionalnih registrov vrhnjih domen (ccTLD), kakršni sta, na primer, .de za Nemčijo ali .si za Slovenijo. CENTR trenutno šteje 55 polnopravnih in 9 pridruženih članov - skupaj so odgovorni za več kot 80 % vseh registriranih domenskih imen po vsem svetu. Cilji združenja CENTR so spodbujanje in sodelovanje pri razvoju visokih standardov in najboljših praks med nacionalnimi registri vrhnjih domen (ccTLD).

Ocenite ta prispevek združenja CENTR

(Hvala za vaše mnenje!)

CENTR vzw/asbl
Belliardstraat 20 (6. nadstropje) 1040 Bruselj, Belgija Tel. št.: +32 2 627 5550
Faks: +32 2 627 5559
secretariat@centr.org
www.centr.org

Če želite biti na tekočem z aktivnostmi in s poročili združenja CENTR, nam sledite na Twitterju, Facebooku ali LinkedInu.