Stanje digitalnih prava i sloboda u Srbiji - pregled za 2016. godinu

Tokom protekle tri godine, od osnivanja stručnog tima SHARE Fondacije - grupe pravnika, sajber forenzičara i stručanjaka, okupljenih da prate, pružaju pomoć i analiziraju napade na naša prava i slobode u onlajn okruženju - zabeležili smo više od 300 pojedinačnih slučajeva i kreirali bazu podataka za monitoring, koja čini i osnovu naše analize.[1]

Svedočili smo različitim povredama prava unutar digitalne zajednice u Srbiji, koje obuhvataju blokiranje ili filtriranje sadržaja, sajber napade na nezavisne onlajn i građanske medije, privođenja i sudske procese protiv korisnika društvenih mreža i blogera, manipulacije javnim mnjenjem različitim tehničkim alatima, nadzor elektronskih komunikacija, kršenje prava na privatnost i zaštitu podataka o ličnosti; pritiske, pretnje i ugrožavanje sigurnosti novinara onlajn i građanskih medija i pojedinaca.

Najčešće korišćen metod tehničkih napada bilo je distribuirano uskraćivanje usluga, DDoS. Ovu vrstu napada koristili su različiti akteri u Srbiji, a na meti su bili sajtovi onlajn medija i nevladinih organizacija, vladajuće partije, pa čak i sajt predsednika države. DDoS napadi su prilično neefikasan metod cenzurisanja: trajanje im je ograničeno i ne uništavaju sadržaj trajno.

Iako napadi na medije predstavljaju tešku povredu prava na slobodu izražavanja i pristup informacijama, kada je usmeren na pojedince, odnosno novinare, napad je još intruzivniji. posledice nisu uvek vidljive u javnosti i često prođu nezapaženo, ali kod novinara ciljani napadi izazivaju strah, osećaj pritiska i zebnje.

“Umreženi” izbori

Kada govorimo o stanju digitalnih prava i sloboda u Srbiji, prvu polovinu godine su svakako obeležili aprilski parlamentarni izbori kao najvažniji društveni događaj u toku godine. Promovisanje političkih ideja u digitalnom okruženju za vreme kampanje je određenim političkim akterima (npr. Dveri, Dosta je bilo, SRS) pomoglo da ostvare svoje izborne ciljeve, tj. da osvoje

[1] http://monitoring.labs.rs/

mesta u parlamentu.[2] Strategija kampanje na mreži, kao i oflajn kampanja, podrazumeva različite vrste podmetanja protivničkim akterima, što smo mogli da primetimo i tokom izbora u Srbiji. Najuočljivija i svakako najinteresantnija taktika koju smo zabeležili je manipulacija sadržajem tako da izgleda kao da pripada određenom političkom akteru. Na primer, kreirani su video-sadržaji, pa čak i čitavi Jutjub kanali koji sasvim verodostojno izgledaju, sa ciljem da se pripišu određenoj političkoj opciji kako bi se ona diskreditovala. Takođe, primećeno je i korišćenje astroturfinga, odnosno "obrnute cenzure" koji podrazumeva upotrebu alata koji omogućavaju korišćenje višestrukih identiteta, zloupotrebljavanje mehanizma glasanja, ometanje javne rasprave i kreiranje lažne slike o javnom mnjenju na mreži. Značaj predstavljanja političkih subjekata na mreži i verodostojnosti sadržaja ne bi trebalo da se dovodi u pitanje, jer očigledno postoje akteri sa dovoljno resursa da unesu potpunu pometnju u pogledu političkih sadržaja na mreži.

Prema našim istraživanjima, prosečan životni vek jedne vesti u onlajn medijima traje između jednog i dva sata. Tokom prva dva sata, vest se šeruje i komentariše, a onda joj se gubi trag u gomili prošlih sadržaja, smenjuju je nove kratkoročne vesti i verovatno se više nikada neće videti. Brzi tempo produkcije informacija diktiraju tri najveće novinske agencije u Srbiji (Tanjug, Beta, FoNet) koje zajedno proizvode više od 60% vesti koje onlajn mediji samo prenose. Originalni sadržaji onlajn medija čine svega jednu četvrtinu analiziranih vesti.[3]

Sa konstantnim protokom informacija na mreži zapravo živimo u vremenu permanentne kampanje, a pravila izborne tišine i političkog marketinga nisu u potpunosti razjašnjena kada je reč o mnogobrojnim onlajn platforamama. Takođe, Republička i druge izborne komisije nemaju kapacitete da isprate svaki pojedinačni slučaj kršenja izborne tišine na internetu. Kao što smo već naveli, analiza tvitova sa popularnim haštagovima na Tviteru tokom kampanje (npr. #izbori2016) pokazala je formiranje polarizovanih mreža korisnika i "čvorišta", u zavisnosti od toga na koji način koriste tviter, tj. da li napadaju Tviter naloge i predstavnike drugih stranaka ili promovišu članove sopstvene političke grupacije.[4] Takva atmosfera zaista ne doprinosi stvaranju uslova za demokratičan i slobodan politički dijalog.

---

[2] #izbori2016: Kampanja na mrežama se isplati, SHARE Fondacija, 2016. Dostupno na: http://www.shareconference.net/sh/defense/izbori2016-kampanja-na-mrezama-se-isplati

[3] Mapping and quantifying political information warfare: part 1 - propaganda, domination & attacks on online media, SHARE Lab, 2016. Dostupno na: https://labs.rs/en/mapping-and-quantifying-political-information-warfare/

[4] Analiza onlajn medija i društvenih mreža tokom izbora 2016. u Srbiji, SHARE Lab, 2016. Dostupno na: https://labs.rs/sr/analiza-onlajn-medija-i-drustvenih-mreza-tokom-izbora-2016-u-srbiji/

Imajući u vidu da nas u 2017. očekuju redovni izbori za predsednika Republike, a možda čak i novi vanredni parlamentarni izbori, pozivamo sve političke aktere da prihvate principe Deklaracije o poštovanju internet sloboda u političkoj komunikaciji, koju je 2014. godine SHARE Fondacija razvila u saradnji sa partnerskim organizacijama i internet zajednicom.[5] Takođe, u našem Vodiču o digitalnim pravima i internet slobodama u političkoj komunikaciji[6] su objašnjene preporuke za otvorenu, slobodnu i uravnoteženu političku debatu o pitanjima od javnog interesa, kao i mehanizmi za prijavljivanje povreda prava u izbornoj kampanji.

Tehnički napadi - "prošla opasnost" ili razlog za oprez?

Tokom 2016. SHARE tim je zabeležio petnaestak slučajeva tehničkih napada, ali ne možemo da ne podsetimo na činjenicu da napadi iz prethodnih godina još uvek nisu dobili ishod pred sudom, uprkos naporima nadležnih organa.

Primećeno je da su se, kada je reč o medijima, u najmanje dva primećena navrata sajber napadi na sajtove (Danas, Pištaljka) dogodili neposredno posle izveštavanja o temama koje su u vezi sa najvišim državnim funkcionerima i njihovim neposrednim okruženjem. Takođe zanimljiva pojava bili su slučajevi "zaključavanja naloga" na društvenim mrežama pojedincima koji su izražavali mišljenje o problemima i pokretali debate o značajnim pitanjima u društvu. Novinari, lokalni odbornici, ali i "obični" građani su prijaviljivali probleme sa svojim nalozima na Tviteru i Fejsbuku, koji su na nepoznat način suspendovani, tj. onemogućeno im je da pristupaju nalozima. Tehnička analiza SHARE Fondacije u jednom slučaju, a reč je o Tviter nalogu, nije uspela da utvrdi koji je mehanizam ova platforma iskoristila da iz "bezbednosnih razloga" suspenduje nalog, kako je navedeno u mejlu koji je Tviter poslao korisniku. Naša pretpostavka je da postoje načini da se tehničkim metodama kod platformi podigne "uzbuna" da neko pokušava da nasilno (*brute force*[7]) pokušava da preuzme nalog, te da se tako onemogući pristup nalogu sve dok pravi vlasnik putem mejla ne "otključa" nalog.

Iako je u 2016. godini zabeležen pad povreda digitalnih prava tehničkim putem, ne bi trebalo zanemariti pretnju koju sajber napadi na integritet sadržaja predstavljaju, naročito po slobodu izražavanja i informisanja na internetu. Svaki DDoS napad na sajtove medija ili izmena

[5] http://deklaracija.net/
[6] Vodič o digitalnim pravima i internet slobodama u političkoj komunikaciji, dostupan na: http://www.shareconference.net/sites/default/files/u742/9_-_vodic_political_web.pdf
[7] http://searchsecurity.techtarget.com/definition/brute-force-cracking

naslovne strane ubacivanjem malicioznog koda (*defacing*) šalje poruku koje su teme i informacije "nepoželjnje" u javnom diskursu, što može obeshrabiti druge medije da profesionalno, istinito i potpuno izveštavaju.

Upravljanje sadržajem i algoritamske nedoumice

Protok informacija u onlajn sferi sve je više posredovan algoritmima koji nam na osnovu naših aktivnosti prikazuju vesti, reklame, objave drugih korisnika i ostale sadržaje. Društvene mreže i druge onlajn platforme, u skladu sa svojim uslovima korišćenja, uklanjaju sadržaje i suspenduju naloge koji krše pravila same platforme i/ili zakonske norme, bilo da je reč o kršenju prava intelektualne svojine, govoru mržnje ili vređanju korisnika.

Sadržaji se najčešće uklanjaju po prijavi korisnika, putem mehanizama (report, flag) koji korisnicima omogućavaju da ukažu administratorima na problematične sadržaje. Međutim, sama procedura za uklanjanje sadržaja se pokazala netransparentnom, što dovodi do situacija da je nečiji sadržaj uklonjen pod veoma čudnim okolnostima. Neprijatno iskustvo u protekloj godini sa algoritamskim urednicima Jutjuba imao je čak i nezavisni državni organ sa mandatom da štiti pravo građana Srbije na slobodu izražavanja. Naime, u avgustu je zvanični Jutjub kanal Zaštitnika građana bio suspendovan, navodno zbog kršenja pravila te platforme koja zabranjuju govor mržnje, pretnje i tome slično, iako su na kanal postavljani samo video-snimci nastupa Zaštitnika građana Saše Jankovića u medijima. Žalba koju je Jutjubu uputila kancelarija Zaštitnika je najpre odbijena, a kako se ispostavilo da je reč o nesporazumu, pristup Jutjub kanalu je ubrzo ponovo omogućen.[8]

U određenim slučajevima je teško utvrditi da li je reč o koordinisanim manipulacijama mehanizama uklanjanja sadržaja u digitalnom okruženju ili propustima algoritama - to dodatno otežava netransparentnost samog procesa uklanjanja sadržaja. Međutim, brza reakcija Tvitera, ponovo u slučaju Zaštitnika građana Saše Jankovića, prilikom suspenzije njegovog lažnog naloga pokazuje značaj verifikacije identiteta na ovoj društvenoj mreži, koja je odnedavno

[8] Kako mreže uređuju javni prostor: YouTube protiv Ombudsmana, SHARE Fondacija, 2016. Dostupno na: http://www.shareconference.net/sh/defense/kako-mreze-ureduju-javni-prostor-youtube-protiv-ombudsmana

omogućila “potvrdu” naloga širem krugu korisnika pomoću jednostavne procedure.[9] Ipak, pitanje je koliko će druge platforme raditi na verifikaciji identiteta korisnika i njihovih profila, što može da implicira prikupljanje dodatnih podataka o ličnosti. Međutim, za sada nema naznaka da će se broj lažnih profila, botova i trolova smanjiti sa porastom “potvrđenih” profila.

Pretnje, uvrede i pritisci

Veliki deo slučajeva koje beležimo u monitoringu digitalnih prava čine različite vrste prekoračenja slobode izražavanja i pritisaka zbog aktivnosti i izražavanja na mreži (iznošenje neistina, uvrede, omalovažavanje, pretnje i ugrožavanje sigurnosti...). U poređenju sa 2015. godinom, kada je tokom monitoringa zabeleženo 104 slučaja iz ove kategorije, SHARE Fondacija je 2016. godine primetila 91 slučaj, što govori o blagom padu. Međutim, utisak je da se u 2016, kao i prethodnih godina, broj pretnji, uvreda i drugih pritisaka drži visoko jer zapravo nema dovoljno slučajeva sa pravnim posledicama, naročito kada su mete novinari ili aktivisti civilnog društva. Kao što smo napominjali i ranije, selektivnost reakcije[10] nadležnih organa u slučajevima upućivanja pretnji samo doprinosi da se trend nekažnjivosti nastavi, naročito jer je za ugrožavanje sigurnosti novinara Krivičnim zakonikom zaprećena stroža kazna.

Pod “selektivnom reakcijom” podrazumevamo različite pristupe nadležnih organa u slučajevima pretnji u onlajn okruženju kada je reč o nosiocima javnih funkcija sa jedne i novinarima i aktivistima sa druge strane. U nekoliko navrata, na percipirane i stvarne pretnje državnim funkcionerima koje su upućivane na društvenim mrežama odgovoreno je brzom i efikasnom reakcijom, odnosno privođenjem osumnjičenih. Problem je u tome što novinari[11] i predstavnici civilnog sektora[12] koji se suočavaju sa kontinuiranim pretnjama dugo čekaju ishode istraga, u kojima gotovo da nema napretka, iako se iz drugih primera vidi da itekako postoje načini da se pronađu i procesuiraju potencijalni počinioci. Kao izuzetak možemo da izdvojimo slučaj pretnji na Fejsbuk stranici portala Cenzolovka, čija je meta bio kolumnista i gl. i odg. urednik Danasa Dragoljub Draža Petrovića, kada je za veoma kratko vreme pronađena i privedena osoba osumnjičena za postavljanje pretećih komentara. Zanimljivo je da se ovaj primer brze i efikasne

[9] https://support.twitter.com/articles/20174631
[10] Milica Jovanović, Selektivna zaštita, SHARE Fondacija, 2015. Dostupno na: http://www.shareconference.net/sh/blog/selektivna-zastita
[11] https://twitter.com/SlobaGeorgiev/status/811171343190360064
[12] https://twitter.com/goranmiletic/status/806189745692938240

reakcije na pretnje novinaru podudara sa objavljivanjem izveštaja Evropske komisije o napretku Srbije za 2016. godinu, u kome se upravo ističe da su istrage i pravosnažne presude za napade i zastrašivanje novinara retkost.[13]

Kada je reč o napadima na medije i novinare, uprkos svim teškoćama, uočen je razvoj mehanizama koji mogu doprineti bližoj saradnji medijske zajednice i nadležnih organa. Krajem decembra, novinarska udruženja, Republičko javno tužilaštvo i Ministarstvo unutrašnjih poslova potpisali su Sporazum o saradnji i merama za podizanje nivoa bezbednosti novinara[14], koji bi trebalo da služi kao osnov bolje zaštite integriteta novinara. Razume se, zaštita od pretnji i verbalnih napada nije rezervisana isključivo za novinare, već za sve građane, bez obzira na njihov društveni položaj. Međutim, važno je napomenuti da upravo zbog svoje funkcije "pasa čuvara" (*watchdog*) u demokratskom društvu, napadi i pritisci na novinare i civilno društvo moraju da se sankcionišu na adekvatan način i budu stvar prioriteta. Bez garancije bezbednosti, oflajn i onlajn, ne može se dostići pun nivo slobode izražavanja i informisanja.

Agencija za privatizaciju - "zastarela" privatnost

Kraj 2016. godine obeležilo je zastarivanje postupka[15] protiv odgovornih lica u Agenciji za privatizaciju, koji se vodio zbog najvećeg prodora u privatnost građana Srbije. Posle intervencije kancelarije Poverenika za informacije od javnog značaja i zaštitu podataka o ličnosti, 12. decembra 2014. sa sajta tadašnje Agencije za privatizaciju uklonjena je baza sa podacima o ličnosti više od 5 miliona građana Srbije,[16] koja je do tada bez ikakvog pravnog osnova bila javno dostupna na internetu preko 10 meseci. U pitanju je bila baza podataka iz evidencije nosilaca prava na besplatne akcije, koja je sadržala imena, srednja imena, prezimena i jedinstvene matične brojeve građana (JMBG).

---

13 http://seio.gov.rs/upload/documents/eu_dokumenta/godisnji_izvestaji_ek_o_napretku/godisnji_izvestaj_16_eng.pdf

14 http://www.ndnv.org/2016/12/27/potpisan-sporazum-o-saradnji-i-merama-za-podizanje-bezbednosti-novinara/

15 https://twitter.com/PoverenikRS/status/808421403020165120

16 Neovlašćeno objavljeni podaci o ličnosti više od 5 miliona građana Srbije, SHARE Fondacija, 2014. Dostupno na: http://www.shareconference.net/sh/defense/neovlasceno-objavljeni-podaci-o-licnosti-vise-od-5-miliona-gradana-srbije

Poverenik Rodoljub Šabić je na svom blogu još u septembru upozorio javnost[17] da će prekršajni postupak gotovo izvesno zastariti i opisao tok suđenja, tokom koga se odgovorna lica Agencije nisu nijednom pojavila na zakazanim ročištima u Prekršajnom sudu u Beogradu, čak ni posle izdate naredbe za dovođenje i urgencije koja je poslata MUP-u. Kako je Šabić naveo, nema informacija da je nadležno tužilaštvo bilo šta preduzelo povodom krivične prijave koju je kao Poverenik podneo.

Čini se da je na kraju 2016. godine privatnost građana u stanju "zastarelosti", ne samo zbog slučaja Agencije za privatizaciju i masovne kompromitacije podataka o ličnosti, već i u pogledu pravnog okvira. Naime, još uvek nije usvojen novi Zakon o zaštiti podataka o ličnosti, iako je javna rasprava okončana krajem 2015. godine.[18] U međuvremenu, Evropska unija je usvojila novi regulatorni okvir, Regulativu o zaštiti podataka o ličnosti, koja na snagu stupa već 2018, dok je u Srbiji ova oblast od izuzetnog značaja za privatnost građana "na čekanju".

Analizirani slučajevi napada na prava i slobode u onlajn okruženju

U protekloj godini, značajno je smanjen broj tehničkih napada na onlajn medije, bar u odnosu na 2014. i 2015. kada su napadi po broju i obimu bili mnogo veći. Jedan od razloga je povećana svest onlajn media u sferi zaštite informacionih sistema, ali i pojava drugih mehanizama pritiska koje ne podrazumevaju onlajn napade.

U ovom delu monitoring izveštaja smo obradili slučajeve koji su bili specifični i na kojima je tim SHARE Fondacije radio u smislu pružanja tehničke i pravne pomoći.

1. Slučaj I

Vrsta napada: Promena izgleda sajta istraživačkog medija (*defacement*)
Vreme restauracije: Nakon tri sata na domen je podignuta verzija samo za čitanje (*read-only*) iz sigurnosne kopije. Za uspostavljanje pune funkcionalnosti sajta sa editovanjem i objavljivanjem novih članaka, bilo je potrebno četiri dana.

[17] http://blog.b92.net/text/26924/ILUSTRACIJA-NE-KARIKATURA/
[18] Tražimo bolju zaštitu podataka o ličnosti,SHARE Fondacija, 2015. Dostupno na: http://www.shareconference.net/sh/defense/trazimo-bolju-zastitu-podataka-o-licnosti

Opis: Izgled sajta promenjen je 26. juna 2016, nekoliko minuta posle 11 sati uveče. Napadač je sa IP adrese 185.67.177.228 pristupio sajtu kao administrator i koristeći sistem za dinamičko upravljanje sadržajem, promenio izgled sajta postavljanjem slike.

Od prve posete sa IP adrese korišćene za napad, do pristupa sajtu sa administratorskim ovlašćenjem prošao je samo jedan minut, što bi moglo značiti da je napadač iskoristio očiglednu grešku u softveru da bi ukrao lozinku ili lansirao napad. Postoji mogućnost i da su administratorske lozinke bile jednostavne za pogađanje, ili da ih je neko iz organizacije, svesno ili slučajno, prosledio napadaču.

Pre ovog napada nisu postojale indicije da sajt ima bezbednosnih problema.

Inspekcija SHA1 lozinki koje se nalaze u bazi podataka, pokazala je da su se pojedine lozinke koristile više puta za pristup sajtu kroz administratorske (super-admin) naloge. Jedna lozinka je korišćena dva, a druga tri puta.

Rešenje: Prvi korak podrazumevao je uklanjanje izmenjenog sajta, a zatim njegovo vraćanje u režimu samo za čitanje (*read-only*) iz sigurnosne kopije koja nije zaražena malicioznim kodom. Pošto sistem pravi sigurnosne kopije sajta dva sata posle ponoći, poslednja sigurnosna kopija napravljena je blizu 24 sata pre napada.

S obzirom na to da je napadač imao potpuni pristup sistemu, pošlo se od pretpostavke da su kompromitovane sve lozinke, uključujući i one koje se koriste za pristup bazi podataka. Ove lozinke su odmah promenjene, dok su ostale lozinke generisane pre vraćanja sajta u punu funkcionalnost (*write-read*).

Kada je sajt u potpunosti restauriran, sledećeg jutra je nastavljeno istraživanje tačnog vektora koji je omogućio pristup sa administratorskim ovlašćenjima.

Preporuke: Potpuni pristup za čitanje i editovanje (*read-write*) trebalo da je moguć samo u direktorijumima gde je to nephodno za njihovo korišćenje. Potpuni pristup drugim direktorijumima bi trebalo ukinuti. Pokretanje PHP skripti u tim direktorijumima ne treba da bude moguće. Protokoli za autentifikaciju SSL/TLS bi trebalo da budu obavezni za sve pristupe i

korisničke i administratorske. Akreditacije za sve sajtove treba promeniti, ukloniti sve suvišne naloge i promeniti slabe lozinke.

2. Slučaj II

Vrsta napada: DDoS napad na veb sajt istraživačkog medija

Vreme restauracije: Zbog migracije sadržaja, bilo je potrebno sat vremena da se sajt podigne na novi server.

Opis: Napad je lansiran 2. septembra 2016, slanjem ogromne količine zahteva za pristup sajtu. U trenutku napada, administrator sajta je pripremao migraciju sadržaja na novi i bolji server. Kao izvore poplave zahteva, logovi pokazuju veliki broj IP adresa iz celog sveta, najviše iz SAD, što upućuje na zaključak da je u pitanju tzv. bot mreža, odnosno grupa zaraženih uređaja.

Postojeći server nije omogućavao logovanje preko standardnog porta za SSH (22 TCP port), već je izabran nestandardni port za SSH pristup serveru, što je pozitivna bezbednosna praksa. Logovanje je bilo omogućeno samo sa osam IP adresa, zbog čega nije bilo moguće logovanje na server sa korenskim (*root*) pristupom. To znači da je logovanje bilo omogućeno samo na korisničkom nivou, dok bi se osobe ovlašćene za korenski pristup logovale kao obični korisnici a zatim bi određenom komandom (*switch user*) menjali vrstu pristupa u korenski.

Sve lozinke su bile nasumične, sa 16 karaktera. Na serveru je bio implementiran *"fail2ban"* servis koji beleži svako pogrešno logovanje na server i zabranjuje pristup korisniku koji lozinku pogreši tri puta zaredom.

Organizacija je planirala migraciju sajta na novi server upravo na dan kada je došlo do napada. Nakon početka napada, administrator je odlučio da odmah započne migraciju, zbog čega je sajt bio nedostupan oko sat vremena. Sam napad je trajao 20 minuta, kada je pristup sajtu bio vrlo usporen.

S obzirom na okolnosti, malo je verovatno da je došlo do upada na server, jer su svi bezbednosni standardi ispunjeni. Za napad je odabrana poplava ogromnim brojem zahteva spolja, koji praktično onemoguće rad servera.

Serverski log generisan tokom napada je jako veliki (130 GB), a analizom njegovih segmenata utvrđeno je da IP zahtevi dolaze iz celog sveta, najviše iz SAD.

Rešenje: Nakon migracije, sajt je prebačen na novi server sa svežim hardverom i softverom. Uspostavljene su sve standardne mere tehničke zaštite, uključujući i mitigaciju DDoS napada u dva sloja - kroz serverska podešavanja za blokiranje svake IP adrese koja pošalje više od 10 zahteva na 5 sekundi, kao i mitigaciju hosting provajdera (*Hetzner*), koji posebnim filterom (*firewall*) ublažava DDoS i druge vrste napada na server.

Preporuke: Implementacija mehanizma za mitigaciju DDoS napada. Podešavanje servera za blokiranje upornih zahteva nakon određenog vremena.

3. Slučaj III

Vrsta napada: DoS/DDoS napad na medijski veb sajt

Vreme restauracije: Nekoliko sati

Opis: Na samom kraju izborne kampanje, 21.04.2016. napadnut je medijski sajt iz sandžačke oblasti. Napad je počeo oko 17 časova, a trajao je nekoliko sati. U tom periodu pomenuti sajt je bio nedostupan. Nakon završetka napada, funkcionalnost sajta je normalizovana i sajt je ponovo dostupan.

U trenutku napada, na serveru koji hostuje sajt nisu bila aktivna podešavanja za sigurnosnu kopiju (*back-up*), te su se nakon restartovanja servera log fajlovi automatski brisali. Po okončanju napada, server je restartovan a log fajlovi trajno obrisani, zbog čega nije bilo moguće precizno utvrditi detalje napada ni njegov izvor.

Rešenje: Incident je prijavljen posle napada kada je sajt već bio ponovo funkcionalan. Usled nedostatka serverskih logova, nije bilo moguće uraditi detaljniju analizu.

Preporuke: Implementacija mehanizma za mitigaciju DDoS napada. Podešavanje servera za blokiranje upornih zahteva nakon određenog vremena. Uspostavljanje mehanizma za čuvanje sigurnosnih kopija sajta i serverskih logova na redovnom, dnevnom nivou.

4. Slučaj IV

Vrsta napada: DoS napad na veb sajt organizacije civilnog društva

Vreme restauracije: Nekoliko sati

Opis: Organizacija civilnog društva iz Beograda prijavila je da je sajt bio meta napada 29.02.2016. Nekoliko dana ranije, organizacija je dobila obaveštenje od svog hosting provajdera da je pristup sajtu ograničen usled velikog broja zahteva, što upućuje na zaključak da je tada lansiran DoS napad.

Sistem za monitoring saobraćaja hosting provajdera je zabeležio povećanu aktivnost na pomenutom sajtu sa IP adrese 132.150.226.76, registrovane kod kompanije Telenor u Norveškoj. Da bi se sprečio napad većeg obima, sistem je automatski onemogućio pristup sajtu i o tome obavestio organizaciju. Istovremeno, na Tviter nalogu @SRBnetw0rk objavljena su dva tvita u vezi sa napadom na veb sajt organizacije.

Rešenje: Prvi korak bilo je unapređenje hosting paketa, tako da on uključuje veći mesečni protok podataka. Iz ponude hosting provajdera takođe je aktivirana usluga mitigacije DoS/DDoS napada. Pregledani su serverski logovi i utvrđeno je da je IP adresa sa koje je napad upućen, registrovana na mreži Telenora u Norveškoj.

Preporuke: Implementacija mehanizma za mitigaciju DDoS napada. Podešavanje servera za blokiranje upornih zahteva nakon određenog vremena.

Pravni dodatak

U delu koji sledi predstavićemo pravnu analizu presuda koje su donete 2016. godine, a važne su za razumevanje ljudskih prava u digitalnom okruženju. Posebno ćemo pokušati da analiziramo rezon sudova ukada su u pitanju onlajn platforme, društvene mreže i kako sudovi primenjuju pravo na digitalno okruženje.

Ugrožavanje sigurnosti putem Interneta

1. **Slučaj Boris Malagurski protiv forumaša**

Na forumu *Parapsihopatologija* [19] 28.08.2012. godine je otvorena diskusija u kojoj su se pojavili uvredljivi komentari protiv oštećenih u ovom predmetu. Oštećeni u septembru 2012. godine podnose krivičnu prijavu protiv **12 članova foruma** *Parapsihopatologija* zbog organizovanih pretnji po život i ličnu i profesionalnu bezbednost prema članu 138, stav 3 Krivičnog zakonika. Identitet trojice forumaša, protiv kojih je pokrenut krivični postupak, utvrdili su internet provajderi Orion Telekom i SBB.

Proces koji sledi sastojao se iz nekoliko etapa:

1. Prvostepeni postupak - Viši sud u Beogradu 24.03.2015. donosi prvostepenu osuđujuću presudu protiv trojice optuženih i izriče krivične sankcije izdržavanja kazne zatvora u trajanju od godinu dana, uslovno 3 godine. Iako je utvrđena kazna zatvora od jedne godine, istovremeno se određuje da utvrđene kazne neće biti izvršene ukoliko okrivljeni u roku od tri godine od pravnosnažnosti ne izvrše neko novo krivično delo.
2. Drugostepeni postupak po žalbi okrivljenih - Apelacioni sud u Beogradu 09.09.2015. godine delimično uvažava žalbe branioca okrivljenih i preinačuje presudu Višeg suda u Beogradu, tako da dvojicu optuženih osuđuje na 6 meseci zatvora, uslovno 2 godine, a jedno lice na 4 meseca zatvora, uslovno 2 godine. Žalba je bila do određene mere uspešna u delu smanjivanja kazne, ali i dalje nedovoljno.
3. Postupak po vanrednom pravnom leku - okrivljeni nisu odustajali i iskoristili su zahtev za zaštitu zakonitosti, što je vanredni pravni lek, nakon čega Vrhovni kasacioni sud 20.01.2016. donosi oslobađajuću presudu.

Analiza presude Vrhovnog kasacionog suda kzz 1203/2015 od 20.01.2016. godine

Vrhovni kasacioni sud je naveo da je u zahtevu za zaštitu zakonitosi osnovano istaknuto da je primenjen zakon koji se nije mogao primeniti, što bi značilo da se radnje koje su preduzete od strane okrivljenih ne mogu smatrati krivičnim delom ugrožavanja sigurnosti.

Sud je zaključio da u izreci pravnosnažne presude nedostaje bitan element krivičnog dela ugrožavanja sigurnosti, a to je **pretnja da će se napasti na život i telo oštećenog**. Pretnja da bi bila element krivičnog dela mora biti ozbiljna, jer je krivično-pravno relevantna samo ukoliko je

[19] http://www.parapsihopatologija.com/forums/

ozbiljna i mora se odnositi na napad na život ili telo oštećenog lica. Posebno kada govorimo o verbalnoj pretnji, što je ovde slučaj, kojom se najavljuje napad, ona mora biti jasna i nedvosmislena u smislu da se iz toga može zaključiti da će izvršilac zaista i napasti oštećeno lice, bez obzira da li on to namerava da učini.

Međutim, nakon analize svakog pojedinačnog sadržaja koji je bio predmet ovog slučaja, sud je zaključio da su to bile izjave **šta okrivljeni misli da bi trebalo učiniti oštećenom, kakav poriv okrivljeni ima u odnosu na oštećenog, kao i šta bi okrivljeni voleo da neko učini oštećenom**, ali ne i da te izjave sadrže jasne i nedvosmislene pretnje da će upravo okrivljeni napasti na život i telo oštećenog.

Stoga, može se zaključiti da pretnja mora biti ozbiljna, jasna i nedvosmislena da bi postojao bitan element krivičnog dela ugrožavanja sigurnosti, što u ovom predmetu nije bio slučaj.

2. Južne vesti protiv komentatora

Još jedan slučaj pravnosnažno okončanog postupka[20] povodom krivičnog dela ugrožavanja sigurnosti, ovog puta onlajn medij Južne vesti podneo je krivičnu prijavu protiv lica koji je na njihovom sajtu ostavio komentar sledeće sadržine: *"Južne vesti su najveća medijska go..a u Nišu, **treba zapaliti da ne postoje**, lažljive, iskompleksirane degenerike koji tamo rade".*

Pravnosnažnom presudom Višeg suda u potvrđena je prvostepena oslobađajuća presuda Osnovnog suda u Nišu u korist okrivljenog. Kao što smo gore naveli kada govorimo o krivičnom delu ugrožavanje sigurnosti, pretnja je jedan od bitnih elemenata ovog krivičnog dela, a sud je došao do zaključka da se ni u ovom slučaju ne može govoriti o pretnji, iz razloga što okrivljeni "*niti jednog momenta **nije izrazio lične namere** za preduzimanjem bilo kakve radnje koje bi kod oštećenih ugrozila sigurnost. Samo u situaciji da je okrivljeni izrazio lične namere u pogledu delovanja prema oštećenima, pri čemu je bez uticaja da li bi te namere bile stvarne, moglo bi se govoriti o postojanju krivičnog dela ugrožavanje sigurnosti*".

[20] https://www.juznevesti.com/Drushtvo/Sud-Treba-zapaliti-novinare-nije-pretnja-vec-sloboda-govora.sr.html

Razmatrajući presude nadležnih sudova u Srbiji, stekli smo utisak da u slučajevima ugrožavanja sigurnosti nije bilo bitnog elementa ovog krivičnog dela, a to je pretnja, koja mora biti ozbiljna, jasna i nedvosmislena, kao i lična namera u pogledu delovanja da će se napasti na život i telo određenog lica. U svakom pojedinačnom slučaju mora se uzeti u obzir i celokupan kontekst u kojem su informacije objavljene, kao i tumačiti sve reči koje su izrečene na određenoj platformi.

Slučajevi uvrede putem Fejsbuka i Tvitera

Do Vrhovnog kasacionog suda došao je i predmet okrivljenog I.P. koji je podneo zahtev za zaštitu zakonitosti protiv pravnosnažnih presuda Osnovnog suda u Novom Sadu K 266/15 od 21.12.2015. godine i Višeg suda u Novom Sadu Kž1 110/16 od 24.06.2016. godine. U ovom slučaju osuđeno je lice zbog produženog krivičnog dela uvreda koje je učinjeno putem Fejsbuka iz člana 170. stav 2. KZ na novčanu kaznu od 250.000,00 dinara, zbog toga što je uvredio privatnu tužilju objavljivanjem više tekstova na svojoj Fejsbuk stranici.

Sud je ipak nakon razmatranja slučaja došao do zaključka da je zahtev neosnovan i potvrdio je presudu kojom je okrivljeni proglašen krivim. Navodi okrivljenog u zahtevu da se Fejsbuk stranica ne može smatrati sredstvom javnog informisanja nisu prihvaćeni. Sud je smatrao da Fejsbuk stranica na kojoj su objavljene informacije za koje se smatraju uvredljivim po stanovištu suda predstavlja sredstvo javnog informisanja. Ovim putem ćemo citirati kako Vrhovni kasacioni sud rezonuje Fejsbuk kao društvenu mrežu:

"...po nalaženju Vrhovnog kasacionog suda Fejsbuk stranica kao deo društvenih mreža, upravo zbog dostupnosti iste korisnicima ovih mreža na internetu predstavlja sredstvo ***slično*** *sredstvima štampe, radija ili televizije i sledstveno tome putem ovog sličnog sredstva - Fejsbuk stranice se može uputiti uvredljiva izjava i samim tim izvršiti krivično delo uvreda."*

Smatramo da se ovakvo rezonovanje Vrhovnog kasacionog suda svakako ne može prihvatiti, prvenstveno definisanje Fejsbuka kao sredstva koje je **slično** štampi, radiju ili televiziji. Evo i razloga za to:

Viši sud u Beogradu je u pravnosnažnoj presudi[21] koja je doneta 25.08.2015, u predmetu koji se ticao takođe krivičnog dela uvrede putem društvene mreže Tviter, došao do potpuno drugog zaključka. U prvostepenom postupku Osnovni sud u Beogradu je učinio istu stvar kao i Vrhovni kasacioni sud u predmetu gore navedenom, i oglasio krivim okrivljenog za krivično delo uvrede iz čl. 170 stav 2, tj. za kvalifikovani oblik dela koje je učinjeno putem štampe, radija, televizije ili sličnih sredstava ili na javnom skupu. Međutim, Viši sud je ovu presudu preinačio sa sledećim obrazloženjem:

"Odredbom člana 11 Zakona o javnom informisanju (koji je bio na snazi u vreme izvršenja krivičnog dela…) propisano je da su javna glasila novine, radio programi, televizijski programi, servisi novinskih agencija, Internet i druga elektronska izdanja navedenih javnih glasila….namenjene javnoj distribuciji i neodređenom broju korisnika. Međutim, kako društvena mreža Tviter predstavlja grupu individualno određenih internet korisnika koji su međusobno povezanih radi interpersonalne komunikacije i međusobne ramene informacija, mišljenja i ideja njenih članova, to se po oceni Višeg suda u Beogradu, ***ne može smatrati da je društvena mreža Tviter slična štampi, radiju ili televiziji koji predstavljaju sredstva javnog informisanja i namenjeni su javnoj distribuciji i neodređenom broju korisnika."***

Na osnovu prethodno navedene odluke Višeg suda, smatramo da je to jedino pravilno tumačenje. Posebno imajući u vidu važeći Zakon o javnom informisanju i medijima[22] koji u članu 30, stav 2 taksativno i nedvosmisleno propisuje šta nisu mediji, osim ako nisu registrovani u Registru medija, a u tu definiciju pored platformi i foruma izričito spadaju i **društvene mreže**. Stoga bi se moglo zaključiti da Vrhovni kasacioni sud nije u obzir uzeo celokupni pravni okvir, odnosno novi Zakon o javnom informisanju i medijima, koji je usvojen još avgusta 2014, ali ni stari Zakon o javnom informisanju. Na taj način se stvara sudska praksa koja direktno ugrožava slobodu mišljenja i izražavanja.

Na osnovu svega gore navedenom smatramo da na društvene mreže nikako ne može primenjivati čl. 170, stav 2 Krivičnog zakonika, posebno sa novim i jasnim odredbama Zakona o javnom informisanju i medijima. Što se tiče same uvrede, ona je i dalje krivično delo u našem Krivičnom zakoniku, iako se u celom svetu deži dekriminalizaciji krivičnih dela klevete i uvrede.

[21] Presuda Kž1 br. 465/15
[22] http://www.paragraf.rs/propisi/zakon_o_javnom_informisanju_i_medijima.html

Republika Srbija je 2013. dekriminalizovala klevetu kao krivično delo, ali iz nekih razloga krivično delo uvrede je ostalo u našem krivičnom sistemu. Problem kod krivičnog dela uvrede jeste to da ona predstavlja izjavu ili drugu radnju kojom se po objektivnoj oceni izražava omalovažavanje određenog lica. Ovaj pojam je jako širok i primenjiv na veliki procenat situacija koje se svakodnevno dešavaju na društvenim mrežama, te treba imati u vidu da, naravno u zavisnosti od svakog pojedinačnog slučaja, postoji velika verovatnoća da budete osuđeni za krivično delo uvrede, ali svakako ne i za kvalifikovani oblik koji je učinjen putem sredstava javnog informisanja.

Prvenstveno, ovo su sve nove pojave i novi slučajevi koji se javljaju pred sudovima, pa se ne bi moglo reći da postoji potpuno razumevanje digitalnog okruženja i svih stvari koji se u njemu dešavaju. Ali važno je da smo videli kako dobre tako i loše primere prakse. Nadamo se da će se u budućnosti sudska praksa više razvijati u dobrom smeru, kao i da će korisnici podići svest i biti odgovorniji prilikom slobodnog izražavanja na mreži, kako bi ovakvih slučajeva bilo sve manje.

Preporuke i budući koraci

Ključne posledice ugrožavanja digitalnih prava i internet sloboda ogledaju se u pravnoj nesigurnosti jer počinioci retko budu otkriveni i procesuirani. Takođe, u sajber prostoru, odbrana je uobičajeno skuplja nego napad, što prilično obeshrabruje male i nezavisne onlajn i građanske medije koji ne mogu sebi da priušte skupe stručnjake za sajber bezbednost ili tehnička rešenja za zaštitu. Smanjenje broja tehničkih napada većih razmera takođe ne znači da ne treba raditi na unapređenju odbrambenih kapaciteta. Osvajanje višeg nivoa digitalne bezbednosti često podrazumeva složene procedure, promenu uobičajenih navika pri korišćenju tehnologije, što može umanjiti efikasnost novinara i organizacija.

Napadi i pritisci na novinare i pojedince zbog blogova, komentara ili drugih oblika onlajn izražavanja ima za posledicu efekat zebnje ne samo na novinare i medijske organizacije, već i na širu onlajn zajednicu, koja danas čini 60% stanovništva Srbije. Stoga, čini se da se građani ne osećaju osnaženo i zaštićeno u digitalnom okruženju, što umanjuje potencijal primenu novih tehnologija.

Svesni smo da nadležni organi vlasti imaju ograničene tehničke i organizacione kapacitete za efikasniju reakciju u određenim situacijama. Međutim, problem leži u činjenici da reakcije nadležnih (tužilaštva, policije i sudstva) zavise od slučaja do slučaja - nekada su veoma efikasne, a nekada spore i bez pravog odgovora. Vrlo spore reakcije, ili njihovo potpuno odsustvo, u najvećem broju slučajeva povezane su sa sajber napadima i pretnjama upućenim na onlajn medijima, istraživačkima novinarima i građanskim medijima kritičnim prema postupcima vlasti. Takva praksa obeshrabuje poverenje građana i onlajn medijskih organizacija u zaštitu države, koja treba da preuzme aktivniju ulogu u obezbeđivanju poštovanja prava u digitalnom okruženju.

Od naročitog značaja je Sporazum o saradnji i merama za podizanje nivoa bezbednosti novinara,[23] koji su krajem decembra potpisali predstavnici predstavnici Ministarstva unutrašnjih poslova, Republičkog javnog tužilaštva i 7 novinarskih i medijskih udruženja (Udruženje novinara Srbije, Nezavisno udruženje novinara Srbije, Udruženje novinara Vojvodine, Nezavisno udruženje novinara Vojvodine, ANEM, Asocijacija medija i Asocijacija onlajn medija). Sporazum ima za cilj da ustanovi sistem mera koje bi obezbedile efikasniju krivičnopravnu zaštitu novinara. Među najvažnijim aktivnostima koje su predviđene sporazumom jesu formirane radne grupe za sprovođenje sporazuma čiji će članovi biti ovlašćeni predstavnici potpisnika, određivanje kontakt osoba, vođenje evidencija krivičnih dela na štetu novinara, formiranje registra o krivičnim delima protiv novinara, medija i informativnih internet portala, obuke novinara i vlasnika medija o osnovama informacione bezbednosti, kao i edukacija zaposlenih u Ministarstvu i tužilaštvu.

SHARE Fondacija će i tokom 2017. godine pratiti stanje internet sloboda u Srbiji i analizirati slučajeve povreda. Kako nas na proleće očekuju predsednički izbori, kojima će možda biti priključeni i vanredni parlamentarni, posvetićemo naročitu pažnju praćenju poštovanja digitalnih prava u političkoj komunikaciji, u skladu sa principima Deklaracije iz 2014. godine.[24]

[23] http://www.aom.rs/wp-content/uploads/2016/12/Sparazum-o-saradnji.pdf
[24] http://deklaracija.net/