DIGITALNA PRAVA U SRBIJI

2014-2019

SHARE FOUNDATION

IMPRESUM

GREŠKA 404: Digitalna prava u Srbiji 2014-2019
SHARE Fondacija, oktobar 2019.
Urednici: Andrej Petrovski, Danilo Krivokapić
Autori: Bojan Perkov, Kristina Ćendić, Anka Kovačević, Filip Milošević
Obrada teksta: Milica Jovanović
Dizajn i prelom: Olivia Solis Villaverde
Ilustracije: Milan Dog
Štamparija: NS Press doo Novi Sad
Tiraž: 200
Podrška projektu:

Kingdom of the Netherlands

CIP - Каталогизација у публикацији
Народна библиотека Србије, Београд

004.738.5:343.4/.6(497.11)”2014/2019”
004.738.5:341.231.14

GREŠKA 404 : Digitalna prava u Srbiji : 2014-2019 / [autori Bojan Perkov ... [et al.]. - Beograd : SHARE fondacija, 2019 (Novi Sad : NS Press). - ilustr., 97 str. ; 24 cm

Tiraž 200. - Str. 9-11: Predgovor / Danilo Krivokapić i Andrej Petrovski.

ISBN 978-86-89487-17-6

1. Перков, Бојан, 1988- [аутор]
а) Интернет -- Злоупотребе -- Србија -- 2014-2019 б) Људска права -- Заштита -- Интернет

COBISS.SR-ID 280536844

GREŠKA

404

DIGITALNA PRAVA U SRBIJI
2014-2019

SADRŽAJ

PREDGOVOR

Pre samo deset godina, činilo nam se da internet ispunjava obećanje slobode. Svet se ubrzano povezivao, a pokušaji regulisanja planetarnog internet saobraćaja tretirani su kao poslednji impuls zastarelih ideja. Davne 2011. godine, SHARE je organizovao konferenciju koja je u Beograd dovela nekoliko hiljada internet entuzijasta. Bili su tu Sem Grejem-Felsen, blog-direktor prve Obamine predsedničke kampanje, Peter Sunde, osnivač portala „The Pirate Bay“, zatim Amelija Andersdoter, najmlađa poslanica Evropskog parlamenta i jedina iz redova Piratske partije, SF pisac Brus Sterling, Rafi Kaplan iz Gugla... Usledila su slična okupljanja u Novom Sadu i Rijeci, a potom u Libanu i Tunisu, poprištima borbe u kojoj se sloboda osvajala uz pomoć društvenih mreža.

Izgledalo nam je da će internet spasiti svet.

Malo ko se osvrtao na mračnu stranu tehnologije, a priče o zloupotrebama otpisivane su kao teorije zavere – sve dok 2013. Edvard Snouden, kompjuterski tehničar pod ugovorom u američkoj Nacionalnoj bezbednosnoj službi, nije otkrio da svet već uveliko nije onakav kakvom smo mu se nadali u digitalnoj eri.

Godinu dana kasnije, u Srbiji je disruptivni atak na internet bio izazvan prirodnim nepogodama – u februaru je zavejan Feketić, a u maju se čitav region našao pod vodom, uz velike ljudske i materijalne žrtve. Komentari događaja u zavejanom vojvođanskom selu i informacije o poplavama iznenada su nestajali sa interneta, nekad silom, nekad telefonskim pozivom. Neko je organizovano i planski pokušavao da briše memoriju iz digitalnog okruženja koje sve zauvek pamti.

Kako bismo uhvatili korak sa sve mračnijim izgledima budućnosti, SHARE Fondacija se transformisala u organizaciju kojoj je osnovni cilj bio da istraži nepoznato, brani ljudska prava na internetu, akumulira znanje u ovoj oblasti i uspostavi mrežu saboraca.

Uz tehnološki razvoj, ubrzavao se i razvoj alata za zloupotrebe. Države, korporacije, političke organizacije, svi su se uključili u trku za kontrolu naše svakodnevice: šta gledamo, slušamo, kupujemo, s kim se družimo, o čemu razgovaramo a šta prećutkujemo, za koga glasamo i kome doniramo - informacije o nama i našem ponašanju na internetu postale su pogonsko gorivo nove industrije, ali i strateški resurs stare politike. Afera Kembridž analitike i Fejsbuka pokazala je razmere uticaja novih tehnologija na temelje političke zajednice; pod

razornim uticajem nano-marketinga i digitalne manipulacije, građani Ujedinjenog Kraljevstva glasali su za izlazak iz Evropske unije, a građani SAD izabrali su Donalda Trampa za predsednika. Alternativne činjenice zavladale su svetom u eri post-istine, kojoj globalna povezanost samo ide na ruku.

Korak ka zauzdavanju industrije podataka preduzela je Evropska unija, najveće tržište na svetu, usvajanjem Opšte uredbe o zaštiti podataka čiji se efekti na zaštitu prava građana sa jedne, i preduzetnički duh internet inovacija s druge strane, još uvek odmeravaju.

Algoritamsko odlučivanje, veštačka inteligencija i neuralne mreže danas su novi horizont razvoja internet tehnologija. Ovog puta, prati ih daleko veći oprez korisnika, programera i javnih politika.

U međuvremenu, pravnici, umetnici, tehnički forenzičari, novinari, aktivisti i mnogi drugi, okupljeni oko vrednosti SHARE Fondacije, nastavljaju da grade slobodnu bazu znanja, uz učešće u različitim evropskim i svetskim forumima o budućnosti interneta. Sprovodimo istraživanja o infrastrukturi interneta, Fejsbukovoj algoritamskoj fabrici, pratimo globalni razvoj alata za državni nadzor građana i njihovu primenu u Srbiji. Aktivno učestvujemo u zagovaranju novih i kritičkoj analizi postojećih zakonskih predloga koji se tiču regulisanja našeg života na internetu. Upozoravamo i mobilišemo javnost u slučajevima povreda prava i sloboda građana.

Snimili smo obrazovni serijal od deset epizoda, emitovan na nekoliko televizija u zemlji i regionu. Objavljujemo priručnike o bezbednosti na internetu za istraživačke novinare, pomažemo onlajn medijima kada trpe pritiske zbog svog rada i u odbrani od sajber napada. Osnovali smo prvi poseban Centar za prevenciju bezbednosnih rizika u informacionim sistemima za onlajn medije, organizacije civilnog društva i aktiviste u Srbiji - SHARE CERT.

Uspostavili smo stalni monitoring prava i sloboda građana u digitalnom okruženju, uz redovne godišnje izveštaje o nalazima i trendovima. Publikacija pred vama upravo predstavlja presek prilika na internetu u Srbiji u prethodnih pet godina. Značaj dokumentovanja povreda digitalnih prava prepoznat je i u regionu pa od septembra ove godine, u saradnji sa istraživačkom mrežom BIRN, pratimo stanje u Bosni i Hercegovini, Hrvatskoj, Mađarskoj, Rumuniji i Severnoj Makedoniji.

Najveća zasluga za dokumentovanje 500 slučajeva povreda prava i sloboda na internetu u Srbiji, pripada našem kolegi Bojanu Perkovu koji je tokom pet

godina svakodnevno pratio najznačajnije incidente.

SHARE ne bi postojao bez svojih saradnika, široke mreže organizacija, stručnjaka i aktivista koji ulažu u znanje kao javno dobro.

Posebnu zahvalnost dugujemo Svetlani Lukić, Sofiji Todorović, Dragani Pećo, Branku Čečenu, Rodoljubu Šabiću i Nedimu Sejdinoviću na ličnom učešću u nastanku ove publikacije. Veličina njihovog doprinosa javnom dobru u Srbiji se ne može opisati rečima.

Hvala.

Danilo Krivokapić i Andrej Petrovski
Beograd, oktobar 2019.

O MONITORINGU

Tehničke sabotaže, gušenje slobodne reči i misli, lični napadi i kampanje mržnje u digitalnom okruženju postaju učestaliji s jačanjem uloge onlajn medija, društvenih mreža i drugih platformi u zemlji u kojoj su tradicionalni medijski akteri često kontrolisani i instrumentalizovani u političke i druge svrhe. Vremenom su postale vidljive naznake organizovanog napora da se u javnom prostoru Srbije ostvari nadmoć kroz kontrolu društvenog narativa i primenu tehnika informacionog ratovanja.

U okolnostima sve češćih tehničkih napada na onlajn medije, pritisaka na novinare i zloupotreba alata digitalnog okruženja, SHARE Fondacija je pre pet godina počela da dokumentuje slučajeve povreda digitalnih prava i sloboda. Na osnovu kontinuiranog praćenja prilika u onom delu javne komunikacije koja se odvija na internetu, kroz periodične izveštaje prikazujemo svoje nalaze i uočene trendove u ovoj oblasti. Da bi se dokumentovani slučajevi povreda prava pregledno klasifikovali, izradili smo metodološki okvir sa podacima o vrsti povrede, sredstvu izvršenja, ugroženoj strani i napadačima, vremenskom periodu i relevantnim izvorima za svaki pojedinačni slučaj, uz kratak opis slučaja i ishod, ukoliko ga je u konkretnom slučaju bilo. Povrede prava smo grupisali prema kategorijama narušavanja informacione bezbednosti, povreda informacione privatnosti i zaštite podataka o ličnosti, pritisaka zbog izražavanja i aktivnosti na internetu, manipulacija i propagande u digitalnom okruženju, pozivanja posrednika na odgovornost, blokiranja i filtriranja sadržaja.

Tim SHARE Fondacije je u periodu od maja 2014. do kraja avgusta 2019. prikupio, klasifikovao i opisao blizu 500 slučajeva, od kojih znatna većina nije imala adekvatan pravni epilog, odnosno pravnosnažnu odluku da je došlo do povrede nekog prava ili slobode. Monitoring baza SHARE Fondacije je dostupna na adresi monitoring.labs.rs.

PRVIH PET GODINA

Događaj koji je nesumnjivo označio prekretnicu za digitalna prava i slobode u Srbiji odigrao se u maju 2014. godine, kada su poplave teško pogodile mnoge opštine u zemlji i regionu, ostavljajući za sobom ljudske žrtve i veliku materijalnu štetu. Na internetu su se posledice poplava osetile kroz rastući pritisak na informacije i komentare građana, objavljivanih u nedostatku pravovremenih, tačnih ili potpunih vesti iz zvaničnih izvora. Građani su privođeni zbog objava na društvenim mrežama, čitave blog sekcije medijskih portala brisane su bez objašnjenja, dok su pojedini sajtovi bivali nedostupni upravo kada bi objavili kritičke tekstove o postupcima države za vreme i nakon poplava.

Za nešto više od pet godina sprovođenja monitoringa digitalnih prava i sloboda u Srbiji, u periodu od maja 2014. do kraja avgusta 2019. godine, najčešći oblik povreda digitalnih prava predstavljaju objavljivanje pretećih sadržaja i ugrožavanje sigurnosti. Od ukupno prikupljenog 481 slučaja, zabeleženo je 115 ovakvih incidenata, što čini skoro četvrtinu povreda. Zajedno sa sledećom najbrojnijom potkategorijom povreda prava, uvredama i neosnovanim optužbama kojih je bilo 95, ove dve vrste povreda čine gotovo polovinu ukupnog broja dokumentovanih slučajeva.

Zabrinjava činjenica da se pretnje i ugrožavanje sigurnosti na internetu prihvataju kao nužno zlo onlajn komunikacije, dok najčešće izostaje efikasna pravna zaštita, posebno kada su na meti novinari. Poslednjih godina zabeleženo je više privođenja osumnjičenih za pretnje, što svakako predstavlja napredak, ali su pravnosnažne presude retke, na njih se dugo čeka, a kazne su blage. Takav je, recimo, epilog za pretnje smrću novinarki i njenoj kćerki na Tviteru, gde je Apelacioni sud u Beogradu osudio počinioca na osam meseci kućnog zatvora sa elektronskom nanogicom i rokom provere od tri godine. Pretnje, zastrašivanje i nasilje nad novinarima našli su se i u izveštaju Evropske komisije o napretku Srbije za 2019. godinu, u kom se ističe da nadležni organi moraju reagovati efikasno, dok se od nosilaca vlasti očekuje da javno osude govor mržnje i pretnje novinarima. Klima nekažnjivosti podstiče netrpeljivost u javnom prostoru, što se vidi i po rastućem broju uvreda, dok posledično stvara „efekat zebnje“ (chilling effect) po slobodu izražavanja.

Žrtve najtežih napada po pravilu su novinari, uključujući istraživačke novinare (ukupno 135 slučajeva). S druge strane, u najvećem broju obrađenih slučajeva

povrede digitalnih prava i sloboda napadač je nepoznat (151 slučaj), posebno kada je reč o tehničkim napadima, budući da najčešće podrazumevaju metode za sakrivanje digitalnih tragova upravo zato da bi počinioci izbegli identifikaciju i procesuiranje. Najčešće sredstvo napada bilo je onesposobljavanje servisa, što obuhvata DDoS (Distributed Denial-of-Service) napade na servere na kojima su ciljani sajtovi hostovani. Do sada je zabeleženo 37 takvih slučajeva u kojima su mete uglavnom bili medijski portali koji su kritički izveštavali o postupcima vlasti, ali i sajtovi organizacija civilnog društva.

DDoS napad se izvodi zagušenjem servera na kome je hostovan određeni onlajn resurs, vebsajt ili aplikacija. Zahtevi za pristup se istovremeno upućuju preko brojnih uređaja, dolazi do preopterećenja servera i sadržaj postaje nedostupan.

Podaci ukazuju da su prava građana u digitalnom okruženju ugrožena u različitim kontekstima, od kojih je naročito problematičan pritisak na novinare, čija je društvena uloga ključna za unapređenje slobodnog protoka informacija i ideja na internetu. Pored toga, u jednom od ranijih periodičnih monitoring izveštaja 2018. godina je identifikovana kao godina povreda privatnosti, imajući u vidu kontinuirano narušavanje informacione privatnosti i zaštite ličnih podataka, gde su građani najčešće ispaštali zbog neodgovornog rukovanja ličnim podacima. Tokom dosadašnjeg monitoringa, posebno su interesantni bili društveni događaji čije su se posledice prelile u digitalno okruženje, kao što su izborne kampanje tokom kojih su beleženi značajni slučajevi manipulacija, ili puštanje drona na fudbalskoj utakmici Srbija - Albanija.

„Efekat zebnje“ (chilling effect) je posledica svesnog podsticanja straha kako bi se obeshrabrilo uživanje nekog prava, najčešće slobode govora i informisanja.

METODOLOGIJA

Razvoj metodološkog okvira za klasifikaciju i praćenje povreda prava na internetu takođe je kontinuiran proces, s obzirom na ekspanziju tehnologija i alata u digitalnom okruženju. Tokom monitoringa metodologija je unapređena nekoliko puta, dok je aktuelna verzija objavljena u junu 2019. godine (verzija 2.1).

Povrede digitalnih prava i sloboda podelili smo u sedam osnovnih kategorija, koje se dalje mogu razvrstati u nekoliko potkategorija:

A. Narušavanje informacione bezbednosti: slučajevi u kojima je predmet povrede bezbednost informacionih sistema, npr. kroz upade u sistem, DDoS (Distributed Denial-of-Service) napade kako bi se onemogućio pristup nekom sadržaju, krađu i uništavanje podataka i tome slično. Potkategorije koje detaljnije opisuju ove vrste povreda su sledeće:

1. Činjenje sadržaja nedostupnim putem tehničkih metoda
2. Uništavanje i krađa podataka i programa
3. Računarska prevara
4. Neovlašćeni pristup - neovlašćena izmena i postavljanje sadržaja
5. Onemogućavanje kontrole nad nalogom ili sadržajem

B. Povrede informacione privatnosti i zaštite podataka o ličnosti: povrede kao što su curenje podataka, nedozvoljena obrada podataka ili nezakonit nadzor komunikacija. Takve vrste povreda bliže su opisane sledećim potkategorijama:

1. Objavljivanje informacija o privatnom životu
2. Nezakonito presretanje elektronskih komunikacija
3. Curenje podataka o ličnosti građana
4. Nedozvoljena obrada podataka o ličnosti
5. Narušavanje informacione privatnosti na radnom mestu
6. Ostale povrede informacione privatnosti

C. Pritisci zbog izražavanja i aktivnosti na internetu: povrede digitalnih prava koje se odnose na čast i ugled, ugrožavanje sigurnosti, poruke diskriminacije i mržnje, pitanja slobode izražavanja u radnom okruženju, kao i pritiske na pojedince zbog objavljivanja informacija onlajn. Slučajevi povreda iz ove kategorije su takođe podeljeni u nekoliko potkategorija:

1. Objavljivanje neistina i neproverenih informacija sa namerom ugrožavanja reputacije
2. Uvrede i neosnovane optužbe
3. Preteći sadržaji i ugrožavanje sigurnosti

4. Govor mržnje i diskriminacija
5. Sloboda izražavanja na internetu u radnom okruženju
6. Pritisci zbog objavljivanja informacija

D. Manipulacije i propaganda u digitalnom okruženju: povrede koje obuhvataju različite oblike ciljanog širenja i manipulisanja sadržajem na internetu radi ostvarivanja određenih ciljeva, koji su često i ekonomske prirode. Radi preciznijeg definisanja slučajeva povreda, kategorija je podeljena na nekoliko potkategorija:

1. Kreiranje lažnih naloga i plaćeno promovisanje lažnog sadržaja
2. Manipulacije sadržajem i organizovano prijavljivanje na društvenim mrežama
3. Izmena ili uklanjanje sadržaja od javnog značaja
4. Plasiranje komercijalnog sadržaja kao informativnog
5. Druge manipulacije u digitalnom okruženju

E. Pozivanje posrednika na odgovornost: povrede u vezi sa pritiscima na pružaoce usluga informacionog društva, tj. internet posrednike kao što su hosting provajderi, da uklanjaju sadržaje i odbijaju usluge kroz pretnje pravnim postupcima, kaznama ili blokiranjem. Ova kategorija za sada sadrži jednu potkategoriju:

1. Pritisci zbog sadržaja korisnika

F. Blokiranje i filtriranje sadržaja: povrede u slučajevima kada je određeni sadržaj tehnički blokiran na nacionalnom nivou ili nivou određene organizacije, ili kada algoritmi na platformama blokiraju ili suspenduju legitiman sadržaj (npr. video-parodiju). Potkategorije koje preciznije opisuju povrede u ovim slučajevima su sledeće:

1. Blokiranje/filtriranje na nivou mreže
2. Algoritamsko blokiranje ili suspenzija sadržaja

G. Ostalo: ostale povrede digitalnih prava i sloboda koje se ne mogu podvesti ni pod jednu od za sada definisanih kategorija.

Pored kategorija povrede, obeležja slučajeva čine i informacije o **napadaču i ugroženoj strani**, što mogu biti novinari, javne ličnosti, državni funkcioneri, građani, aktivisti, i drugi. Ukoliko ga je moguće odrediti, slučajevima se dodeljuje i **sredstvo povrede**, koje može biti tehničke (maliciozni softver, ubacivanje malicioznog koda, izviđački napadi, presretanje komunikacije, upadi u sistem, onesposobljavanje servisa) ili pravne prirode (privatne tužbe, krivične prijave, privođenja i pritvori, značajne presude, oduzimanje stvari i pretres, prekršajne prijave). Takođe se prati ishod slučaja, tj. koji su pravni i drugi koraci preduzeti povodom slučaja i da li postoji pravosnažna sudska odluka u navedenom slučaju.

TEHNIČKI NAPADI

HRONOLOGIJA

2014

Učestali problemi sa pristupom onlajn sadržajima primećeni su za vreme velikih poplava u maju 2014. godine, što je na neki način i podstaklo monitoring digitalnih prava i sloboda. U početku su problemima najčešće bili izloženi slabije posećeni portali, posebno oni iz manjih sredina, koji su objavljivali kritike postupaka državnih službi i javnih funkcionera tokom poplava. Tokom te godine dokumentovano je 13 slučajeva tehničkih napada na integritet onlajn sadržaja i narušavanja informacione bezbednosti. U čak 11 slučajeva mete su bili onlajn mediji, dok su napadači uglavnom nepoznati. Onesposobljavanje usluge bilo je najčešće primenjeno sredstvo tehničkih napada, i to devet puta, što odgovara najbrojnijoj potkategoriji povreda u 2014. godini, činjenje sadržaja nedostupnim putem tehničkih metoda. Uočeno je da su tehnički napadi sa ciljem onemogućavanja ili otežavanja pristupa sadržaju, često bili povezani sa konkretnim društvenim događajima, slično kao u vreme poplava. Tako su u oktobru iste godine zabeleženi napadi na srpske i albanske sajtove posle fudbalske utakmice Srbija - Albanija koja je prekinuta posle pojave drona na stadionu. Pored činjenja sadržaja nedostupnim, zabeležena su i dva primera iz potkategorije neovlašćenih izmena i postavljanja sadržaja.

2015

Tehnički napadi na onlajn medije nastavljaju se i tokom 2015. godine, kada su bili mete u 12 od ukupno 19 slučajeva, od čega pojedini i u više navrata. Mada su većinom tehnički napadi izvođeni da bi se sadržaj učinio nedostupnim, čak 14 puta, među udarima na informacionu bezbednost onlajn medija bilo je i slučajeva neovlašćenog pristupa; zabeleženo ih je šest. U jednom od tih incidenata nepoznati počinioci su ubacili diskreditujuće tekstove na sajtove dva medija. Takođe, tokom 2015. godine i nekoliko lokalnih medija našlo se na meti tehničkih napada. Tehnički pritisci su dodatni problem za medije iz manjih sredina, koji nemaju sredstava za unapređenje odbrane. Najupečatljiviji napad u toku 2015. dogodio se u aprilu, kada je potpuno onesposobljen portal „Teleprompter“, tada već izložen čestim pritiscima. Iste godine su po prvi put zabeležena dva napada iz potkategorije uništavanja i krađe podataka i programa: jednom je na meti bio onlajn medij, a drugi put istraživački novinari, kojima je bila oduzeta oprema a snimci sa nje su obrisani.

U 2016. godini, slučajevi neovlašćenog pristupa informacionim sistemima, kojih je zabeleženo osam, izjednačavaju se po broju sa incidentima u kojima je sadržaj učinjen nedostupnim. Budući da su te godine u Srbiji organizovani

2016

vanredni parlamentarni izbori, prvi put su dokumentovani napadi na političke aktere, i to iz opozicije. Medijski sajtovi su ponovo bili najčešće mete napada, tačnije u 50 posto slučajeva, dok su u dva navrata mete napada bili sajtovi organa vlasti, tačnije sajtovi predsednika Republike i Grada Beograda. Među značajnim incidentima koji su obeležili 2016. godinu izdvaja se blokiranje Tviter naloga novinara kada je nepoznat napadač pokušao da mu kompromituje nalog. Zabeležena su i dva slučaja računarskih prevara u kojima su bili targetirani građani.

2017

Tokom 2017. godine učestali su pritisci na onlajn medije kroz tehničke napade na njihove informacione sisteme: od ukupno 15 zabeleženih slučajeva iz ove kategorije, onlajn mediji su bili mete sedam puta. Jedan od zanimljivijih slučajeva tehničkih napada obrađen je kada su nepoznati napadači ubacili afirmativne tekstove u baze sajtova medija. Takođe su primećeni slučajevi računarskih prevara većih razmera, kojih je bilo četiri, a kojima su targetirani građani i državni organi, poput Narodne banke Srbije. U sva četiri incidenta korišćene su lažne imejl poruke. Upad u sistem koji je mogao da ima ozbiljne posledice po građane dogodio se u avgustu 2017, kada je meta bio server na kome su čuvane kontakt informacije i lični podaci korisnika usluga švedske kompanije koja hostuje veliki broj srpskih sajtova.

2018

Narušavanje informacione bezbednosti u 2018. godini zabeleženo je u 13 slučajeva. Mete napada bili su građani, organizacije civilnog društva, novinari i onlajn mediji. Te godine je prvi put primećen veći broj napada na organizacije civilnog društva. Kao i prethodnih godina, napadači su najčešće ostali nepoznati. Kao sredstvo napada pet puta je onesposobljen servis, a četiri puta je došlo do upada u sistem. Najviše narušavanja informacione bezbednosti svrstano je u potkategorije računarske prevare i činjenja sadržaja nedostupnim putem tehničkih metoda, po pet. Za njima slede napadi iz potkategorije neovlašćene izmene i postavljanje sadržaja, četiri puta, te onemogućavanje kontrole nad nalogom ili sadržajem, zabeležene u tri slučaja.

2019

U periodu do septembra 2019. godine značajno je smanjen broj dokumentovanih tehničkih napada. Zabeležena su svega tri incidenta, od čega su dva napadi na onlajn medije, a jedan na privatnu kompaniju. Po jedan slučaj svrstan je u kategorije neovlašćenog pristupa i činjenja sadržaja nedostupnim putem tehničkih metoda, a jedan napad obuhvatio je obe ove potkategorije.

SPECIFIČNI SLUČAJEVI

Sve korisnike interneta koji su 8. decembra 2013. godine hteli da pročitaju važnu vest na novosadskom portalu Radio 021, sačekala je ista poruka: HTTP Error 404. Takođe poznata kao '404 Not Found', ova poruka govori da traženi sadržaj ne postoji na toj adresi, ili je nekada postojao, ali je uklonjen. To se ponekad dešava sa zastarelim linkovima i stranicama koje nisu aktivne. Međutim, na ovoj adresi se nekoliko sati ranije nalazio tekst o privilegijama za kćerku guvernerke Narodne banke Srbije, Jorgovanke Tabaković.

Osim na portalu 021.rs, greška 404 je umesto iste vesti korisnike čekala i na stranici alo.rs. Ispostavilo se da su ovo bili slučajevi redakcijske cenzure. Očigledna manipulacija informacijama od javnog značaja razljutila je deo onlajn zajednice i javnosti, dok se tekst viralno množio po ličnim profilima, blogovima i sajtovima nezavisnih medija. Nepoznatim nalogodavcima cenzure postalo je jasno da je potrebno pronaći neke manje direktne oblike pritiska na one koji objavljuju nepoželjne vesti.

Nekoliko hiljada inficiranih računara istovremeno je napalo servere na kojima su se nalazile stranice cins.rs i autonomija.info, a koji su takođe preneli ovu vest. Svim korisnicima interneta koji su u tom trenutku hteli da je pročitaju, pojavljivala se nešto drugačija poruka: HTTP Error 503. Karakteristična za DDoS napade, greška 503 govori da je u pitanju privremeni problem tehničke prirode, na primer da je server zbog nečega nedostupan. Za ovakve napade nisu potrebni veliki resursi i politička moć, a njihov cilj je čisto maltretiranje; sprovode se isključivo u mraku, skrivenim kanalima interneta, računajući na odsustvo odgovornosti.

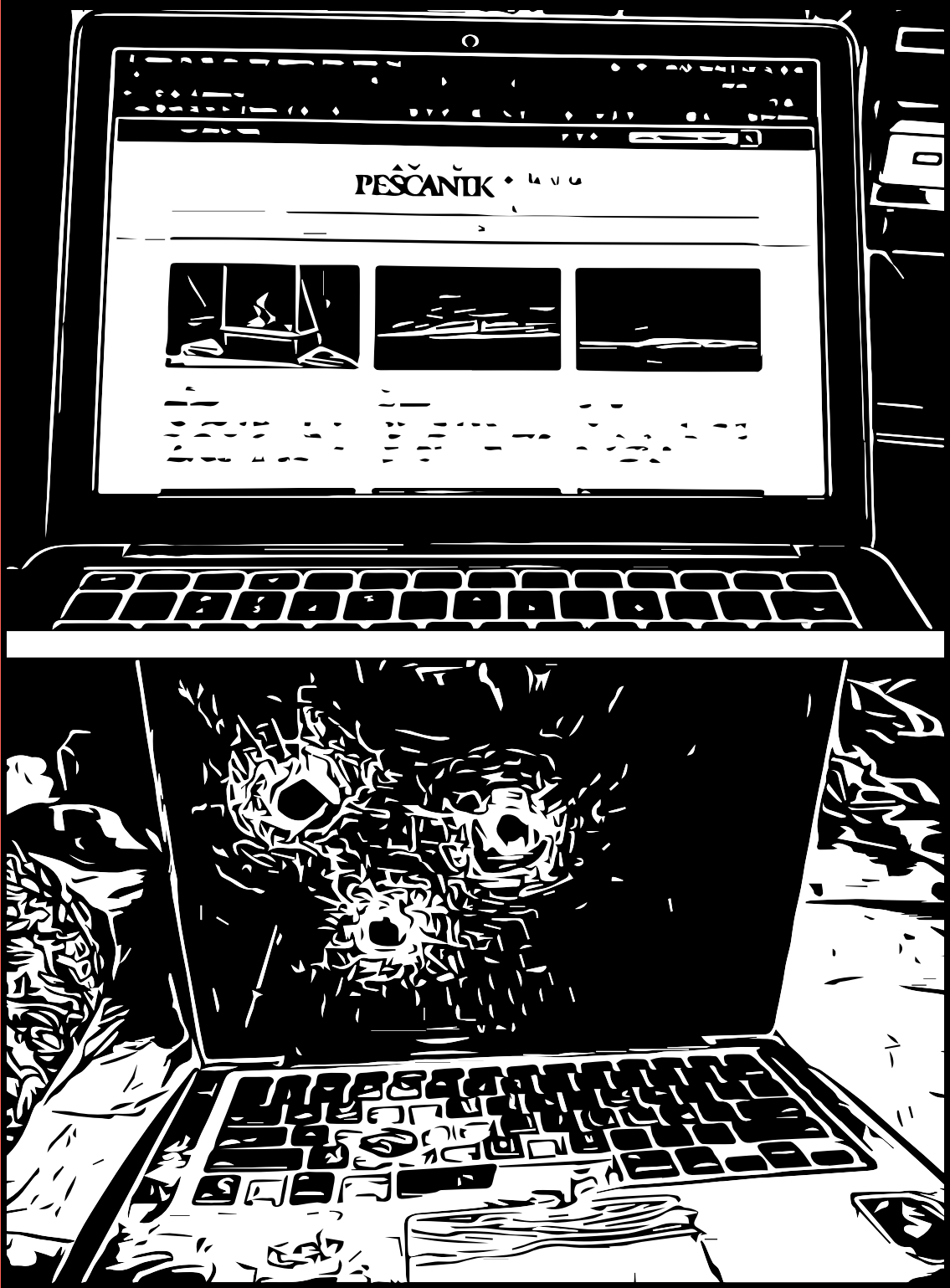
Mada je u to vreme bio prilično popularan, DDoS je ubrzo pao u senku sofisticiranijih tehnika onlajn napada. Sa portala Centra za istraživačko novinarstvo Srbije (CINS) tekst o cenzuri na 021.rs konačno je uklonjen ručno, neovlašćenim i neopaženim pristupom njihovom sistemu. Par meseci kasnije, pošto je CINS objavio istraživanje o kockarnicama, otkriveni su neovlašćeni pristupi serveru, svim podacima i komunikacijama zaposlenih tokom perioda od 10 dana. Incidenti su vremenom postajali kompleksniji i teži.

Urednika portala Teleprompter su jednog jutra probudile brojne SMS poruke sa kodovima i notifikacije o promenjenim šiframa na imejl nalozima vezanim za sve privatne i poslovne servise. Obrisani su svi sadržaji na sajtu, kao i nalozi na društvenim mrežama. Analiza slučaja pokazala je da su svi dostupni sistemi zaštite bili na mestu (kompleksne šifre, multifaktorska autentifikacija i drugo), pa je sumnja usmerena ka neovlašćenom pristupu SMS-u (verovatno preko kompromitovanih službenika operatora) ili instaliranom malveru (zlonamernom softveru) u telefonu vlasnika koji bi napadaču prosleđivao poruke sa kodovima. Na sumnjama koje je nemoguće proveriti bez nadležnih organa, ostali su i mnogi drugi, misteriozni slučajevi neovlašćenih pristupa, uništavanja i krađe podataka, onemogućavanja kontrole nad nalozima i sadržajima. Dodatno, slučajevi su nepogrešivo koincidirali sa aktuelnim društveno-političkim aferama. Privatna mejl prepiska naučnice Miljane Radivojević, koja je otkrila da doktorat rektora Megatrend univerziteta ne postoji, dostavljena je medijima i objavljena uživo u programu nacionalne televizije. Nakon objavljivanja teksta „Glavni fantom iz Savamale“ Tviter nalog Nikole Tomića, urednika u nedeljniku NIN, blokiran je zbog pokušaja kompromitovanja.

Kontekst ovih incidenata jedini je putokaz u utvrđivanju motiva, a time i mogućih strana zainteresovanih da se napadi izvedu. Nedvosmislenih dokaza o nalogodavcima i napadačima nema, dok priroda tih napada i sama struktura interneta čine da nezavisni istraživači veoma teško mogu ući u trag napadačima, dobro sakrivenim iza anonimnih mreža i višestrukih IP adresa, obično kroz virtuelne privatne tunele. Istovremeno, na izabranim adresama sprskog interneta svako malo se desi možda i najpopularniji, ali i najbenigniji primer tehničkih napada u popularnoj kulturi - neovlašćena izmena naslovnih stranica (defacing). Tako se na zvaničnom sajtu Grada Beograda pojavila zastava Republike Hrvatske, na sajtu CINS-a grb OVK, a na portalu Tanjuga poruka lokalnih haktivista: „Nažalost, nismo dovoljno profesionalni da bi preneli vesti takve kakve jesu, nego moramo da izmenimo po neki video zbog hleba i igara“.

PEŠČANIK

- Tehnički napadi na Peščanik intenzivirani nakon objavljivanja tekstova o plagiranom doktoratu ministra policije i nepostojećem doktoratu rektora Megatrenda.
- Peščanik više puta na meti različitih vrsta tehničkih napada, od DDoS do neovlašćenog ubacivanja tekstova.
- Najveće zagušenje Peščanikovog servera vršeno je sa 30.000 IP adresa.
- Državni funkcioneri podnose privatne tužbe zbog povrede časti i ugleda protiv uredništva i autora tekstova na Peščaniku.


PEŠČANIK

SVETLANA LUKIĆ

NOVINARKA, UREDNICA PORTALA PEŠČANIK.NET

Ne brojim tužbe protiv autora i redakcije Peščanika. Ne zato što ih je bilo mnogo, već zato što se trudim da marginalizujem taj pritisak. Koliko znam, još uvek su aktuelne četiri: tu su tužbe ministra policije Nebojše Stefanovića i bivšeg direktora Elektromreže Srbije Nikole Petrovića; fotograf Tanjuga nas je tužio zbog teksta (autora koji je pisao i o plagijatima) u kom je postavljeno pitanje o različitim fotografijama posle pada helikoptera; i, ako se ne varam, još uvek se vuče proces po tužbi Ištvana Kaića. Pojavimo se kad nas pozovu advokati koji nas zastupaju pro bono, pa se vratimo na posao. Zbog formalnog statusa u takvim procesima, upisale smo Peščanik u Registar medija.

Ne vredi da brojimo tužbe, pretnje ili napade. U maloj redakciji kao što je Peščanik, neće preostati niko da radi posao umesto nas ako se Svetlana Vuković i ja prepustimo paranoji zbog onoga što se dešava ili što bi nam se moglo desiti. To ne znači da nismo odgovorne – prijavile smo najteže napade na sajt, uložile smo jako mnogo sredstava u odbranu, i još uvek ih ulažemo, ali smo izgradile barijere da bismo mogle da nastavimo da radimo.

S druge strane, prednost male redakcije jeste činjenica da se neke strateške odluke lako donose. Jednu od njih, možda najvažniju za novinarski rad u Srbiji, Svetlana i ja smo donele još davnih 1990-tih: sve što radimo ne sme zavisiti od toga da li ćemo biti bezbedne ili ne, uključujući i fizičku bezbednost. Naša

imena su čitana sa spiskova 'unutrašnjih neprijatelja' na RTS-u u najmračnija vremena ratova i zločina. Od tada živimo s tim da naša bezbednost, kao i bezbednost nemalog broja ljudi u Srbiji, zaista može sutra biti dovedena u pitanje. Dakle, to se podrazumeva i nas dve o tome više ne moramo da raspravljamo.

Međutim, naši sagovornici i autori nisu dužni da donose odluke na koje smo nas dve prinuđene, jer oni nisu novinari koji bi bili svesni rizika i pritisaka profesije. To su ljudi koji su stekli svoj profesionalni i intelektualni dignitet, mnogi od njih i pre više decenija, i nemaju potrebu da se dokazuju bilo kome, niti da se izlažu pretnjama i tužbama.

To je naša, uslovno rečeno, slaba tačka i čini se da je izvršna vlast to prepoznala pa je preduzela novi pristup prema Peščaniku – podnose se tužbe protiv naših autora i time šalje poruka drugim našim autorima, šta ih čeka. To je zaobilazni pritisak koji se oseća u redakciji. Dodatni problem predstavlja svest da je javni prostor u međuvremenu preotela mašinerija koja je u stanju da pokrije svaku kritiku, svaku polemiku. Mnogi smatraju da zbog toga više nema smisla učestvovati u javnoj diskusiji.

Kako da privolite autore da pišu, da ne uzimaju u obzir sve te probleme? Što je Vesni Pešić potrebno da se mesecima povlači po sudnicama, dok se ministar nekoliko puta uopšte nije pojavljivao na ročištima? Autore moramo da ohrabrujemo, osim što im garantujemo pravnu zaštitu; stalno ih podsećamo da trenutne prilike ne uzimaju kao kriterijum, već samo svoju etičku obavezu da javno govore o problemima u državi i društvu. Bilo je slučajeva da su pojedine naše autore zvali iz ministarstva na kafu, da im objasne da nisu u pravu. To je, naravno, pritisak svoje vrste; kazale smo im da to se ne radi tako. Ako je objavljeno nešto što nije tačno ili jasno, postoji procedura za slanje i objavu ispravki. Kad nam sagovornici i autori kažu, 'ma šta će mi to u životu' odgovorimo im: treba vam to u životu, treba da pišete, da naši čitaoci ne vide da se bilo ko od nas povlači zato što se plaši.

Najava dubokog društvenog razdora osetila se u redakciji posle izbora 2012. u vreme kada se na sajtu vodila burna rasprava za ili protiv belih listića. Deo naših sagovornika i autora koji su tada prestali da sarađuju s Peščanikom i dan-danas se ljuti na one koji su argumentovali u prilog belih listića. Ostao je mučan utisak da se prostor za razgovor sužava ne samo pod pritiskom spolja, i ne samo usled autocenzure ili odustajanja.

Za nas novo doba nastaje 2014. Do tada su napadi bili manji i pričinjavali su nam manju štetu; s razlogom ili bez, uglavnom su nas tretirali kao marginalni medij. Međutim, krajem maja 2014. objavile smo tekst o plagijatu u doktorskoj tezi ministra policije. Volela bih da možemo da stavimo sebi u zasluge nas-

tanak serije o plagijatima, ali treba podsetiti da su ti tekstovi prvo ponuđeni medijima koji nisu smeli da ih objave. Nas dve smo prihvatile, uz uslov da se sačeka da prođe metež u javnom prostoru stvoren u vreme poplava. Smatrale smo da nema smisla pokretati takvu temu kada je ugroženo na stotine hiljada ljudi. Očekivale smo probleme, pa smo objavu teksta o plagijatu ministra policije Nebojše Stefanovića tempirale za nedeljni ručak, kako bi priča uspela da stigne do mreža i drugih medija. Napad je počeo iste večeri.

Zajedno sa saradnicima branile smo sajt danima i noćima, koliko smo mogle. Usledio je tekst o plagijatu Siniše Malog, pa o rektoru Megatrenda. Napadi su trajali nedeljama, a mi smo svo raspoloživo vreme i snagu ulagali u golo održavanje na površini. Onda smo shvatile da je to upravo i bio cilj napada. Onaj ko raspolaže kapacitetima, ko ima daleko više novca od nas i nebrojeno mnogo ljudi, može da nas sruši kad god hoće. Zato smo donele odluku da nećemo da učestvujemo u tom ratu. Naprosto, treba postaviti stvari tako da im se ne isplati da nas ruše. U tome su nam mnogo pomogle društvene mreže; fan stranica Peščanika na Fejsbuku nam je bila podrška i preko njih smo širile tekstove do srodnih medija i javnosti. Inače, više od 450 medija preuzima naše tekstove (prema: alexa.com). Čemu onda rušenje jednog sajta, kad ćete time samo skrenuti još veću pažnju na 'nepoželjan' sadržaj?

Prijavile smo napade, nosile smo zapise sa servera u policiju, više puta smo bile u odeljenju za visokotehnološki kriminal. Međutim, jasno nam je stavljeno do znanja da od istrage neće biti ništa. Videlo se to iz načina na koji su nas ispitivali, iz činjenice da nas niko nikad nije obavestio o razvoju istrage, a posebno iz javnih istupa načelnika odeljenja za visokotehnološki kriminal, ministra policije, pa i samog Aleksandra Vučića. Mogli su da nas slažu da nešto preduzimaju, ali i to ih je mrzelo. Zapravo, time što su odbili da bilo šta urade hteli su da pošalju poruku da je lov na nas nekažnjiv. Ne verujem da bih se ponovo izlagala tim neprijatnostima.

Prilike za rad medija u Srbiji su dovoljno teške i mučne. Peščanik posebno ima tu neprijatnu ulogu podsetnika da stanje u kom se mediji i javna reč nalaze danas, nije iznenada nastalo dolaskom na vlast aktuelnog režima pre sedam godina.

U početku kao uređivački autonomna radijska emisija, Peščanik se godinama emitovao na Radiju B92. Uprkos sve većoj koliziji sa uređivačkom politikom B92, poštovan je nepisani dogovor o potpunoj uređivačkoj slobodi. Ipak, 2006. smo se registrovale kao udruženje građana i pokrenule sajt koji je služio i kao slobodno dostupna arhiva i rezervna kopija emisije, ali i kao mesto za prošireni sadržaj sa tekstovima koji nisu nužno u vezi sa temama pokrenutim u emisiji. Sajt smo vremenom razvijale kao rezervni položaj na koji se možemo povući u slučaju potrebe.

U tehničkom pogledu, bile smo sastavni deo redakcije B92; produkcija i emitovanje se odvijalo kroz njihovu infrastrukturu, a tako je bilo i sa sajtom koji se u početku nalazio na .info domenu. Bio je to uzajamno koristan odnos: B92 ima frekvenciju koja je nama potrebna, a mi smo njima bile neka vrsta legitimacije prema publici koju su stekli 1990-tih godina, pa i prema donatorima. Kada smo osnovale udruženje građana, počele smo same da obijamo pragove donatora, uz dogovor da gotov sadržaj besplatno isporučujemo Radiju B92. Oni su sa svoje strane zadržali pravo da prodaju prostor unutar emisije za reklame, dok prihode nisu delili. Naš prvi i jedini pokušaj da dobijemo makar mali deo sredstava od reklama odmah je odbijen. U međuvremenu, povremeno je dolazilo do napada na sajt, emisija je bila ometana, ali brigu o tome je vodila B92.

Postepeni razlaz sa B92 nije izazvan samo odnosom prema ratovima 1990-tih, već i s obzirom na teme kojima je B92 trebalo da se bavi, pre svega u odnosu prema vlastima. B92 je krenula putem kolektivne samocenzure, a oštrica kritike prema izvršnoj vlasti osetno je otupela.

Početkom leta 2009. godine, u istom danu je napadnut Peščanikov sajt, ometana je radio emisija – što je u to vreme već trajalo mesecima – i demoliran je moj auto na parkingu ispred RTV B92. Tog dana je postalo jasno da smo Svetlana i ja prepuštene same sebi. Koliko znam, preduzimane su neke pravne mere, ali bez efekta. Sećam se da me je tadašnji ombudsman Saša Janković zvao da vidi o čemu se radi, jer sam rekla da je policijski izveštaj o demoliranju auta bio neistinit. Napisala sam izjavu o tome šta se zapravo dogodilo i šta nije tačno u policijskom zapisniku; ombudsman se ponovo javio posle nekoliko dana i rekao da policija ostaje pri svom stavu. To je bilo sve.

Za razliku od najvećeg napada pet godina kasnije, tih dana nije bilo jedne konkretne teme koja bi generisala agresivne reakcije prema Peščaniku. Tačnije, takvih tema je bilo bezbroj. To je vreme kada vladajuća koalicija oko Demokratske stranke ulazi u svoju dekadentnu fazu, korupcija dostiže zenit; u svetu je ekonomska kriza koja se oseća i ovde, Srbija prodaje NIS i stavlja se u položaj energetske zavisnosti od Rusije, ugošćava Medvedeva uz neprimerenu pompu, Vuk Jeremić se svađa sa svima po regionu... U svakom slučaju, sagovornici i autori Peščanika su redom vrlo kritični prema tadašnjoj vlasti. Rečeno mi je čak i da je Tadić zvao glavnog i odgovornog urednika RTV B92 da se žali na odnos Peščanika prema vlastima i njemu lično. Dakle, to je vreme kada počinje da eskalira situacija koja će 2012. rezultirati porazom te političke garniture.

Krajem 11. sezone mesecima smo čekale da nas neko iz redakcije B92 obavesti o planovima s kojima bismo aplicirale za sledeći ciklus grantova. Promene u kući su već bile vidljive: neki ljudi su odlazili, neke emisije su ukinute. Bilo je jasno da nam se sprema rastanak. Ključni momenat je bilo gostovanje Ljiljane

Bulatović i Koste Čavoškog u udarnom televizijskom terminu, kada im je omogućeno ne samo da negiraju genocid u BiH, već da veličaju i genocid i zločince.

U prvoj narednoj emisiji sam javno zatražila da se B92 izvini žrtvama. Sledeća je premijerno emitovana sa sajta. Od jeseni 2011. Peščanik se više nije emitovao na B92.

Sa sobom smo ponele dragocenu mrežu od desetak lokalnih radio-stanica koje su redovno preuzimale emisiju. Propadanje lokalnih medija počelo je pre ove vlasti, ali sa dolaskom Vučića na vlast od te mreže nije ostao ni kamen na kamenu. Nauštrb radijske emisije, posvetile smo se razvoju Peščanika kakav je danas - onlajn medij zasnovan pre svega na autorskim tekstovima.

Svetlana i ja nismo na društvenim mrežama i one nisu integrisane u rad Peščanika kao kod ostalih medija. Nemamo ni resursa ni znanja da koristimo mreže na najbolji mogući način; one su nam i dalje samo podrška za dalju distribuciju sadržaja. Na sajtu nemamo otvorenu opciju za komentarisanje, što nam se ponekad zamera. Iz tuđih iskustava smo shvatile da to neko mora brižljivo da moderira, kao prostor gde bismo svi zajedno učili kako se nešto komentariše, kako se vodi dijalog. Pošto je taj deo prostora na internetu potpuno okupirala ogromna vojska botova, držimo se izolovano. To, naravno, ima svoju cenu, ali kad bismo to pripustile u ovu ionako užasno komplikovanu jednačinu, cena bi bila još gora; žongliramo sa deset tanjira u vazduhu, ne možemo više.

Sadržaj na Peščaniku je slobodan i tako će biti sve dok Peščanik postoji. Uskoro ćemo se upustiti u crowdfunding kampanju: deo poziva čitaocima za pomoć biće i poruka da će Peščanik zauvek biti otvoren.

CINS

- Novinari CINS-a, zajedno sa novinarima BIRN-a i KRIK-a, na meti napada i kampanje koju je protiv njih vodio Informer, tabloid blizak vlasti, optužbama da se finansiraju iz inostranstva kako bi destabilizovali Srbiju.
- Na sajt CINS-a izvršen tehnički napad; izmenjen izgled naslovne stranice na koju su postavljeni grb OVK i političke poruke u vezi sa Kosovom.
- Novinari CINS-a na meti kampanje uvreda na Tviteru.
- Redakcije CINS-a i KRIK-a, kao i novinar Slobodan Georgijev, na meti neistina i uvreda u videu objavljenom na Tviteru. Posle objave snimka, usledili brojni komentari sa uvredama i pretnjama.


PROCUREO SPISAK ZA PRITISAK?
DA, ALI SAD GA ZOVEMO
LISTA SLOBODNIH MEDIJA!
BIRN
CINS
KRIK

BRANKO ČEČEN

NOVINAR, DIREKTOR CENTRA ZA ISTRAŽIVAČKO NOVINARSTVO SRBIJE (CINS)

Istraživačko novinarstva je oblast novinarstva u kojoj je obuka o bezbednosti, digitalnoj i fizičkoj, deo posla, kao i primena naučenog, naravno. Postoje izvesna pravila u našim životima, koja drugima mogu izgledati sasvim neuobičajeno. Svi koji sa istraživačkim novinarstvom imaju ozbiljna posla imaju ogromne, komplikovane i dvostruke šifre za sve što šifru traži; ne ostavljamo svoje kompjutere i telefone drugima na uslugu, pa čak ni u parkiranom automobilu; enkriptujemo gomilu mejlova i dokumenata; koristimo alate za bezbednu komunikaciju; podaci o izvorima činjenica za naše priče, kao i najvažnija dokumenta, pohranjeni su na uređajima koji ne dolaze u kontakt sa internetom; stalno proveravamo da li nas neko prati. Paranoja je, ukratko, deo posla.

Osnovni princip glasi: „Bolje je da uzalud budeš paranoičan nego da te jednom uhvate nespremnog“. Šteta može da bude ogromna, ljudske sudbine su u pitanju. Ovo je zemlja u kojoj ubistvo novinara nije hipoteza, a ni paljenje kuće, prebijanje... Ovo je zemlja u kojoj jedna mala organizacija sa desetak zaposlenih ima u svojoj relativno kratkoj istoriji čitav katalog vrlo konkretnih nasrtaja na bezbednost, zbog kojih prosto mora da se štiti kako zna i ume. Mnogo je više digitalnih napada i pretnji, ali je bilo i onih drugih. Zapravo, te dve stvari su povezane na veoma zanimljiv način.

Jedan iskusni američki kolega mi je pričao da je čitao istraživanje o svim fizičkim napadima na novinare u SAD ikada i da se 70 procenata svih nasrtaja dogodilo bez ikakve pretnje ili upozorenja. Što je i logično, ako neko hoće fizički da vam naudi, neće da vam javlja svoje namere. U isto vreme, ogromna većina tih napada podrazumevala je i praćenje novinara, istragu o njihovom ponašanju i navikama. Zbog toga nas najviše brine kada neko pokušava da neprimećeno sakuplja podatke o nama.

Novi oblik praćenja novinara nije fizičko praćenje, već upad u njihove telefone i kompjutere. Kada smo 2014. godine radili priču o vezi između organizovanog kriminala i kockarske industrije u Srbiji, neko je primetio da jedna anketa za korisnike našeg veb sajta ne radi baš kako treba. Programeri su brzo rekli da to nije slučajno, pa smo angažovali stručne ljude da vide šta je. Ispostavilo se da je neko upao na server u Nemačkoj, na kojem je pored našeg bilo još nekoliko stotina veb sajtova, te kroz server upao u naš sajt i „injektirao" program koji prikuplja podatke i šalje ih negde, nekome. Da ta anketa nije slučajno onesposobljena tokom upada, ko zna da li bismo ikada išta primetili.

Injektirani program je prikupio sve naše lozinke, imena i adrese osoba sa kojima smo komunicirali, dokumenta, razne brojeve (telefona, matične brojeve preduzeća i sl.)... Ukratko, sve što liči na podatak. Uskoro je neko nepoznat mogao jako dobro da zna mnogo toga o nama, našem kretanju, adresama na kojima živimo, da iz mejlova pokupi skenove naših ličnih dokumenata, zvaničnu komunikaciju sa dokumentacijom koju šaljemo... E, toga se već prilično plašimo.

Ovaj napad nije imao ozbiljnije posledice zato što je sve što je bilo važno bilo i – enkriptovano. Enkriptujemo oko deset puta više sadržaja nego što je potrebno, logika je jednostavna – ako se i odluče da pokušaju to da razbiju, šanse da otvore nešto bitno su 1:10, kao i da se uzalud trude. Ali to je manje važno u ovom kontekstu. Važno je da ovo nije bio jedini napad i da je naš oprez, na žalost, potpuno opravdan. Da pokušamo, dakle, da napravimo listu svih dosadašnjih digitalnih pretnji po bezbednost Centra za istraživačko novinarstvo Srbije:

Više puta smo upozoreni da smo na „merama", odnosno da našu komunikaciju prati, a možda i snima tajna služba i/ili policija. I jedno i drugo je više puta dokumentovano na primerima drugih kolega novinara, na suđenjima i u dokumentaciji raznih državnih organa. Meni je, kao vid zastrašivanja, pušten audio snimak kako se prepirem sa svojom suprugom u sopstvenom stanu.

Sajt nam je hakovan i oboren dva puta – jednom samo stranica sa tekstom o tome kako ćerka Jorgovanke Tabaković službenim vozilom ide na studije iz Novog Sada u Beograd svake nedelje, drugi put su to uradili neki ovdašnji hakeri i ostavili na početnoj strani neko ludilo sa „velikom Albanijom" da zavaraju trag.

Dva puta do sada smo otkrili nekoga ko se tajno uvukao u sistem i kopirao podatke, a naši programeri misle da su prepoznali tragove još bar dva slična upada koje nismo otkrili na vreme, od kojih je bar jedan bio nasumičan, iz Kine.

Pretnje putem društvenih mreža i raznovrsnih aplikacija za poruke stižu periodično, ali ne tako često i nisu tako ekstremne kao one upućene nekim drugim kolegama i, posebno, koleginicama (ovo je, izgleda, vrlo mizogino društvo).

Paralelno sa digitalnim pretnjama, odvijaju se i druge. Najozbiljniji incident dogodio se kada smo radili priču o povezanosti fudbala, organizovanog kriminala i vlade Srbije. Kriminalna grupa je dodelila našim novinarkama po jednog siledžiju da ih otvoreno prate, na par metara odstojanja, danima, kao vid zastrašivanja. Policija je sprovela istragu i praćenje je prestalo, ali su nam inspektori otvoreno rekli da ih ne zanima ko su organizatori. Audio snimak moje prepirke sa suprugom u našem stanu pušten mi je kao „dobronamerno upozorenje“ i to je učinio „kolega“ sa kojim sam davno radio u novinama. Iako je taj snimak sasvim lepo mogao biti napravljen upadom u moj telefon, ili bilo koji telefon u našoj porodici, mogao je i drugačije, pa se ne može definitivno svrstati u digitalne nasrtaje na bezbednost i privatnost.

U isto vreme, politički gospodari Srbije vredno rade na atmosferi linča prema istraživačkim novinarima. Kada vašu organizaciju, ili bilo koga od nas lično, tabloidi označe kao „izdajnika“ i „kriminalca“, što je uobičajena reakcija pro-vladinih medija na dobru istraživačku priču, to zaista može podstaći nekoga na nasilje prema nama. Što nas manje brine od situacije u kojoj organizovana kriminalna grupa, povezana sa poslovnim sektorom i politikom, iskoristi višednevne optužbe i histeriju u medijima za kakvu planiranu akciju, što se nije jednom dogodilo u Srbiji, na žalost. Dovoljno je setiti se Slavka Ćuruvije i razularene tajne službe koja je odlučila da iskoristi ludilo Miloševićevih medija da fizički ukloni novinara. Nedemokratska, protivzakonita, neprofesionalna i, na kraju krajeva, nepristojna i neljudska propaganda protiv istraživačkih i drugih profesionalnih novinara u pro-vladinim „medijima“ uvek se završi nasiljem, to je pravilo koje nikad ne „omane“. Za sada je jednom novinaru izgorela kuća nakon višegodišnje kampanje maltretiranja i blaćenja u medijima, ali je isto tako u Crnoj Gori naša koleginica Olivera Lakić dobila, kao upozorenje, metak u nogu.

Iako sve ovo, kada se navede na jednom mestu, izgleda sasvim nenormalno i nenaviklima verovatno uznemirujuće, to je deo našeg sveta i našeg posla. Ne događa se prečesto i, po našim procenama, mali procenat nasrtaja je zaista opasan po naše izvore i nas same. Nije nam svejedno, sve to vrlo ozbiljno tretiramo, ali niti trčimo u krug po redakciji sa rukama na glavi vrišteći u panici, niti se pravimo da sve ovo ne postoji i da nije opasno. Dakle, kakav je naš odgovor?

Pre svega, treba imati u vidu naše resurse. U pogledu broja ljudi, količine novca (bezbednost uvek košta) i samim tim i tehničke opremljenosti, mi se ne možemo meriti ni sa jednom prosečnom advokatskom kancelarijom, a kamoli organizovanom kriminalnom grupom ili tajnom službom. Ono čega nam ne nedostaje, međutim, jeste velika glad za znanjem i brzina kojom ga usvajamo.

Možda je i najvažniji deo naše strategije – disciplina. Bezbednost „pada" na nemaru: ostavljenom uključenom računaru među nepoznatim osobama, unošenju lozinke pred neznancima, napuštanju redakcijskog računara bez izlaženja iz svojih naloga na elektronskoj pošti ili društvenim mrežama, provođenju godina sa istim lozinkama, i tako dalje. Protokoli o bezbednosti koje nastavljamo da razvijamo, deo su radne obaveze svakoga ko radi u CINS-u.

Sa ovakvom disciplinom ima mnogo više smisla učiti o enkripciji, korišćenju dvostepenih verifikacija, prepoznavanju napada i upada i tako dalje. Bez nje – nema sve to mnogo smisla. Mnogo je jednostavnije nekome maznuti nezaštićen ili loše zaštićen računar nego hakovati server u Nemačkoj.

Kako smo, ipak, disciplinovani paranoici, reklo bi se po tome što naše izvore nikad niko nije provalio, što je apsolutno najvažniji razlog za skrivanje važnih dokumenata i obezbeđivanje komunikacije, imamo razloga da pretpostavljamo da sve što radimo i učimo u vezi sa bezbednošću verovatno ima adekvatan efekat.

Veoma je važno što smo članovi međunarodne mreže istraživačkih centara i novinara OCCRP (Organized Crime and Corruption Reporting Project). Mreža ima vrhunske eksperte koji prate razvoj digitalne bezbednosti i pretnji i stalno nas obučavaju kako bi i mi bili spremniji na njih, ili ih predupredili. Neprekidno nas informišu o „rupama" u programima, onlajn servisima, aplikacijama i drugim digitalnim alatima kojima se koristimo. Da nemamo njih, trošili bismo dosta vremena na praćenje više različitih izvora i brda novca (koji nemamo) na profesionalnu pomoć. Povremeno nam pošalju nekoga od svojih ljudi da nam evaluiraju bezbednost sistema i uspostave neke varijante odbrane na licu mesta, pokažu nam trikove i generalno – zatvore veće praznine u zaštiti.

S druge strane, naša generalna strategija je da što više pažnje javnosti skrenemo na mene. Direktor sam i, zapravo, ne objavljujem priče. Najstariji sam, imam iskustvo sa ratišta i novinarstva iz devedesetih, kada je Arkan upao sa četom ljudi i dugim cevima u redakciju u kojoj sam radio, na primer, direktno sa fronta, kriminalci dolazili u „posete" par puta sa mecima u cevima pištolja u nervoznim rukama, i da ne nabrajam više primere nenormalnih iskustava novinarske karijere u nečemu što, verovatno vrlo pogrešno, smatramo relativno normalnom zemljom za život. U svakom slučaju, ja sam tu najmanja šteta ako se nešto

desi, posebno po naše istraživačke kapacitete.

Javnost i transparentnost rada su vrlo važni za našu bezbednost, ali je još važnije uvek objaviti dokaze. Jer, jednom kada izađu na svetlo dana, interesni odnosi u igri između nas i onih koje istražujemo se menjaju. Njihov interes postaje da spinuju i sakriju otkriveno i fokus se premešta sa novinarki i novinara na sam sadržaj medijskog proizvoda.

Još jedan vid odbrane je zajedništvo profesionalaca. Toga baš i nema dovoljno u Srbiji, ali u slučaju problema, međunarodna mreža priskače u pomoć, bez obzira da li treba kod nekoga od kolega u drugim državama da sklonimo novinarku na kratko, dok ne vidimo kakve su posledice objavljene priče, ili je potrebno da par hiljada novinara sveta uputi pozive, upite i zahteve međunarodnim i domaćim institucijama, svojim parlamentima i vladama, digne medije Evrope i sveta na noge. Tako smo ove godine iz pritvora izvukli kolegu Ivana Golunova, kojem je moskovska policija namestila heroin (srećom, gotovo komično trapavo) i nameštena optužnica je odbačena. Šest sati sam pokušavao da dobijem tog inspektora koji ga je uhapsio, a kada sam konačno uspeo, čovek mi se izvrištao na ruskom u uvo i prekinuo vezu. Verovatno sam bio sto osamdeseti po redu. Nije mi ga žao, uopšte. Ali zvali smo sve i svakoga, od OEBS-a do UN-a. Možda ne možemo da vratimo u život Jana Kucijaka i Dafne Karuanu Galiciju, ali ove žive možemo bar da osvetlimo reflektorom medijske pažnje, kako se nekome ne bi dogodilo nešto neočekivano u tim pritvorima i, na žalost, zatvorima. Dok se ne vidi šta još može da se uradi.

Krajnji cilj svakog ugrožavanja ove vrste je da se nekako zaustavi naš rad, odnosno da priča o određenom entitetu ne bude objavljena. Teško je znati šta mi istražujemo, jer smo dosta dobri u skrivanju elemenata istraživačkog procesa. Ali kada završimo, po profesionalnim standardima, a i ljudskim, zovemo osobe o kojima se u priči radi. Za to imamo par nedelja i tih par nedelja, kada oni konačno znaju šta radimo, su najopasnije. Tada nam upadaju u sistem, prate nas, zastrašuju. Upravo tada primenjujemo još jedan element odbrane – komuniciramo jasno prema svima da smo tim i da uklanjanje, ucenjivanje ili zastrašivanje bilo koga neće postići svrhu jer će priču uvek imati ko da objavi i – biće objavljena svakako. Ivan Golunov je frilenser, što znači – sam. Zato se korumpiranim elementima moskovske administracije i policiji učinio lakom metom. Važno je biti deo organizacija, timova, asocijacija i mreža. Bezbednije je. Upravo to mnoštvo oko novinara garantuje da će priča biti objavljena i istražena do kraja šta god da se dogodi, što racionalnijim kriminalcima, recimo, govori da je nasilje bespredmetno.

Malo je to morbidan princip, ali verujemo da pomaže. Na kraju krajeva, svi naši izvori su bezbedni i anonimni ako su to tražili, niko od nas nije fizički napadnut,

tabloidi nisu našli ništa zaista kompromitujuće o bilo kome od nas da objave, a ne samo da još uvek radimo, nego smo sve bolji i bolji, ne samo mi u CINS-u, nego i u KRIK-u, BIRN-u, Insajderu... Znamo mi vrlo dobro da se od hakerskog napada jedan veb sajt ne može zaštititi, ali znamo i da vitalno važna dokumenta i dokazi – mogu. To je naš posao, dužnost i pitanje profesionalne časti, ako to nije previše krupna reč.

Pre tri godine smo u CINS-u izračunali da nam rad na bezbednosti, u zavisnosti od osetljivosti istraživanja koja su u toku, uzima između 10 i 20 procenata radnog vremena. To nije normalno i svakako je previše. Kao što nije normalno živeti sa svim ovim napadima i merama zaštite. Međutim, to je realnost i učenje, vežbanje i primena svih sredstava digitalne bezbednosti koja su nam na raspolaganju, za sada nam omogućavaju da u velikoj meri zaštitimo svoje izvore, našu međusobnu komunikaciju, kao i dokaze i informacije o tome šta istražujemo i šta smo otkrili, pre nego što objavimo priču. A to znači i mnogo mirniji san.

Ne mogu da zamislim savremeno novinarstvo bez stalnog napora da se razume sopstveno digitalno okruženje i rizike koji u njemu postoje. Mislim da bi to bilo jednostavno neodgovorno. Prema građanima koje novinari zastupaju, samim novinarima i njihovim izvorima. Ovaj svet se digitalizovao, pa i mi sa njim. Nema opravdanja za neoprez i ni jedna mera opreza nije uzaludna.

TRENDOVI I ZAKLJUČCI

Tehnički napadi predstavljaju najupečatljivije forme povrede digitalnih prava i sloboda, posebno kada su na meti veb stranice organizacija civilnog društva i nezavisnih medija. Onlajn mediji su pretežno mete većih napada, uglavnom povezanih sa izveštavanjem o nekom aktuelnom događaju. Uobičajeno sredstvo je DDoS, odnosno zagušenje servera zahtevima kako bi sajt bio nedostupan; ovaj trend je poslednjih godina u padu, budući da se DDoS pokazao kontraproduktivnim jer podstiče interes javnosti za sadržaje cenzurisane na ovaj način. Posmatrani u globalnom kontekstu, tehnički napadi kreću se ozbiljnijim i daleko opasnijim pravcem.

Kao prvi trend, istakli su se napredni **„fišing setovi".** Fišing se smatra jednim od najuspešnijih načina za napad prvenstveno zbog brzine jer su fišing sajtovi aktivni najduže 4–5 sati. Danas čak i korisnici sa elementarnim tehničkim znanjem mogu da izvedu napad ove vrste, dok raspoložive tehnologije omogućavaju pojavu četiri nova uzorka malicioznog softvera svake sekunde. Procenjuje se da je samo 65% svih veb adresa na internetu pouzdano. U avgustu 2019. godine, dvadesetak državnih institucija u Teksasu našlo se na meti napada za otkup (ransomware) što incident čini jednim od najvećih i najbolje koordinisanih napada te vrste u SAD. U jednom od okruga pogođenih napadom, oboren je sistem za finansije koji obrađuje plaćanja kreditnim karticama. Mada se tvrdilo da je Odeljenje za informacione resurse u stanju da se nosi sa ovakvim napadima, u ovom slučaju je zatražena pomoć od FBI, državne divizije za upravljanje kriznim situacijama, pa čak i od vojske.

Fišing (phishing) je tehnika manipulacije sa ciljem da navede metu da otkrije poverljive informacije, recimo korisničko ime i lozinku, ili da pokupi virus iz mejla ili sa fišing sajta. Manipulisanje se najčešće izvodi tako što se napadač predstavlja kao osoba ili institucija od poverenja. Spir fišing (spear phishing) je naprednija varijanta ove tehnike, kojom se planski targetiraju specifični pojedinci ili organizacije.
Maliciozni softver (malware) je opšti termin za softver koji se koristi za ometanje rada računara, prikupljanje osetljivih informacija ili pristupanje zaštićenom informacionom sistemu.

Posebnu vrstu čine napadi koji omogućavaju **pristup sistemu na daljinu**. Sve popularniji oblik je potajno korišćenje zaraženog kompjutera za rudarenje kriptovalute (cryptojacking), a očekuje se da će narednih godina upravo krip-

tovaluta biti u središtu debata o sajber bezbednosti. Zanimljiv izazov u tom smislu čini pokušaj Francuske da blokira upotrebu Fejsbukove kriptovalute Libra u Evropi, sa stanovišta bezbednosti čitavog finansijskog sistema. Inače, pokazalo se da su žrtve napada na daljinu najčešće kućne mreže, gde hakeri targetiraju računare, pametne telefone, IP, kamere, itd, prateći razvoj **Interneta stvari** (Internet of Things, IoT). Mnogi korisnici ne smatraju ove aparate podložnim napadima, što izlaže povećanom riziku podatke koje umreženi kućni uređaji prikupljaju i obrađuju. Pametni uređaji mogu se zloupotrebiti i za DDoS napade, dok je nizak stepen njihove bezbednosti uslovljen cenom proizvodnje i održavanja. Stoga se očekuje da će napadi ovog tipa biti sve učestaliji. Najznačajniji takav slučaj bio je virus Mirai, koji je gotovo slučajno iskoristio nebezbedne IoT uređaje jer je skenirao velike blokove interneta za otvorene Telnet portove, a zatim pokušao da se loguje uz pomoć 61 kombinacije postavljenih lozinki, te je na taj način okupio veliku „botnet vojsku".

Značajan pravac razvoja tehničkih napada određuje tzv. veštačka inteligencija (**artificial intelligence, AI**) koju, uz mašinsko učenje (machine learning), velike industrije već koriste kako bi automatizovale svoje procese. AI algoritmi nalaze primenu i u sprečavanju i u izvođenju sajber napada. Sistemi veštačke inteligencije su jeftini, anonimni i automatski, a omogućavaju i fizičku udaljenost napadača. AI je posebno koristan za kreiranje sadržaja koji može da prodre kroz uobičajene filtere za sajber bezbednost, poput alata koji razlikuju mašinski generisan tekst od onog koji je napisao čovek. Korisnici interneta iz Srbije sve su više svesni razmera u kojima je protok informacija u onlajn sferi posredovan algoritmima koji, na osnovu naših onlajn aktivnosti, biraju vesti, reklame, objave drugih korisnika i ostale sadržaje koji će nam biti prikazani. Takođe, algoritmi društvenih medija i drugih onlajn platformi već uveliko samostalno procenjuju koji sadržaji i nalozi krše interne uslove korišćenja ili zakonske norme, bilo da se rukovode unapred zadatim rečima koje nisu dozvoljene ili prijavama drugih korisnika. Takav slučaj zabeležen je kada su algoritamski „urednici" Jutjuba blokirali nalog Ombudsmana Srbije.

S druge strane, na trendove u tehničkim napadima utiče **razvoj regulative i osnivanje novih bezbednosnih instituta**. U sajber prostoru odbrana je ponekad skuplja nego napad, što obeshrabruje male i nezavisne onlajn medije koji ne mogu sebi da priušte skupe stručnjake za sajber bezbednost ili tehnička rešenja za zaštitu. U Srbiji, korak u pozitivnom smeru predstavlja činjenica da se tehnički napadi redovno prijavljuju posebnom tužilaštvu za visokotehnološki kriminal. Međutim, nedostaje povratnih informacija o istrazi, sudskim procesima i pravnosnažnim presudama krivcima za tehnički napad na medije, novinare i druge aktere koji nastupaju u javnom interesu. Uzor Srbiji u procesu pridruživanja EU trebalo bi da bude nedavno usvojen zakon o sajber bezbednosti kojim je ojačana evropska Agencija za sajber bezbednost (EU Agency for cybersecurity, ENISA) i uspostavljen jedinstveni pravni okvir za digitalne proizvode, usluge i procese.

POVREDE PRIVATNOSTI

HRONOLOGIJA

Povrede informacione privatnosti najčešće se tiču nedozvoljene obrade podataka o ličnosti, neadekvatnog odnosa prema podacima građana, kao i bezbednosnih propusta u tehničkim merama zaštite podataka. Tokom skoro čitavog perioda monitoringa digitalnih prava i sloboda, u Srbiji je tekao proces izrade i usvajanja novog Zakona o zaštiti podataka o ličnosti, od kog se očekivalo da podigne nivo standarda privatnosti i zaštite podataka građana. Primena novog propisa počela je u leto 2019, a da li će i kako uticati na odnos prema podacima i privatnosti građana, ostaje da se vidi.

2014

Incidenti iz ove kategorije zabeleženi su ukupno pet puta u 2014. godini, a svakog puta su žrtve povreda prava bili građani, odnosno opšta kategorija populacije bez specifičnih karakteristika zbog kojih bi bili odabrani za mete napada. U slučaju curenja podataka sa sajta Agencije za privatizaciju pogođeno je bilo gotovo celokupno punoletno stanovništvo Srbije, što je do danas najteže kršenje privatnosti građana u našoj zemlji i najveći bezbednosni propust u oblasti zaštite podataka o ličnosti. Najbrojniji incidenti u toj godini zabeleženi su u potkategoriji curenja podataka o ličnosti građana, sa četiri slučaja, a za njom sledi potkategorija nedozvoljene obrade podataka o ličnosti, u tri slučaja. Zabeležen je i jedan slučaj objavljivanja informacija o privatnom životu.

2015

U 2015. godini dokumentovano je gotovo dvostruko više slučajeva nego u prehodnoj, ukupno devet. Građani su i te godine bili česta meta napada, mada ne jedina kao u prethodnoj. Od ukupnog broja slučajeva, prava građana bila su na meti napada šest puta, dok su napadi vršeni i na predstavnike političkih partija, kao i na novinare. U ulozi napadača, odnosno onih koji krše prava javljaju se organi vlasti u pet zabeleženih slučajeva. Dok u prvoj godini monitoringa nije dokumentovan nijedan slučaj nezakonitog presretanja elektronskih komunikacija, naredne godine zabeleženo je pet incidenata. Sledeća potkategorija po brojnosti povreda bila je nedozvoljena obrada podataka o ličnosti građana, tri puta, a desila se i po jedna povreda iz potkategorije objavljivanja informacija o privatnom životu, kao i ostalih povreda informacionih privatnosti.

2016

Godine 2016. zabeleženo je sedam slučajeva povreda informacione privatnosti i zaštite podataka o ličnosti. Iako je reč o izbornoj godini, to nije naročito uticalo na broj slučajeva u ovoj kategoriji, iako je u nekim drugim kategorijama zabeležen značajan porast. Ipak, tri slučaja povreda iz ove kategorije odnosila

su se upravo na izbore, a ticala su se objavljivanja informacija o privatnom životu i nezakonitog presretanja elektronskih komunikacija. Za celu godinu, povreda iz potkategorije objavljivanja informacija o privatnom životu bilo je tri, a nezakonitog presretanja elektronskih komunikacija četiri. Mete napada bili su građani, aktivisti, javne ličnosti, državni funkcioneri, politički akteri i novinari. Zabeležen je jedan slučaj nedozvoljene obrade podataka o ličnosti.

2017

Broj povreda informacione privatnosti i zaštite podataka o ličnosti neznatno je smanjen u 2017. u odnosu na prethodnu godinu - sa sedam na pet zabeleženih slučajeva. Napadači su u tri slučaja bili nepoznati, a dva puta su to bili organi vlasti. Na meti su građani kao nespecifična grupa i aktivisti, po dva puta, te jedan predstavnik političke partije. Najviše zabeleženih povreda bilo je iz potkategorije nedozvoljene obrade podataka o ličnosti, u tri navrata, a desio se i po jedan slučaj iz potkategorija objavljivanja informacija o privatnom životu i curenja podataka o ličnosti građana.

2018

Eskalacija povreda privatnosti zabeležena je 2018. godine, kada su povrede izazivali i javni i privatni akteri, a u nešto manjoj meri građani i novinari. Ukupno je zabeleženo 18 slučajeva povreda iz ove kategorije, od čega su građani kao nespecifična grupa bili na meti napada čak 16 puta. Najmasovnije povrede dogodile su se u potkategoriji nedozvoljene obrade podataka o ličnosti, takođe 16. Upečatljive slučajeve povreda prava iz ove potkategorije čine prikupljanje osetljivih podataka o ličnosti građana putem aplikacije „Izabrani doktor“, koju je promovisalo Ministarstvo zdravlja, kao i nedozvoljena obrada osetljivih podataka građana u centrima za socijalni rad u nekoliko gradova u Srbiji. Izbegavanje odgovornosti za ovakvu vrstu postupanja državnih institucija gotovo je pravilo kada je reč o povredi prava građana na privatnost i zaštitu podataka o ličnosti. Pored ove najmasovnije kategorije, zabeleženo je i šest slučajeva curenja podataka o ličnosti građana, kao i po jedan slučaj nezakonitog presretanja elektronskih komunikacija i objavljivanja informacija o privatnom životu. U 2018. godini prvi put su zabeleženi slučajevi iz potkategorije narušavanja informacione privatnosti na radnom mestu i to tri puta. Ova povreda prava uglavnom je registrovana u paru sa još nekom potkategorijom. U dva od tri takva slučaja, napadači su bili organi vlasti, a u jednom slučaju je napadač ostao nepoznat.

2019

Do septembra 2019. u kategoriji povreda informacione privatnosti i zaštite podataka o ličnosti obrađeno je šest slučajeva, od kojih je pet predstavljalo nedozvoljenu obradu podataka o ličnosti. Često su slučajevi povreda obuhvatali više od jedne potkategorije. Obrađena su i tri slučaja objavljivanja informacija o privatnom životu, dva slučaja curenja podataka o ličnosti građana i jedno narušavanje informacione privatnosti na radnom mestu. Najbrojnije žrtve i u ovoj godini bili su građani, tri puta, a u preostala dva slučaja na meti su bili

novinari. Napadača je bilo sa više strana - od nepoznatih i građana, do organa vlasti i državnih funkcionera.

SPECIFIČNI SLUČAJEVI

6209: Do sada glasao za DS. Neće više. Invalid. Deca 20 i 22 godine. Nezaposlena, žena radi u kafani za 11.000. On invalid iz Bosne.
7382: Žena od Ramiza. Kaže da se pre glasanja da malo ulje, brašno itd. pa će glasati svi Šiptari iz Adica za nas. Puno zna.
34142: Veliki protivnik ove vlasti. Ne kontaktirati.

Ovo su opisi troje od 400.000 građana zavedenih u bazi podataka tzv. kapilarnih glasova koja je pronađena početkom 2017. na jednom javnom serveru. Za razliku od curenja podataka na sajtu Agencije za privatizaciju tri godine ranije, gde su podaci prikupljeni na legalan način, ova baza je osmišljena i realizovana suprotno ustavnim pravima građana. Po veličini, međutim, oba slučaja se izdvajaju kao masovno kršenje zaštite ličnih podataka građana Srbije.

Marko Dragoslavić je godinama vrlo aktivan na Tviteru, sa naloga @tamodaleko. Komunicira uglavnom oštru kritiku prema vlasti. Tviter nalog @Milijan95027889 je takođe aktivan, ali uglavnom retvituje i širi vesti koje veličaju vladajuću stranku, predsednika i druge predstavnike vlasti. Jednog dana, @Milijan95027889 je objavio originalnu fotografiju iz nove lične karte @tamodaleko. Tu fotografiju čak ni Marko nikada nije video u boji.

Nekoliko meseci pre toga, Marko ulazi u sukob sa direktorom Kliničko-bolničkog centra Zvezdara. Tabloid objavljuje Markov zdravstveni karton iz te bolnice.

U februaru 2019. portali provladinih tabloida objavljuju zdravstveni karton Marije Lukić, pošto je prijavila predsednika opštine Brus zbog seksualnog uznemiravanja. Nešto ranije, nakon incidenta u lokalnom Domu zdravlja, portal provladinog tabloida objavljuje podatke o zdravstvenom stanju i navodnoj osuđivanosti jedne žene iz Kragujevca.

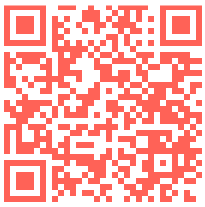
Dejan Milojević iz Aleksinca je oštar, ali elokventan kritičar vlasti na Fejsbuku. Nakon još jednog među brojnim statusima, u posetu mu je došlo dvadeset pripadnika žandarmerije i odeljenja za visokotehnološki kriminal. Tražili

su oružje, bekapovali / konfiskovali sve kompjutere i mobilni telefon i izmenili lozinku za Fejsbuk.

Dragan Murar je tužiocu morao da potpiše da mu se osim telefona i SIM kartice privremeno oduzima i:

- Jedan (1) nalog na društvenoj mreži Tviter “Dragan Murar @muki68” i šifrom za pristupanje “jelena97”.

- Jedna (1) mejl adresa “dragan.murar2@gmail.com”, sa šifrom za pristupanje “jelena97”.



Razni su razlozi za curenje podataka, konfiskaciju opreme, lozinki ili celog digitalnog života građana. Međutim, ponekad neplanirano procuri i drugačija vrsta podataka. Jednom prilikom su nam dokumenti sa Vikiliksa rekli da Srbija intenzivno pregovara o kupovini vrhunskog špijunskog softvera od italijanske firme „Hacking Team“. Kasnije smo saznali da je Vojno-bezbednosna agencija (VBA) već kupila najpopularniji sistem za elektronski nadzor, FinSpy. On takođe služi za targetirano prisluškivanje pametnih uređaja. Analize internet saobraćaja su i ranije potvrdile aktivnost softvera FinSpy na srpskoj mreži.

RODOLJUB ŠABIĆ

- Poverenik intervenisao zbog javno dostupne baze podataka na sajtu Agencije za privatizaciju. Baza je sadržala podatke o ličnosti preko pet miliona građana, što čini gotovo čitavo punoletno stanovništvo Srbije.
- Bazi je nakon intervencije Poverenika onemogućen javni pristup, a do tada je preuzeta više puta.
- Agencija za privatizaciju je podnela krivičnu prijavu nadležnom tužilaštvu protiv NN lica, dok je Poverenik nadležnom sudu za prekršaje podneo zahtev za pokretanje postupka. Agencija je u međuvremenu ugašena, a prekršajni postupak zastareo.
- Poverenik zabranio prikupljanje i obradu podataka o ličnosti putem aplikacije „Izabrani doktor“, namenjene zakazivanju lekarskih pregleda.
- Aplikacija je sadržala niz tehničkih i pravnih propusta iako je namenjena obradi osetljivih podataka o ličnosti građana koji uživaju posebnu zakonsku zaštitu.
- Ministar zdravlja sa omalovažavanjem govorio o Povereniku i njegovoj reakciji povodom sporne aplikacije.


KO SI TI I KAKO ZNAŠ DA MI JE ROĐENDAN???


PIŠE NA SAJTU AGENCIJE ZA PRIVATIZACIJU!

RODOLJUB ŠABIĆ

ADVOKAT, PRVI POVERENIK ZA INFORMACIJE OD JAVNOG ZNAČAJA I ZAŠTITU PODATAKA O LIČNOSTI (2004-2018)

U doba sve češćih povreda digitalnih prava građana Srbije, pored pojedinačnih dešavaju se i povrede prava većeg broja ljudi odjednom. Dva upečatljiva takva slučaja, jedan po broju ljudi kojima je načinjena povreda, a drugi po osetljivosti podataka, bili su i predmeti kojima se bavio Poverenik za informacije od javnog značaja i zaštitu podataka o ličnosti. SHARE Fondacija popričala je sa prvim Poverenikom, danas advokatom i, kako sam sebe naziva, tviterašem, Rodoljubom Šabićem. Prethodni Poverenik se, osim na slučajeve, osvrnuo i na početak svog rada, prepreke koje su pratile njegov tim, kao i na odnos koji država ima prema instituciji na čijem čelu je bio od osnivanja do prošle godine.

Jedan od dva masovna slučaja povrede digitalnih prava građana jeste slučaj Agencije za privatizaciju iz decembra 2014. Na sajtu te agencije su bili su dostupni lični podaci gotovo svih punoletnih građana Srbije. Kakav je utisak na vas lično ostavio ovaj slučaj i koliko je on važan za razumevanje narušavanja privatnosti i zloupotrebe podataka o ličnosti građana?

Ovaj primer spada u markantnije u mojoj dugogodišnjoj praksi. Nije jedini, ali je svakako jedan od upečatljivih. Dešavalo se da se kompromituju daleko veće

zbirke podataka, imamo primer Japana, Rusije, Italije, tako da je broj ličnosti čiji su podaci bili kompromitovani bio veći od tih famoznih 5 miliona i 200 hiljada, kao u našem slučaju. Ali to je bio prvi put da se u nekoj državi kompromituje kompletna baza podataka punoletne populacije - u tom pogledu smo za Ginisa, prvi smo i verovatno ćemo ostati na tronu i nimalo laskavom prvom mestu. Ovaj slučaj govori o više aspekata na koje sam kao Poverenik neuspešno upozoravao nosioce naše izvršne vlasti. Više aspekata koji savršeno idu uz tu potpunu hipokriziju u odnosu države prema tako delikatnoj oblasti kao što je zaštita privatnosti i zaštita podataka o ličnosti.

Kako je uopšte otkrivena ova zbirka ličnih podatka?

U toku noći, na Tviteru počinje nekakva prilično nemušta komunikacija - neko signalizira da bi trebalo pogledati šta se dešava na sajtu Agencije za privatizaciju - jedan sajt za mene u načelu nezanimljiv i dosadan. Uđem na sajt i na prvi pogled ne vidim ništa, ali bio sam dovoljno odgovoran da okrenem nekoliko mlađih saradnika i kažem im, dajte ljudi, obratite pažnju, jer neko nešto pokušava da stavi do znanja. I pronađe se. Brzo smo uspostavili komunikaciju sa SHARE Fondacijom i počeli zajednički da delamo: prvo ono što Poverenik može, a to je da dignemo uzbunu i nateramo ljude iz Agencije da ugase link. Iako smo brzo zatvorili tu rupu, mogli ste ući u tu zbirku podataka i neko sigurno jeste - takve se prilike ne propuštaju i to je priča o pravima i kompromitaciji. Neko je uzeo gomilu ličnih podataka punoletne populacije Srbije. Kasnije je bio pokrenut prekršajni postupak protiv Agencije i odgovornih lica i bila je podneta krivična prijava. Nažalost, to je zastarelo, Agencija je ugašena, umrla, naš tužilac nije našao čak ni nesavesno poslovanje u svemu tome i priča se završila na jedan tragikomičan način. To je ta ružna ilustracija odnosa države prema jednom vrlo važnom pitanju.

Priča o Agenciji za privatizaciju završena je bez pronalaženja krivca za curenje ličnih podataka gotovo svih punoletnih građana. Da li u ovakvom slučaju treba insistirati na odgovornosti?

Naravno da treba insistirati na odgovornosti i to je stvar sa kojom ćemo se pre ili kasnije morati suočiti. To je već potpuno prepoznatljiv manir naše vlasti da ignoriše sve pametne impulse, impulse koje šalje znanje, iskustvo, dobra volja iz civilnog sektora ili nezavisnih institucija, već se prema njima odnosi bahato i prepotentno. Vlast u našoj državi na mnogo manje solidne opservacije koje dolaze spolja, od stranaca, reaguje gotovo servilno. Međutim, na pitanju odgovornosti treba raditi stalno i to ne može biti stvar dresure i spoljašnjeg uticaja. To je naša stvar - sve i kada ne bismo hteli u Evropsku uniju, morali bismo to da obezbedimo građanima Srbije, jer to Ustav i zakoni jemče.

Kako je slučaj Agencije za privatizaciju uticao na Vas lično?

Slučaj je uticao pozitivno na rad Poverenika, budući da je jačao kvalitet i intenzitet veza sa civilnim sektorom i ta dobra interakcija sa građanima bila je kompenzacija za deficite prouzrokovane lošim odnosom države prema instituciji Poverenika. Ali ako se prihvatite nečega kako sam se ja prihvatio funkcije Poverenika, onda morate uraditi sve što možete da gradite instituciju i istrajete. Čitav niz priznanja za aktivnosti predstavlja ozbiljnu satisfakciju za mene. Ali možda i najveća satisfakcija jeste odsustvo nekog priznanja od bilo koje vlasti, a izmenilo ih se pet, šest. Nikada nam nijedna vlast nije odala priznanje i mislim da je to verovatno jedno od najvrednijih priznanja koje smo dobili.

Šta država radi da bi podigla nivo svesti građana o njihovim pravima i zaštiti podataka?

Država ne radi ništa. Dovoljan je podatak da državni Poverenik za informacije od javnog značaja u poslednjih četiri godine svog mandata nije nijednom bio gost na javnom servisu, na državnoj televiziji - i to nije slučajno. To je posledica nečijeg stava i to je potpuno jasno.

Pred kraj Vašeg mandata svedočili smo još jednom slučaju povrede digitalnih prava građana, a reč je bila o osetljivim podacima o ličnosti i aplikaciji „Izabrani doktor“. Naime, Ministarstvo zdravlja pokrenulo je internet aplikaciju i obavestilo građane da preko nje mogu da zakazuju zdravstvene preglede. Ova aplikacija podrazumevala je novu vrstu obrade podataka o ličnosti - obradu naročito osetljivih podataka o zdravstvenom stanju građana. Šta se s njom desilo?

Načelno, nemam ništa protiv elektronske komunikacije, naprotiv. Živimo u eri koja se zove elektronska era, ali valjda imamo nekakve minimalne odgovornosti. Budući da je to, ako ništa drugo, podrazumevalo neku novu vrstu obrade podataka, bio je red - ne samo kulturni, nego i po zakonu - da se zatraži prethodno mišljenje Poverenika. Mišljenje nije zatraženo, pa sam ja na brzinu zatražio od mojih ljudi da pogledaju tu aplikaciju u toku dana, odmah pošto je ministar predstavio inovaciju. Našli su nekoliko naprosto skandaloznih stvari. Odmah sam upozorio građane da oprezno pristupaju aplikaciji, budući da su postojale štamparske greške, dva različita imena firme sa kojima je Ministarstvo zaključilo posao u vezi sa aplikacijom, da je utvrđeno da jedna firma ne postoji, a da je drugoj vlasnik bugarski državljanin, kao i da je politika privatnosti sklonjena sa sajta. Mi smo odmah upozorili građane na konferenciji za štampu, nakon koje sam bio napadnut i pitan zašto trošim sredstva u Medija centru. Mislim da se aplikacija i sama po sebi kompromitovala. Dešava se to da Poverenik šalje upozorenje, daje argumente i razloge, na šta javni servis u

Dnevnik poziva ne Poverenika, nego ministra, koji izjavljuje da on mene ništa ne razume. Pita spikerku da li me ona razume i ona me takođe ništa ne razume i oni tako zaključuju događaj - to je tragikomična zloupotreba i javnog servisa i funkcije.

Kada država na taj način reaguje na pravo na privatnost i stavlja van snage sve pravne mehanizme zaštite, kakve to posledice ima na procese kao što su pristupanje Srbije Evropskoj uniji?

Sa ovakvim odnosom države, nijedan Poverenik, iz bilo koje države članice EU, Srbiju ne bi stavio na listu zemalja za pristupanje. Da ne pominjemo to da smo usvojili jedan katastrofalan Zakon o zaštiti podataka o ličnosti, koji je zapravo loš „Gugl translejt" Opšte uredbe o zaštiti podataka (GDPR). Pa da su bar ceo GDPR preveli, nego su izostavili preambulu koja je više od pola Uredbe i objašnjava čitav niz pitanja koja se u ovoj oblasti pojavljuju. Tokom procedure usvajanja novog propisa, kada je Poverenik insistirao da je Zakon loš, pojavilo se i mišljenje eksperata Evropske komisije, koje je bilo izuzetno negativno, vrlo slično Poverenikovom. Ministarstvo pravde je prvo tvrdilo da to mišljenje ne postoji, pa se kasnije ustanovilo da ipak postoji, ali su ga ignorisali. Vrlo je zanimljivo da je Evropa iz nekakvih oportunističkih razloga prećutala to ignorisanje njihovog mišljenja. Međutim, sad se pojavilo novo mišljenje eksperata Evropske komisije koje je ponovo izuzetno negativno i koje zapravo ukazuje na to da su u najmanju ruku izmene, ako ne i donošenje novog zakona, neophodne.

Cene li građani u Srbiji privatnost i u kojoj meri im je privatnost bitna?

Postojeći nivo svesti među stanovništvom je takav kakav je. Ipak, dobrom delu građana danas je do privatnosti više stalo nego juče. Dobar deo građana danas, zahvaljujući pored ostalog vašim aktivnostima i aktivnostima sličnih subjekata, zna mnogo više o tim standardima i pravima nego što je znao pre. To još uvek nije dovoljno, ali je bolje nego što je bilo i treba nastaviti tim putem. Volim da ponavljam Snoudenovu sentencu, kada neko kaže baš me briga, ja sam pošten čovek, ja nemam šta da krijem, to je isto kao kad kažete baš me briga za slobodu izražavanja, ja nemam šta da kažem! Bez privatnosti, čovek nije čovek, on je nekakav humanoid, definitivno onda nismo više ona vrsta koja jesmo.

TRENDOVI I ZAKLJUČCI

Povrede prava u oblasti privatnosti i zaštite ličnih podataka najčešće se odnose na nedozvoljenu obradu i curenje podataka o ličnosti građana, a zatim na nezakonito presretanje elektronskih komunikacija i objavljivanje informacija o privatnom životu, dok su u manjoj meri zastupljeni slučajevi neovlašćenog pristupa - neovlašćene izmene i postavljanja sadržaja - kao i računarskih prevara i ostalih povreda informacione privatnosti. Ovakve prilike su na tragu globalnih trendova, naročito u pogledu primene pametnog video nadzora, dok delimo i izazove s kojima su u svetu suočena nacionalna pravosuđa i zakonodavci. Zbog stupanja na snagu Opšte uredbe o zaštiti podataka na teritoriji EU, 2018. je bila prelomna godina za regulatore, kompanije i građane. Uredbom je stavljen naglasak na zaštitu ličnih podataka i poštovanje prava pojedinaca u vezi sa ličnim podacima, između ostalog, kako komercijalni interes ne bi prevagnuo nad ljudskim pravom na privatnost. U tom smislu, tri su ključna faktora koji će uticati na zaštitu ličnih podataka u budućnosti.

Prvi faktor čine **aktivnosti samih korisnika**, koji će u značajnoj meri redefinisati opseg prava na privatnost. Pretpostavlja se da će korisnici moći da uđu u trag svojim podacima koje kompanije prikupljaju, da će biti više debata o pravima pojedinaca, njihovoj saglasnosti za obradu podataka, što će uticati i na promenu odnosa korisnika i organizacija čije je poslovanje zasnovano na podacima. Očekuje se da će korisnici aktivnije učestvovati u sprovođenju normi novog pravnog okvira za zaštitu podataka, prijavljivati zloupotrebe i ukazivati na povrede privatnosti.

Drugi izazov već jeste i biće **međunarodna saradnja** u zaštiti ličnih podataka na globalnoj mreži. Evropska Opšta uredba o zaštiti podataka stupila je na snagu 25. maja 2018. i zamenila do tada važeću Direktivu iz 1995, uzimajući u obzir nove tehnologije i uvodeći nova pravila obrade i zaštite ličnih podataka. Novi Zakon o zaštiti podataka o ličnosti u Srbiji, čija je primena počela krajem avgusta 2019. godine, praktično je prevod evropske Uredbe i u domaće zakonodavstvo uvodi istovetne obaveze. Mada se očekuje da će novi evropski standard zaštite podataka postati globalni uzor, usklađenost nacionalnih jurisdikcija u zaštiti podataka o ličnosti još uvek je daleko. Nekoliko značajnih incidenata u vezi sa privatnošću bili su okidači za usvajanje novih zakonskih rešenja, koji bi takođe mogli odrediti dalja kretanja pravne regulative širom sveta. Tako je u Kaliforniji donet Zakon o zaštiti privatnosti potrošača koji će stupiti na snagu 2020. godine, a koji uvodi stroge kazne za kompanije ukoliko zloupotrebe podatke svojih korisnika. Uz napredak veštačke inteligencije i mašinskog učenja, očekuje se odgovarajući razvoj pravnih instrumenata za zaštitu ličnih podataka.

Etička pitanja koja izviru iz primene veštačke inteligencije predstavljaju poseban aspekt debate o ljudskim pravima u takozvanoj četvrtoj industrijskoj revoluciji. Pametni uređaji povezani na internet, premreženost javnih i privatnih prostora kamerama za nadzor, automatizovano odlučivanje na osnovu istorije onlajn ponašanja, samo su neki od zasad prepoznatih izvora spora između građana, javnih politika i industrije. Beograd je nedavno zakoračio u ovo polje, sklapanjem sporazuma sa kineskom kompanijom o nabavci i instaliranju više hiljada kamera za nadzor sa softverskim sistemima za prepoznavanje lica - ali su građani isključeni iz debate o ovom poduhvatu. Posebno zabrinjava činjenica da kasni talas tehnoentuzijazma koji je poslednjih godina stigao i u Srbiju, zanemaruje iskustva razvijenih zemalja koje su već prošle kroz posledice ranijih grešaka. Jedna od njih svakako je i prepuštanje digitalne transformacije tehničarima i programerima, bez učešća društvenih nauka koje imaju kapacitet da promisle pravne, etičke i društvene aspekte inovacija.

Sve je češća upotreba tehnologije za automatsko prepoznavanje lica (Automated Facial Recognition, AFR), a posebno sistema za lociranje traženih osoba poređenjem fotografija iz baze i živog prenosa sa nadzornih kamera (AFR Locate). Ovaj sistem obrađuje velike količine podataka: biometrijske i metapodatke, uključujući vreme i lokaciju, kao i informacije o poklapanjima sa osobama sa liste traženih. U SAD je do sada nekoliko gradova zabranilo upotrebu AFR, dok su u pojedinim evropskim gradovima ovaj i slični sistemi u testnoj fazi. Globalna diskusija o ovom pitanju još uvek je u toku.

PRETNJE, UVREDE I PRITISCI

HRONOLOGIJA

Pritisci zbog izražavanja mišljenja na internetu predstavljaju hronično problematičnu tačku digitalnih prava i sloboda u Srbiji od početka monitoringa SHARE Fondacije. Osim upečatljive brojnosti ovakvih povreda digitalnih prava, glavni problem leži u odsustvu adekvatne reakcije nadležnih organa, pre svega u vezi sa pretnjama i drugim pritiscima na novinare, ali i na aktiviste i predstavnike civilnog društva. Takođe je značajno napomenuti da kod govora mržnje, jedne od potkategorija povreda koje se prate u ovom segmentu, a kojim se targetiraju i diskriminišu manjinske društvene grupe, ne postoji praksa javne osude i efikasnog pravnog procesuiranja takvog ponašanja.

2014

U prvoj godini monitoringa, zabeleženo je 29 slučajeva povreda digitalnih prava iz kategorije pritisaka zbog izražavanja i aktivnosti na internetu. U pogledu pritisaka na pojedince zbog izražavanja mišljenja u digitalnom okruženju, građani širom Srbije su tokom i neposredno posle poplava u maju 2014. godine privođeni zbog sumnje da su izvršili krivično delo izazivanja panike i nereda. Razlog za privođenje bile su objave na društvenim mrežama, odnosno Fejsbuk profilima gde se, u nedostatku zvaničnih informacija od državnih organa, spekulisalo sa podacima u vezi sa poplavama i stanjem na terenu. Drugi društveni događaj iz 2014. godine, identifikovan kao glavni motiv povreda digitalnih prava i u ostalim kategorijama, jeste prekinuta fudbalska utakmica Srbija - Albanija, a pratili su ga govor mržnje, uvrede i pretnje usmerene prema Albancima. Najbrojnije povrede u toj godini obrađene su u potkategorijama pretećih sadržaja i ugrožavanja sigurnosti te uvreda i neosnovanih optužbi, po 14. Sledi potkategorija pritisaka zbog objavljivanja informacija sa osam zabeleženih incidenata. Takođe, dokumentovana su po dva slučaja iz potkategorija govora mržnje i diskriminacije i objavljivanja neistina i neproverenih informacija sa namerom ugrožavanja reputacije. Jedan slučaj ticao se slobode izražavanja na internetu sa posledicama po radno mesto, kada je jedan radnik dobio otkaz zbog statusa na Fejsbuku. Novinari su bili meta povreda devet puta, što ih čini grupom najteže ugroženom napadima u toku te godine.

2015

U 2015. godini zabeleženo je 64 slučaja povrede digitalnih prava u kategoriji pritisaka zbog izražavanja i aktivnosti na internetu, što predstavlja veliki skok u broju povreda i jednu od najproblematičnijih godina od kada SHARE Fondacija vrši monitoring digitalnih prava u Srbiji. U 27 slučajeva mete su bili novinari, uglavnom iz medija koji su kritički izveštavali o postupcima vlasti. Protiv jednog

2015

onlajn medija tadašnji gradonačelnik Niša podneo je tužbu. Najviše obrađenih slučajeva bilo je iz potkategorija uvreda i neosnovanih optužbi, te pretećih sadržaja i ugrožavanja sigurnosti, po 24. Sledeća po brojnosti u 2015. godini bila je potkategorija pritisaka zbog objavljivanja informacija, sa 15 incidenata. Jedan od slučajeva ove potkategorije pokazao je nerazumevanje sudova za digitalno okruženje. Naime, članovi jednog internet foruma osuđeni su zbog ugrožavanja sigurnosti reditelja na uslovnu kaznu zatvora od godinu dana, uz vreme proveravanja od tri godine; po žalbi, oslobođeni su naredne godine. Zabeleženo je i šest slučajeva objavljivanja neistina i neproverenih informacija sa namerom ugrožavanja reputacije. Takođe, dogodila su se i četiri slučaja povreda slobode izražavanja na internetu i radnom okruženju. U tri od četiri ovakva slučaja, napadači su bili organi vlasti. U jednom od tri slučaja govora mržnje i diskriminacije, privedena je književnica zbog objave tekstova koji podstiču diskriminaciju Roma.

2016

Godine 2016. zabeleženo je 57 slučajeva pritisaka zbog izražavanja i aktivnosti na internetu. Veliki broj slučajeva povezan je sa parlamentarnim izborima te godine. Mada su u izbornom periodu dominirale povrede prava vezane za manipulaciju i propagandu, zabeleženo je i nekoliko slučajeva pritisaka. Mete napada najčešće su bili novinari, 26 puta, ali i javne ličnosti i aktivisti, kao i predstavnici političkih partija. Najbrojnije potkategorije bile su uvrede i neosnovane optužbe, 26 puta, kao i preteći sadržaji i ugrožavanje sigurnosti, 23 puta. Zabeležena su i dva slučaja iz potkategorije narušavanja slobode izražavanja na internetu u radnom okruženju, te su dve osobe dobile otkaze zbog aktivnosti na Fejsbuku. Od četiri zabeležena slučaja govora mržnje i diskriminacije, izdvaja se značajna presuda Apelacionog suda u Beogradu kojom je profesorka iz Novog Sada osuđena na uslovnu kaznu od tri meseca zatvora zbog govora mržnje 2011. godine na Fejsbuku. Ovaj slučaj je jasno ukazao na to da odgovornost za širenje govora mržnje važi i na društvenim mrežama. Zabeleženo je 11 slučajeva pritisaka zbog objavljivanja informacija.

2017

Godine 2017. registrovan je pad u brojnosti slučajeva povrede digitalnih prava iz kategorije pritisaka zbog izražavanja i aktivnosti na internetu; obrađeno je 26 incidenata, što je znatno manje u odnosu na prethodnu godinu, kada ih je bilo 57. Preteći sadržaji i ugrožavanje sigurnosti svakako su najbrojnija potkategorija, sa 15 zabeleženih slučajeva. Česte su bile pretnje novinarima, a pretnje su upućivane i javnim ličnostima, kao i političkim akterima. Osim pretećih sadržaja, zabeleženo je nekoliko slučajeva uvreda i neosnovanih optužbi, objavljivanja neistina i neproverenih informacija sa namerom ugrožavanja reputacije, kao i pritisaka zbog objavljivanja informacija. Upečatljivi primeri pritisaka zbog objavljivanja informacija svakako su privođenje jednog građanina na informativni razgovor, kao i oduzimanje telefona i šifre za Tviter i imejl nalog jednom aktivisti. Zabeležena su i dva slučaja govora mržnje i diskriminacije.

Slučajevi iz ove potkategorije često obuhvataju još neku povredu prava, te tako obrađeni primeri govora mržnje često obuhvataju i preteće sadržaje. U 2017. godini primetni su bili pritisci političke prirode, što može biti u vezi sa predsedničkim izborima koji su održani te godine.

2018

U toku 2018. zabeleženo je 24 slučaja pritisaka zbog izražavanja i aktivnosti na internetu. Kao i prethodnih godina, preteći sadržaji i ugrožavanje sigurnosti činili su potkategoriju najčešćih incidenata, samostalno ili udruženi sa govorom mržnje i diskriminacijom ili uvredama i neosnovanim optužbama. Te godine su zabeležena i dva slučaja pritisaka na slobodu izražavanja na internetu i u radnom okruženju. Treba napomenuti da su mete pritisaka zbog izražavanja i aktivnosti na internetu u 2018. godini najviše bili novinari, u polovini od svih zabeleženih slučajeva. Građani su bili najčešći napadači, u 11 slučajeva.

2019

U 2019. godini zabeležen je značajan porast broja incidenata ove vrste. Do septembra, broj slučajeva iznosi 45 sa jasnim naznakama da će se do kraja godine dalje umnožavati. Najbrojnija potkategorija bili su preteći sadržaji i ugrožavanje sigurnosti, 25 slučajeva. Uvrede i neosnovane optužbe, njih 21, druga je po brojnosti potkategorija povreda digitalnih prava u tekućoj godini. U nekoliko slučajeva, incidenti su obuhvatali obe potkategorije. Tako je u februaru uhapšena osoba koja je pretila političarima, novinarima i javnim ličnostima na društvenim mrežama. Istog meseca je Viši sud u Beogradu doneo presudu kojom je optuženi za pretnje smrću novinarki i njenoj kćerki uslovno osuđen na osam meseci kućnog zatvora.

Sve dok pretnje ne budu povlačile adekvatnu kaznu, odnosno dok se sudska praksa ne ujednači i ne budu pooštrene sankcije, može se očekivati da će klima nekažnjivosti pogodovati umnožavanju pretnji. U potkategoriji objavljivanja neistina i neproverenih informacija sa namerom ugrožavanja reputacije, u 2019. godini mete su bili isključivo novinari, koji su i najčešća meta cele kateogrije u više od polovine registrovanih slučajeva. Novinari su zbog svog rada najčešće izloženi pretnjama, ali im društvena uloga s druge strane omogućava da o takvim incidentima odmah izveste javnost, doprinesu podizanju svesti o uslovima u kojima rade i podstaknu pritisak za pravno procesuiranje počinilaca. Građani koji nemaju neposredan pristup kanalima komunikacije sa širom javnošću, ređe prijavljuju pretnje kojima su izloženi.

SPECIFIČNI SLUČAJEVI

Mada su anonimne pretnje i teške uvrede svakodnevna pojava u onlajn sferi, ni uvrede potpisane imenom i prezimenom nisu retkost. Politička kultura u Srbiji podstiče lične napade, diskvalifikacije, pa čak i otvorene pozive na nasilje, gušeći prostor za uljudnu debatu. Nasilna klima u društvu preliva se i na onlajn okruženje.

„Umesto vibratora, ja bih Zorani Mihajlović ponudio desetinu bradatih, zadriglih i mesec dana nekupanih četnika, koji nisu mnogo probirljivi“, napisao je narodni poslanik SRS Vojislav Šešelj na Tviteru. Takođe je pozivao na silovanje Poverenice za ravnopravnost, psovkama i pogrdnim imenima vređao preminulog novinara Dejana Anastasijevića, a političkim oponentima pretio streljanjem.

Predsednik Narodne seljačke stranke i narodni poslanik Marijan Rističević omalovažavao je novinarku iz Inđije koja je bila na meti kampanje zastrašivanja, dok je predsednik opštine Obrenovac Miroslav Čučković novinarku Istinomera nazvao „voajerom i psihopatom“. Ovi i brojni drugi slični slučajevi ukazuju na osionost nosilaca javnih funkcija prema svima koji ih pozivaju na odgovornost.

Međutim, kada su na zatvorenom delu foruma „Parapsihopatologija“ objavljeni postovi protumačeni kao pretnje, trojica građana osuđena su na uslovne kazne zatvora. Oslobođeni su tek posle odluke Vrhovnog kasacionog suda i tri godine sudskih ujdurmi. Građani su u nizu slučajeva privođeni u vreme tokom poplava 2014. godine zbog „širenja panike“ preko blogova i naloga na društvenim mrežama. Problem je navodno bio u spekulisanju brojem mrtvih i razmerama štete, o čemu danima nije bilo zvaničnih informacija.

Zbog statusa na društvenim mrežama deljeni su i otkazi. To je bio slučaj sa radnicama zbog objavljivanja fotografija štrajka u privatnoj kompaniji „Kajzen“; otpušten je jedan inženjer iz RTB Bor koji je tvitovao o situaciji u tom preduzeću, kao i sindikalni aktivista zaposlen u smederevskom Železari. Ugovor

o radu raskinut je bivšem sudskom pripravniku i aktivisti kada je na Fejsbuku i Tviteru izrazio mišljenje da uručenje uramljenog rešenja o rehabilitaciji kao rođendanskog poklona Aleksandru Karađorđeviću, nije dostojno sudije Višeg suda u Beogradu.

Nad novinarima i medijima se pritisci sprovode kroz tužbe i sudske procese koje pokreću javni funkcioneri. Kao primer, izdvaja se privatna tužba bivšeg gradonačelnika Niša Zorana Perišića protiv novinara portala Južne vesti, jer je smatrao da su mu objavljivanjem intervjua u kome se dovodi u vezu sa proneverom novca iz preduzeća „El Niš“ povređeni čast i ugled. Perišić je tražio pola miliona dinara, ali je postupak izgubio odlukom Apelacionog suda u Beogradu 2018. godine. Međutim, bilo je sudskih odluka koje nisu išle u korist slobode izražavanja na internetu, kao što je presuda po tužbi ministra unutrašnjih poslova Nebojše Stefanovića protiv Vesne Pešić i urednica Peščanika Svetlane Lukić i Svetlane Vuković. Povod za tužbu je bila kolumna Vesne Pešić o rušenju u Savamali, a odlukom Apelacionog suda u Beogradu tužene su obavezane da Stefanoviću isplate 150.000 dinara sa zateznom kamatom, uz troškove parničnog postupka.

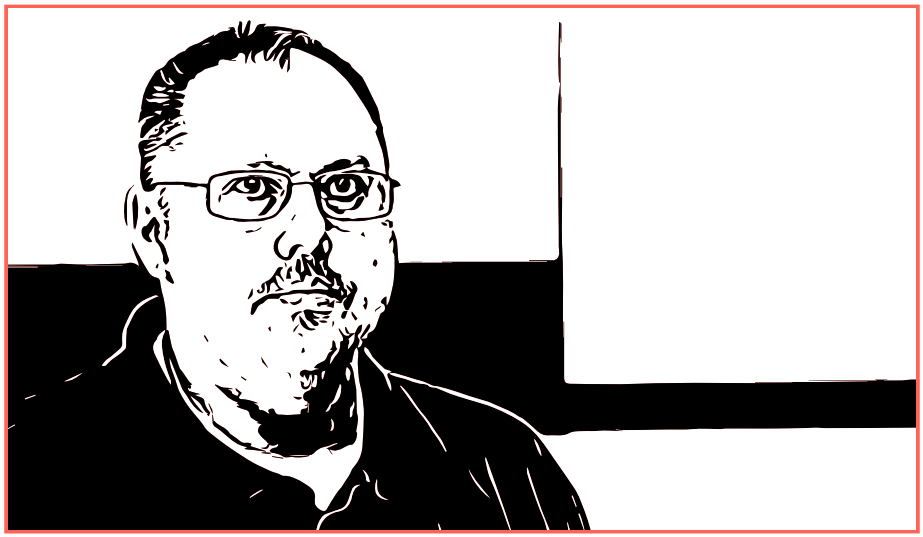
NEDIM SEJDINOVIĆ

- Tadašnji predsednik i članovi Nezavisnog društva novinara Vojvodine (NDNV) dobijali otvorene pretnje na Fejsbuku, potpisane imenom i prezimenom.
- Rukovodstvo NDNV-a dobilo pretnje smrću nakon što su se u pojedinim tabloidima pojavili netačni navodi da su oni organizatori masovnih postizbornih studentskih protesta u Novom Sadu. Pretnje smrću prijavljene MUP-u i Tužilaštvu za visokotehnološki kriminal.
- Nedim Sejdinović, tadašnji predsednik NDNV-a, dobio na desetine uvreda i pretnji nakon što je na svom privatnom Fejsbuk profilu objavio fotografiju žute patke, simbola inicijative Ne davimo Beograd, uz poruku „Srećan Veliki patak“. Osumnjičeni za pretnje je identifikovan i protiv njega je podneta krivična prijava.
- Priveden građanin zbog pretnji koje je na Jutjubu i Fejsbuku uputio tadašnjem predsedniku NDNV i članu izvršnog odbora tog novinarskog udruženja.
- Na Fejsbuk stranici „Srbija Naša zemlja“ upućene pretnje i uvrede tadašnjem predsedniku NDNV Nedimu Sejdinoviću i još jednom novinaru. Pretnje su prijavljene MUP-u, Tužilaštvu i stalnoj radnoj grupi za bezbednost novinara.
- Nedim Sejdinović, tadašnji predsednik NDNV, podneo krivičnu prijavu protiv nepoznate osobe zbog objave i pretećih komentara na Fejsbuk stranici „Srbija naša zemlja“.

PRETNJA DANA!!!

IZABERITE OMILJENOG NOVINARA!

POPUST ZA VOJVODINU!!!



NEDIM SEJDINOVIĆ

NOVINAR, GLAVNI I ODGOVORNI UREDNIK
PORTALA AUTONOMIJA.INFO

Kao novinar, građanski aktivista, ali i bivši „funkcioner“ Nezavisnog društva novinara Vojvodine, veoma često se nalazim na meti napada, pre svega serijskih, kampanjskih pretnji i uvreda koje pristižu preko društvenih mreža. Duboko verujem da su u pitanju organizovani pokušaji zastrašivanja kao odgovor na moj kritički odnos prema vlastima u Srbiji. Kako drugačije objasniti to da sam u poslednjoj seriji napada na fejsbuk stranici „Srbija – naša zemlja“ za manje od 48 sati dobio više od hiljadu pretnji i uvreda, osim da je u pitanju organizovana hajka stranačkih botova. Kampanja je započela objavom moje fotografije na toj stranici, koja je inače poznata po targetiranju „neprijatelja vlasti“, uz tvrdnju da sam „islamski fanatik“ i „vojvođanski separatista“ koji godinama „lustrira Srbe“.

Sličnim kampanjama zastrašivanja bio sam izložen i prethodnih godina, a sve pretnje koje sam dobio prijavljivao sam nadležnim državnim organima. Na žalost, samo u dva slučaja ove krivične prijave su imale nekakav epilog, ali ne pred sudom. Dva puta se tužilaštvo naime nagodilo za okrivljenima, pa je primenjeno tzv. načelo oportuniteta. Dve osobe koje su mi uputile pretnje smrću dobile su „odloženo krivično gonjenje“, koje podrazumeva uplatu određenog novčanog iznosa u humanitarne svrhe ili nekakav društveno koristan rad. Te

„sankcije“ svakako nisu u skladu sa ogromnom količinom nasilničke mržnje kojoj sam godinama izložen i ne smatram da sam dobio odgovarajuću satisfakciju. To je manji problem, a onaj veći glasi: javnosti nije poslana poruka da su takve stvari zabranjene, pa nije ni čudo što se društvene mreže u Srbiji guše od govora mržnje.

Kada sam prvi put bio izložen eksploziji mržnje, bio sam donekle zbunjen. Odakle ona izvire? Pitate se kako ti ljudi ne prepoznaju da to što radite, zapravo radite – bar tako iskreno verujete – u korist svih građana ove zemlje, jer zalažete se za osnovne civilizacijske vrednosti, za demokratizaciju društva, za ljudska prava, medijske slobode... Osećate da tu mržnju nikako niste zaslužili, kao da je u pitanju nekakav nesporazum kojeg je moguće razrešiti. Emotivno imate potrebu da im objasnite da niste onakvi kakvim vas smatraju, ali istovremeno znate da je to uzaludan posao, pa to i ne činite. Pogađa vas činjenica da su vas neki ljudi stavili u neke svoje fioke, koje su snažno zabravili, i da ne postoji šansa da iz njih ikada više izađete. Iako ste anacionalni agnostik, shvatate da to vaše lično opredeljenje ništa ne znači, i da vas ime i prezime određuje više od onoga što mislite i radite. I to je tako poražavajuće za vas.

Niste, kao neki političari i drugi moćnici, zaštićeni i okruženi telohraniteljima, već se vozite gradskim prevozom i susrećete svakodnevno sa „običnim ljudima“. Pogotovo kada su kampanje zastrašivanja u toku, okrećete se oko sebe u autobusu i posmatrate ljude, hvatate njihove poglede. Pokušavate u njima da razaznate da li vas prepoznaju i šta misle o vama. Ponekad u tim pogledima vidite mržnju, ili vam se možda samo to učinilo. Neko vas ipak gleda s neskrivenom mržnjom, a dešavalo se da neko nešto i dobaci. Pogotovo ako vas je prethodno prozivao neki uticajni političar. Istovremeno, neretko vas na ulici zaustavi nepoznata osoba koja vam pruži podršku. Iako se pravite da vam to nije tako važno i samo se ljubazno zahvalite, nastavite put s osmehom na licu, ohrabreni, i učini vam se da to što radite ipak ima nekog smisla.

Ponekad se sami sebi čudite kako hladno, bez ikakvih osećanja, možete da čitate stotine pretnji i uvreda koje su vam upućene. Više biste se uzbudili da su one odaslate nekome drugome, bilo kome, jer zaista znaju biti grozomorne. Potom shvatite da ste, zapravo, nesvesno izgradili nekakvu emotivnu barikadu, koja vas sprečava da se uzbudite, naljutite, uplašite, koja sprečava da vas takve stvari izvedu iz takta. Možda je ta emotivna barijera delom i posledica svesne odluke da treba da ostanete pribrani, jer znate da te kampanje i imaju za cilj da vas psihički razore, da vas demobilišu i demorališu.

Ipak, ta barijera nije od čelika, s vremena na vreme poklekne, i tada se budite noću. Ponekad vas proganjaju neki od likova koji su vam pretili ili su vas, onako zdušno, izvređali. Često i ne kriju svoj identitet – to vidite po njihovim profilima

na društvenim mrežama. Posebno su jezivi slučajevi kada vam neko, recimo, preti da će vas „nabiti na kolac“, a na svom profilu kao noseću drži svoju nasmejanu fotografiju sa malim detetom. Pitate se, da li to dete može da nasluti ko je zapravo taj čovek koji ga drži u naručju?

Ipak, najgore sam se osećao ne onda kada sam bio izložen pretnjama i uvredama nego kada su mi, za vreme uskršnjih praznika 2017. godine, pristizale, putem mesindžera i SMS-a, bezbrojne uskršnje čestitke. Naime, posle jedne moje objave na fejsbuku, koja je imala za cilj da podrži proteste koje je organizovao pokret „Ne davimo Beograd“, dobio sam seriju pretnji i uvreda. One su zaustavljene nakon što sam alarmirao javnost i nakon što su reagovala domaća udruženja i međunarodne organizacije. Umesto pretnji i uvreda odjednom su počele da pristižu čestitke, stotine uskršnjih čestitki od nepoznatih ljudi i sa nepoznatih brojeva telefona. Bio je to organizovani sadistički cinizam. Sticajem okolnosti, tih dana sam bio sam kod kuće, sedeo sam u fotelji, mrak je bio napolju, odnekud laje neki pas, i čuju se komšijski glasovi. A meni telefon luduje od silnih čestitki. Osećao sam se kao da sam uleteo u film Dejvida Linča. Proverio sam da li sam zaključao vrata od kuće.

SOFIJA TODOROVIĆ

- Narodna poslanica Srpske radikalne stranke Vjerica Radeta pretila aktivistkinji Inicijative mladih za ljudska prava (YIHR) Sofiji Todorović i vređala je povodom festivala „Mirdita, dobar dan“, koji organizuje YIHR u cilju predstavljanja kosovske umetničke i kulturne scene u Srbiji.
- Aktivistkinji Sofiji Todorović blokiran nalog na Tviteru, nakon što je upozorila javnost na nacionalističke napade na albanskog pekara u Borči. SHARE Fondacija kontaktirala je predstavnike Tvitera, nakon čega je Sofija uspela da povrati pristup nalogu.
- Nakon što je aktivistkinja Sofija Todorović uživo objavljivala tvitove sa nacionalističkih demonstracija protiv albanskog pekara u Borči, upućene su joj pretnje i govor mržnje.
- Povodom napada na Sofiju reagovao je i Evropski sud za ljudska prava, tražeći od Republike Srbije da dostavi sva dokumenta o slučaju.


MEGAPA
MIRDITA!!!
DOBAR DAN!!!
ПОЛИЦИЈА
ПОЛИЦИЈ

SOFIJA TODOROVIĆ

AKTIVISTKINJA ZA LJUDSKA PRAVA I KOORDINATORKA PROJEKATA ZA BIRN

Kako pripadam generaciji koja je odrastala u periodu u kom društvene mreže preuzimaju primat u sprovođenju interakcije, internet je postao prostor koji je veoma važan za moj rad i društveni angažman generalno. Međutim, to je u kriznim situacijama sa sobom donelo mnoge neželjene posledice. Kada sam krajem aprila ove godine odlučila da se zauzmem za svog komšiju, koji je albanske nacionalnosti i poreklom je sa Kosova, društvene mreže koje sam koristila kako bih svoju poruku podelila sa što širom javnošću, pretvorile su se u bojno polje koje me je učinilo dostupnom velikom broju ljudi koji nisu želeli samo da mi kažu da se potencijalno ne slažu sa mnom.

Tačno se sećam jutra kada odlazim u pekaru ispred koje je najavljen skup, za koji se već po načinu pozivanja nije moglo reći da je mirno iskazivanje demokratskog neslaganja. Iako sam sve već prijavila policiji, nije mi bilo svejedno, ali sam ujedno bila veoma odlučna da ovog čoveka, koji se tereti za činjenicu da je „šiptar“ - jer je to postupkom njegovog brata postalo „nedozvoljeno“ - neću ostaviti samog. To nije bilo nikakvo milosrđe, već jedina zdravorazumska opcija za mene. Sugrađani leve obale ne ostavljaju svoje komšije na milost i nemilost samovoljnih nacionalističkih skupina koje sebi tepaju nazivajući se građanima.

Snimci i fotografije „protesta“ koje sam objavila na Tviteru, a koji je trajao više od četiri sata, svedoče o glasnom skandiranju pesama koje sadrže i pozive na ubistva i mržnju prema određenim grupama, ostavljanju svinjskih glava, traumiranju radnica u pekari, lepljenju plakata po kolima vlasnika i samom objektu. Nakon ovoga sledi niz uvreda i pretnji, a posebno se ističu vređanja zasnovana na činjenici da sam žensko.[1] Policija me je nakon protesta posavetovala da napustim kuću na nekoliko dana, jer je bezbednije. Poslušam, odem kod drugarice na par dana.

Vreme mi prolazi tako što se trudim da ne obraćam pažnju na sve što se dešava na mrežama; znala sam da ovo neće proći tek tako i sad - šta je tu je. Ponavljam sebi da je jedino važno da ostanem pribrana i da se ne nerviram oko atmosfere na internetu. To je ipak onlajn svet. Često se okrećem na putu do kuće, u autobusu 95 mislim da me muškarci gledaju čudno, stalno imam osećaj da me neki muškarac prati; niko me ne prati, valjda. Blokirala sam mami pristup Tviteru, ne želim da moja porodica čita ove stvari. Međutim moja sestra ih čita, čita svaki komentar, zove me telefonom svakoga dana i moli me da prestanem. Na moje pitanje s čim ja da prestanem, zaćuti i spusti mi slušalicu. Razumem je, razume i ona mene, ali briga je ogromna, jer šta ako nekoj od tih dokonih budala padne na pamet da... Nećemo preterivati, da, nećemo. Dve osobe su iz Borče, ne tako zavidnih biografija, dok jedan ima i dosije da se njime pohvali. Uglavnom, samo ne treba preterivati.

Uvredama i „kritikama“, da ne kažem napadima, priključuju se i desničarski portali, razne desničarske ogranizacije kao i političari desnih pogleda na region. Svi žele nešto lepo da mi poruče i da iskažu svoje duboko neslaganje, a to uglavnom rade tako što me nazivaju izdajnicom, plaćenicom, ispostavom britanske službe. Takođe, uglavnom su obmanjivali javnost o visini moje plate, radnom mestu ili poziciji. U ovom periodu, na Jutjubu je osvanuo video u kome sam ja glavna protagonistkinja.[2]

Ubrzo nako objave ovih postova, moj Tviter nalog biva suspendovan, a zatim ubrzo uspešno vraćen; dva dana nakon izveštavanja sa lica mesta ostajem bez naloga na ovoj mreži po drugi put i to na osam dana. Tviter je mreža preko koje sam informisala javnost o dešavanjima u Borči, vrlo svesno odabran, jer sam samo tu mogla da generišem relevantnu i značajnu podršku za čoveka u nevolji.

Prestala sam da brojim zahteve za slanje privatnih poruka, a takve poruke sam u nekom trenutku prestala i da čitam. Kako je javno objavljena slika mog instastorija, a time i moj Instagram nalog, broj zahteva dostiže neslućene razmere.

1 Serbian Nationalists Target BIRN Staffer for Defending Baker, BIRN, May 6, 2019; birn.eu.com

2 Jutjub video „Ko je Sofija?“ bit.ly/2obnhVL

Moj Instagram nalog je uvek bio zaključan, jer sam želela da imam kontrolu nad brojem ljudi koji imaju pristup sadržaju koji delim na toj mreži. Ime na Fejsbuku sam morala da promenim, jer je postalo psihički i fizički neizdrživo da se nosim sa brojem tagova i poruka.

Nisam bila fizički napadnuta; jedna osoba me je izvređala na ulici u blizini pekare, ali u tom momentu nisam bila sama. Podnela sam i nekoliko prijava protiv određenih pojedinaca. Obratila sam se i Evropskom sudu za ljudska prava zbog nereagovanja institucija.[3] Napadi su se pretežno dešavali u onlajn prostoru, ali sam strah osećala oflajn. Taj strah je bio vrlo realan, manifestovao se na čudne načine i bilo je strašno, a posebno jer nije doticalo samo mene, već i ljude oko mene.

Sada, sa ove vremenske distance, znam da sam mnogo više mogla da učinim za sebe i moje internet blagostanje. Za početak, počela sam više da razmišljam o šiframa koje postavljam, a uvidela sam i koliko je internet postao sastavni deo mog života; kada je nešto deo svakodnevice zaboravite na neophodan oprez. Ceo taj prostor je veoma nemilosrdan i kada se nešto desi uglavnom se poseže za argumentom: „Znala si da to sve ide javno onog momenta kad si rešila da sve radiš onlajn“. Mene to iskreno podseća na argument „kratka suknja“, no dobro.

Ovakva vrsta napada u Srbiji tretira se kao javni društveni dijalog i sukob mišljenja. Ne vidim nikakvu promenu u odnosu prema sličnim situacijama, od momenta kada sam ja prolazila kroz to do danas. Više puta sam ponovila da se iznošenje drugačijeg mišljenja ili neslaganje ne smeju poistovetiti sa govorom mržnje, diskriminacijom i pretnjama. Inicijalno, sloboda na internetu postoji, takva je da je stvar vašeg slobodnog izbora da zauzmete bilo kakav stav. Ali, ako imamo osobu koja će tri puta razmisliti pre nego što stane uz Albanca kome su ugrožena osnovna ljudska prava, a da razlog nije to što se neće složiti već ne želi da se objektivno brine za svoju bezbednost, bojim se da smo onda pod slobodom počeli da podrazumevamo stvari koje je ograničavaju. Na internetu nema ničega čega nema i u fizičkom svetu. Nemojmo olako tretirati određena dešavanja samo zbog činjenice da su se desila onlajn. Nakon učestalih i dugogodišnjih napada u onlajn prostoru, životi ljudi bivaju ponekad i zauvek promenjeni, u negativnom smislu, a na kraju za to niko ne bude odgovoran. Važan je prostor koji nam internet nudi, ali važno je i ono što nam nekada uzima. O tome se ne sme ćutati.

Za potrebe pisanja ovog teksta, otvorila sam fajl na svom kompjuteru pod nazivom „Pekara-Borča“ u kome se nalaze sve dokumentovane pretnje, uvrede, laži i kampanje uterivanja straha koje su za metu imale mene ili moju

3 European Court Probes BIRN Serbian Staffer's Online Targeting, BIRN, July 2, 2019; balkaninsight.com

porodicu. Prošla sam kroz sve, još jednom, kako bi ovaj tekst bio „dobar“. Želim vam prijatan dan.

TRENDOVI I ZAKLJUČCI

Na internetu, pretnje mogu da upućuju i ljudi i mašine, ponekad spontano, a ponekad plaćeno. Nove tehnologije omogućavaju da se pritisci na ciljane mete brzo i lako omasove, dok su za svako društvo posebno rizične pretnje onima koji rade u javnom interesu, kao što su novinari i aktivisti za ljudska prava. U autoritarnim režimima na meti organizovane kampanje zastrašivanja i ućutkavanja nalaze se i politički protivnici vlasti. Istraživači posebno upozoravaju na prilike koje vladaju na internetu u Iranu, Turskoj, Alžiru, Kini. Među zemljama u kojima je sloboda izražavanja delimična, ili ugrožena, nalazi se i Srbija. Od štetnih posledica ugrožavanja slobode govora posebno se izdvaja efekat zebnje, vrsta samocenzure kojoj pribegavaju i građani i mediji, ugrožavajući istovremeno i pravo na slobodu izražavanja i pravo javnosti na informisanost.

Izveštaj Reportera bez granica iz 2018. prepoznaje onlajn uznemiravanje sa ciljem zastrašivanja i ućutkavanja kao poseban oblik pritiska na novinare i medijske aktere. Između ostalog, poplava dezinformacija služi da uguši sadržaj koji novinari objavljuju na portalima i društvenim medijima; viralnost interneta pogoduje širenju mržnje, dok mreže plaćenih komentatora i automatizovanih naloga umnožavaju provladine sadržaje; konačno, ciljane kampanje protiv pojedinih novinara koriste društvenu polarizaciju i atmosferu nepoverenja, u kojoj su mete izložene uvredama i pretnjama.

Novinarke su sve češće na meti **sajber proganjanja**, dugotrajnog fokusiranog uznemiravanja koje može uključivati praćenje aktivnosti, krađu identiteta, pretnje, širenje laži, sramoćenje, ucenjivanje i slično. Serijski progonitelj iz Oklahome osuđen je prošle godine na 15 godina zatvora, nakon što je uznemiravao novinarke preko Fejsbuka. Stupao je s njima u kontakt tako što je pravio naloge nepostojećih novinara ili stvarnih javnih ličnosti, dok je javno dostupne podatke o njima koristio da bi stekao poverenje. Na meti progonitelja novinarke se uobičajeno nađu kada svojim radom i istupima skrenu širu pažnju javnosti, dok je povlačenje sa mreža česta reakcija žrtava. Iako mete ove vrste pritiska mogu biti i muškarci i organizacije, mnoge države su sajber proganjanje prepoznale kao poseban oblik nasilja nad ženama.

Neslavni rekord po broju primljenih **pretećih ili uvredljivih poruka** drži italijanska novinarka koja je na službeni mejl primila 7000 pretnji smrću nakon

što je objavljeno njeno istraživanje o povezanosti organizovanog kriminala i turizma na Siciliji. Danas živi pod stalnim policijskim obezbeđenjem, što bitno ometa njen novinarski rad.

Lažno predstavljanje i trolovanje mogu obuhvatati različita sredstva sa ciljem da se meti nanese reputaciona šteta, izazove stres, strah i neizvesnost. Ponekad je za to dovoljno otvoriti lažni nalog ili širiti laži na mrežama, a ponekad podrazumeva izgradnju čitavih portala i sistematsko širenje lažnih vesti. Na tzv. mračnim delovima globalne mreže mogu se kupiti ili iznajmiti lažni nalozi, mreže botova, softveri i drugi alati koji služe kao pojačalo za zlonamerne aktivnosti napadača.

Doksovanje obuhvata pretraživanje istorije internet aktivnosti odabrane mete, prikupljanje i objavljivanje ličnih podataka i privatnih dokumenata, u kontekstu koji i druge ohrabruje da meti upućuju pretnje i uključe se u kampanju zastrašivanja. Kada je novinarka iz Finske izveštavala o policijskoj istrazi napada na jednu četrnaestogodišnju devojčicu, kritikovala je policiju zbog objavljivanja etničkog porekla osumnjičenog, zbog čega je desničarski anti-imigracioni informativni portal pokrenuo kampanju protiv nje. Portal je objavio njen broj telefona i podstakao čitaoce da je kontaktiraju, čime je izložena pretećim i uznemirujućim porukama.

Onlajn uznemiravanje predstavlja pretnju slobodnom toku informacija i demokratskom poretku, te novinarska udruženja širom sveta zahtevaju da se takvi slučajevi tretiraju kao hitni. Tako su u Francuskoj dvojica počinitelja ekspresno kažnjena na šest meseci uslovne kazne zatvora i po 2000 evra zbog onlajn pretnji upućenih jednoj radijskoj novinarki. Takođe, medijske organizacije razvijaju interne protokole u slučajevima onlajn uznemiravanja, kako bi se novinari efikasnije zaštitili. U Srbiji su pretnje novinarima često povezane sa govorom mržnje, podsticanjem netrpeljivosti prema drugim nacijama i političkim progonom. Oznaka da je neko pripadnik druge nacije, da radi za organizaciju iz druge države ili da zastupa političke ideje koje nisu u skladu sa vladajućim politikama u zemlji, najčešća je uvertira kampanje zastrašivanja i progona novinara na internetu.

Govor mržnje na internetu praktično je eksplodirao poslednjih godina širom sveta. Mada u međunarodnim dokumentima ne postoji univerzalna definicija govora mržnje, kao ni jedinstveni pravni instrumenti, osnovne karakteristike ove pojave prepoznatljive su svuda: dehumanizujući i preteći govor koji izražava predrasude protiv određenih društvenih grupa, bilo po osnovu etničkog porekla, verskih i političkih uverenja, roda ili seksualnog opredeljenja. Izlivi mržnje na internetu uobičajeno odražavaju političke odnose iz fizičkog sveta, pa je poslednjih godina registrovana eskalacija onlajn sadržaja usmerenih

protiv migranata, kao i ponovno širenje antisemitizma naročito u evropskim zemljama. Žene su centralni predmet mržnje rastuće onlajn potkulture koja sebe naziva „incel“ (od: involuntary celibates, nedobrovoljni celibati), iz koje su regrutovani počinioci više terorističkih napada. Dehumanizacija LGBT+ ljudi i kampanje mržnje na internetu uobičajeno su na tragu uspona desničarskih partija na vlast, ili kao reakcija na uključivanje ove zajednice u opseg zakonskih prava koja važe za većinu.

Pored nacionalnih pravosuđa, govorom mržnje na internetu bave se i kompanije u čijem su vlasništvu blogovi, forumi i društveni mediji, a koje su u pojedinim zemljama obavezane strogim kaznama da sporne sadržaje uklone u roku od 24 sata po prijavi. Platforme sa milionskim brojem korisnika najčešće se oslanjaju na automatizovano uređivanje sadržaja prema ključnim rečima ili prijavama drugih korisnika, dok ljudi u ulozi moderatora pregledaju sporne prijave. Ogromna količina sadržaja koji se svakodnevno objavljuje, kao i jezičke ili kulturalne barijere, čine posao uređivanja onlajn sfere praktično nemogućim. Zloglasni primer svakako je Fejsbuk u Mijanmaru, gde su sadržaje moderirale samo dve osobe koje govore burmanski jezik u vreme kada je ova popularna mreža masovno korišćena za širenje mržnje i progon tamošnjih muslimana.

MANIPULACIJE I PROPAGANDA

HRONOLOGIJA

2014

Imajući u vidu mogućnost da na internetu svako postane medij, uz minimalne resurse, digitalno okruženje postalo je plodno tle za propagandu, manipulacije i raznovrsno trolovanje. Onlajn mediji, društvene mreže, blogovi i druge platforme pretvoreni su u bojno polje političko-informacionog ratovanja, koje nije zaobišlo ni Srbiju. Godine 2014. zabeleženo je dvanaest slučajeva manipulacije i propagande u digitalnom okruženju. Najviše dokumentovanih slučajeva čine izmene ili uklanjanje sadržaja od javnog značaja, njih sedam. U ulozi počinilaca javljaju se sami onlajn mediji, dok je žrtva javnost, odnosno građani. Među posledicama velikih poplava koje su u maju 2014. pogodile Srbiju, našlo se i nekoliko takvih slučajeva. Tri slučaja ticala su se kreiranja lažnih naloga i plaćenog promovisanja lažnog sadržaja. Zabeležene su i dve manipulacije sadržajem i organizovano prijavljivanje na društvenim mrežama, a obe su se dogodile na Fejsbuku.

2015

Sličan broj slučajeva manipulacije i propagande u digitalnom okruženju dokumentovan je i 2015, svega jedan manje nego prethodne godine. Preovladalo je kreiranje lažnih naloga i plaćeno promovisanje lažnog sadržaja, u pet slučajeva, kao i izmena ili uklanjanje sadržaja od javnog značaja, u jednom slučaju manje. Zabeležene su i dve manipulacije sadržajem i organizovano prijavljivanje na društvenim mrežama. Na društvenim mrežama primećena su tri slučaja lažnih profila. Zabeležena su dva uklanjanja video snimaka na Jutjubu, a primećen je i slučaj izmene konteksta teksta iz stranog medija koji je prenela domaća novinska agencija. Uočeno je manje digitalnih napada na građane kao nespecifičnu populaciju, a više na ciljane pojedince, bilo da su oni novinari, blogeri ili politički akteri.

2016

Godine 2016. naglo je porastao broj zabeleženih slučajeva manipulacije i propagande u digitalnom okruženju. Broj povreda ove kategorije skočio je skoro tri puta, od 11 slučajeva za prethodnu godinu, do 29 u ovoj. Povećanje broja takvih incidenata u direktnoj je vezi sa parlamentarnim izborima koji su održani u aprilu iste godine. Izborna kampanja nije vođena samo u tradicionalnim medijima, već je u znatnoj meri proširena na digitalni prostor. Obrađene su pojave manipulacije sadržajem, kreiranja lažnih naloga i lažnog sadržaja. Glavna meta manipulacija, čak u 15 zabeleženih slučajeva, bili su građani, u ovom slučaju u ulozi glasača, sa ciljem da se dovedu u zabludu kako bi se time naškodilo drugim političkim opcijama. Pored građana, mete

napada bile su uglavnom javne ličnosti koje su podržavale pojedine političke aktere, pretežno iz opozicije. Izvršitelji ovih napada ostali su nepoznati u većini zabeleženih slučajeva. Više od pola povreda digitalnih prava, njih čak šesnaest, odigralo se u kategoriji kreiranja lažnih naloga i plaćenog promovisanja lažnog sadržaja. Osam zabeleženih manipulacija ticalo se izmena ili uklanjanja sadržaja od javnog značaja, zatim četiri manipulacije sadržajem i organizovanog prijavljivanja na društvenim mrežama, a jedna je smeštena u nespecifičnu potkategoriju drugih manipulacija u digitalnom okruženju.

2017

Naredne, 2017. godine broj slučajeva manipulacije i propagande u digitalnom okruženju neznatno se smanjio. Čak 26 incidenata delimično je bilo vezano za predsedničke izbore koji su se održali u aprilu te godine. Napadi su ponovo bili usmereni na građane, čak 14 puta. Napadači su u 16 slučajeva ostali nepoznati, a neretko su se u toj ulozi javljali i sami onlajn mediji (šest puta). U kategoriji kreiranja lažnih naloga, najčešće je kreiranje lažnih naloga na društvenim mrežama, Fejsbuku i Tviteru. Žrtve lažnih naloga bile su i poznate ličnosti, političari, kao u slučaju jednog od kandidata za predsednika Srbije. Izmenu ili uklanjanje sadržaja od javnog značaja najviše su činili onlajn mediji, a sa pojedinih sajtova uklanjani su ili menjani tekstovi od javnog značaja. Od ostalih zabeleženih manipulacija u digitalnom okruženju, u jednoj je meta bila javna ličnost, a u drugoj novinar.

2018

Godine 2018. u monitoring je uvrštena nova potkategorija manipulacija i propagande u digitalnom okruženju, zbog sve češće pojave neobeleženog reklamnog sadržaja u onlajn medijima. Prikriveno oglašavanje proizvoda ili usluga čitaoce dovodi u zabludu, sa potencijalno ozbiljnim posledicama. Nova potkategorija nazvana je plasiranje komercijalnog sadržaja kao informativnog. U prošloj godini zabeleženo je 13 ovakvih slučajeva, u kojima su počinioci onlajn mediji a mete građani, na čije potrebe i aktivnosti želi da se utiče. U 2018. godini, nespecifična, opšta populacija građana je u svim potkategorijama bila najčešća žrtva povreda, što govori da su manipulacije uglavnom usmerene ka široj javnosti, umesto ka ciljanim pojedincima, mada je bilo i takvih slučajeva. Kreiranje lažnih naloga smanjeno je u odnosu na prethodnu godinu, ali je i dalje bilo među najbrojnijim sredstvima manipulacije. Izmene i uklanjanje sadržaja od javnog značaja kontinuirano se dešavaju, te je u 2018. godini zabeleženo pet ovakvih slučajeva. U većini ovih incidenata ciljani su tekstovi koji obrađuju teme osetljive po vladajuću administraciju.

2019

Zaključno sa avgustom 2019. godine, uočeno je 23 slučaja povreda digitalnih prava iz kategorije manipulacija i propagande u digitalnom okruženju. Obrađen je podjednak broj slučajeva kreiranja lažnih naloga i plaćenog promovisanja lažnih sadržaja, izmena i uklanjanja sadržaja od javnog značaja i plasiranja komercijalnog sadržaja kao informativnog, po šest. Jedan od upe-

čatljivijih slučajeva odigrao se u januaru 2019. godine, kada su sa više lažnih imejl adresa državnih organa Srbije upućivane zlonamerne i netačne tvrdnje. Za razliku od prethodnih godina, kada su napadači uglavnom bili nepoznati, u slučaju manipulisanja sadržajem najveći broj povreda ove godine izvršili su onlajn mediji, koji menjaju ili uklanjaju sopstvene vesti bez vidljive oznake naknadne intervencije. Reakcije čitalaca koji upozoravaju na manipulisanje sadržajem od javnog značaja, zasad nemaju uticaja na praksu redakcija pojedinih onlajn medija. Ostale, odnosno neklasifikovane manipulacije u digitalnom okruženju zabeležene su češće nego prethodnih godina, u četiri slučaja.

SPECIFIČNI SLUČAJEVI

Monitoring digitalnih prava i sloboda otkrio je i različite tehnike manipulisanja sadržajem i identitetom aktera na mreži, od kojih su neke vrlo sofisticirane.

Tokom izborne kampanje 2016. godine, 8. marta je objavljen mizogini video o odnosu žena prema svojim muževima. Oznake na snimku kao i kanal na Jutjubu sa kog je emitovan, oponašali su politički pokret Dveri. Postavljen anonimno, video se brzo raširio internetom. Nedugo pošto što je prvi video raskrinkan kao lažan, pojavio se novi, veštije napravljen lažni kanal Dveri, ovog puta sa „kloniranim" video klipovima nalik onima sa pravog kanala Dveri, s jasnim ciljem da dovede građane u zabludu. Drugi vid onlajn manipulacija tokom te izborne kampanje bilo je sponzorisanje političkih objava sa nezvanične Fejsbuk stranice Crvene zvezde, u kojima je davana podrška listi Vladana Glišića i Milana Parovića.

Onlajn manipulacije mogu imati naročito ozbiljne implikacije kada je reč o sadržajima od javnog interesa. Kritična situacija u kojoj su pravovremene informacije od presudnog značaja svakako je bilo vanredno stanje za vreme poplava u maju 2014. godine. Apel tadašnjeg gradonačelnika Beograda Siniše Malog stanovnicima Obrenovca da ne napuštaju svoje domove najpre je objavljen na zvaničnom sajtu Grada Beograda i prosleđen novinskim agencijama, a zatim je bez objašnjenja uklonjen sa sajta.

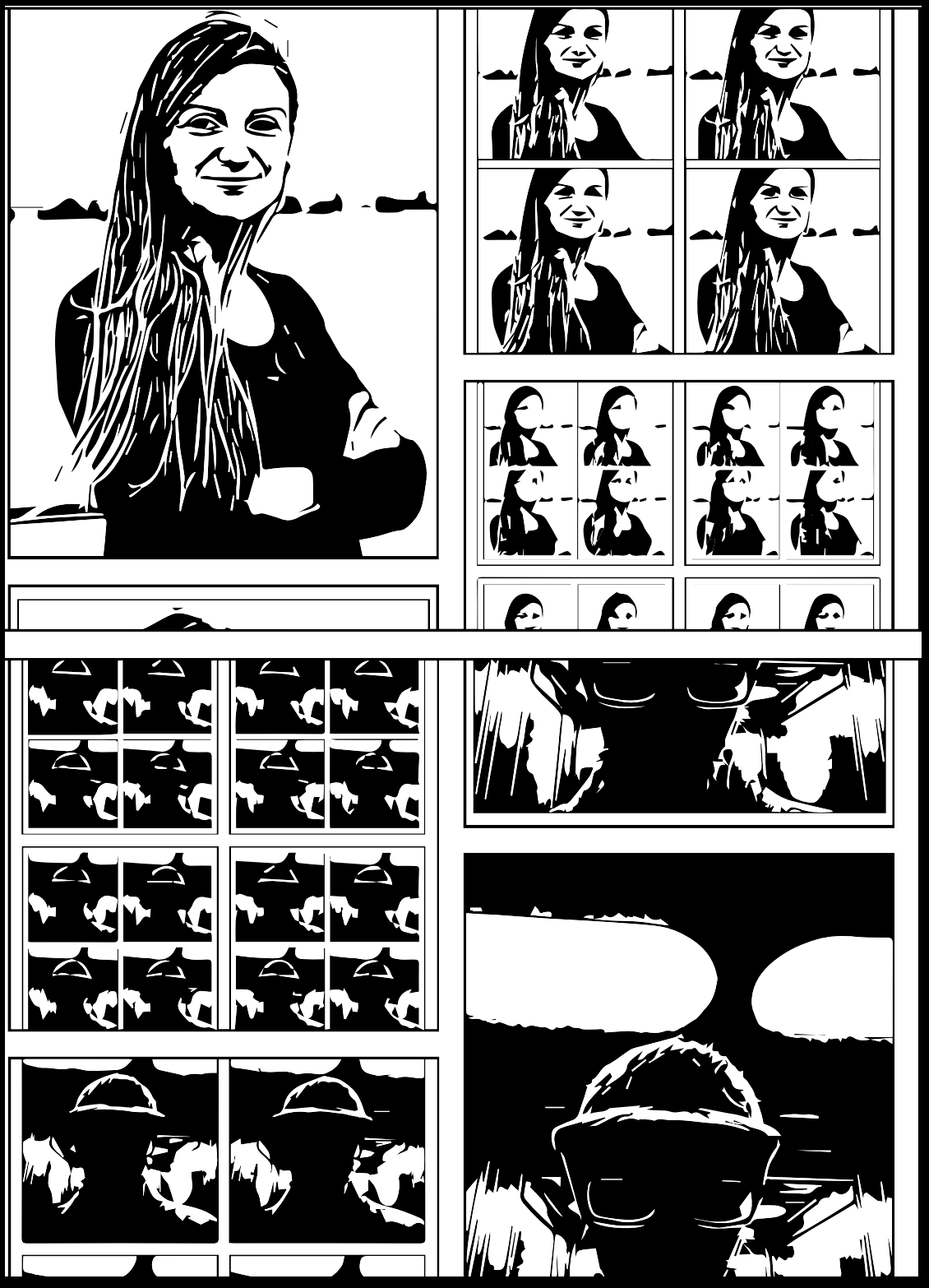
Mnoge platforme za deljenje sadržaja na internetu imaju različite mehanizme za identifikaciju spornog sadržaja ili naloga. Jedan od njih čine prijave drugih korisnika, preko kojih se moderatorima skreće pažnja na kršenje internih pravila korišćenja platforme ili zakona, od trolovanja i vređanja do kršenja autorskih prava i pedofilije. Istovremeno, korisničke prijave su najčešće sredstvo zloupotrebe radi isključivanja društveno ili politički nepovoljnih sadržaja. Umreženi uređaji po komandi mogu slati mnoštvo prijava „spornog" sadržaja, a slično će se po komandi ponašati i ljudi angažovani da pojačavaju ili utišavaju sadržaje, u zavisnosti od interesa za koje rade.

Tako je registrovano blokiranje Fejsbuk naloga blogeru Milanu Kamponeskom, poznatog kao Amitz Dulniker. Nalog je blokiran nakon što je objavio fotografiju kojom kritikuje zločine Ratka Mladića, krajem novembra 2017. kada je Haški tribunal izrekao Mladiću prvostepenu presudu za zločine počinjene u ratovima na prostoru bivše Jugoslavije.

Zbog brojnih prijava teksta „S kim ratuju moji odbornici“ Fejsbuk nalog bio je blokiran i Ljubiši Preletačeviću Belom, odnosno Luki Maksimoviću koji je u to vreme bio odbornik u beogradskoj opštini Mladenovac, a kasnije kandidat za predsednika Srbije. Preletačević je za lokalni portal pisao o mogućoj neispravnosti vode za piće u Mladenovcu i odbornicima opštinske vlasti.

DRAGANA PEĆO

- NN osoba ili osobe poslali veliki broj zahteva za informacije od javnog značaja u ime Dragane Pećo, tadašnje novinarke Centra za istraživačko novinarstvo Srbije (CINS) sa mejl adrese koja ne pripada njoj.
- Novinarki KRIK-a Dragani Pećo krajem juna 2016. upućene preteće uvrede na Tviteru, uz poruku da novinare portala krik.rs „treba postrojiti i streljati kao strane agente u Srbiji“.



DRAGANA PEĆO

ISTRAŽIVAČKA NOVINARKA, KRIK

Nisam bila svesna svih mogućih opasnosti, sve dok tog januarskog jutra 2015. nisam dobila poziv iz jedne institucije. Nisam znala kako neko može da mi „ukrade“ i zloupotrebi identitet, pa ni kojim sve napadima mogu da budem izložena - a da je pritom potpuno bezuspešna institucionalna borba za moju zaštitu i kažnjavanje krivaca, koja bi trebalo da bude primer drugima kako da postupaju u takvim situacijama, pogotovo kada su u pitanju nezavisni istraživački novinari.

Mada u toj borbi nema rezultata, smatram da je jako važno da se svi takvi slučajevi prijave, da negde budu pribeleženi, da se ne zaborave. Jednom se možda i reše.

Dakle, tog dana me je pozvala osoba iz Javnog preduzeća Gradske pijace, zadužena za zahteve za pristup informacijama od javnog značaja. U prvi mah nisam znala na koji zahtev misli, što zaista nije čudno s obzirom na broj zahteva koje šaljem. Ispostavilo se, međutim, da se ovom javnom preduzeću nikad nisam obraćala. U to vreme sam radila u Centru za istraživačko novinarstvo Srbije (CINS) i čim sam stigla u kancelariju proverila sam mejl i sve poslate zahteve. Mislila sam da je po sredi neka zabuna, dok nisam primila još jedan poziv od osobe takođe zadužene za takve zahteve, samo iz druge institucije. Shvatila sam da im se neko obraćao u moje ime i uplašila se. Na neki način mi je

„ukraden“ identitet kredibilne istraživačke novinarke, što znači da neko može bilo kome da se obraća i traži bilo šta, a da ja za to ne moram nikad ni saznati.

Na kraju sam utvrdila da je najmanje deset institucija dobilo identičan zahtev sa adrese koju ja nisam napravila, draganacins@gmail.com, ali sa mojim potpisom. Podnela sam krivičnu prijavu, dala izjavu u Službi za borbu protiv organizovanog kriminala (SBPOK), a policiji sam prenela i svoje sumnje o tome ko bi mogao da stoji iza krađe identiteta. U tom periodu sam se najčešće obraćala kancelariji tadašnjeg predsednika Tomislava Nikolića, čija se savetnica za medije Stanislava Pak u više navrata žalila na negativne tekstove Blica i Kurira tokom 2013. i 2014. godine. Zahtev koji je neko slao u moje ime upravo se odnosio na finansiranje ovih medija u tom periodu iz budžeta javnih preduzeća i institucija. Takođe, dokument sa zahtevom bio je sačuvan pod imenom „simon“ što sam povezala sa osobom koja je u predsednikovoj službi bila zaposlena kao veb administrator.

Nisam imala dokaze za svoju tvrdnju, niti je bilo prilike da se ove sumnje ispitaju pred sudom jer slučaj nikada nije rešen; nije mi poznato ni da li je istraga uopšte ikad odmakla dalje od mojih izjava u policiji. Ostala mi je sumnja da je u zloupotrebu umešan neko iz kancelarije predsednika Republike i duboka zebnja koju sam tada osetila da je tako nešto moguće u najvišim državnim institucijama.

Sličan incident desio se novembra 2017, u vreme kada smo već osnovali KRIK. Neko je napravio lažnu adresu dragana.peco.krik@gmail.com i poslao pitanja Jeleni Kovačević, tadašnjoj predstavnici za medije premijerke Ane Brnabić. Pitanja su se odnosila na poslovanje Komercijalne banke i njenu privatizaciju.

Iz načina na koji su pitanja bila formulisana bilo je očigledno da to nije moj stil obraćanja, ali nisam mogla očekivati od drugih da to znaju. Onaj ko ih je poslao tražio je da se odgovori pošalju na pravi redakcijski mejl office@krik.rs što je i učinjeno, te sam tako saznala za ovaj slučaj. Pretpostavljam da je u pitanju bio neko povezan sa Komercijalnom bankom ko je želeo da dobije odgovore na neka pitanja, ali i da meni i mojoj redakciji skrene pažnju na tu temu.

Ovog puta nisam bila iznenađena, ali sam ponovo osetila strah. Još jednom sam se našla u situaciji da se neko krije iza mog imena, što se može neprestano ponavljati dok sam ja potpuno nemoćna da to sprečim. Štaviše, pošto nadležne institucije ne rešavaju ovakve slučajeve, krivci prolaze nekažnjeno što dodatno ohrabruje one koji su spremni na tako nešto.

Među svim neželjenim stvarima u digitalnom svetu, za mene su ipak najstrašnije pretnje preko društvenih mreža. Mnogo je neprijatnih reči koje sva-

kodnevno dobijamo i ja i cela moja redakcija. Navešću samo neke od novijih, koje su upućene meni: ***pazi da tebe neko ne otprati do smetlišta jer drugo ništa ni ne zaslužuješ; marš iz Srbije; plaćenice, uskoro će običan narod početi da vas istražuje, slika, proganja, maltretira psihički...*** ili redakciji: ***Ko ste vi da tražite podatke o radnom stažu za predsednika države i vlade, pa jebo vam pas majku izdajničku više; kada budete došli da tražite te podatke, doći ću i ja tamo da vam se najebem majke;*** uz poruke da nas treba sve postrojiti i streljati i da „nećemo još dugo".

Teško je savladati strah da se pretnje ne pretvore u napade koji nisu ograničeni samo na digitalno okruženje. Učim da živim sa oprezom, da svakodnevno obraćam pažnju na to kuda se krećem, ko mi ide u susret ili kojim ću putem ići. Nažalost, obeshrabruje me činjenica da smo ja i druge kolege novinari usamljeni u ovoj borbi. Većina napada nikada nije rešena, dok nama ostaje samo naša novinarska solidarnost i javnost kojoj neprestano ukazujemo na ove probleme. Nemamo pomoć institucija, ali imamo podršku javnosti koja je tu da nas zaštiti.

Sve pretnje upućene meni i redakciji KRIK-a tokom 2016. prijavili smo policiji. Čak smo se služili veštinama novinarskog istraživanja, da saznamo što više o onima koji nam šalju pretnje kako bismo i te podatke predali policiji. U istrazi do danas nije bilo nikakvog pomaka i, nažalost, ne verujem da će ga biti. Ipak, ne treba se povlačiti, treba podnositi prijave i ohrabrivati ljude koji se mete napada da ih prijavljuju. Lično se nadam da će jednog dana institucije koje su za to nadležne raditi svoj posao kako treba, kazniti sve one koji prete novinarima i time poslati jasnu poruku da se takve stvari neće tolerisati.

Sredinom 2017. obijen je stan u kom stanujem i to je incident koji je najviše uticao na mene i moj rad. Ništa nije ukradeno, ali su sve moje stvari bile ispreturane, sva garderoba skinuta sa polica, smeće iz kante prevrnuto, nakit iz kutijica prosut. Stvari koje pripadaju mom vereniku nisu dirane, što je u meni izazvalo sumnju. Kada me je verenik pozvao da mi kaže šta je zatekao u stanu, uplašila sam se ali i osetila izvesno olakšanje. Nedeljama pre toga u meni je rastao nemir, a da nisam mogla da utvrdim konkretan razlog. Osećala sam sve veću tenziju od koje nisam znala kako da pobegnem; dan pre obijanja stana sam otputovala baš zato što nisam bila u stanju da na miru sedim u kancelariji i radim, što sam i rekla svom uredniku Stevanu Dojčinoviću. Pretpostavljam da je stan obijen u ranim jutarnjim časovima, kada su susedna dva stana bila prazna. Spolja je delovalo da je sve u redu, brava je bila razvaljena a onda vraćena na mesto da ne bi izazvala sumnju.

Povodom tog slučaja oglasio se i ministar policije koji je rekao kako će učiniti sve da nađu ko je to uradio, ali mene nije uverio. Tih dana je MUP objavio saopštenje u kojem je pokušao da relativizuje moj slučaj, navodeći da se u to

vreme u Beogradu obije po pet stanova dnevno. Mediji su to prenosili, a jedan od najčitanijih informativnih portala objavio je tekst o tome šta treba raditi ako putujete, kako treba javiti komšijama, šta učiniti kako vam ne bi obili stan, zašto će baš vaš stan biti obijen. Tekst je ilustrovan fotografijom pogleda niz ulicu u kojoj se nalazi moj obijeni stan.

Sve su to za mene bile jasne poruke sa ciljem da me zastraše. Objavljivala sam sve više priča koje se najmoćnijim ljudima u državi ne dopadaju, pa sam i obijanje stana doživela kao vrstu zastrašivanja. Ta poruka nije bila upućena samo meni, već i mojim kolegama koji istražuju korupciju. Svima nama to treba da služi kao upozorenje šta će da nam se desi ako se usudimo da se bavimo onim što moćni ljudi na vlasti žele da sakriju.

Nisam dozvolila da me svi ovi incidenti obeshrabre, da me zaplaše, naprotiv. Trudila sam se svaki put da nađem u tome snagu, da upijem sve pozitivne reči, pohvale i poruke podrške koje sam dobijala. Na čudan način, kao što mi je neko iz bliskog okruženja ukazao, napadi su imali i jedan pozitivan ishod – mnogi ljudi, ako do tada nisu, saznali su za moj novinarski rad. Mogli su da pretpostave da dobro radim svoj posao čim sam postala meta prorežimskih tabloida, pretnji i pokušaja stranačkih botova da me diskredituju, a da se u toj kampanji zastrašivanja nije prezalo ni od obijanja stana.

TRENDOVI I ZAKLJUČCI

Dezinformacija je netačna informacija koja se smišlja i deli s namerom da obmanjuje i time nanese štetu - pojedincima, društvenim grupama, organizacijama ili državama; pogrešna informacija je netačna, ali nije nastala iz zle namere; maliciozna informacija (malinformation) je tačna, ali se koristi s namerom da nanese štetu.

Propaganda nije nova pojava, ali je uz pomoć novih tehnologija naprosto okupirala javnu sferu. U globalnim i lokalnim informacionim ratovima, informacije postaju oružje u vreme izbornih kampanja, na konfliktnim područjima, u korumpiranim državama ili među rivalskim kompanijama. Veštačka inteligencija pokazala se kao izuzetno efikasno bojno sredstvo, dok su svest i obaveštenost korisnika praktično jedina solidna zaštita.

Za uspešnu propagandu i manipulacije potrebni su dobri alati i još bolja motivacija. U onlajn okruženju laži se najlakše šire društvenim mrežama i otvorenim portalima za deljenje sadržaja, kritika se cenzuriše a kritičari napadaju. Armije se regrutuju među ljudima i mašinama, novcem ili drugim podsticajima, bilo da se koriste za pozitivno ocenjivanje robe i usluga, političku promociju ili raznovrsna krivična dela.

Poslednjih godina, pretvaranje informacija u oružje (weaponisation of information) postalo je ozbiljan biznis, a njime se podjednako usrdno bave države, političke organizacije i kompanije. Veliki igrači povlače visoke uloge, a za ljudska prava, slobodu govora i informisanja retko ima mesta na njihovim agendama. Do građana povremeno stignu priče o džinovskim mrežama uređaja, ili botova, farmama trolova, crnom tržištu naloga na Fejsbuku i Tviteru, međudržavnim incidentima ili unutrašnjim sukobima izazvanim lažnim vestima. Izbori u Americi, Francuskoj, Nemačkoj, referendum u Britaniji, okupacija Krima, nemiri u Kataloniji, sukob Indije i Pakistana, protesti u Hong Kongu... izveštaji o događajima u svetu sada već po pravilu sadrže i priče o uzajamnom uticaju fizičkog i onlajn sveta, sa prizvukom teorije zavere. Tehnički nezamislivo kompleksne infrastrukture, internet je zakomplikovao i odnose u fizičkom svetu. U svakodnevnoj poplavi informacija, teško je definisati problem, objasniti njegove posledice i, što je najvažnije, utvrditi metode efikasne zaštite.

Razvoj veštačke inteligijencije dodatno je podigao lestvicu, dok se pred građane postavlja sve veći izazov: potrebno je da savladaju tehnička znanja o mašinama i programima, da bi znali za šta se sve mogu upotrebiti i kako da se zaštite od rizika, kako da provere poreklo usluga koje koriste na internetu ili da potvrde informaciju koju su dobili. U toku su različiti pokušaji nacionalnih jurisdikcija da regulišu onlajn sferu, dok se medijske i građanske organizacije hvataju u koštac s lažnim vestima. Ishod borbe je neizvestan.

OSTALE POVREDE

HRONOLOGIJA

Pozivanje posrednika na odgovornost

U pravnim i aktivističkim krugovima širom sveta, odgovornost posrednika predstavlja značajnu tačku debate o pravima i slobodama na internetu. Stoga se pritisak na posrednika zbog sadržaja korisnika našao i među kategorijama povreda koje prati SHARE Fondacija, iako do danas nije zabeležen nijedan takav slučaj. Internet posrednici ili, kako ih naš zakonodavac naziva, pružaoci usluga informacionog društva, mogu biti hosting provajderi, vlasnici društvenih medija, foruma i sličnih platformi za deljenje sadržaja. Pravo posrednika na oslobođenje od odgovornosti za sadržaj korisnika može imati ograničenja, ali je njih potrebno precizno utvrditi zakonom. Princip oslobođenja od odgovornosti za sadržaj trećih strana, odnosno korisnika onlajn platformi, primenjuje se i na komentare čitalaca na sajtovima medija, mada je praksa Evropskog suda za ljudska prava u toj materiji raznovrsna i ne daje definitivne odgovore: primer su slučajevi Delfi protiv Estonije, MTE i Index.hu protiv Mađarske i Pil protiv Švedske. Pritisci na pružaoce usluga potencijalno mogu ozbiljno ugroziti slobodu izražavanja građana. Iseljavanje sadržaja u zemlje u kojima se poštuje neutralnost posrednika nije rešenje, naprotiv; verujemo da prava i slobode treba da uživamo u državi čiji smo građani, i u digitalnom i u fizičkom okruženju.

Blokiranje i filtriranje sadržaja

Povrede iz ove grupe na godišnjem nivou su najređe, ali su značajne za bolje razumevanje uticaja onlajn platformi na slobodu izražavanja. Ukupno je od maja 2014. do septembra 2019. godine bilo 19 povreda ove vrste. Zabeležena su četiri slučaja iz potkategorije blokiranje/filtriranje na nivou mreže i 15 slučajeva iz potkategorije algoritamskog blokiranja ili suspenzije sadržaja. Blokiranje sadržaja uglavnom vrše privatne kompanije, u čak 11 od svih zabeleženih slučajeva. Često je reč o velikim kompanijama, vlasnicima društvenih medija kao što su Fejsbuk, Tviter i Jutjub. Najviše povreda digitalnih prava u kategoriji blokiranja i flitriranja sadržaja zabeleženo je tokom 2017. godine, čak devet od ukupno 19. Naredne godine je registrovano četiri slučaja algoritamskog blokiranja ili suspenzije sadržaja. Važno je napomenuti da su i u kategoriji blokiranja i flitriranja sadržaja mete napada uglavnom bili građani, čak 10

puta. Do septembra 2019. godine zabeležen je jedan slučaj povrede digitalnih prava iz ove kategorije, a ticao se blokiranja Tviter naloga jedne aktivistkinje. U ovoj kategoriji uočeno je nekoliko slučajeva u kojima je razlog blokiranja bilo navodno kršenje autorskih prava privatnih kompanija. Primećeno je učestalo blokiranje sadržaja koje se ticalo osetljivih društveno-političkih tema.

Ostalo

Kategorija povrede digitalnih prava pod nazivom „Ostalo“ rezervisana je za incidente koji ne pripadaju nijednoj od povreda definisanih za monitoring, ali koje je važno pratiti zbog budućeg razvoja metodologije. Do sada su u ovoj kategoriji zabeležena dva slučaja, oba 2018. godine, a ticala su se polnog uznemiravanja na Fejsbuku. Osumnjičeni u tim slučajevima su privedeni. Pretpostavka istraživača je da se ovakvi slučajevi često dešavaju, samo nisu uvek prijavljeni i ne dođu do šire javnosti. Do zaključenja ove publikacije u 2019. godini nije zabeležen nijedan slučaj „ostalih“ povreda.

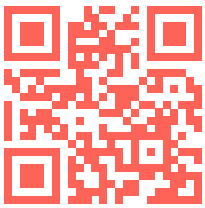
SPECIFIČNI SLUČAJEVI

4. februar 2014, saopštenje SHARE Fondacije povodom afere „Feketić“ i blokiranja video-parodije spašavanja građana iz snežne oluje (odlomak):

„Kako bi utvrdila odgovornost za pokušaje cenzure i ograničavanje slobode razmene sadržaja na internetu koji se desio tokom prethodnog vikenda, SHARE Fondacija podnosi krivičnu prijavu protiv odgovornih lica u kompaniji ‘Matricon’ d.o.o, ovlašćenog predstavnika za teritoriju Srbije bugarske kompanije registrovane u Austriji ‘KVZ Music’, po čijoj su prijavi uklanjani sadržaji sa internet platformi. Takođe, SHARE Fondacija podnosi i Zahtev za informacije od javnog značaja RTS-u kako bi utvrdio eventualnu odgovornost javnog servisa u ovom slučaju.

SHARE Fondacija se na ove poteze odlučila jer smatramo da je ovo bitka za internet slobodu i internet kulturu. Zamislite internet bez miliona satiričnih ilustracija ili remiksovanih video-snimaka. Ovakvi sadržaji predstavljaju samu srž internet kulture i naša je dužnost da stvorimo pravni okvir koji će omogućiti da slobodno izražavamo našu kreativnost, kritički sagledavamo stvarnost i sačuvamo slobodu izražavanja. Želimo da ukažemo na slobodu korišćenja dela zaštićenih autorskim pravima u svrhe parodije i satire kao legitimnog načina izražavanja mišljenja."

Iako je šaljivi video vrlo brzo ponovo bio dostupan na Jutjubu, afera „Feketić" je na neki način postala paradigma pokušaja da se internet okruženje oblikuje i kontroliše na sličan način kao tradicionalni mediji. Međutim, u ovakvim slučajevima često dolazi do suprotnog efekta jer internet drugačije reaguje na cenzuru - potražnja za informacijom postaje veća i o sadržaju se zapravo više govori.



Više od pet godina kasnije, algoritamske „crne kutije" onlajn platformi su i dalje velika nepoznanica. Na leto 2016. blokiran je zvanični Jutjub kanal Zaštitnika građana na kome su objavljivana televizijska gostovanja tadašnjeg Ombudsmana Saše Jankovića, navodno zbog prijava povodom uvredljivog i nasilnog sadržaja. Nakon žalbe koja je odbijena, nalog je pod čudnim okolnostima ipak odblokiran. Takođe, televizijski sadržaj prolazi kroz daleko stroži kontrolni filter u pogledu zakonskih normi, te zapravo nije postojala mogućnost da inserti na kanalu Zaštitnika građana zaista budu uvredljive ili nasilne prirode.

Vredi spomenuti i pokušaje uvođenja filtriranja internet sadržaja u Srbiji na nivou mreže. Provajderi imaju mogućnost da putem posebnih uređaja i softvera blokiraju pristup određenim sajtovima, prema URL adresi sajta ili IP adresi. Tako je Uprava za igre na sreću u martu 2014. godine poslala dopis internet provajderima da izvrše hitnu blokadu pristupa internet stranicama stranih priređivača igara na sreću koji nemaju odobrenje Uprave i upozorila da ukoliko ne blokiraju tražene internet stranice mogu snositi pravne sankcije.

Pored toga, predlog izmena i dopuna Zakona o igrama na sreću, koji je po hitnom postupku krajem 2014. upućen u Skupštinu, sadržao je i odredbu prema kojoj bi svi internet provajderi u Srbiji morali da blokiraju pristup stranim sajtovima za igre na sreću koji nemaju odobrenje ili saglasnost Uprave za igre na sreću. Predlog zakona nije usvojen nakon što je SHARE Fondacija uzbunila javnost i upozorila na opasnosti po pravo da se informacije primaju i šalju posredstvom interneta.

TRENDOVI I ZAKLJUČCI

Očekuje se da će odgovornost posrednika, problemi sa zaštitom autorskih prava na internetu, zatim blokiranje i filtriranje sadržaja, te komercijalni aspekti uživanja digitalnih sloboda, umnogome diktirati buduće regulatorne incijative i diskusije aktivista i pravnika.

Zakonski okvir za onlajn usluge na tržištu EU postavljen je Direktivom o elektronskoj trgovini, čija je svrha uklanjanje prepreka za prekogranične onlajn usluge u Evropskoj uniji. S druge strane, netransparentno uklanjanje sadržaja ili njegova moderacija, posledica su nedostatka jasnih pravila za uklanjanje sadržaja po obaveštenju. Nemački Zakon o kontrolisanju sadržaja na internetu (Netzwerkdurchsetzungsgesetz, skraćeno NetzDG) koji je stupio na snagu 2018. godine, pokušaj je da se **društvene mreže** učine odgovornim za borbu protiv govora mržnje. Iako nije uveo nove kategorije nezakonitog onlajn sadržaja, već samo okupio već postojeće odredbe sadržane u Krivičnom zakonu, ovaj propis je pokrenuo brojne debate o uticaju na slobodu izražavanja i potencijalni efekat zebnje. Od društvenih mreža se, naime, traži da osiguraju mehanizme kojima bi korisnici podnosili žalbe u vezi sa nezakonitim sadržajem, a zatim bi trebalo da platforme ispitaju da li je sadržaj zaista nezakonit i da ga, ukoliko je tako, uklone u roku od 24 sata. Ako to ne učine, novčane kazne mogu dostići i 50 miliona evra. Pored toga, ako jedna platforma primi 100 žalbi godišnje, tada se od nje očekuje da objavljuje polugodišnje izveštaje o moderaciji sadržaja. U Srbiji, novi domaći Zakon o elektronskoj trgovini u članu 16, stav 3 navodi: „pružalac usluga informacionog društva koji prenosi elektronske poruke koje mu je predao korisnik, dužan je da tokom pružanja usluge informacionog društva i minimum 30 dana nakon prestanka pružanja usluge čuva podatke o korisniku usluge informacionog društva, a naročito podatke o IP adresi sa koje korisnik pristupa uslugama informacionog društva tog pružaoca."

Onlajn filteri:

- TCP/IP header filtering - pristup se onemogućava ako se pokaže da je destinacija na „crnoj listi"
- TCP/IP filtriranje sadržaja - ispituju se šabloni ili ključne reči koje su zabranjene, odakle dolaze i kome su upućene;
- Hyper Text Transfer Protocol (HTTP) Proxy Filtering - ako korisnici moraju da koriste proksije za pristup internetu, čitav sadržaj koji kroz

njih prolazi može da se prati;
- Hybrid TCP/IP i HTTP proksi filtriranje - obuhvata zabranjene IP adrese, preusmeravanje i filtriranje sadržaja;
- Uklanjanje celog servera.

Posle burne debate, Evropski parlament je usvojio izmene nacrta Direktive o autorskim pravima, a kao problematični ocenjeni su članovi 15 i 17 kojima se uvodi „porez na linkove“ i filtriranje internet sadržaja. Neke države članice su se otvoreno suprotstavljale takvim rešenjima, dok se u maju 2019. Poljska obratila evropskom Sudu pravde u vezi sa članom 17 o autorskim pravima na jedinstvenom digitalnom tržištu. Poljska je od Suda zatražila poništenje članova 17(4)(b) i 17(4)(c), a ukoliko Sud odluči da to nije moguće bez izmene čitavog člana 17, Poljska će insistirati da Sud poništi ceo član. U Srbiji je predlog izmena Zakona o autorskim pravima usvojen bez sprovedene javne rasprave i uvažavanja komentara stručne javnosti. Prvobitni tekst Nacrta koji je bio na javnoj raspravi 2013. godine imao je 44 člana, dok sadašnja verzija ima 72. Izveštaj o sprovedenoj javnoj raspravi o prvom tekstu nacrta, objavljen u julu 2014. godine, nije sadržao plan da se piše potpuno novi tekst zakona.

Filtriranje i blokiranje na internetu može imati političke namere, kada se ciljaju sajtovi i sadržaji neistomišljenika ili onih koji iznose činjenice nepovoljne po političke aktere; motivi mogu biti društveni, poput suzbijanja kockanja, trgovine drogom, i slično; konačno, ove metode se sprovode u kontekstu bezbednosti, kada je meta sadržaj vezan za oružane konflikte i vojna pitanja. U ulozi onih koji nalažu ili sprovode filtriranje i blokiranje mogu se naći vlasti, pružaoci internet usluga, institucije, ali i pojedinci - kućni softver za filtriranje često je rešenje za kontrolu sadržaja dostupnih deci. Na nivou državne administracije, instraživači su registrovali blokiranje i filtriranje onlajn sadržaja u Severnoj Koreji, Kini, Saudijskoj Arabiji, Iranu, Etiopiji, Belorusiji, Rusiji, Turskoj. Jedan od najznačajnijih slučajeva blokiranja sadržaja našao se pred Evropskim sudom za ljudska prava zbog povrede člana 10 Evropske konvencije o ljudskim pravima: Ahmet Jildirim protiv Turske. Naime, vlasnik i korisnik veb stranice izrađene na Guglovoj platformi, objavljivao je svoje akademske radove i lične stavove o različitim temama. U odvojenom slučaju, turske vlasti su u skladu sa svojim zakonom odlučile da blokiraju pristup jednom blogu na istoj platformi zbog navodnog vređanja osnivača republike, Kemala Ataturka. Usled tehničkih karakteristika, nije postojala mogućnost da se blokira samo jedan blog, pa je blokiran pristup čitavoj Guglovoj platformi. Jildirim zbog toga nije mogao da pristupi svojoj veb stranici čime mu je, mada nije prekršio turske zakone, uskraćeno pravo na slobodnu razmenu informacija. Sud je odlučio u njegovu korist.

2019