Council of European National
Top-Level Domain Registries

Регистри назива домена и онлајн-садржај

Садржај

Сажетак 4

Увод 6

Циљ овог документа 6

Оквир овог документа 6

Интернет, систем назива домена и онлајн-садржај 7

DNS као део инфраструктуре интернета 7

Интернет и IP инфраструктура 7

Систем назива домена 7

Онлајн-садржај 8

Доступност онлајн-садржаја 8

Употреба DNS-а као алата за лакше проналажење садржаја 9

Предузимање радњи против нелегалног садржаја на интернету 12

Шта је нелегалан садржај? 12

Дефинисано локалним правним оквирима 12

Ко може да донесе одлуку о легалности садржаја? 13

Где се налази онлајн садржај? 14

Локација на интернету 14

Физичка локација 14

Уклањање нелегалног садржаја 14

Обавештавање лица које објављује садржај или пружаоца услуга хостинга 14

Обавештавање регистранта назива домена 15

Отежавање проналажења садржаја 15

Даљи кораци који се предузимају када брисање нелегалног садржаја није успело 15

Ризици и недостаци у случају брисања назива домена из регистра 15

Тренутне праксе националног домена највишег нивоа 19

Едукација и подизање свести, с посебним освртом на отворени дијалог и сарадњу с надлежним органима и органима за спровођење закона 19

Едукација и подизање свести у заједници 19

Едукација и блиска сарадња с надлежним органима и органима за спровођење закона 21

Регистри као даваоци релевантних података о називу домена 22

Дељење података о регистрацији с трећим странама 24

Одговарање на извештаје о сумњивом садржају 25

Одговарање на извештаје из спољних извора 25

Октривање незаконитих радњи додатним мерама 26

Закључак 28

Сажетак

Чланови *CENTR*-а су национални регистри који управљају националним интернет доменима највишег нивоа (*ccTLD*). Распон одговорности регистара креће се од обезбеђивања *DNS* техничке инфраструктуре и управљања њоме за њихове домене највишег нивоа, преко организовања процеса регистрације назива домена, до проактивног одржавања базе регистра тако да интернет може несметано да се користи помоћу назива интернет домена.

Увредљиви и нелегални садржаји смањују поверење у интернет као платформу за иновацију, креативност и пословне могућности. Регистри националног домена највишег нивоа настоје да допринесу свеобухватном и ефикасном приступу у борби против нелегалног онлајн-садржаја.

Интернет је глобални скуп међусобно повезаних рачунарских мрежа и омогућава комуникацију коришћењем јединствених нумеричких IP адреса. Систем назива домена (*DNS*) функционише као сервис на апликативном слоју. Називи домена олакшавају корисницима употребу интернета. На пример, када корисник укуца назив домена веб-локације, *DNS* ће корисниковом уређају послати информацију о одговарајућој IP адреси на којој се може наћи садржај те веб-локације.

Да би садржај био доступан преко интернета, он мора бити сачуван на најмање једном рачунару или серверу који је повезан на интернет. Да би се садржај ефикасно уклонио са интернета, он мора бити избрисан са уређаја на којем се хостује или тај уређај мора бити искључен са интернета.

Квалификовање садржаја као „нелегалног" зависи од локалног правног оквира и може да се разликује чак и у зависности од контекста. Надлежност за доношење оваквих одлука утврђује се на локалном нивоу.

Уклањање нелегалног садржаја са интернета је једини ефикасан начин да се спречи приступ таквом садржају и да се он користи. Две стране имају директан приступ садржају или уређају на ком се садржај налази: онај ко садржај објављује и пружалац услуга хостинга. Они су први које је потребно обавестити.

Када се назив домена користи за лакши приступ садржају, регистрант назива домена може бити и онај ко објављује садржај и пружа услуге хостинга или онај ко може да укаже на њихов идентитет. Релевантна база података регистра са информацијама о свим називима домена може да помогне у идентификовању и обавештавању регистранта.

Када уклањање нелегалног садржаја са интернета (што је једино ефикасно решење) није могуће, може се покушати да се корисницима отежа проналажење таквог садржаја и приступ таквом садржају. Постоје различити методи „блокирања" интернет садржаја на различитим нивоима који укључују различите актере. Међутим, свима је заједничко то што садржај увек остаје доступан и таква радња може произвести непредвиђену

колатералну штету. Стога се они морају сматрати привременом мером, која треба да се користи у хитним случајевима или када се све друго већ покушало без успеха. Блокирање или брисање назива домена представља једну од таквих мера.

Локални правни оквири дефинишу садржај који је нелегалан, надлежне органе за решавање такве ситуације и процесе који су дозвољени у оквиру правног система. То се може разликовати у зависности од земље. Регистри националног домена највишег нивоа имају различите захтеве у погледу лица које може да региструје називе домена, као и његових дужности. С тим у вези, у оквиру .rs и .срб домена не постоје ограничења у смислу географског порекла. Једина ограничења која постоје односе се на поддомене које могу да региструју само одређене категорије лица.

Ове политике обично потичу из локалне заједнице и у складу су са локалним законима, испуњавају локалне потребе и често су развијене у сарадњи са другим локалним заинтересованим странама и уз консултације с њима. Успешне политике и праксе за један национални домен највишег нивоа могу бити инспирација другима. Међутим, због локалног порекла и особености, не постоји гаранција да ће копирање пројекта или политике довести до истог позитивног резултата или да ће уопште бити легално у случају другог националног домена највишег нивоа.

Између осталих приступа решавању проблема нелегалног садржаја, регистри националног домена највишег нивоа фокусирају се на:

- едукацију и подизање свести у целој заједници;
- едукацију и блиску сарадњу с надлежним органима и органима за спровођење закона;
- одржавање базе података регистра да би се побољшао квалитет података о регистрацији. Овај поступак може да има индиректан позитиван утицај, јер није вероватно да би неко с лошим намерама регистровао назив домена користећи тачне личне податке;
- успостављање процедура за дељење података о регистрацији с трећим странама у оквиру ограничења локалних закона о заштити података о личности;
- развој процеса и процедура за одговарање на пријаве о сумњивом садржају. Овим процедурама је обично заједничко то што су применљиве на ограничен број случајева и на добро дефинисане случајеве, као и то да је укључена трећа страна са експертизом у процени таквог типа садржаја.

Увод

Чланови *CENTR*-а управљају регистром за један или више националних интернет домена највишег нивоа (*ccTLD*-ова). Распон одговорности регистара креће се од обезбеђивања *DNS* техничке инфраструктуре и управљања њоме за њихов домен највишег нивоа, преко организовања процеса регистрације назива домена, до проактивног одржавања базе регистра тако да интернет може несметано да се користи помоћу назива интернет домена.

Чланови *CENTR*-а верују да су онлајн-поверење и безбедност од кључне важности да би интернет остао платформа за иновацију, креативност и пословне могућности. Увредљиви и нелегални садржај смањује поверење и поузданост. Регистри националног домена највишег нивоа настоје да допринесу свеобухватном и ефикасном приступу у борби против нелегалног онлајн-садржаја.

Циљ овог документа

Заједнички напор и успешна сарадња подразумевају да заинтересоване стране разумеју и поштују међусобне функције, улоге и ограничења. Циљ овог документа је да се корисницима приближи улога регистра националног домена највишег нивоа; да се објасни његов однос према онлајн-садржају; истраже могућности и ограничења радњи и поставе очекивања у вези с тим шта регистар може или не може да уради када је у питању нелегални онлајн-садржај.

Оквир овог документа

Први одељак овог документа пружа увид у то како интернет ради, где се налази онлајн-садржај и на који начин му се може приступити, а уз то објашњава и олакшавајућу улогу коју има систем назива домена (*DNS*).

Други део документа се бави питањем нелегалног садржаја на интернету и испитује како регистри националних домена највишег нивоа могу да допринесу радњама које воде ка уклањању нелегалног садржаја.

Трећи део је посвећен тренутним политикама и праксама регистара. Ту се листом примера која није коначна показује како различити регистри националног домена највишег нивоа развијају политике и предузимају радње да би на најбољи начин испуњавали потребе својих локалних заједница како би и оне допринеле заједничкој борби против нелегалног онлајн-садржаја.

Интернет, систем назива домена и онлајн-садржај

DNS као део инфраструктуре интернета

Интернет и IP инфраструктура

Интернет представља скуп рачунарских мрежа које су међусобно повезане и које заједно формирају глобални комуникациони систем. Интернет протокол (*IP*) је метод или скуп правила у складу с којима се подаци шаљу преко интернета са једног уређаја на други. Да би се успешно извршио пренос, важно је да се пошиљалац и прималац могу идентификовати и лоцирати међу више милиона рачунара, паметних телефона, сервера и других уређаја који су повезани на интернет. Стога сви повезани уређаји имају најмање једну *IP* адресу која им даје јединствену идентификацију и разликује их од свих других уређаја. *IP* адреса може имати облик нумеричке ознаке[1]: на пример, *IP* адреса 2001:db8:85a3::8a2e:370:7334[2] може да идентификује интерфејс сервера на којем се налази садржај веб-локације.

Систем назива домена

Људима је тешко да читају и памте нумеричке *IP* адресе. Зато систем назива домена (*DNS*) омогућава употребу назива домена, која се односи на *IP* адресу. *DNS* функционише као сервис на апликативном слоју. На пример, када корисник укуца назив домена у прегледач или када кликне на везу с називом домена, апликација ће потражити одговарајућу *IP* адресу преко *DNS*-а. Када се назив домена разреши – а „разреши се" значи да се *DNS* врати на *IP* адресу – уређај тог корисника зна где се на интернету може пронаћи садржај веб-локације.

DNS карактерише његова хијерархијска структура, која се састоји од различитих домена највишег нивоа (TLD-ова) у оквиру заједничког корена. Екстензија назива домена, односно део после последње тачке, означава у оквиру којег домена највишег нивоа је назив регистрован (на пример, .de, .com, .fr, .срб). Хијерархијска структура је битна за функционисање *DNS*-а и итеративан начин за претрагу назива домена.[3]

Регистар назива домена одговоран је за управљање једним доменом највишег нивоа или више њих. Сви регистри треба да поштују техничка правила и захтеве *DNS*-а, али што се тиче политике, сваки домен највишег нивоа прописује сопствена правила. Док

1 IPv6 адресе имају дужину од 128 битова и представљене су хексадецималним низом, док је старија IPv4 верзија дужине 32 бита и наведена је у групама децималних бројева раздвојених тачкама.

2 Ова *IP* адреса служи само за документовање и није повезана с јавним интернетом (*RFC 3849*, префикс *IPv6* документације).

3 За детаљније информације о функционисању *DNS*-а: https://www.centr.org/about-the-industry/item/the-dns.html.

генерички домени највишег нивоа (*gTLD*-ови) морају да поштују опште политике и процесе које је развио ICANN, национални домени највишег нивоа (*ccTLD*-ови) прописују сопствену политику у складу с потребама својих интернет заједница.

Онлајн-садржај

Садржај се мора креирати, складиштити и учинити доступним пре него што се може пронаћи на интернету. Начин на који се ово одвија описан је у овом одељку кроз идентификовање улога и одговорности различитих актера у овом процесу[4].

Доступност онлајн-садржаја

Објављивање садржаја

Садржај објављује лице које на интернет поставља текст, звук, слике, видео-снимке, анимације и друге облике садржаја који се отпремају путем веб-локација, блога или су доступни на друштвеним мрежама итд. Онај ко објављује садржај може, али не мора да буде првобитни аутор садржаја.

Да би садржај био доступан преко интернета, он мора бити сачуван на најмање једном рачунару или серверу који је повезан на интернет. Лице које објављује садржај може да користи сопствени рачунар или сервер или, што је вероватније, да користи услуге и инфраструктуру пружаоца услуга хостинга.

Пружалац услуга хостинга

Пружалац услуга хостинга обезбеђује складиштење података и повезивање на интернет, има техничку експертизу и, што је још важније, потребну инфраструктуру, капацитет и пропусни опсег да се избори са саобраћајем који може да дође са било ког места на интернету у било ком тренутку. Пружаоци услуга хостинга обезбеђују платформу за хостинг садржаја, али не одлучују о томе шта се објављује – то раде њихови корисници (они који објављују садржај). Уз мали број изузетака – а то су углавном велике организације које имају сопствену инфраструктуру и мреже – они који објављују садржај ослањају се на услуге пружаоца услуга хостинга. Пружаоци услуга хостинга имају велике центре података са серверима на којима се налази садржај њихових клијената. Ови сервери су повезани на интернет и могу се идентификовати преко јединствене *IP* адресе. Постоје различите врсте хостинга: најчешћи су веб-хостинг и имејл-хостинг. Хостинг кориснички генерисаних садржаја (нпр. видео-снимци које су генерисали корисници) може се сматрати посебним случајем, који би се налазио између објављивања садржаја и хостинга.

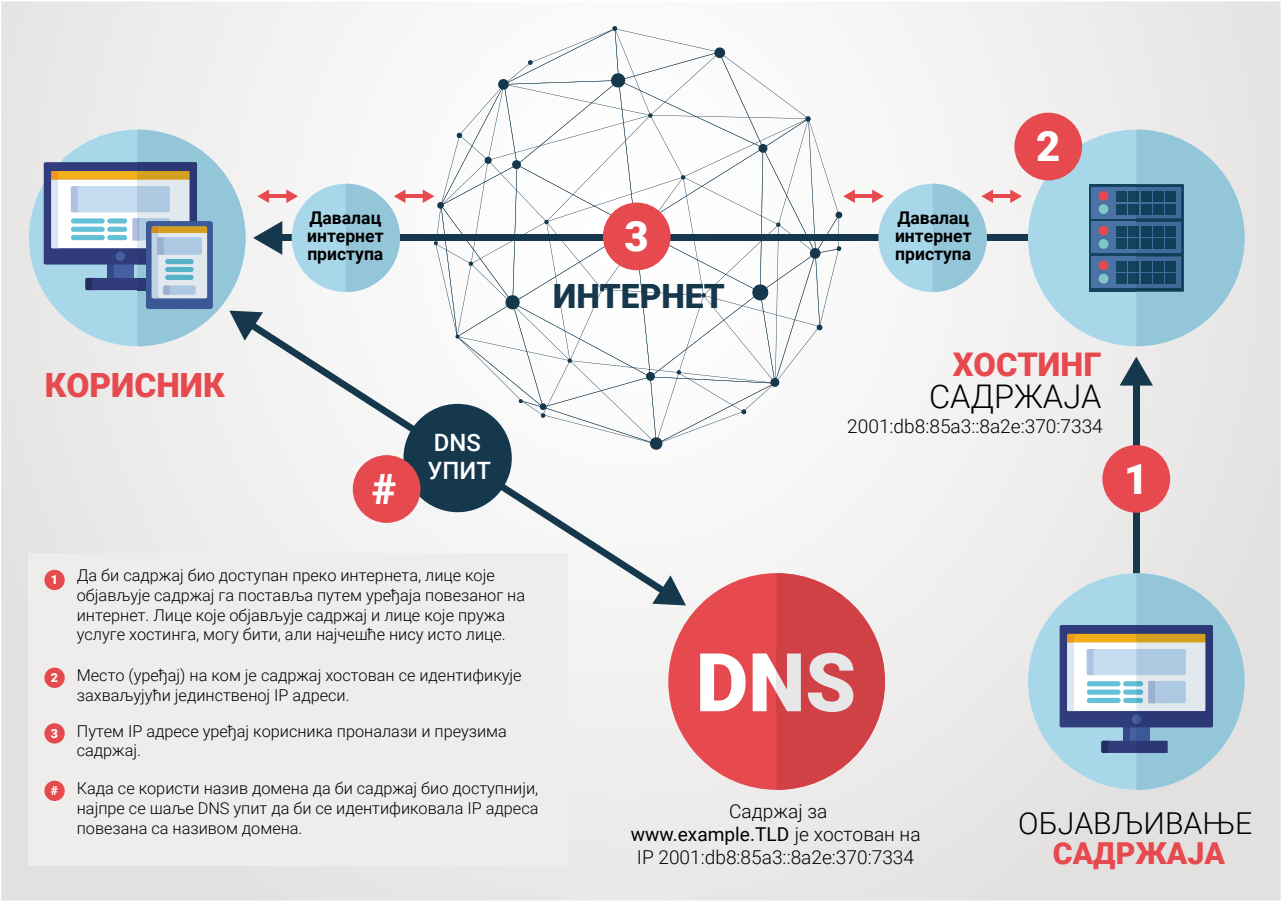
Пружалац интернет услуга / давалац интернет приступа

Пружалац интернет услуга (*ISP*) обезбеђује приступ интернету. Преко мреже и инфраструктуре *ISP*-а његови корисници могу да приступе интернету. *ISP* ће доделити *IP* адресе уређајима који су повезани на његову мрежу, на пример серверима пружалаца услуга хостинга, модему интернет корисника итд. *ISP* је давалац приступа, тако да он не

4 Актери могу да обављају једну или више улога које су описане у овом одељку; на пример *ISP* такође може да пружа услуге хостинга.

складишти никакав садржај, већ се садржај преноси преко његове инфраструктуре.

Постоје и други актери који обезбеђују пренос и размену података између мрежа, као што су тачке за размену интернет саобраћаја (*IXP*-ови) и оператори преносних мрежа (на кратке или велике раздаљине) или мреже за испоруку садржаја (*CDN*)[5] , које хостују копије садржаја својих клијената на серверима на различитим географским локацијама како би садржај био брже испоручен крајњим корисницима (нпр. *Cloudflare*). Овде нећемо даље дискутовати о њиховом односу са садржајем.



Употреба DNS-а као алата за лакше проналажење садржаја

Систем назива домена (*DNS*) обезбеђује функцију која помаже приликом „навигације" интернетом и она омогућава утврђивање *IP* адресе повезане с називом домена. Зато се *DNS* пореди са телефонским именником, катастром или регистром предузећа[6].

Регистрант

Лице које објављује садржај може да региструје назив домена тако да корисницима интернета олакша преузимање садржаја који је поставило на интернет. Назив домена функционише као ознака поврх *IP* адресе, лакши је за памћење од нумеричке адресе и може да садржи корисне информације као што су назив компаније у имејл-адреси или

5 https://sr.wikipedia.org/wiki/Мреже_за_доставу_садржаја

6 https://sr.wikipedia.org/wiki/Систем_имена_домена

референца на садржај у називу домена веб-локације.

Регистрант назива домена није обавезно (или није једино) лице које објављује садржај у оквиру назива домена. На пример, веб-локације великог универзитета, странице блогова или веб-локације друштвене мреже дозвољавају другима да објављују садржај на локацији која се идентификује једним називом домена.

Регистрант је корисник одређеног назива домена за одређени временски период. Да би стекло то право, физичко или правно лице региструје назив у регистру домена највишег нивоа, директно или преко овлашћеног регистра. Регистрант је одговоран за начин на који се назив домена користи.

Услови, поступак регистрације и начин коришћења назива интернет домена у оквиру .RS и .СРБ домена, којима управља РНИДС, као и међусобни односи РНИДС-а, као администратора Регистра националних интернет домена, и регистраната назива домена уређени су Општим условима о регистрацији назива националних интернет домена.

Овлашћени регистар назива домена

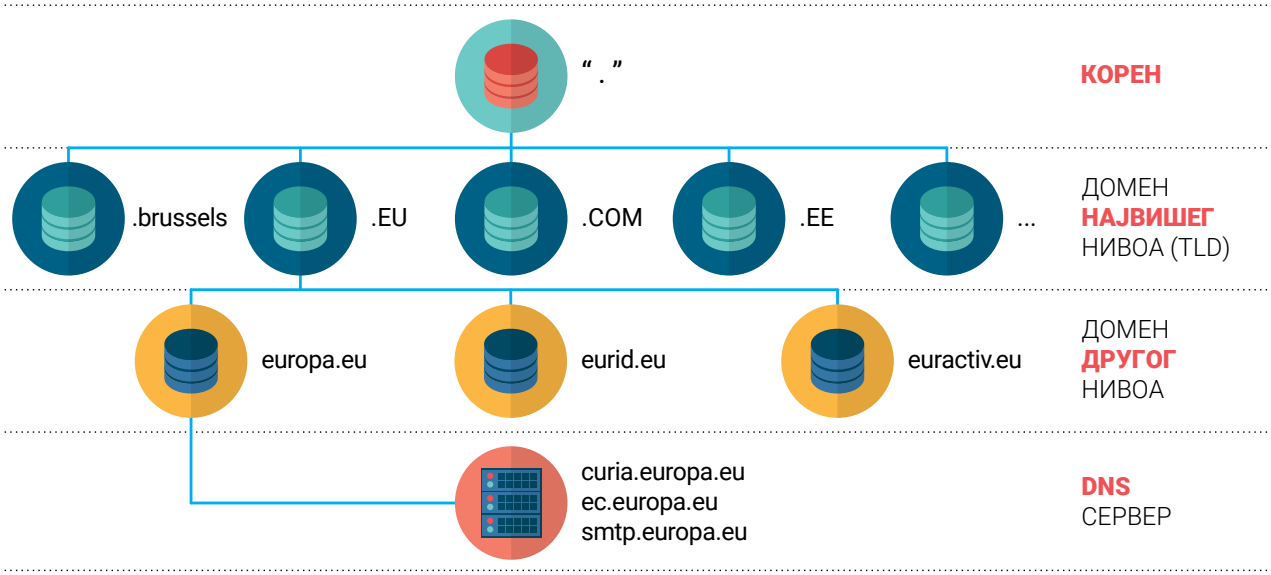
Овлашћени регистар (регистрар) је фирма која пружа услуге регистрације домена компанијама и појединцима, директно или преко мреже препродаваца. Овлашћени регистар је акредитован од стране једног или више регистара да нуди називе домена у оквиру свог домена највишег нивоа. Овлашћени регистар проверава расположивост назива домена и спроводи процес регистрације, а национални регистар управља доменом највишег нивоа. Као део процеса регистрације, овлашћени регистар подноси контакт-информације регистранта домена и техничке информације у вези с називом домена (на пример, који *DNS* сервери садрже записе који веб-прегледачима и корисницима имејла саопштавају где да пронађу сервер на коме се налази садржај веб-сајта или имејл). Овлашћени регистар не хостује садржај и садржај се не преноси путем његове инфраструктуре. Међутим, у пракси, велики број овлашћених регистара својим клијентима такође пружа услуге хостинга и друге интернет услуге.

Услови за стицање статуса и начин рада овлашћених регистара у оквиру .RS и .СРБ домена уређени су Општим условима о раду овлашћених регистара РНИДС-а.

Регистар домена највишег нивоа

Регистар управља једном и једином релевантном базом података регистрованих назива домена у оквиру домена највишег нивоа за који је задужен и објављује ове податке у склопу *DNS* система. Сервери регистра домена садрже информације о регистранту домена, регистрацији домена (нпр. датуму истека), *IP* адресама које су повезане с називом домена и друге техничке податке. Регистар неколико пута на дан објављује ажурирани зонски фајл, а то је текстуални фајл који садржи мапирања између назива домена и *IP* адреса сервера који пружају податке о интернет сервисима везаним за сваки регистровани назив домена, као и друге ресурсе. Тај фајл садржи информације о начину лоцирања *IP* адреса и друге информације потребне за навигацију на интернету. Регистри не складиште садржај и не утичу на њега.

Напомена: Већина пружалаца интернет приступа привремено чува *DNS* информације о недавно претраживаним називима домена из различитих домена највишег нивоа на тзв. неауторитативним *DNS* серверима да би убрзали сурфовање за своје клијенте. Захтев се шаље *DNS*-у тек ако скорашњи одговор није доступан на серверу *ISP*-а. Стога може бити потребно одређено време пре него што промене које се изврше у *DNS*-у (као што је уклањање назива домена из *DNS*-а од стране регистра) постану доступне свуда на интернету.



Предузимање радњи против нелегалног садржаја на интернету

Шта је нелегалан садржај?

Дефинисано локалним правним оквирима

Термин „нелегалан" користи се за описивање садржаја који је забрањен у националном контексту, без обзира на разлог. Европска комисија нпр. дефинише нелегалан садржај као „било коју информацију која није усклађена са прописима Уније или прописима одређене државе чланице".[7] Осим проблема у вези са сексуалним злостављањем деце, постоји врло мало сагласности на међународном нивоу око тога шта чини неприкладан садржај с гледишта јавног поретка. Оно што је дозвољено у једном законодавству може бити забрањено у неком другом. Допуштеност садржаја може такође да зависи од контекста: садржај који се прогласи нелегалним у једном контексту (нпр. непристојна комедија коју гледају деца) може бити прихватљив у другом (нпр. када је гледају одрасли), чак и у оквиру истог законодавства.[8]

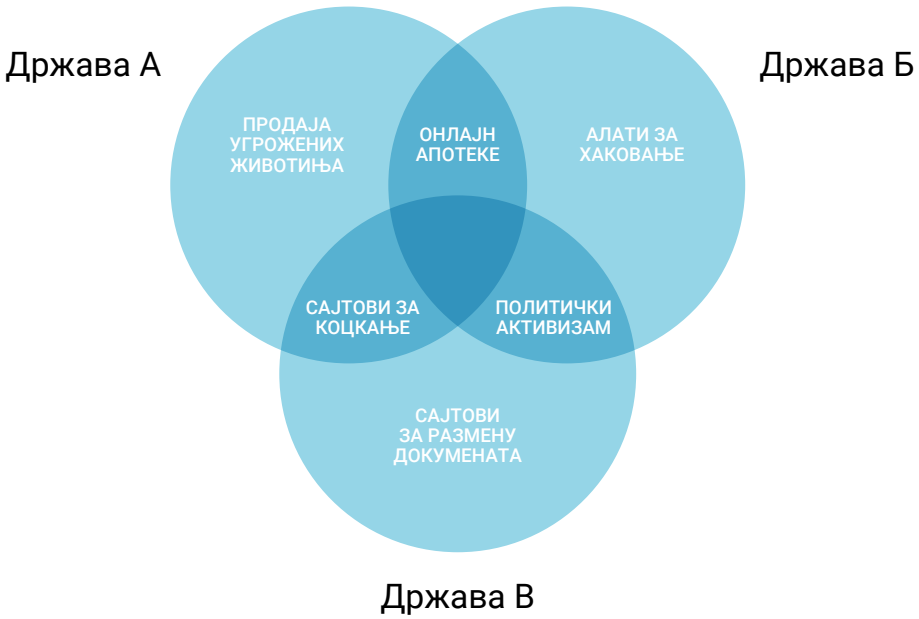
Неке земље су успоставиле посебан правни оквир за онлајн-садржај, док се у другим законодавствима проблеми у вези са онлајн-садржајем решавају на основу постојећих општих оквира који нису специфични за интернет. Компаративна студија у 47 земаља чланица Савета Европе открила је четири шире категорије правних основа за доношење одлуке о легалности онлајн-садржаја:

- заштита здравља и морала (укључујући материјале о сексуалној злоупотреби деце или нелегално коцкање);
- заштита националне безбедности, територијалног интегритета или јавне безбедности (укључујући борбу против тероризма);
- заштита права интелектуалне својине и
- заштита од клевете и неовлашћене обраде личних података.[9]

7 *Commission Recommendation of 1.3.2018 on measures to effectively tackle illegal content online*, C(2018)1177, Европска комисија, март 2018. г, https://eur-lex.europa.eu/TodayOJ/

8 *Internet Society Perspectives on Internet Content Blocking: An Overview, Internet Society,* март 2017. г, 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, децембар 2015. г, https://www.coe.int/en/web/freedom-expression/study-filtering-blocking-and-take-down-of-illegal-content-on-the-internet (приступљено 7. јуна 2018. г.).



Венов дијаīрам коју īриказује да шīа је леīално у неким државама није у друīима

Ко може да донесе одлуку о легалности садржаја?

Квалификовање садржаја као „нелегалног" зависи од локалног правног оквира и може се разликовати чак и у зависности од контекста, како смо поменули. За одлуку да ли је садржај легалан или не надлежни су локални судови или други органи. Поред тога, процес који се следи може се разликовати чак и оквиру истог законодавства. Неки органи могу имати надлежност да донесу одлуку у вези са легалношћу садржаја и да поступе директно на основу те одлуке, док неки други органи морају тражити одлуку суда да би имали право да поступају у вези са садржајем.

Онај ко објављује садржај одговоран је за садржај који је учинио доступним другим корисницима интернета. Регистрант је дужан да се стара да се његов назив домена не користи за проналажење нелегалног садржаја на интернету. Да ствар буде још сложенија, онај ко објављује и корисник који преузима садржај можда нису обухваћени истим законодавством. Штавише, сам садржај може бити хостован у некој другој географској регији, која има своје законе, морална начела и дефиниције оног што је легално и оног што није.

Регистар националног домена највишег нивоа у погледу онлајн-садржаја је у истом положају као и било која организација или чак појединац. Регистар може да процени шта сматра да је у границама закона или изван њих и да формира мишљење о томе, али нема посебну надлежност да ефикасно донесе одлуку о легалности садржаја који је постављен онлајн. Када регистар приступи онлајн-садржају, то ради на исти начин као и било која особа која би претраживањем интернета дошла до неке веб-локације и учитала садржај. Не постоји други начин на који би регистар могао да стекне увид у садржај који објављују регистранти. Регистри националног домена највишег нивоа не хостују садржај и никакав садржај се не преноси преко њихове инфраструктуре.

Неки регистри предвиђају могућност предузимања радњи у очигледним случајевима нелегалног садржаја, када не постоји много сумње, а ризици од одговорности су минимални у оквиру њихових општих услова. По правилу, регистри нису довољно опремљени, немају кадар који би могао да врши оцену законитости садржаја или нису у доброј позицији да проактивно траже нелегални садржај на интернету.

Где се налази онлајн садржај?

Локација на интернету

Да би садржај био доступан преко интернета, он мора бити сачуван на најмање једном рачунару или серверу који је повезан на интернет. Локација садржаја је одређена јединственом *IP* адресом (или адресама) уређаја на којем/којима је садржај ускладиштен.

Физичка локација

Географски, уређаји на којима се садржај налази могу бити било где у свету, на месту где постоји струја и веза са интернетом. Осим тога, не постоје строга правила или захтеви у погледу тога где би садржај технички требало да буде хостован, иако физичка локација може да утиче на брзину и квалитет везе.

Садржај се може ускладиштити на само једном серверу или поставити на различите сервере (нпр. хостовање у облаку, хостовање у кластеру). Садржај може бити на једном серверу или на више њих, у истој земљи као и онај ко објављује садржај и корисник садржаја. Ови сервери такође могу бити било где у свету и потпадати под правила различитих законодавстава.

Уклањање нелегалног садржаја

Уклањање нелегалног садржаја са интернета је једино ефикасно решење које спречава приступ таквом садржају и његово коришћење. То се може постићи или брисањем садржаја са уређаја на којем је ускладиштен или искључивањем таквог уређаја са интернета.[10]

Обавештавање лица које објављује садржај или пружаоца услуга хостинга

Две стране имају директан приступ садржају или уређају на којем је ускладиштен садржај: онај ко садржај објављује и пружалац услуга хостинга. Онај ко објављује садржај има алате и шифре за приступ да промени или уклони садржај који је поставио на веб-локацију или учинио доступним на платформи друштвених медија или на другом месту. Пружалац услуга хостинга може да уклони садржај са својих сервера или ефикасно спречи приступ сопственој инфраструктури.

10 Технички гледано, *IP* адреса идентификује интерфејс преко којег уређај размењује информације, а не сам уређај.

Битно је приметити да пружаоци услуга хостинга обично складиште садржај различитих клијената на истој физичкој машини, стога искључивање или заплена сервера може да утиче на различите актере који објављују садржај и да учини легитимни садржај недоступним. Оператери друштвених мрежа и блогова често имају могућност да уклоне само спорне поруке или нелегални садржај који је објављен на њиховим платформама.

Обавештавање регистранта назива домена

Регистрант назива домена је први ког треба обавестити ако се назив домена користи за омогућавање приступа нелегалном садржају. Може се десити да регистрант домена буде истовремено и лице које објављује садржај или је у блиском контакту с њим. Регистрант домена можда није онај ко је поставио нелегалан садржај или му можда није познато да се његов назив домена користи за лашки приступ нелегалном садржају[11]. Међутим, у већини таквих случајева регистрант назива домена може да помогне у идентификацији извора нелегалног садржаја и предузме радње да би га уклонио.

Регистар одржава ауторитативну базу података са информацијама о свим називима домена регистрованим у оквиру домена највишег нивоа и може да помогне у идентификовању и обавештавању регистранта. База података регистра, између осталог, садржи информације о регистранту домена, регистрацији домена (нпр. датум истека) и адресе *DNS* сервера повезане с називом домена.

Регистри националног домена највишег нивоа улажу велики напор у одржавање своје базе података и прихватају легитимне захтеве за достављање информација о регистрантима и регистрованим доменима. Обраћање регистру за добијање информација о регистранту домена може да буде први корак у процесу уклањања нелегалног садржаја са интернета. Више о томе у III одељку, о тренутним праксама регистара.

Напомена: за надлежне органе и органе за спровођење закона може бити од користи да се обрате овлашћеним регистрима, који некада могу да саопште додатне корисне информације, као што су подаци о фактурисању или кредитној картици и информације о другим доменима које је регистровао исти клијент итд.

Отежавање проналажења садржаја

Даљи кораци који се предузимају када брисање нелегалног садржаја није успело

Када није могуће идентификовати ко објављује садржај или пружаоца услуга хостинга, нити ступити с њима у контакт да би уклонили нелегални садржај са интернета, што представља једино ефикасно решење, корисницима се може отежати проналажење таквог садржаја или приступ таквом садржају. Постоје различити методи блокирања интернет-садржаја, на различитим нивоима, који укључују различите актере. Извештај из

11 На пример, у случају великих универзитета или друштвених мрежа, где велики број корисника објављује садржај итд. или када је сервер компромитован и користе га криминалци да би хостовали садржај.

2017. године који је објавио *Internet Society (Интернет друштво)*[12] описује најновије методе и процењује колико су ефикасне. У извештају се разматра блокирање на основу *IP* адресе и протокола, блокирање на основу дубинске анализе пакета (*DPI*), блокирање на основу URL-а, блокирање на основу платформе и блокирање на основу *DNS*-а, на нивоу мреже или *ISP*-а. У извештају се закључује да, без обзира на ниво и метод, „употреба интернет блокирања за решавање проблема нелегалног садржаја најчешће није ефикасна и може корисницима интернета да проузрокује непланирану колатералну штету". Блокирање садржаја не решава проблем: садржај остаје доступан и стога блокирање треба да се посматра као привремена мера у хитним случајевима или када други приступи нису уродили плодом.

Овај документ се усредсређује на радње које се предузимају на нивоу регистра домена, као нпр. у случају када регистар спречава да се назив домена преведе у важећу *IP* адресу привременим блокирањем назива домена или његовим брисањем из зоне.

Ризици и недостаци у случају брисања назива домена из регистра

Блокирање или брисање назива домена и његово уклањање из *DNS*-а значе да корисник више неће добити валидну *IP* адресу приликом претраге назива домена. Корисник ће уместо учитавања очекиване веб-локације добити поруку о грешци која га обавештава да назив домена не постоји[13].

Брисање или блокирање назива домена је прилично једноставна операција, али и драстична интервенција у *DNS*-у, с последицом да се назив домена више не може користити за навигацију до садржаја (нелегалног, а такође ни легалног) који је објављен под називом домена и његових различитих поддомена, као и да све услуге које су повезане с тим називом домена, као што је имејл, престају да раде. Ово се обично дешава у року од неколико сати, али може да потраје и неколико дана, због кеширања. Било која одлука о брисању или блокирању треба да узме у обзир све последице и размотри оправданост таквог потеза наспрам жељеног исхода. Уредба ЕУ о сарадњи и заштити потрошача (ступила на снагу јануара 2020) нпр. јасно наводи да наређивање регистрима да избришу називе домена треба размотрити само „када нису доступни други ефикасни начини који би зауставили или забранили прекршај обухваћен овом уредбом, како би се избегао ризик од озбиљне штете по заједничке интересе потрошача".[14]

Поједини национални домени највишег нивоа, у складу с локалним законом и надлежностима, имају успостављене односе са локалним органима за спровођење

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

13 Domain Conflicts in the Legal System, Norid, септембар 2017, https://www.norid.no/en/om-domenenavn/veilede-re/domenekonflikter-i-rettssystemet/

14 Уредба (ЕУ) 2017/2394 од 12. децембра 2017. г, ступа на снагу 17. јануара 2020. г, члан 9, члан 4. став е) , https://eur-lex.europa.eu/TodayOJ/

закона и/или реномираним компанијама из сектора безбедности или националним ЦЕРТ-овима да би повећали кредибилитет свог националног домена највишег нивоа брзим брисањем или деактивирањем назива домена који се користе у незаконите сврхе. Такве односе по правилу карактерише обострано разумевање по питању обраде и контроле таквих захтева како би се обезбедиле правно утемељене и транспарентне одлуке. Радње које се могу предузети зависе од оквира локалног права земље националног домена највишег нивоа и од питања одговорности у вези са обавештавањем од стране трећих лица.

Следећи пасуси баве се појединим ризицима и проблемима који су повезани с блокирањем или брисањем назива домена.

Блокирање или брисање назива домена може отежати проналажење нелегалног садржаја на интернету, али не решава проблем нити санкционише кривично дело, будући да садржај остаје доступан онима који знају да га пронађу. Поврх тога, постоје још неки ризици и недостаци, који се разматрају у наставку.

Сумњива ефикасност и лажни осећај сигурности, будући да садржај остаје доступан

Блокирање или брисање назива домена не уклања нелегални садржај са интернета. Садржај остаје доступан и може му се директно приступити преко *IP* адресе уместо назива домена. Начин на који се ово ради није посебно компликован, те је једноставном веб-претрагом могуће добити више него довољно објашњења и видео-материјала који објашњавају како се локацији приступа помоћу њене *IP* адресе. Брисање назива домена смањује шансу да се корисници случајно суоче с нелегалним садржајем, али неће зауставити оне који активно траже такав тип садржаја. „Због архитектуре интернета, блокирање према називу домена корисници могу лако да заобиђу, стога су велике шансе да буде неефикасно на дужи рок и да повлачи неочекиване последице за краћи рок."[15]

Поред тога, онај ко објављује нелегалан садржај може да предвиди блокирање и предузме превентивне мере да смањи његов ефекат. За даље умањење ефекта ове мере може нпр. да региструје више назива домена у оквиру истог домена највишег нивоа или у оквиру различитих домена највишег нивоа, у различитим законодавствима, и омогући да сви указују на исту *IP* адресу, и самим тим на исти садржај. Везе које се користе у електронској пошти или које се постављају на платформе и веб-локације могу директно да садрже *IP* адресу, без коришћења *DNS*-а.

Ризик од масовног прекомерног блокирања и колатералне штете

Када се назив домена избрише или блокира, то утиче на сав садржај који је доступан у оквиру тог назива домена и поддомена, укључујући циљани нелегални садржај, али и сав остали садржај. Брисање назива домена друштвене мреже или локације блога, где појединачни корисници могу да објаве сопствени садржај или креирају свој лични блог, утиче на све кориснике; не само на оне који су објавили нелегални садржај, већ

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

и на све оне који су објавили своје породичне слике, изразили политичко мишљење, компаније које користе ту веб-локацију за промоцију и трговину преко интернета итд. Када се блокира назив домена, све услуге повезане с тим називом домена, нпр. имејл, одмах престају да раде.

На овакву ситуацију указао је у фиктивној студији случаја „Конфликти домена у правном систему" норвешки регистар *Норид*. Студија описује утицај и последице блокирања назива домена Универзитета у Ослу, након што је један студент објавио нелегални садржај на веб-локацији у оквиру домена универзитета.[16] Преведена и прилагођена Норидова публикација доступна је на сајту РНИДС-а.

Ризик од прекомерног блокирања и грешке које се лако праве

Техничка лакоћа с којом се називи домена могу блокирати подиже ризик од несразмерне примене такве мере.[17] Трошкови евентуалне грешке су мали за оног ко спроводи, али, насупрот томе, могу имати драстичан утицај на страни регистранта чији је домен грешком блокиран[18] , нпр. предузеће чија је локација за трговину преко интернета блокирана или институција са којом се више не може ступити у контакт путем имејла.

> Напомена: постоје други начини блокирања или интервенције у *DNS*-у, нпр. на нивоу *ISP*-а или овлашћеног регистра. Већина њих су праћени истим проблемима и могу се заобићи. Ниједна мера блокирања не представља свеобухватно решење, будући да ниједна од њих не уклања садржај.

16 Погледајте на стр. 10, *Domain Conflicts in the Legal System, Norid,* септембар 2017. г, https://www.norid.no/en/om-domenenavn/veiledere/domenekonflikter-i-rettssystemet/

17 *Notice and Takedown in the Domain Name System: ICANN's Ambivalent Drift into Online Content Regulation:* (странице 1379–1383)

18 Пример је описан у следећој објави на блогу: *"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/

Тренутне праксе националног домена највишег нивоа

Као што је раније поменуто, локални правни оквири дефинишу садржај који је нелегалан, надлежне органе за решавање такве ситуације и процесе који су дозвољени у оквиру правног система. То се може разликовати у зависности од земље. Поред тога, регистри националног домена највишег нивоа имају различита правила у погледу лица које може да региструје називе домена, као и његових дужности. Комбинација ових правила и локалног правног оквира утиче на активности које регистар може да развија како би решио проблеме нелегалног садржаја на интернету.

Ова правила обично потичу из локалне заједнице, у складу су са локалним законима, испуњавају локалне потребе и често су развијене у сарадњи и уз консултације с другим локалним заинтересованим странама. Успешне политике и праксе за један национални домен највишег нивоа могу бити инспирација другима. Међутим, због локалног порекла и особености, не постоји гаранција да ће копирање правила или политике довести до истог позитивног резултата или да ће уопште бити легално у случају другог националног домена највишег нивоа.

Едукација и подизање свести, с посебним освртом на отворени дијалог и сарадњу с надлежним органима и органима за спровођење закона

Постоје различите врсте ризика и опасности с којима се корисници суочавају када користе интернет (технички, приватност итд), а препознавање и решавање проблема нелегалног садржаја је један од таквих ризика и опасности. Један број регистара националног домена највишег нивоа сматра да је њихова дужност да упозоре своју заједницу на опасности на интернету. Они едукују кориснике и обезбеђују им смернице како могу боље да заштите себе и како да умање ризике или реше проблеме.

Едукација и подизање свести у заједници

Регистри националног домена највишег нивоа баве се подизањем свести у својим локалним интернет заједницама и едукацијом како да интернет постане сигурније место. Регистри покрећу иницијативе за упозоравање регистранта домена и шире локалне заједнице корисника интернета на нежељени садржај и едукацију о томе. Они обезбеђују и смернице о начину на који треба поступати. Постоји велики број начина на који регистри могу да информишу своје заједнице, нпр. организовањем састанака или учествовањем у радионицама, организовањем презентација, дискусија итд.

Сајтови многих регистра садрже страницу или одељак о нелегалном садржају. Ту се описују потенцијални проблеми и опасности, објашњава се политика регистра, разјашњава улога регистра и оно шта он (технички) може или не може да уради по питању нелегалног садржаја.

Регистри често помажу сваком кориснику који жели да поднесе жалбу у вези с потенцијалним нелегалним онлајн-садржајем организацијама или државним агенцијама које су специјализоване за процену и поступање са одређеним типовима онлајн-садржаја (нпр. нелегално коцкање, материјали о сексуалној злоупотреби деце, кривотворена роба итд).

Примери

Nic.at (.at): веб-сајт аустријског регистра, пружа савете корисницима интернета како да се изборе са нелегалним активностима на интернету и садржи везе ка *Stopline*, националној канцеларији за пријаву материјала о сексуалној злоупотреби деце и нацизму на интернету. Погледајте овде и овде.

Nominet (.uk): британски регистар, објавио је политику о криминалним праксама како би објаснио како се регистар бори са криминалним активностима и обезбеђује везе ка разним органима из Уједињеног Краљевства који могу да помогну. Уместо уклањања назива домена из зонске датотеке, *Nominet* преусмерава кориснике интернета на образовну одредишну страницу. Погледајте овде.

Afnic (.fr)*:* француски регистар, обезбеђује везу с наменском платформом Министарства унутрашњих послова путем које се може пријавити „садржај веб-локације или понашање које је незаконито или супротно јавном закону и поретку”. Веб-локација регистра *Afnic* такође садржи формулар који корисници могу да испуне за пријаву спорних назива домена.

Norid (.no): веб-локација норвешког регистра, обезбеђује везу с веб-локацијом полиције, уз савете о начину за обавештавање полиције о нелегалној онлајн-активности, и сервис за смернице slettmeg.no, који нуди савете о начинима за уклањање информација са интернета.

DNS.PT (.pt): португалски регистар, у сарадњи с другим организацијама које се баве роблемом неовлашћене дистрибуције садржаја заштићеног ауторским правом развио је и хостује веб-локацију, која обезбеђује брз и лак приступ сервисима за куповину легалних дигиталних садржаја. *DNS.PT* такође објављује квартални часопис посвећен искључиво сајбер-безбедности како би подигао свест о онлајн-претњама.

SWITCH (.ch): шведски регистар, подржава интернет заједницу платформама за подизање свести и нуди услуге образовања и обуке корисника за развој безбедносних вештина. Погледајте овде.

Регистри понекад користе сопствене канале за комуникацију да би упозорили на преступнике који користе лажне веб-локације, нпр. да би дошли до лозинки корисника за електронско банкарство или електронску трговину и показали како корисници могу да потврде веродостојност одређене веб-локације. Лажне веб-локације обично се региструју под доменом највишег нивоа неке стране земље, често и веома удаљене од локације регистранта, а сам регистар нема приступ нити утицај на назив домена који се користи.

Примери

- *SIDN's* (.nl) савети за препознавање лажних веб-продавница

- *Norid's* (.no) савети за идентифацију превара путем електронске поште

- *TRAFICOM's* (.fi) веб-локација под називом „дисциплиновани преваранти – пројекат", са предлогом пакета за идентификацију и препознавање дигиталних превара

Едукација и блиска сарадња с надлежним органима и органима за спровођење закона

Велики број регистара посебну пажњу поклања подизању свести и успостављању добрих односа са органима за спровођење закона и другим органима (као што су агенције за заштиту потрошача или комисије за контролу коцкања). Важно је да ове агенције и органи, који су у великом броју случајева надлежни за утврђивање легалности садржаја, разумеју посао регистра, шта он може да уради да би им помогао у случајевима нелегалног садржаја, као и да успоставе добре канале за комуникацију. Тиме се избегава губљење драгоценог времена, када они од регистра траже да предузме радње које он није у могућности да предузме, или не упуте своје захтеве лицу или сервису који могу адекватно да реагују. Надлежни органи играју важну улогу у борби против нелегалног садржаја и у већини случајева их треба посматрати као прву адресу у случају жалби.

Важно је да људи који раде у органима за спровођење закона и надлежним органима добро разумеју начине на који интернет и *DNS* раде, као и улогу регистра и његове могућности и ограничења у погледу предузимања одређених радњи. Неки регистри такође могу да развију смернице или процедуре за неометану и брзу комуникацију између наведених агенција или органа и регистра.

Примери

Norid (.no) је аутор информативног водича за органе за спровођење закона, полицију и особље који раде у правосудном систему – Конфликти домена у правном систему. Регистар је такође у сарадњи с тужилаштвом развио посебне смернице за поступање органа за спровођење закона приликом суспензије назива домена. Погледајте овде и овде.

CZ.NIC (.cz) је потписао Меморандум о сарадњи са чешким Одељењем за посебне активности Криминалистичке полиције и Службе за истрагу. Циљ Меморандума је повећање сарадње између *CZ.NIC* и органа за спровођење закона у области спречавања и праћења криминалних активности и кривичног гоњења злочина, уз истовремено

смањење административних оптерећења. *CZ.NIC* је такође потписао Заједничку декларацију са Полицијском и истражном службом Националног штаба за борбу против организованог криминала како би се боље ухватио у коштац са материјалима о сексуалној злоупотреби деце, а недавно је потписао и Меморандум о сарадњи са чешком Управом за инспекцијске послове у области трговине ради лакшег откривања ризичних електронских продавница.

SWITCH (.ch): У случајевима кривичног или управног поступка надлежни органи могу регистру да пошаљу захтеве за опозив или блокирање назива домена. У сарадњи с регулаторним телом, регистар је развио смернице за то како надлежни орган треба да поступа у таквим случајевима и које могућности су доступне *SWITCH*-у у погледу предузимање радњи приликом одговора на налог од надлежног органа.

Nominet (.uk) је, кроз консултације са својом локалном интернет заједницом, развио процес сарадње са органима за спровођење закона у Уједињеном Краљевству. У оквиру овог процеса, органи за спровођење закона могу *Nominet*-у да упуте званичне потврде о кривичном делу почињеном при коришћењу .uk домена или у вези са садржајем на њему, што доводи до суспендовања таквог домена у року од 48 сати од обавештења регистранту и овлашћеном регистру домена. Годишње се објављује извештај о криминалитету.

Ирски регистар (.ie) ради на реализацији кооперативног аранжмана са локалном управом полиције.

Политика *DK Hostmaster*-а (.dk) омогућава регистру слање података о регистрантима низу органа, укључујући полицију и тужилаштво, Министарство културе, Одбор за жалбе за називе домена, пореске органе и инспекторат за податке. Погледајте овде.

Регистри као даваоци релевантних података о називу домена

Као што је претходно поменуто, једино ефикасно решење за нелегални садржај је уклањање садржаја са интернета. Ако корисник или организација открију нелегални садржај на некој веб-локацији, једна од првих радњи коју треба предузети је обавештавање регистранта домена који може да уклони или измени садржај.

Регистар прикупља податке зато што му је потребна могућност да идентификује лице које је регистрант (његов клијент) и са којим може да ступи у контакт у случају спора, техничких проблема, промена одредаба и услова, уплата које нису извршене итд. Општи услови регистра обично изричито захтевају од регистранта да приликом регистрације наведе тачне податке и информације за контакт, као и да ове информације ажурира. Навођење погрешних или нетачних података представља кршење одредаба и услова и може да доведе до брисања назива домена.

Регистри улажу значајно време и труд у одржавање базе података назива домена. То не само да побољшава квалитет *WHOIS* података о регистрацији, већ такође може индиректно да има позитиван утицај, јер није вероватно да би неко с лошим намерама регистровао назив домена користећи тачне личне податке. Радње и праксе за одржавање базе података високог квалитета зависе од фактора који су специфични за одређени

регистар, као што су локално законодавство, величина регистра, број обрађених регистрација итд. и могу да се састоје од:[19]

- површне провере података наведених приликом регистрације, ради филтрирања очигледно нетачних уноса;
- аутоматизованих провера формата наведених података (нпр. формата имејла, броја телефона);
- провере правне документације коју је доставио регистрант, у земљама где таква обавеза постоји;
- насумичне верификације података регистрације за већ регистроване називе домена (нпр. регистар насумично бира и верификује одређени број домена дневно, месечно или годишње);
- верификације података у случају притужбе;
- унакрсне провере наведених података са званичним базама података (нпр. важећи поштански број, важећи број телефона, број компаније/организације или национални идентификациони број, ако су такве информације обавезне приликом регистрације).

Важно је приметити да многи регистри националног домена највишег нивоа немају директан контакт с регистрантом назива домена. Тамо где је то случај, сви контакти, укључујући давање и ажурирање података регистрације, одвијају се преко овлашћеног регистра.

Примери напора које регистар предузима ради добијања и одржавања тачних података о регистрацији

Norid (.no) захтева да сви регистранти буду регистровани или у Норвешком централном координационом регистру за правна лица или у Националном регистру за физичка лица. Такође, .no регистар редовно проверава да ли правна лица као власници домена још увек постоје према Централном координационом регистру за правна лица. Домени у власништву правних лица која су угашена аутоматски се бележе за уклањање.

DK Hostmaster (.dk) захтева од данских регистраната домена да се идентификују користећи *MitID*, решење за пријаву које користе данске банке, државне веб-локације и друге приватне компаније. Инострани регистранти подлежу провери ризика која ће утврдити да ли ће они добити захтев за подношење доказа о идентитету пре регистрације (високи ризик) или у року од 30 дана после регистрације (ниски ризик); неризични корисници нису обавезни да поднесу доказ. Ако регистрант не може или одбија да обезбеди доказ о свом идентитету, назив домена се суспендује. *DK Hostmaster* је такође увео и формулар за контакт који корисницима омогућава да пријаве нетачне податке о регистрантима, након чега је регистар у законској обавези да додатно испита случај како би обезбедио тачност података. Погледајте овде и овде.

19 Ови примери су засновани на анкети чланица *CENTR*-а из 2017. г

SIDN (.nl) сматра да лажне веб-продавнице наносе штету репутацији .nl домена, као јаког и сигурног домена највишег нивоа. Увео је системе за рано откривање домена који се користе за лажне веб-продавнице и проверава извештаје жртава превара и информације добијене од Националне канцеларије за извештавање о интернет преварама. Ако су подаци о регистрацији назива домена лажни, регистар може да их деактивира.

SWITCH (.ch): Регистрација назива .ch домена не захтева проверу идентитета регистранта. Међутим, ако постоји разлог да се верује да регистрант (a) даје лажне идентификационе податке или незаконито користи идентитет треће стране и (b) да ће користити тражени назив домена у незаконите сврхе или на незаконит начин, регистар .ch има право да не активира назив домена све док не потврди идентитет регистранта. Овај нови инструмент предвиђен је Правилником о интернет доменима и заснива се на обавези регистранта назива домена да дају тачне идентификационе податке. У случају да се регистрант не идентификује исправно у року од 30 дана, назив домена се опозива. Погледајте овде.

Неки регистри имају успостављене посебне процедуре за пријаве или жалбе у вези с лажним подацима о регистрацији:

Nominet (.uk) жалбе на нетачне WHOIS податке

Afnic (.fr) захтев за верификацију информација о регистранту, што доводи до блокирања назива домена у року од седам дана.

DNSBelgium (.be): Revoke/Revoke+

Дељење података о регистрацији с трећим странама

Регистри морају да поштују локалне законе о заштити података о личности приликом дељења информација о регистрантима с трећим странама. Политика и процедура добијања контакт-информација могу се наћи на веб-локацији регистра. Постоје различите праксе. Неки регистри захтевају ручно уношење информација преко онлајн-обрасца, други регистри обезбеђују директан (ограничено после *GDPR*-а) приступ бази података о регистрацијама (преко *WHOIS* протокола), док су други креирали алат који омогућава директно слање поруке регистранту.

Примери

AFNIC (.fr) поседује образац захтева за откривање личних података приватног лица које је регистрант назива домена и обезбеђује интерфејс који омогућава трећим лицима да пошаљу поруку регистранту без познавања њиховог имејла.

DomReg (.lt) поседује образац који корисницима омогућава да ступе у контакт с регистрантима назива домена.

Norid (.no) нуди ограничену претрагу домена у оквиру које јавност може да пронађе имејл регистранта и додатне информације о регистранту, у случају када је регистрант правно лице. Погледајте овде.

DENIC (.de) подржава и опште захтеве и контакт за пријаву злоупотребе назива домена

електронском поштом било контакту регистранта било овлашћеном регистру без дељења података регистранта. Поред тога, *DENIC* нуди различите обрасце за агенције за спровођење закона и носиоце легитимног интереса како би омогућио ефикасно подношење пратеће документације за откривање података у потпуној сагласности са *GDPR*-ом.

AFNIC (.fr) Обраћање административној контакт особи назива домена

DomReg.lt (.lt) „Обраћање регистранту домена“

РНИДС (.срб, .rs) члан 14. Општих услова

Одговарање на извештаје о сумњивом садржају

Одговарање на извештаје из спољних извора

Неки регистри имају успостављене процедуре за блокирање или суспендовање назива домена у одређеним случајевима, као одговор на извештаје о сумњивом садржају. Ове процедуре обично имају заједничко то што су применљиве на ограничен број случајева, као и на добро дефинисане случајеве, те да је укључена трећа страна са експертизом у процени таквог типа садржаја.

Таква процедура може бити корисна када је потребно доста времена да се донесе судска одлука за опозив домена. Једна од опасности је да подносиоци жалбе нису свесни ограниченог утицаја мере коју је предузео регистар и не предузимају даље радње за уклањање садржаја са интернета.

Примери

SIDN (.nl) је успоставио добровољну процедуру „Notice-and-Take-Down“ (Обавести и уклони), која је заснована на холандском националном кодексу понашања *„Notice-and-Take-Down”*. Процедура „Notice-and-Take-Down“ се може покренути само када подносилац жалбе може да докаже да су предузете све потребне мера да би се ступило у контакт с онима који су објавили садржај, администратором веб-локације, регистрантом и овлашћеним регистром назива домена, јер је реч о странама које могу ефикасно да реше проблем и уклоне садржај. Само у недвосмисленим нелегалним случајевима *SIDN* може одлучити да (привремено) уклони *DNS* сервере за неки домен.

Switch (.ch): Правилник о интернет доменима садржи правни основ за блокирање назива домена у случају „оправдане сумње да је тај домен коришћен (a) за приступ кључним подацима нелегалним методама; (b) за дистрибуцију злонамерног софтвера или (c) за обе активности. Ако су критеријуми Правилника о интернет доменима испуњени, тела која је Савезна канцеларије за комуникације (*OFCOM*) признала могу захтевати суспензију назива домена на ограничени период од 30 дана. Ако се по истеку рока од 30 дана не предузму додатне мере, суспензија се укида. Погледајте овде.

DNS Belgium (.be) је успоставио процедуру за обавештавање и деловање у сарадњи са *FPS Economy*. Ово подразумева да по достављању извештаја *FPS Economy* о озбиљним кршењима, *DNS Belgium* онемогућава приступ .be доменима у питању тако што мењања *name server*-е и преусмерава корисника на страницу са упозорењем. Ако регистранти назива домена не могу да докажу своју добру вољу и намеру, називи домена се уклањају. Погледајте овде и овде.

EURid (.eu, .ею, .ευ) сарађује са различитим организацијама и институцијама чији је циљ борба против сајбер-криминала (фалсификовање производа, пиратерија, фишинг, итд.). Ова сарадња помаже да се *EURid*-ова база података за регистрацију очисти од лажних назива домена, те да се успостави сигурнији доменски простор за кориснике интернета.

TRAFICOM (.fi): члан 172. Закона о услугама електронске комуникације TRAFICOM-у обезбеђује право да предузме неопходне мере за откривање, спречавање, истрагу значајних кршења информационе безбедности усмерених против јавних комуникационих мрежа или услуга које употребљавају .fi домен или су његови регистранти и предузимање предистражних радњи у вези с тим. Мере могу бити усмерене на податке централног регистра о .fi домену и могу укључивати следеће: 1) спречавање и ограничавање саобраћаја ка називу домена; 2) преусмеравање саобраћаја ка називу домена на другу адресу и 3) било које упоредиве техничке мере у смислу пододељака 1–2. Регистар може да уклони домен у случају нетачних и застарелих података о регистранту назива домена на основу којих није могуће утврдити идентитет, при чему регистрант назива домена није, без обзира на захтев, исправио или допунио податке или је суд забранио коришћење домена или у случају да Управа Финске за заштиту конкуренције и потрошача или тела за надзор тржишта донесу одлуку о уклањању домена.

Октривање незаконитих радњи додатним мерама

Како би подржали унапређење заштите потрошача и безбедност на мрежи, поједини регистри су развили алате и/или аутоматизоване процесе који помажу у идентификацији нелегалних активности или злоупотребе на мрежи. Ове праксе се крећу од редовног скенирања назива домена ради откривања превара до техничких алгоритама чији је циљ откривање покушаја крађе идентитета.

Примери

SIDN Labs (.nl) је развио *DMAP*, програм трагач који сваког месеца, између осталог, скенира све .nl домене у потрази за карактеристикама повезаним са преварама како би идентификовао незаконите активности (нпр. лажне веб-продавнице). Погледајте овде и овде.

EURid (.eu, .ею, .ευ) је развио механизам за спречавање злоупотребе под називом *APEWS*, који предвиђа злонамерне регистрације, тј. да ли се назив домена потенцијално користи за злоупотребе. У случају да *APEWS* утврди да би регистровани назив домена могао бити повезан са злоупотребом, одложиће се његов унос у .eu зону. *EURid* потом проверава ове називе домена и може захтевати од регистраната да потврде своје податке пре него што донесе одлуку о уносу назива домена у .eu зону или о суспензији. Погледајте овде.

Nominet (.uk) је развио систем за заштиту од крађе идентитета под називом Domain Watch, који идентификује и суспендује домене који покушавају да украду идентитет техничким алгоритмима и ручним интервенцијама. Ако је домен суспендован, овлашћени регистри и регистранти се обавештавају имејлом. Домен се поново активира у случају да регистрант потврди легитимну употребу назива домена.

Закључак

Увредљиви и нелегални садржаји смањују поверење у интернет. Локални правни оквири дефинишу садржај који је нелегалан и органе који су надлежни за поступање с њим у оквиру правног система. То се може разликовати од земље до земље.

Уклањање нелегалног садржаја са интернета је једино ефикасно решење које спречава приступ таквом садржају и његово коришћење. Онај ко објављује садржај и пружалац услуга хостинга имају директан приступ садржају или уређају на којем је ускладиштен садржај. Регистри националног домена највишег нивоа немају приступ садржају, не хостују нити преносе садржај путем своје инфраструктуре.

Регистри националног домена највишег нивоа посвећени су давању доприноса свеобухватном и ефикасном приступу борби против нелегалног онлајн-садржаја, развијају политике и предузимају иницијативе:

- за подизање свести и едукацију својих заједница о опасностима на интернету;
- за унапређење сарадње са органима за спровођење закона и надлежним органима;
- за обезбеђивање података о регистрацији у случају сумњивих назива домена;
- за одговарање на извештаје о називима домена коришћеним да се омогући приступ сумњивом садржају, у оквиру локалне надлежности.
- као помоћ у идентификацији нелегалних активности на добровољној основи.

Успешне политике и праксе приказане у овом документу могу да инспиришу друге националне домене највишег нивоа. Међутим, због локалног порекла и особености, не постоји гаранција да ће копирање пројекта или политике довести до истог позитивног резултата или да ће уопште бити легално у случају другог националног домена највишег нивоа.

Council of European National Top-Level Domain Registries

О CENTR-у

CENTR је европско удружење националних регистара домена највишег нивоа (*ccTLD*), као што су .de у Немачкој и .rs и .срб у Србији. CENTR тренутно има 52 пуноправна члана и 9 придружених чланова који су заједно одговорни за више од 80% регистрованих назива домена на свету.

Циљ CENTR-а је да промовише развој и учествује у развоју високих стандарда и најбољих пракси међу *ccTLD* регистрима.

Пуноправни чланови могу бити организације које су национални регистри домена највишег нивоа.

КОНТАКТ

CENTR VZW/ASBL
Belliardstraat 20
1040 Brussels, Belgium
0885.419.166 | RPR Brussels

+32 2 627 5550

secretariat@centr.org

www.centr.org

ПРАТИТЕ НАС

Да бисте се информисали о активностима и извештајима, пратите CENTR на Twitter-у и LinkedIn-у.

Датум: 13. мај 2022.

Превод документа омогућила је Фондација Регистар националног интернет домена Србије (РНИДС).
рнидс.срб | rnids.rs