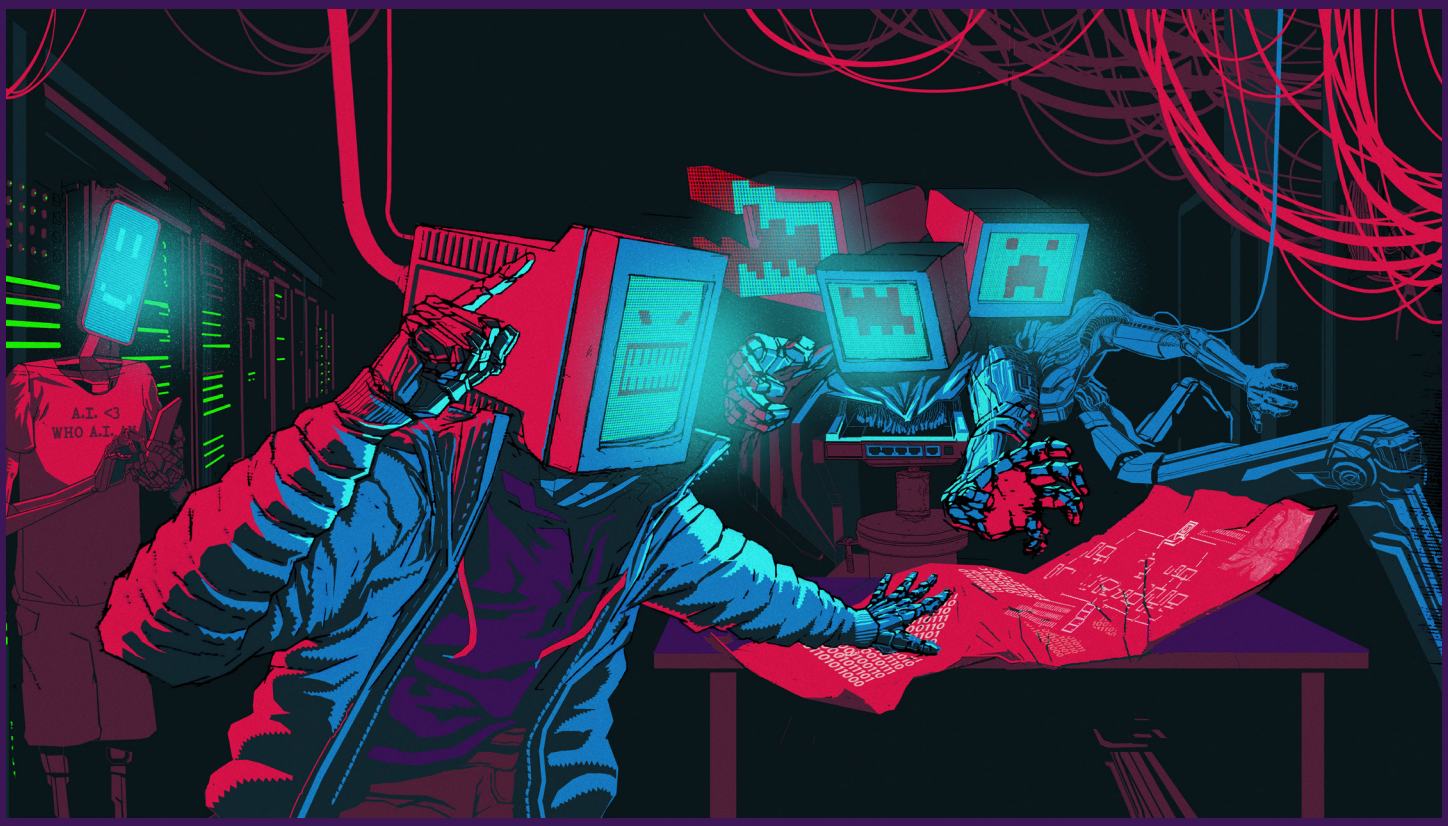


SPIRALA DIGITALNOG NASILJA

GODIŠNJI IZVEŠTAJ MONITORINGA POVREDA DIGITALNIH PRAVA U SRBIJI ZA 2023.

Impresum:

Urednica: Mila Bajić
Autori: Mila Bajić, Snežana Bajčeta,
Ninoslava Bogdanović, Bojan Perkov
Autorski tekstovi: Bojana Jovanović, Emilija
Milenković, Teodora Uzelac
Lektura: Milica Jovanović
Dizajn i prelom: Olivia Solis Villaverde
Ilustracije: Ruben Cruces-Perez

SHARE Fondacija, Beograd, Januar 2024

SADRŽAJ

UVOD 4

SAJBER INCIDENTI 11

U PRVOM LICU: PEGAZUS U SRBIJI 16

PRIVATNOST I ZAŠTITA PODATAKA 19

U PRVOM LICU: LIČNI PODACI U JAVNOJ KAMPANJI ZASTRAŠIVANJA 25

PREVARE, PRETNJE I MANIPULACIJE 28

U PRVOM LICU: VEŠTAČKI SADRŽAJ, PRAVE OPASNOSTI 36

RODNO ZASNOVANO ONLAJN NASILJE 41

U PRVOM LICU: VEŠTAČKI SADRŽAJ, PRAVE OPASNOSTI 45

UVOD

ŠTA JE NOVO?

Prethodne godine smo značajno unapredili svoj rad na praćenju i dokumentovanju povreda digitalnih prava. Naime, metodologija SHARE Monitoring projekta je 2023. prošla kroz detaljnu reviziju, kako sadržinsku tako i estetsku. Imajući u vidu da monitoring baza postoji već dugi niz godina, bilo je potrebno uskladiti je sa dosadašnjim praksama i predstaviti nov način prikupljanja podataka o povredama digitalnih prava u Srbiji. Nakon više meseci rada na novoj metodologiji, završni proizvod predstavljao je spoj dobro ustaljenih praksi i novog, osveženog pogleda na stanje digitalnih prava u zemlji. Kako bismo držali korak sa novonastajućim pretnjama i povećanim brojem povreda i napada u digitalnom okruženju, revizija metodologije pokazala se kao jedini logičan zaključak. Uz revidiranu metodologiju, cela monitoring baza dostupna je na novom sajtu, koji je takođe preuređen kako bi podaci i slučajevi bili pregledniji, a svi izveštaji dostupni na jednom mestu.

Metodološke promene obuhvataju izmenu kategorija kako bi nova klasifikacija što vernije odrazila najveće i najzastupljenije povrede. Nakon ekstenzivnog pregledanja svih slučajeva koji su se dosad našli u bazi, odabrane su četiri oblasti koje, prema zaključcima istraživačkog tima SHARE Fondacije, predstavljaju najbolji presek.

SAJBER INCIDENTI uključuju svaki uticaj na integritet ili dostupnost informacionog sistema, mreže ili uređaja s namerom da se nad njima preuzme kontrola, da se ometa ili prekine njihov rad, ili da se podaci na njima izmene, ukradu, izbrišu ili blokiraju. U ovu kategoriju svrstani su svi slučajevi opstrukcije računarskih infrastruktura kao što su DDoS napadi, bilo na medije, sajtove državnih institucija ili civilnog sektora, zatim neovlašćeni pristupi sistemima kroz fišing napade,

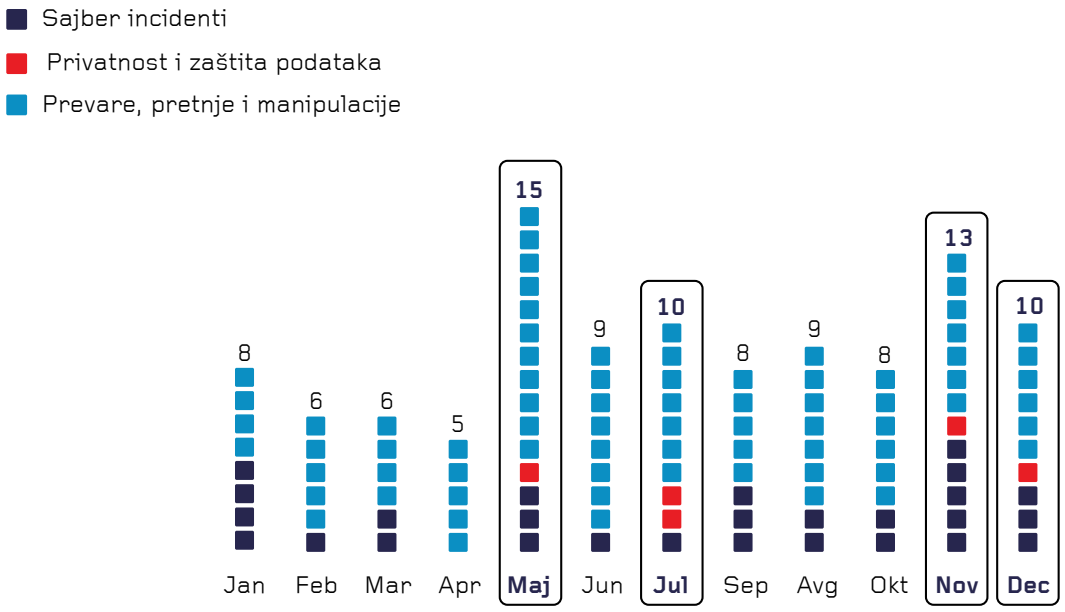
korišćenje zlonamernih sistema, socijalni inženjering u cilju onlajn prevara, kao i preuzimanje kontrole nad tehničkom infrastrukturom.

PRIVATNOST I ZAŠTITA PODATAKA odnosi se na povrede privatnosti i podataka o ličnosti u digitalnom prostoru, od faze prikupljanja podataka do njihovog eventualnog uništenja, uključujući i neovlašćeno korišćenje putem objavljivanja, ili neadekvatnu zaštitu koja dovodi do njihovog curenja u javnost. Slučajevi povrede privatnosti mogu biti masovni - kao u slučajevima curenja ili objavljivanja podataka građana iz državnih baza, bilo kroz spoljašnje napade ili nedovoljnu unutrašnju kontrolu - ili pojedinačni, koji mogu podrazumevati prisluškivanje pojedinaca ili objavljivanje ličnih podataka u medijima ili na društvenim mrežama bez saglasnosti.

PREVARE, PRETNJE I MANIPULACIJE obuhvataju različite oblike pretnji i uznemiravanja zbog aktivnosti i izražavanja na internetu, kao i manipulacije i širenje sadržaja u digitalnom okruženju radi postizanja određenih ciljeva. Reč je o širokom spektru pojedinačnih slučajeva i sistemskog kršenja digitalnih prava i sloboda, uključujući ugrožavanje bezbednosti i reputacije pojedinki i pojedinaca diskreditujućim sadržajem, diskriminaciju i govor mržnje, zatim širenje dezinformacija, malinformacija i zloupotrebe moderiranja sadržaja na internetu, kao i ograničavanje slobode izražavanja organizovanom instrumentalizacijom pravnih mehanizama.

RODNO ZASNOVANO ONLAJN NASILJE predstavlja najveću promenu u odnosu na prethodne verzije monitoring metodologije. Ovaj oblik nasilja prevashodno pogađa žene, devojčice i seksualne manjine i kao takav zavređuje posebnu pažnju u okviru monitoringa povreda. Kao horizontalna kategorija, zaključeno je da slučajevi koji se nalaze u ovoj kategoriji mogu uporedo pripadati i bilo kojoj od prethodno navedenih kategorija. Budući da je tehnološki zasnovano rodno nasilje sveprisutno i dalekosežno, jasan je bio zaključak da slučajevi sa elementima ovakvog nasilja podležu višestrukim kategorijama.

PREGLED PROŠLOGODIŠNJIH TRENDOVA



Prema NUNS-ovoj bazi napada na novinare, u 2023. godini zabeleženo je 183 napada na novinarke i novinare i medijske radnice i radnike u Srbiji. Čak dve trećine napada bili su pritisci koji uglavnom dolaze ili direktno od vlasti ili od onih koji su joj bliski. Na ovaj način vlast šalje jasnu poruku da je zlostavljanje i napadanje novinara opravdano, najčešće zbog njihovih kritičkih stavova, što vidno doprinosi atmosferi nasilja u društvu. Onlajn mediji su najviše izloženi napadima, uglavnom verbalnim, od uvreda sve do direktnih pretnji fizičkim nasiljem. Rastuća polarizacija u društvu doprinosi stvaranju nesigurnog okruženja za one koji se ne nalaze na pozicijama moći, pre svega na one koji iznose kritičke stavove prema vlasti i svojim radom osporavaju status kvo koji je nametnuo vladajući kadar. Kao jedna od glavnih tema ovog izveštaja izdvaja se činjenica da onlajn nasilje vrlo retko ostaje u domenu digitalnog prostora i da se neminovno preliva u fizički svet. Tome svedoče činjenice, kao na primer da su prema UNS-ovom saznanju novinari koji su izveštavali sa decembarskih protesta protiv izbornih rezultata napadnuti od strane uniformisanih policijskih službenika. Iako je bilo očigledno da

su u pitanju novinarske ekipe, čak i nakon što im je to potvrđeno, uvrede i fizički nasrtaji nisu prestali, dok je jedan policajac pokušao i da fotografu oduzme aparat.

Takođe, realnost za novinare u Srbiji predstavljaju i neprestane ucene i pritisci kroz zloupotrebe pravnih mehanizama, takozvane strateške tužbe protiv učešća javnosti (SLAPP). SLAPP tužbe karakteriše očevidna neujednačenost moći između tuženog, uglavnom medija, i tužioca, koji su uglavnom bliski vlasti i finansijski mnogo moćniji. Samim tim, SLAPP tužbe imaju složeniju ulogu - osim zastrašivanja medija i sprečavanja da se određene informacije objave, po sredi je i finansijsko i neretko psihičko iscrpljivanje. Za mnoge manje, lokalne medije nemoguće je da uopšte stupaju u parnice sa bogatim pojedincima bliskim vlastima ili velikim kompanijama, pa pod samim pritiskom najave tužbe povlače ili cenzurišu svoje priče. Kao apsolutni rekorder, KRIK trenutno ima preko deset postupaka koje su protiv njih pokrenuli ljudi bliski državnom vrhu, uključujući Predraga Koluviju, biznismena optuženog za organizovani kriminal u slučaju Jovanjica, kuma predsednika Vučića Nikolu Petrovića i ministra spoljnih poslova, bivšeg šefa Bezbednosno-informativne agencije Bratislava Gašića. KRIK je prošle godine osuđen i zbog svog pisanja o strateškim tužbama koje su protiv njih pokrenute, uz novčanu kaznu od 374.200 dinara. Ovaj perpetuum mobile predstavlja ozbiljnu i opasnu situaciju za stanje nezavisnog novinarstva u Srbiji i šalje jasnu poruku da politički nepodobne teme mogu imati skupu cenu.

Pored medija, i građani su tokom prošle godine trpeli pritiske zbog stavova izraženih na mrežama. U junu prošle godine, nuklearna inženjerka koja se na mreži X predstavlja pod pseudonimom Mila Sila dobila je otkaz u Direktoratu za radijacionu i nuklearnu sigurnost i bezbednost. Kako je navela na svom nalogu, otkaz je usledio kao odgovor na njene tvitove koji su neretko sadržali kritike na stavove i ponašanje visokih državnih funkcionera, pogotovo nakon majskih tragedija. Ovo nije bio prvi put da je Mila sankcionisana, kako se i ranije susretala sa disciplinskim merama na radnom mestu zbog

izražavanja stavova na svom privatnom nalogu. Otklanjajući svaku sumnju u motive, Mila je navela da joj je direktor pri uručenju otkaza vrlo jasno poručio da "tako zahtevaju službe". Nejasno je kako su privatni nalozi na društvenim mrežama legitimni razlog za otkaz, kao i na koji način ih službe povezuju sa zaposlenima. Pretnje i zastrašivanje neistomišljenika uglavnom je pojačano tokom i neposredno nakon predizborne kampanje, kada su neistomišljenici dodatno napadani od strane pristalica vlasti, pa su se tako posle decembarskih izbora studenti koji su protestvovali zbog izbornih neregularnosti našli u žiži koordinisanog napada od strane vlasti i režimskih medija.

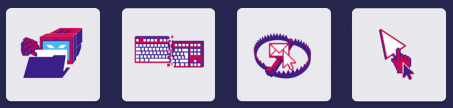
Objavljivanje informacija o privatnom životu pojedinki i pojedinaca predstavljalo je najčešći oblik kršenja prava na privatnost u prethodnoj godini. Nakon majskih tragedija u kojima je 18 osoba ubijeno, tabloidni mediji su vrlo brzo objavili svaki delić informacija do kojeg su mogli da dođu, uključujući i ime maloletnog izvršioca koji je u Osnovnoj školi "Vladislav Ribnikar" usmrtio devetoro učenika i čuvara škole. Podaci iz privatnog života maloletnog dečaka, kao i podaci iz života njegove porodice, pre svega roditelja, i danas služe kao tema u neprestanoj trci za pažnju i reakcije publike. Poštovanje privatnosti ljudi o kojima mediji pišu, najčešće tabloidna onlajn izdanja, problem je koji se ponavlja i koji se u poslednjih godinu dana u više navrata našao u centru javnih debata. Kada je u julu, posle dve nedelje intenzivne potrage, utvrđeno da je Noa Milivojev ubijena u centru Beograda od strane svog partnera, društvene mreže su bile preplavljene reakcijama, besom ali i uvredljivim komentarima. Portal Republika, digitalni produžetak Srpskog telegrafa, istakao se i među najgorima, objavljujući slike porodične grobnice i u delu svog izveštavanja koristeći Noino ime pre tranzicije (dednejmovanje) i oslovljavajući je u muškom rodu. Iako se Noa veoma otvoreno predstavljala kao trans žena, mnoštvo portala oslanjalo se na dodatnu dozu senzacionalizma čestim objavljivanjem slika Noe pre tranzicije i korišćenja muških zamenica u izveštavanju.

Neovlašćeno deljenje ličnih podataka i sadržaja kulminiralo je krajem godine kada je u Srbiji zabeležen prvi pokušaj napada špijunskim softverom Pegazus. Dve osobe iz civilnog sektora prijavile su poruke koje su dobili od Epla u kojima se navodi da su njihovi mobilni telefoni prepoznati kao uređaji koji su se našli na meti "državno sponzorisanog" napada. Srećom, njihovi uređaji nisu kompromitovani tako da je zabeležen samo pokušaj. Doduše, činjenica da su zabeležena dva ovakva pokušaja sada otvara prostor za ozbiljna pitanja o odnosu državnih službi prema ličnim podacima članica i članova organizacija civilnog društva, novinarki i novinara, pa i samih građanki i građana. Ovakva vest takođe svrstava Srbiju u neslavno društvo zemalja u kojima su ovakvi napadi sponzorisani od strane državnih organa, među kojima je nama najbliža Mađarska, gde je slobodno izražavanje i kritički stav prema vlasti u sve većoj opasnosti iz godine u godinu.

Zlonamerni napadi na informacione sisteme i mreže, kao i onlajn prevare postaju sve češće oružje za digitalne napade. Razlozi za pokretanje ovakvih napada mogu biti razni, od finansijskih do osvetničkih. U toku 2023. godine, četvrtina svih zabeleženih incidenata bili su tehničke prirode, a među najčešćim našli su se napadi na onlajn medije. JUGpress, RTS, Južne vesti, Demostat i Beta su svi napadnuti prošle godine, a podaci ukazuju da DDoS napadi postaju sve jači i uporniji. Pored medija, i tehnička infrastruktura države takođe je početkom godine pretrpela ozbiljne napade, navodno od strane internet kolektiva Anonymus. Jedan zaključak iz ovoga može biti da je bezbednost sajtova i dalje nedovoljno razrađena, pa je samim tim i teže izaći na kraj sa ovakvim napadima. Deluje da kultura sajber bezbednosti i dalje nije na dovoljno visokom nivou, kao i da se nedovoljno ulaže u promociju i podršku bezbednog korišćenja interneta. Prema istraživanju SHARE Fondacije krajem 2022. godine, od 30 analiziranih sajtova javnih preduzeća u Srbiji, skoro trećina nema bezbednosni protokol za pristupanje sajtu, što znači da su korisnici ovih sajtova potencijalno lake mete u slučaju neovlašćenog pristupanja sajtovima od strane zlonamernih aktera.

Fišing napadi, kojima se često ciljaju korisnici poštanskih usluga i e-trgovine, takođe su bili među najzastupljenijim tehničkim napadima. Napadači šalju lažne e-poruke u kojima traže lične podatke korisnika i finansijske informacije. Zatim, pod izgovorom da su već izvršili uplatu putem aplikacije, šalju lažne linkove oglašivačima i traže da unesu bankarske podatke (broj kartice i CVV broj) kako bi se navodno izvršila uplata. Nacionalni CERT je izdavao obaveštenja i saopštenja o fišing napadima kako bi upozorio građane na ovu prevaru. Ipak, Yettel, Pošta, Narodna banka Srbije i druga javna preduzeća su se pronašla među adresama preko kojih su građanke i građani targetirani. Učestalost ovakvih napada takođe može ukazivati na nedovoljnu digitalnu pismenost za prepoznavanje pokušaja socijalnog inženjeringa, koje najčešće za cilj imaju finansijsku korist od oštećenih.

SAJBER INCIDENTI



27
SLUČAJEVA

Proteklu godinu obeležile su promene u normativnom okviru informacione bezbednosti. Na međunarodnom nivou, 14. decembra 2022. godine usvojena je Direktiva 2022/2555 (NIS2 direktiva) sa 14. oktobrom 2024. kao predviđenim rokom za transpoziciju. To je dovelo do inicijalne izrade Nacrta zakona o informacionoj bezbednosti u Srbiji. Kako je navedeno u obrazloženju uz Nacrt zakona, pored usklađivanja sa Direktivom 2022/2555 (NIS2 direktiva), pravni okvir se usklađuje i sa Uredbom 2019/881 (Akt o sajber bezbednosti) u delu koji se odnosi na usklađivanje sertifikacija u oblasti informacione bezbednosti. Ono što je novina u izmenama i dopunama zakona jeste drugačija podela sektora prema njihovoj kritičnosti, na prioritetne i važne. Takođe, novim zakonom biće ojačana uloga CERT-ova, biće formirana nova tela koja će se baviti zaštitom informacione bezbednosti na državnom nivou, a doći će i do redefinisanja obaveza operatora sistema od posebnog značaja. Nacrtom zakona predviđa se osnivanje dva tela koja će se na nacionalnom nivou baviti informacionom bezbednošću: to su Telo za koordinaciju poslova informacione bezbednosti i Kancelarija za informacionu bezbednost. Telo za koordinaciju će služiti kao koordinaciono telo Vlade, a Kancelarija će u svojoj nadležnosti imati većinu poslova Nacionalnog

CERT-a, dok će Nacionalni CERT imati manji opseg nadležnosti. Novina je i revidiran pristup deljenju informacija o incidentima i pretnjama, izrada nacionalnog plana delovanja u slučaju velikih incidenata, kao i formiranje baze ranjivosti. Tokom avgusta protekle godine, održane su rasprave o Nacrtu zakona, ali do usvajanja još uvek nije došlo.

Međutim, fokus ne bi trebalo da bude samo na nominalnom usklađivanju sa EU propisima, već na suštinskom stvaranju bezbednijeg digitalnog okruženja za građane, kao i da se osigura da svi ključni IKT sistemi u Republici Srbiji budu adekvatno spremni da odgovore na bezbednosne incidente i izazove.

Kada su u pitanju sajber incidenti, prethodnih godinu dana u Srbiji obeležili su DDoS napadi, ransomver napadi na kritičnu infrastrukturu i veoma učestale fišing kampanje. Međutim, ono što se posebno izdvaja jeste prvi zabeleženi pokušaj napada špijunskim softverom na naš civilni sektor, koji dodatno ugrožava slobodu izražavanja i udruživanja, kao i pravo na privatnost i tajnost komunikacije garantovano domaćim i međunarodnim propisima. Napadi u kojima se koriste špijunski softveri poslednjih godina sve su češće aktuelni širom sveta, dok je jedna od zajedničkih karakteristika umešanost državnih struktura u takve operacije. U slučajevima koji su do sada otkriveni u Meksiku, SAD, Turskoj, Saudijskoj Arabiji, Mađarskoj i Azerbejdžanu između ostalih, utvrđeno je da je softver korišćen za prisluškivanje ili zastrašivanje pojedinaca koji su iznosili kritične stavove prema vlastima u ovim zemljama. Imajući ove informacije u vidu, korišćenje ovih alata u Srbiji otvara ozbiljna pitanja o načinu na koji se državne službe odnose prema kritici.

RANSOMVER NAPAD NA ELEKTROPRIVREDU SRBIJE

Ransomver napadi na kritičnu infrastrukturu države sve su učestaliji. Svedoci smo takvih napada ne samo u Srbiji, već širom regiona. Meta napada ucenjivačkim softverom bio je i portal Uvid u račun EPS-a na kome građani mogu da plaćaju svoje račune. Kako navode iz EPS-a, IT sistemi su stavljeni van funkcije sve dok IKT stručnjaci ne budu potpuno sigurni da je virus eliminisan. Obavešteni su nadležni organi i, kako navode, ovaj napad nije ugrozio proizvodnju, niti snabdevanje električnom energijom. Za ransomver napade karakteristično je da su počinioci poznati, jer napadači sami preuzmu odgovornost za svoja dela kako bi mogli da traže otkup od meta napada. Kako navode stručnjaci, iza napada na EPS stoji Qilin ransomver grupa.

DDOS NAPADI TOKOM GODINE

Česti DDoS (Distributed Denial of Service) napadi na portale onlajn medija predstavljaju ozbiljan izazov u Srbiji. Ovi napadi imaju za cilj da onesposobe ili otežaju normalno funkcionisanje sajta, sprečavajući pristup korisnicima i stvarajući tehničke probleme za medijske platforme. Medijske organizacije obično su mete napadača koji žele da izazovu prekid rada, naruše ugled ili ostvare druge ciljeve. Ponekad nije moguće prepoznati motiv ili cilj zbog kog se napadi izvode, dok je u nekim situacijama moguće predvideti verovatnoću da će do napada doći, recimo kada se objavljuje neka važna vest na sajtu, kada se očekuje velika posećenost ili kada se izveštava o važnim događajima.

Praćenje incidenata tokom 2023. godine ukazuje na kontinuitet ove vrste napada na lokalne medije u Srbiji. Krajem godine, sajt i aplikacija RTS-a našli su se na meti DDoS napada, što je otežalo pristup čitaocima tokom većeg dela prepodneva. Portal Demostat takođe je doživeo ozbiljan sajber napad koji je korisnicima onemogućio

pristup sajtu nekoliko dana. Sajt Južnih vesti pretrpeo je DDoS napad početkom jula, ali su posledice uspešno otklonjene. Tokom juna, sajt JUGpressa je nekoliko puta bio na meti DDoS napada, koji su bili vrlo česti i u ranijem periodu, što ukazuje na vršenje određenog pritiska na njih, najverovatnije zbog njihove dosledne uređivačke politike. Početak protekle godine obeležili su DDoS napadi na sajtove državnih institucija u januaru, uključujući sajtove Vojske Srbije, Ministarstva odbrane, Ministarstva spoljnih poslova, MUP-a, kao i sajt predsednika Aleksandra Vučića. Nalozi koji se predstavljaju kao članovi hakerske grupe Anonymous ubrzo su se oglasili preko X i preuzeli odgovornost za napade. Kao motiv, naveli su zvanični diplomatski stav Srbije prema Rusiji, koji se ogleda i u odluci o neuvođenju sankcija nakon početka rata. Teško je potvrditi da li stvarno iza napada stoje članovi ove svetske decentralizovane grupe sajber odmetnika, dok se domaće institucije nisu dodatno izjašnjavale o slučaju. Sajt Agencije za privredne registre (APR) takođe je nakratko bio nedostupan zbog DDoS napada, ali je agencija uspešno odbila napad i normalizovala rad svojih veb-servisa.

Napadi na sajtove onlajn medija mogu imati ozbiljne posledice: mogu dovesti do gubitka posetilaca, gubitka prihoda od oglašavanja, narušavanja reputacije i poverenja korisnika. Osim toga, ovi napadi mogu izazvati tehničke probleme, zaustaviti pristup informacijama ili ometati proces objavljivanja vesti i sadržaja. I dalje je nejasno zašto su DDoS napadi ovoliko zastupljeni, ali činjenica da targetiraju prevashodno one medije koji su uglavnom kritički nastrojeni prema vlasti može objasniti zašto reakcije državnih organa često ili izostaju ili su nedovoljno transparentne da bi mete napada razumele kako da se zaštite od budućih incidenata.

FIŠING PREVARE NE JENJAVAJU

Uprkos učestalom obaveštavanju građana da ne klikću na linkove i ne skidaju priloge poruka, a time i povećanoj svesti građana o ovim

vrstama prevara, fišing napadi se ne smanjuju. Glavna karakteristika fišinga je upravo u brojnosti i učestalosti napada. Cilj je zlonamernu poruku poslati što većem broju ljudi, jer će se bar neko i "upecati" na poruku. Ono što razlikuje scenu fišing kampanja od prethodnih godina, jeste povećan broj takozvanih smišing napada, kada se zlonamerne poruke šalju preko čet aplikacija, a ne mejlom. To otežava analizu takvih poruka, jer umesto značajnog dela podataka koji se inače dobija iz zaglavlja mejla, ovde jedino ostaje broj telefona. Najčešće će sa nekog stranog broja telefona stići poruka, što nam pomaže da prepoznamo fišing. U protekloj godini, fišing poruke su najčešće zloupotrebljavale logo Pošte Srbije. Veoma su česte i fišing prevare na osnovu poruka poslatih navodno u ime raznih banaka, kao i operatora telekomunikacionih usluga. Prošle godine zabeležena je i fišing kampanja koja je zloupotrebila logo Narodne banke Srbije. Karakteristično je da se broj fišing poruka povećava za vreme praznika.

OTKRIVENI POKUŠAJI ŠPIJUNSKIH NAPADA NA PREDSTAVNIKE CIVILNOG DRUŠTVA

Zabrinjava pojava nove vrste napada na civilni i medijski sektor malicioznim špijunskim programima, među kojima su zasad najpoznatiji Pegazus i Predator. U novembru su otkriveni pokušaji špijunskih napada na mobilne uređaje dvoje pripadnika civilnog sektora u Srbiji. Ekspertske organizacije potvrdile su da su na oba mobilna uređaja pronađeni tragovi pokušaja napada od 16. avgusta prošle godine. Rezultati analize ukazuju da je u inicijalnoj fazi napada korišćena ranjivost u funkcionalnosti iPhone uređaja. Za ovaj pokušaj napada korišćen je špijunski softver Pegazus, koji je već ranije bio povezan sa različitim metodama iskorišćavanja HomeKit ranjivosti, uključujući i poznati PWNYOURHOME.

U PRVOM LICU

Anonimni autor, meta pokušaja napada softverom Pegazus u Srbiji

PEGAZUS U SRBIJI

Kada sam saznao da je moj telefon bio napadnut Pegasus spyware-om, osećao sam se kao da je privatnost u mom životu narušena na najintimnijem nivou. Bes i frustracija su se mešali s osećajem ranjivosti, dok sam pokušavao da shvatim razmere napada i posledice koje mogu proizaći iz toga.

Osećaji koje sam imao su na prvom mestu bili velika nelagoda i osećaj izgubljene sigurnosti, jer sam shvatio da su moji lični podaci, poruke i fotografije intimnih trenutaka pod prismotrom nepoznatih lica, nepoznate institucije, i „neke" države. Postao sam svestan da se informacije koje sam smatrao privatnim sada nalaze u rukama neovlašćenih pojedinaca.

Politička situacija u Srbiji, predizborni period u kome smo se našli, kao i momenat objavljivanja privatnog snimka opozicionog političara još više su doprineli da postanem anksiozan i da skoro stalno razmišljam o svemu što se dešava.

Osećao sam se kao meta, lišen osnovnog prava na privatnost. Strah od gubitka kontrole i osećaj izloženosti postali su dominantni u mom svakodnevnom životu. Razmišljao sam o svakom koraku u komunikaciji, bankarskim transakcijama i svakodnevnom radu, bojeći se da će moji poslovni, ali i najličniji trenuci biti zloupotrebljeni. Poverenje u tehnologiju koje sam nekada imao značajno je poljuljano, postavljanjem pitanja o granicama digitalne privatnosti i sigurnosti.

Ovaj subjektivni doživljaj suočavanja s Pegasus spyware-om označio je prelazak iz nevinosti digitalnog sveta u bolnu stvarnost gde je privatnost postala luksuz koji se čini nedostižnim.

KONTEKST NAPADA

Dvoje pripadnika civilnog sektora iz Srbije je 30. oktobra dobilo do tada potpuno novu sistemsku notifikaciju od kompanije Apple na svojim telefonima, da su potencijalne mete državno-sponzorisanih napada. Pripadnici civilnog društva su najpre kontaktirali tim SHARE Fondacije kako bi proverili autentičnost notifikacije, imajući u vidu da može biti reč o fišing prevari. Kroz međunarodne kontakte, dobijena je potvrda predstavnika kompanije Apple da su upozorenja autentična i da ih ne treba ignorisati. Dodatni razlog za sumnju bio je to što su opozicioni političari u Indiji u isto vreme dobili slična upozorenja ove kompanije.

Uz koordinaciju sa partnerima iz organizacija Access Now, Amnesty International i Citizen Lab, SHARE Fondacija je prikupila neophodne podatke sa telefona kako bi se utvrdilo da li su uređaji trenutno ili ranije bili zaraženi malicioznim softverom. Iako postoje javno dostupni alati za forenzičku analizu, poput Mobile Verification Toolkit (MVT) i Android Quick Forensics, indikatori kompromitovanosti (IoC) za napredne špijunske softvere se ne objavljuju javno kako se njihovim proizvođačima i kupcima ne bi davala upozorenja da promene operativne metode i tehničku infrastrukturu sa koje se vrši špijunaža. Iz istog razloga, javno se ne iznose detaljne informacije o procesu prikupljanja podataka i forenzike telefona.

Indicije na osnovu nalaza partnera bile su da se pokušani napad podudarao sa metodama Pegazusa, ozloglašenog softvera za špijunažu koji je izazvao političke potrese širom sveta zbog targetiranja novinara, političkih disidenata, aktivista i političara. Bio je to prvi javno poznati slučaj da je u Srbiji pokušano korišćenje jednog od dva najpoznatija alata za špijuniranje telefona, koje skoro po pravilu sponzorišu države. Iako nije bilo zvaničnih potvrda o

tome ko je rukovodio pokušanim napadom, jasno je da je cilj bilo zastrašivanje onih koji su se našli na meti.

Kao što je i do sada bio slučaj, mete napada Pegazusom odlučile su da ostanu anonimne. Ovaj tekst nastao je u saradnji jedne od osoba čiji je uređaj bio na meti špijunskog napada, i članova tima SHARE Fondacije koji su učestvovali u analizi napada. Ukoliko posumnjate da ste na meti napada koji ne prepoznajete, savetujemo vam da se obratite SHARE Fondaciji ili nadležnim institucijama kao što je Posebno tužilaštvo za VTK. Bez obzira da li ste već u riziku od sajber napada ili ne, važno je da se redovno informišete o mogućim opasnostima i načinima zaštite.

PRIVATNOST I ZAŠTITA PODATAKA

5
SLUČAJEVA

Kategorija monitoringa digitalnih prava i sloboda posvećena povredama privatnosti i podataka o ličnosti obuhvata ne samo direktno ugrožavanje ovih prava, već i slučajeve u kojima je utvrđeno da nisu ispunjene mere propisane Zakonom o zaštiti podataka o ličnosti. Novim metodološkim pristupom fokus je stavljen na objavljivanje, curenje i nezakonito prikupljanje podataka, kao i na neovlašćeno prisluškivanje komunikacije i snimanje. Zabeleženi slučajevi razlikuju se prema razmerama povrede u zavisnosti od toga da li je u pitanju pojedinačna povreda prava određenog lica ili masovna povreda poput curenja podataka velikog broja ljudi.

Vlada Srbije je krajem avgusta usvojila Strategiju zaštite podataka o ličnosti za period od 2023. do 2030, skoro deceniju i po od prvog strateškog dokumenta u ovoj oblasti iz 2010. godine. Kao osnovni cilj strategije utvrđeno je "poštovanje prava na zaštitu podataka o ličnosti u svim oblastima života". Na predlog predstavnika SHARE Fondacije u radnoj grupi, osnovni kriterijum za ispunjenost ovog cilja jeste donošenje odluke o adekvatnosti Evropske komisije, koja bi potvrdila da zaštita podataka ličnosti u Srbiji odgovara EU standardima. Imajući u vidu trenutno stanje zaštite podataka o ličnosti u Srbiji, to

će biti veoma izazovan proces, zbog čega nova Vlada što pre treba da usvoji Akcioni plan za primenu strategije.

Namera da se biometrijski elementi pametnog video-nadzora, poput prepoznavanja lica, uvrste u pravni sistem Srbije i naknadno legalizuje njihova upotreba usvajanjem Zakona o unutrašnjim poslovima obeležio je kraj 2022. godine, kada je predlog zakona po drugi put povučen iz procedure nakon pritiska stručne zajednice i civilnog društva. Predsednica Vlade Ana Brnabić je tom prilikom najavila "široke konsultacije" u radu na novoj verziji dokumenta. U prvim mesecima 2023. godine, civilnom društvu su na interno razmatranje dostavljeni novi radni dokumenti koji jesu sadržali mala unapređenja u odnosu na ranije verzije, poput sistemskog žurnala za beleženje aktivnosti u sistemu, ali su suštinski i dalje bili na liniji legalizovanja biometrijskog nadzora javnih površina. Zvanična javna rasprava o novim predlozima zakona iz oblasti unutrašnjih poslova nije održana tokom 2023. i po svemu sudeći će sačekati formiranje nove Vlade i izbor novog ministra unutrašnjih poslova.

Čini se da će sudbina propisa koji bi u Srbiji uredili pametni video-nadzor i ostale vidove biometrijskog nadzora na javnim mestima, biti povezana sa Aktom o veštačkoj inteligenciji EU, odnosno AI aktom. Očekivanja od AI akta su velika zbog uverenja da može da predstavlja globalni standard regulisanja sistema veštačke inteligencije, slično kao GDPR za podatke o ličnosti. SAD, kao veoma značajna jurisdikcija za ova pitanja, takođe su najavile nameru da regulišu razvoj i upotrebu sistema veštačke inteligencije krajem oktobra prošle godine.

Organi EU su tokom prethodne godine kroz više etapa išli ka političkom dogovoru o tekstu AI akta, čija je ključna komponenta utvrđivanje rizika sistema veštačke inteligencije po ljudska prava i društvene procese. Pregovaračka pozicija Evropskog parlamenta usvojena u junu bila je ohrabrujuća, pošto je predviđala zabranu sistema biometrijske identifikacije na daljinu u realnom vremenu, npr. prepoznavanje lica uživo na gradskim trgovima ili ulicama. Dugo

očekivani trijalog predstavnika država članica i Evropskog parlamenta uz posredovanje Evropske komisije okončan je početkom decembra, kada je postignut politički dogovor o AI aktu.

Konačna verzija teksta AI akta, čije se zvanično objavljivanje očekuje uskoro, prema poslednjim informacijama nije ostala u duhu zabrana kada je reč o upotrebi sistema biometrijske identifikacije na daljinu, već će formalno omogućiti upotrebu izuzetno intruzivnih tehnologija za nadzor ukoliko se usvoji u tom obliku. U finalnim fazama trijaloga, SHARE Fondacija promovisala je knjigu "Beyond the Face: Biometrics and Society" u Evropskom parlamentu u Briselu, koja kroz istraživanje i analizu tehnoloških, pravnih i praktičnih aspekata biometrijskog nadzora ukazuje na suštinske probleme po ljudska prava na globalnom nivou, naročito u pogledu ranjivih i istorijski diskriminisanih društvenih grupa.

Bez obzira na razvoj evropske legislative, u Srbiji već postoje primeri sistema koji obrađuju podatke građana i donose automatizovane odluke sa potencijalno negativnim posledicama po njihov svakodnevni život. Inicijativa A11, koja se bavi zaštitom ekonomskih i socijalnih prava, analizirala je informacioni sistem Socijalna karta, osnovan prema odredbama Zakona o socijalnoj karti čija je primena počela u martu 2022. godine. U IS Socijalna karta beleže se i obrađuju podaci o ličnosti u više od 130 stavki i to ne samo korisnika socijalne pomoći, već i njihovih članova porodica i povezanih lica. Pored problema sa prekomernom obradom podataka o ličnosti i dehumanizacijom socijalne zaštite, nalazi A11 ukazuju da je posle nešto više od godinu dana rada sistema, broj ljudi koji koriste socijalnu zaštitu smanjen za skoro 35.000.

MEDIJSKA SENZACIONALIZACIJA NASILJA I LIČNIH TRAGEDIJA

Nezapamćeni majski masakri u beogradskoj školi "Vladislav Ribnikar" i mestima Malo Orašje i Dubona izazvali su ogromne potrese u društvu, ali i čitave talase tabloidnog izveštavanja koje je duboko zadiralo u detalje iz privatnih i porodičnih života ljudi pogođenih tragičnim događajima. Recimo, portal republika.rs je pisanjem i pratećim multimedijalnim sadržajima o sahrani ubijenih u okolini Mladenovca, u danima nakon ubistava duboko ugrozio privatnost porodica, povodom čega je reagovalo Nezavisno udruženje novinara Srbije i pozvalo medije da se uzdrže od skandaloznog izveštavanja i poštuju novinarsku etiku.

Najsitniji detalji izvršenja zločina, spekulacije o privatnom životu žrtava i njihovim ličnim odnosima, uznemirujuće fotografije i slični sadržaji ostaju lako pretraživi na internetu čime se povrede privatnosti produbljuju. Na portalima tabloida postoje tagovi, odnosno oznake tekstova sa imenom žrtve ili ključnim rečima poput "Vladislav Ribnikar", pomoću kojih se na jednostavan način može doći do više desetina tekstova, objavljivanih iz dana u dan sa novim detaljima.

Mediji su početkom jula objavili da je Noa Milivojev, trans devojka za kojom se tragalo više od dve nedelje, pronađena ubijena u centru Beograda. Noino ubistvo pratile su salve govora mržnje u onlajn prostoru, objavljivanje imena pre tranzicije (tzv. dednejmovanje) i rušenje posvete na Trgu Republike gde su građani položili cveće i zastave trans ponosa. Tabloid "Srpski telegraf" je na portalu republika.rs senzacionalistički objavljivao mnoštvo detalja o Noinom privatnom životu, ubistvu i okolnostima nakon što je ubijena. Udruženje novinara Srbije osudilo je ovakvo izveštavanje i nazvalo ga gaženjem Zakona o javnom informisanju i medijima i Kodeksa novinara Srbije. Mržnja prema LGBTQ+ osobama u onlajn prostoru nije ograničena na pseudoanonimne komentatore i naloge na društvenim mrežama - takvo ponašanje podstiču i javni funkcioneri poput poslanice

Narodne stranke Ivane Parlić, koja je početkom avgusta na mreži X širila homofobiju prema pevaču Filariju na osnovu njegovog fizičkog izgleda.

LIČNO I POLITIČKO

Izbori održani 17. decembra na parlamentarnom, pokrajinskom i lokalnom nivou takođe su bili igralište za povrede prava i zloupotrebe. Ali pre nego što su izbori raspisani, javnost su tokom leta uzdrmale informacije o identitetima političkih "botova". Naime, X nalog @protivdictature objavio je tabelu sa podacima velikog broja ljudi - imena, prezimena, okrug i opštine prebivališta, sa linkovima ka nalozima na društvenim mrežama. Uz tabelu je navedeno da su ovi ljudi "botovi", odnosno politički aktivisti i provokatori Srpske napredne stranke na zadatku da u onlajn prostoru šire prorežimsku propagandu i napadaju političke protivnike. Redakcija portala Fake news tragač stupila je u kontakt sa jednom od osoba čiji su se podaci našli na spisku i potvrdila da su autentični. Izvor spiska ostao je nepoznat, a prema analizama na njemu je bilo oko 3000 ljudi koji kontrolišu više od 14.000 naloga na mreži X, Fejsbuku, Tik Toku i Instagramu.

Razmere onlajn propagande potvrdile su prethodnih godina i velike platforme: najpre Tviter koji je 2020. godine ukinuo više od 8000 naloga povezanih sa organizovanom promocijom SNS sadržaja, dok je sličan korak kompanija Meta preduzela na Fejsbuku i Instagramu podrobno pišući o mreži naloga koji su učestvovali u koordinisanom neautentičnom ponašanju na ovim platformama. U svom izveštaju za poslednji kvartal 2022. godine, Meta je navela da je organizovana mreža naloga, rasprostranjena po celoj Srbiji, nastojala da širi narative i ideje koje zastupa SNS, na naizgled "organski" način, odnosno bez eksplicitnog izražavanja svojih namera.

Propagandna snaga vladajućih struktura je i tokom poslednje predizborne kampanje iskorišćena za medijske obračune sa političkim protivnicima, a među kolateralnim žrtvama našla se i

intima. Kandidat liste "Srbija protiv nasilja" na beogradskim izborima Đorđe Miketić objavio je da su mu sa nepoznatog broja telefona na Vajber stigli pretnja i snimak ekrana preuzet iz njegovog intimnog videa. Pre curenja snimka, Miketića su targetirali visoki državni funkcioneri, uključujući i predsednika Vučića, nakon što je u javnosti komentarisao navode o fantomskim glasačima. Privatni snimak, čija je autentičnost potvrđena, kasnije je prikazan na Pinku, televiziji sa nacionalnom frekvencijom. Snimak je danima cirkulisao po društvenim mrežama, dižući popularnost afere na još veći nivo, što je na kraju dovelo i do Miketićevog povlačenja iz predizborne kampanje.

Nakon decembarskih izbora, građanski protesti zbog izbornih neregularnosti i glasačkog inženjeringa izveli su studente i mlade na ulice. Nakon jednog protesta, na društvenim mrežama pojavio se snimak na kojem nepoznata osoba lista fotografije mladih koji su se istakli na protestima, nalik na one iz baze ličnih karata kojima pristup ima jedino MUP. Biometrijska fotografija predstavnika grupe mladih demonstranata Nikole Ristića pojavila se i u provladinom tabloidu "Alo", u tekstu koji ga je targetirao zbog političkog aktivizma. Postavlja se pitanje ko je i kako imao pristup fotografijama iz biometrijske baze podataka svih građana Srbije, kao i zbog čega nadležne institucije nisu reagovale na ovaj incident.

U PRVOM LICU

Emilija Milenković, studentkinja FPN

LIČNI PODACI U JAVNOJ KAMPANJI ZASTRAŠIVANJA

Celog života se trudiš da na društvenim mrežama imaš najlepše i najsređenije slike, a na kraju najviše ljudi vidi onu najružniju - iz lične karte i to protiv tvoje volje. Moje ime je Emilija i da, ja sam ona studentkinja čiju sliku iz lične karte u telefonu lista neka random žena na protestu. Do skoro nisam znala šta tačno znači konstrukt "biometrijski podaci", na koji način se oni čuvaju, ko sme da ima pristup njima i zašto se vrlo strogo koriste i štite. Verujem da su retke mlade osobe koje imaju 21 ili više godina i koje znaju šta to znači i koje to zanima. Međutim, ispostaviće se da za tu mladalačku naivnost nema mesta u jednom nedemokratskom društvu sa očiglednim naznakama policijske države.

Kada sam preko društvenih mreža videla snimak žene koja lista sliku iz moje lične karte na viber grupi, na protestu protiv izborne krađe, osetila sam se zbunjeno i zabezeknuto. Znala sam da moram da reagujem, ali nisam znala kako, znala sam da je taj događaj pogrešan ali ipak nisam znala do kog nivoa je to zapravo povreda mojih prava. Znala sam da sam verovatno kao istaknuta aktivistkinja na protestu imala možda malo drugačiji tretman u bezbednosnim strukturama, što je za mene i dalje špansko selo, ali nisam znala da su te strukture ipak toliko neorganizovane i neprofesionalne da bilo ko na protestu može da snimi njihove telefone. Od te ideje sam odmah odustala iz očiglednih razloga, a logičan odgovor je definitivno da je to bio pokušaj zastrašivanja, poruka "znamo ko si, pazi šta radiš" i narušavanje moje privatnosti. Pokušaj zastrašivanja i targetiranja u tabloidima kroz zloupotrebu biometrijskih podataka je slučaj koji je iznenadio i naljutio mnoge ljude, pogotovo mlade aktiviste,

i probudio empatiju i solidarnost. Iznenadio je i međunarodnu zajednicu kao i mnoge pravnike, advokate i organizacije. To je bio i pokušaj narušavanja bezbednosti ljudi koji koriste svoje pravo na mirno izražavanje kroz protest, pokušaj zastrašivanja pojedinaca kao i pokazivanje primera ostalima na ulici. Ono što je meni najteže palo je reakcija moje porodice i moj pokušaj uveravanja njih da je sve u redu iako u tom trenutku ja sama ne znam da li zapravo jeste. Nisam ekspertkinja u oblasti zaštite privatnosti, zloupotrebe ličnih podataka i slično, i nikada nisam mislila da ću kao mlada osoba i aktivistkinja biti primorana da se time bavim kroz tužbe, žalbe i da ću sličnim sredstvima tražiti pravdu. Pogotovo ne u sistemu u kojem ne verujem da ću ikada dobiti odgovor na moje zahteve, jer institucije skoro nikad ne štite one koje kritikuju taj isti sistem, bar ne u Srbiji.

Međutim i pored nepoverenja i nefunkcionalnosti institucija, potrebno je iskoristiti svaki pravni lek, i u ovom slučaju tražiti zaštitu i pravdu. Na mom mestu je mogao da bude bilo ko, možda i jeste a mi to još uvek ne znamo jer nismo videli na snimcima ili u tabloidima. Zato je potrebno stalno u javnosti podsećati na ovaj slučaj, vršiti pritisak na institucije da rade svoj posao, i buniti se protiv stavljanja policije u službu targetiranja studenata u prorežimskim tabloidima.

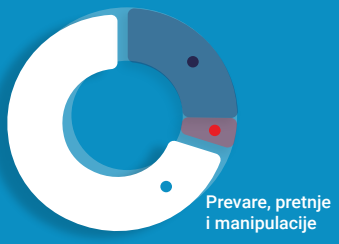
Čudan je osećaj videti sliku iz lične karte koju ne poseduješ u prorežimskim tabloidima. Taj osećaj ogoljenosti, nezaštićenosti i nemoći u svakom smislu ne treba da oseti nijedan građanin. Normalizaciju toga kao društvo ne smemo da dozvolimo, a država mora da zaštiti svaku osobu, a pogotovo mlade, koji se bore za svoja demokratska prava pritom koristeći svoje demokratsko pravo na mirno okupljanje.

Emilija Milenković, studentkinja treće godine Fakulteta političkih nauka koja je podelila svoje iskustvo zastrašivanja kroz zloupotrebu ličnih podataka nje i njenih kolega na protestima, posetila je institucije Evropske unije krajem januara. Emilija i još jedna koleginica prenele su zahtev grupe studenata “Borba” da se ne prizna legitimitet

decembarskih izbora i da se pokrene međunarodna istraga povodom izbornih nepravilnosti. U uslovima aktivnijeg učešća studenata i mladih na protestima, vlast je reagovala ne samo zastrašivanjem poput slučaja “listanja” fotografija, već i kroz hapšenje i određivanje pritvora.

PREVARE, PRETNJE I MANIPULACIJE

75
SLUČAJEVA



Većina povreda u 2023. godini bile su direktno ili indirektno povezane sa političkom neposlušnošću i ličnim stavovima koji se razilaze od zvaničnih državnih narativa. Na ovaj način na meti su se našle članice i članovi društva koji su se na razne načine borili za ravnopravno, transparentno i pošteno društvo, uključujući medijske radnice i radnike, aktivistkinje i aktiviste, ali i građanke i građane koji su učestvovali na masovnim i čestim anti-režimskim protestima organizovanim tokom prošle godine. Ove salve napada uglavnom su orkestrirale i vodile pristalice Srpske napredne strane, kolokvijalno nazivane botovima, mada je to sada za njih više degradirajuća titula, osim kad su tako samoprozvani. Naime, u poslednjih nekoliko godina u različitim navratima otkrivene su velike mreže neautentičnih naloga koji su korišćeni za koordinisano pružanje podrške vladajućoj stranci i napade na opoziciju i organizacije civilnog društva. U 2020. godini, Tviter je uklonio preko osam i po hiljada naloga koji su prema istraživanjima za četiri godine objavili više od 40 miliona tvitova.

U okviru ovogodišnjeg monitoringa posebno su mapirane i manipulacije plasirane posredstvom informativnog sadržaja na vodećim onlajn medijima u Srbiji u periodu predizborne kampanje,

koje su za rezultat imale sistemsko marginalizovanje relevantnih informativnih sadržaja uz izrazito favorizovanje vladajuće većine.

PRETNJE UPUĆENE MEDIJIMA, NOVINARIMA I NOVINARKAMA

Medijski sektor i novinarska zajednica predstavljaju posebno ranjivu kategoriju u pogledu digitalnih prava i sloboda u Srbiji već godinama. Ni u 2023. godini ne možemo govoriti o poboljšanju situacije. Naprotiv, posebno su kritički mediji i novinari i novinarke koji nastoje da ukažu na najznačajnije političke i društvene probleme u zemlji, bili mete pretnji koje su dolazile kako iz državnih i političkih struktura, tako i sa adresa njima naklonjenih medija, ali i pojedinih građana čiji "aktivizam" zaokružuje spektar standardizovanih targetiranja u digitalnom okruženju.

Tako su društvene mreže bile poligon za pretnje urednici „Podrinskih" Isidori Kovačević, koje su joj upućene zbog toga što je komentarisala prisustvo načelnika Policijske uprave Šabac na predizbornom skupu SNS. Dve godine ranije je grad u kojem živi bio oblepljen plakatima sa njenim likom, a povodom njenog pisanja o huliganskim napadima na građane koji su protestovali. Usled minimiziranja značaja pretnji koje dobija godinama, nisu postojale prepreke za pozivanje na njeno proterivanje iz grada i zemlje u kojoj živi. Samo su promenjena sredstva. Umesto plakata, to su sada komentari na društvenim mrežama, čiji je doseg potencijalno mnogo veći. Pretnje koje su se prevashodno oblikovale u tabloidnom bloku štampanih i televizijskih medija, već godinama unazad nalaze svoje mesto i u digitalnoj sferi, bilo da govorimo o digitalnim pokretačima ili oštećenim stranama. Tako je povodom teksta o zaplenjenom naoružanju kod Banjske, Gradski odbor Srpske napredne stranke u Vranju optužio portal Vranjenews da je glasilo "teroriste i ratnog zločinca Aljbina Kurtija" koji opravdava "ubice Srba sa Kosova i Metohije".

Ono što se nije promenilo je "klijentelističko-opoziciono-izdajnički" okvir pretnji koji se orkestrirano perpetuira u krugu vladajućih struktura i njihovih medijskih i pojedinačnih pristalica. Pretnje kritičkim medijima se, dakle, argumentuju pripisivanjem servisne uloge prema pojedinim strukturama ("šolakovski" mediji) u zamenu za neku vrstu uglavnom finansijske koristi. Zatim kao opozicija, kako vlastima tako i državi i ukupnom poretku ("đilasovski" mediji). Najzad, kroz predstavljanje nezavisnih novinara/ki kao svojevrsnih neprijatelja države, "srpske kulture i pravoslavlja".

Uticaj i značaj koji pojedinačni medij ima u društvu koincidira sa intenzitetom verbalnih napada, kao i pozicijama sa kojih se plasira. Dnevni list Danas je, primera radi, svojim pisanjem izazvao talas verbalnih napada od strane vrha vladajuće strukture. Premijerka Ana Brnabić je novinare ovog medija na svom X nalogu označila kao "necivilizovane sadiste i mrzitelje", zbog pokretanja pitanja "Ko je Fahri Musliu, za koga Vučić govori da mu nije otac?". Tekst se odnosio na svojevrsnu "aferu" na kojoj se zasnivao deo predizborne kampanje za decembarske izbore, tokom koje je Aleksandar Vučić "branio" članove svoje porodice od konstruisanih "napada" nejasno identifikovanih aktera. Napadi za obranu predsednika Vučića uglavnom nisu usamljeni, pa na društvenoj mreži X nalazimo i podršku premijerki u napadima na Danas, i to od strane nosilaca najviših državnih funkcija, predsednika Narodne skupštine ("Od gebelsovskih 'filmova' do klasičnih bljuvotina u tajkunskim tabloidima"), ali i na Instragram nalogu ministra u Vladi Srbije („Đubrad najveća! Kakav neopevani šljam! Platićete za ovo i bićete i vi počišćeni na ovim izborima, filijalo Dragana Đilasa za najprljavije poslove"). Pažljivo organizovane pretnje uglavnom imaju svoj oflajn pandan, kao što su narativno potpuno usklađena saopštenja (Član Predsedništva SNS Milenko Jovanov: „Ljudi koji ovo rade nisu poremećeni, nisu ni ološ, ni šljam, jer kada bi ih neko tako nazvao, to bi za njih bili komplimenti").

Dok predstavnici/e vlasti kreiraju konfrontirajući ambijent u javnoj sferi, posebno je upozoravajuća činjenica da tokom 2023. godine

nisu izostale ni pretnje smrću. Najozbiljnije pretnje bile su upućene novinarki Žaklini Tatalović i novinarima Stevanu Dojčinoviću, Peru Jovoviću, Vojinu Radovanoviću i Nikoli Krstiću. Pored političkih tema i rada vlasti, primetno je da je najveća verovatnoća da će novinarima/kama u Srbiji biti upućene pretnje ukoliko se bave temama korupcije i organizovanog kriminala, ali i pitanjima u vezi sa SPC ili Kosovom. Pored sve učestalijih napada od strane desničarskih organizacija, posebno zabrinjava korišćenje pravnih mehanizama u svrhu ograničavanja slobodnog novinarstva. Pored privođenja i oduzimanja sredstava za rad, SLAPP tužbi, presuda, u digitalnom svetu zabeleženo je i korišćenje sofisticiranijih metoda, poput moderiranja sadržaja ili fabrikovanja "istraživačkih priča" o ugrožavanju vlasti uz lažno pripisivanje autorstva kredibilnim medijima. Ovo predstavlja samo još jedan alat u svojstvu diskreditacije medija koji ne prate jasno ispisane zvanične narative servirane od strane vlasti, i samim tim ne služe kao glasila i pojačala tih zvaničnih politika koje su često konfliktne, netransparentne i polarizujuće.

Digitalno okruženje u Srbiji postaje značajna arena za ugrožavanje bezbednosti novinara, kao svojevrsna platforma za upućivanje pretnji i uvreda od strane sve organizovanijeg mehanizma u kojem uloge imaju država, vladajuća struktura sa svojim aktivistima/simpatizerima i tabloidi, uključujući resurse od lokalnog do nacionalnog nivoa. S druge strane, istim mehanizmom se iznalaze i načini kako da se, pored strogo kontrolisanog sveta tradicionalnih, uspostavi kontrola i nad onlajn medijima, odnosno da se upotrebom novih tehnologija ograniči slobodno, kritičko i nezavisno novinarstvo i u digitalnom okruženju.

MANIPULACIJE VEŠTAČKOM INTELIGENCIJOM U POLITIČKE SVRHE

Kao što nove tehnologije mogu doprineti razvoju različitih oblasti i opšte dobrobiti društva, tako njihova upotreba može pojačati

postojeće izazove u digitalnom okruženju, posebno kada je reč o zemljama u kojima pravni mehanizmi njihove regulacije nisu dovoljno razvijeni, a društveno-politički kontekst ne afirmiše etičke principe pri njihovoj upotrebi.

Ekspanzivni razvoj veštačke inteligencije našao je svoje mesto i u Srbiji, pa smo u prethodnoj godini svedočili njenom javnom testiranju. Sudeći po "eksperimentalnoj" primeni, koja je predstavljena kao svojevrsna šala i parodija Željka Mitrovića na račun opozicionara, opravdana je bojazan da ovaj alat može poslužiti kao digitalna ekstenzija diskreditacije društvenih i političkih aktera prema principu koji je u oflajn sferi prethodno razvio Pink.

Iako još uvek ne možemo govoriti o specifičnim trendovima manipulacije veštačkom inteligencijom u Srbiji, pojedinačni primeri ukazuju na mogućnosti njene političke zloupotrebe. Naime, scenario kontrolisanja digitalnog okruženja putem digitalnih medija, organizovanim aktivnostima na društvenim mrežama i sada dodatno veštačkom inteligencijom, mogao bi još drastičnije da naruši prava i slobode građana i građanki, i to ne samo u digitalnom okruženju. Prvo, za manipulisanje informacijama i dovođenje u zabludu digitalni prostor je samo odgovarajuća platforma, ali su društvene i političke posledice dalekosežnije. Drugo, ekspanzivna upotreba veštačke inteligencije najavljena u Nacionalnom dnevniku Pinka upućuje i na strukturno favorizovane aktere u raspolaganju ovim resursima, čime se nadograđuju njihovi kapaciteti za dalje učvršćivanje političkog statusa kvo.

Stoga je pred stručnom i zainteresovanom zajednicom zadatak da na sveobuhvatan način pristupi ovim izazovima i, prateći korake novih regulatornih standarda Evropske unije, sačini sistemska rešenja u ovoj oblasti, naravno, vodeći računa o specifičnostima i lokalnim izazovima karakterističnim za Srbiju.

SISTEMSKO MANIPULISANJE DIGITALNIM INFORMATIVNIM SADRŽAJEM

Godina za nama ostaje obeležena i po izuzetno razvijenim mehanizmima sistemskog manipulisanja informativnim sadržajem u digitalnom okruženju. Na osnovu analize 15 najposećenijih medijskih portala u Srbiji u periodu predizborne kampanje za parlamentarne, pokrajinske i lokalne izbore koji su održani 17. decembra 2023. godine, SHARE Fondacija je mapirala nekoliko mehanizama putem kojih su vladajuće strukture kontrolisale digitalni informativni prostor u Srbiji, čiji je sadržaj dominantno favorizovao vlast, a uz pažljivo konstruisanu poziciju i ulogu koju je u medijima imao Aleksandar Vučić. Međutim, karakter većine manipulativnih mehanizama ukazuje na njihov značaj i kontinuiranu učinkovitost, nezavisno od izbora.

U periodu koji je prethodio izborima, identifikovano je vrlo pažljivo manipulisanje temama od javnog značaja u digitalnim medijima. Naime, analiza pokazuje da je informativni prostor bio dominantno rezervisan za zabavno-nasilni tematski blok. To znači da su izbori i društveno-politički relevantne teme istisnute na informativnu marginu i u svega nekoliko medijskih portala, a u korist tema iz sfere zabave, rijalitija, života poznatih i sporta sa jedne strane, odnosno rata, nasilja, i vesti o nesrećama i tragičnim događajima, sa druge.

Skroman opseg izveštavanja o izborima sveden je na vesti o uspesima vlasti u različitim oblastima, događajima koje su inicirali, ali i perpetuiranjem informacija koje pojedini mediji generišu, a većina drugih distribuira kroz digitalni prostor. Tako se manipulisanje informativnim prostorom odvijalo kroz definisane uloge koje su mediji imali, bilo da kreiraju sliku vlasti ili da njenom favorizovanju doprinose daljim širenjem pažljivo konstruisane slike vlasti. Neizostavno, generičko-distributerske medijske uloge prepoznaju se i kada je reč o diskreditovanju opozicije, civilnog društva i retkih kritičkih i nezavisnih medija.

Afirmativna slika vlasti koju kreira većina onlajn medija nije istovetna, niti je intenzitet podrške uvek isti. Tabloidni onlajn mediji eksplicitno podržavaju vlast kroz narative koji obiluju mišljenjima naspram retkih činjenica, uključujući i senzacionalističke naslove koji već tradicionalno izražavaju divljenje, pohvale i pozive na podršku. Sličan medijski rad primećuje se i kod medija koji nemaju isključivo tabloidnu tradiciju, što ukazuje i na trend širenja podrške koju vlasti u Srbiji diktiraju u digitalnom medijskom pejzažu. Dodatno, favorizovanje vlasti odvija se i na implicitan način, tako što se manipulativnim odnosom prema društvenoj i političkoj stvarnosti pažljivo selektuju sadržaji koji doprinose promociji vlasti, uz potpuno ignorisanje kontroverznih tema.

Ipak, treba zabeležiti specifičan trend vesti o "digitalnim aktivnostima" predstavnika/ca vlasti u 2023. godini. Tako nisu izostale informacije o tome da je, primera radi, Aleksandar Vučić "objavio novi video na TikToku", uz parafraziranje i prenošenje samog videa, bez obzira na njegov isključivo promotivni karakter bez ikakve informativne vrednosti.

Deo sistemske manipulacije oslikava se i kroz upotrebu i predstavljanje mišljenja, komentara, promocije, osvrta - kao činjenica. Ovaj novinarski trend značajno doprinosi manipulativnom mehanizmu u kojem se vest redefiniše i uspostavlja na vrednostima koje ne uključuju nužno novost, činjenicu, javno relevantnu informaciju. Informativni prostor tako postaje polje stavova i to uglavnom bez debatnog potencijala, u kojem dominiraju osude, ocene, vrednovanja i slično.

Značajna odlika informativnog ambijenta u demokratskim društvima, a posebno u predizbornom periodu, jeste debata. Razmena argumenata omogućava racionalno razmatranje pitanja i problema od javnog značaja. Takođe, spektar argumenata omogućava građanima i građankama da donose odluke o tome kako će se odnositi prema društvenoj stvarnosti i političkom životu. U Srbiji, međutim, potpuno zatvaranje medija za bilo kakvu vrstu debate u kojoj bi se snagom

argumenata dovodili u pitanje potezi i odluke vlasti, anestezira javnost i deli je na konfrontirajuće strane u kojima jedna sasvim isključuje drugu. Digitalni svet potvrđuje da je struktura javnosti u Srbiji "za ili protiv vlasti", koja svakako nije ravnopravna, budući da politička i društvena moć koncentrisana u rukama vladajuće većine uključujući i resurse kao što su mediji, minimizira društveni i politički značaj opozicije i drugih oponirajućih glasova javnosti.

Sistemskim kreiranjem digitalnog informativnog ambijenta sačinjena je slika društvene zajednice čija se "sudbina" nalazi u rukama jednog čoveka. Aleksandar Vučić je centralni donosilac ("najboljih") odluka i kada su u pitanju teme od nacionalnog značaja, kao i specifični problemi pojedinaca koji se javno afirmišu kao ilustracije dobrobiti koju ceo "narod" ima zahvaljujući jednom čoveku. U tom mehanizmu uloge su podeljene između medija, aktera čije konfirmacije usklađeno doprinose ovoj slici, kao i samog Vučića čija je samoreprezentacija u poslednjem izbornom ciklusu augmentovana i TikTokom.

U PRVOM LICU

Bojana Jovanović, novinarka i zamenica urednika KRIK

SLAPP TUŽBE – NAJNOVIJE ORUĐE ZA OBRAČUN SA NOVINARIMA

Od kada smo kolege i ja osnovali KRIK 2015. godine nismo imali mirnu godinu kada su u pitanju pritisci. Otkrivanje koruptivnih poslova ljudi iz vlasti i njihovog najužeg kruga, veze koje imaju sa ljudima iz podzemlja, načini zaštite ljudi iz organizovanog kriminala ključne su stvari koje godinama kao istraživački novinari otkrivamo i na koje bacamo svetlo. Upravo to nas je bacilo u nemilost onih u čije poslove zalazimo, a koji su na važnim pozicijama u državi, vladari iz senke ili ljudi iz kriminalnog miljea pod zaštitom države.

Tako smo, tokom godina, bili pod različitim pritiscima – protiv nas su provladini mediji pokretali i vodili prljave medijske kampanje, javno nas targetirajući kao državne neprijatelje i objavljujući laži s pokušajem da nas diskredituju, u Skupštini su nas poslanici vladajuće partije javno optuživali da smo mafijaši i da peremo novac. Godinama nas prate agenti bezbednosnih službi, prisluškuju nam telefone i redakciju, članovima redakcije su obijane kuće i stanovi (policija nikada nije otkrila počinioce), prete nam na društvenim mrežama i pritiskaju nas na druge načine.

Pritisci se, međutim, menjaju. Poslednje oružje koje moćnici koriste da nas ućutkaju su tužbe – SLAPP tužbe, odnosno strateške tužbe protiv javnog učešća. Drugim rečima, u pitanju su neosnovane tužbe koje se podnose s namerom da nas preusmere na bavljenje samima sobom, da vreme trošimo na tužbu i suđenje, a ne na posao, da redakciju finansijski iscrpe, a novinare fizički i mentalno – sa krajnjim ciljem da nas zastraše i ućutkaju kako više ne bismo pisali o njima.

Ovakve tužbe su od 2021. godine postale gotovo uobičajena stvar u KRIK-u. Bilo je tužbi i ranije, ali su one bile izuzetak. Od pre tri godine pretvorile su se u pravilo, verujem, ukorak sa trendom u brojnim evropskim zemljama u kojima je takođe došlo do njihove ekspanzije. Do danas je u našu redakciju stiglo čak 13 tužbi – 10 parničnih, jedna krivična i dve pred privrednim sudom. KRIK nije izuzetak u Srbiji, iste pritiske trpe i kolege u BIRN-u, NIN-u, ali i u lokalnim medijima.

Tužbe su, u većini slučajeva, podneli ljudi iz vlasti ili njima bliski biznismeni. Tako, tužili su nas, između ostalih, Predrag Koluvija, optužen da je organizovao proizvodnju više od tonu i po marihuane; Bratislav Gašić, raniji direktor Bezbednosno-informativne agencije i ministar policije; Nikola Petrović, kum predsednika Srbije; Dijana Hrkalović, bivša državna sekretarka u MUP-u, ali i načelnici policijske Jedinice za zaštitu svedoka, tajkuni bliski vlasti, ljudi koji su se nalazili na Interpolovim poternicama, izdavač provladinog tabloida Kurira i međunarodna korporacija. Gotovo niko od njih pre podnošenja tužbe nije nam poslao upozorenje, nije tražio demanti niti se javio redakciji sa zahtevom za ispravku teksta. Uglavnom nisu želeli da pričaju sa nama, odnosno da nam daju komentare, ni pre objavljivanja priče.

Jedan od ključnih problema je to što ove tužbe nisu prepoznate u našem zakonodavstvu. Da jesu, situacija bi nesumnjivo bila povoljnija po nas. Ukoliko bi postojala anti-SLAPP regulativa, mi bismo sačuvali mnogo vremena, novca, ali i energije – u tom slučaju bi se pre početka postupka preispitivalo da li je u pitanju SLAPP tužba ili ne. Ako bi se ispostavilo da je u pitanju prva opcija, ona bi se odbacila, a u suprotnom bi se zakazalo suđenje. Budući da toga nema, svaka tužba se usvaja, a sudije je tokom suđenja ne posmatraju kao pritisak na novinare, već kao bilo koju parnicu. Drugim rečima, nema razlike između postupka u kome je KRIK tužio šef obaveštajne agencije Bratislav Gašić i suđenja u kome se, recimo, dvojica komšija tuže zbog međe.

Borba u sudnici svakako nije ravnopravna.

Naspram nas su ljudi koji su moćni i uticajni, bilo zbog položaja na kome se nalaze, bilo zbog svoje političke pripadnosti i pozadine, bilo zbog veza koje imaju u državnim strukturama.

Tako, u pojedinim postupcima, poput onog u kome nas je tužio Koluvija, suđenju prisustvuje, kao njegov advokat, čovek koji ima važnu ulogu u pravosuđu. Novopečeni advokat Vladimir Đukanović je uticajni član vladajuće stranke, ali je bio i narodni poslanik i predsednik skupštinskog odbora za pravosuđe koji igra važnu ulogu u izboru sudija i tužilaca. S obzirom na ove funkcije, samo njegovo prisustvo u sudnici veliki je pritisak.

Sa druge strane, same tužbe izazivaju velike probleme. SLAPP predstavlja i vid finansijskog pritiska i ekonomskog iscrpljivanja. Ovi postupci u Srbiji ne koštaju mnogo, poput recimo, postupaka u Velikoj Britaniji. Ali, kada imate 13 tužbi, troškovi se multiplikuju i značajno utiču na budžet organizacije. Poseban je slučaj sa malim, lokalnim medijima, jer oni imaju dosta manje budžete i ovakve tužbe jesu veliki finansijski problem i mogu da dovedu do zatvaranja medija.

Veći problem, međutim, za nas je trošenje vremena i energije. Svaka tužba zahteva podroban rad sa našom advokaticom na pripremi odgovora na tužbu, prikupljanju dokaza koje ćemo predložiti u svoju odbranu i koristiti tokom suđenja, pripreme za davanje iskaza ili svedočenje. To su zapravo dani (nekada i nedelje) potrošeni na tužbu, vreme i energija koji su otišli u nepovrat i uticaj na rad cele organizacije. U trenutku kada tužba stigne, zbog kratkih rokova za odgovor na nju, ona postaje prioritet i sve drugo trpi, ostavlja se sa stane – bilo da je to rad na istraživanju, sastanci sa novinarima, uređivanje tekstova, priprema za obavljanje intervjua ili objavljivanje istraživačke priče. Od tog trenutka postoji samo tužba jer jedino potpuno fokusirani možemo da se borimo, a svaki propust može kasnije mnogo da nas košta.

Upravo gubljenje postupka i jeste najveći strah. Ne zbog novca, nego zbog diskreditacije. Zbog situacije u pravosuđu i činjenice da Srbija nije zemlja u kojoj (i dalje) postoji vladavina prava, nije neizvesno da se i to desi. Postupak nećemo izgubiti jer smo napravili grešku, to nije moguće da se desi jer vodimo računa o tome da sve informacije budu tačne i istinite (zbog toga ih i proveravamo i imamo proces "provere činjenica"), da ispoštujemo novinarska načela i postupamo sa dužnom novinarskom pažnjom. Nekada to nije dovoljno, jer sudije presudu ne donose samo na osnovu dokaza i zakona već se vode drugim principima. Sudija, recimo, koja nas je osudila u prvostepenom postupku koji se vodio po Gašićevoj tužbi, kako smo kasnije otkrili, imala je političke veze – njen suprug bio je blizak bivšem ministru pravde Nikoli Selakoviću (ova presuda je ukinuta i slučaj dodeljen drugom sudiji).

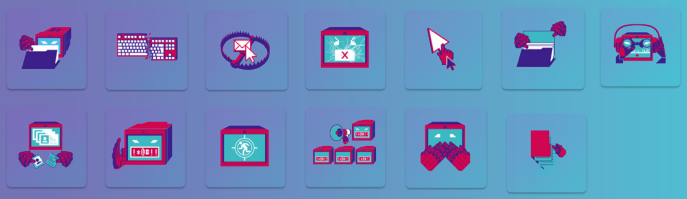
U slučaju da izgubimo postupak, to bi nam nanelo ogromnu štetu i negativan uticaj na reputaciju. Predstavnici vlasti koji sada lažima pokušavaju da nas diskredituju, u tom slučaju bi imali jako oružje u rukama – presudu na koju bi mogli da se pozovu.

Posledica ovakvih tužbi je i autocenzura. Sasvim je sigurno da se zbog SLAPP-a novinari često zapitaju da li uopšte i da objave priču ili tekst o nekome ko ih je već tužio (možda i nekoliko puta ili svaki put kada pišu o toj osobi). Stoga, ne bi bilo iznenađenje da nekada nešto prećute ili ne objave – samocenzurišu se kako bi se spasili buduće patnje koju SLAPP sobom nosi.

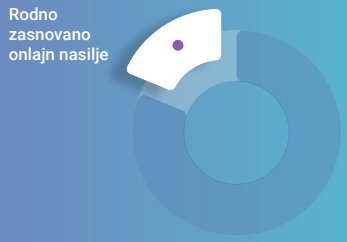
U KRIK-u je potpuno drugačija situacija. Baš zbog toga što znamo da je cilj tužbi autocenzura i ućutkivanje, trudimo se da budemo još glasniji. To znači da nastavljamo da istražujemo poslove, zloupotrebe, koruptivne ili kriminalne veze ljudi koji su nas tužili i pokazujemo im da njihovo najnovije oruđe ne radi – nismo zastrašeni i nećemo prestati da istražujemo i objavljujemo. Pokazujemo da smo spremni da se borimo i da ćemo da se odupremo svakom pritisku.

Bojana Jovanović je novinarka i zamenica urednika u KRIK-u. Dobitnica je mnogih međunarodnih priznanja za svoj istraživački rad i, kao i ostatak redakcije KRIK-a, ne ćuti pred nepravdom i zlostavljanjem koje novinarke i novinari u Srbiji trpe zbog svog etičkog, hrabrog i istinitog izveštavanja.

PREVARE, PRETNJE I MANIPULACIJE



20
SLUČAJEVA



Kao najskoriji dodatak monitoringu povreda digitalnih prava, predstavljena je nova kategorija koja se posebno odnosi na slučajeve rodno zasnovanog onlajn nasilja. Rodno zasnovano nasilje posredstvom tehnologije (gender based online violence) predstavlja samo produžetak tradicionalnih povreda ljudskih prava žena, devojčica i seksualnih manjina i to se jasno oslikava u slučajevima koji su zabeleženi tokom 2023. godine. Najveći broj zabeleženih povreda predstavljao je pretnje i diskriminatorni govor na društvenim mrežama, uključujući mizogine i homofobne uvrede. Ženske članice porodica opozicionih političara, novinara i aktivista su se takođe našle na meti uvreda i pretnji što dodatno potvrđuje ustaljenu patrijarhalnu podelu društva u kojoj se uvrede upućene ženama i drugim rodnim manjinama smatraju skoro standardnom praksom.

Simptomatično je da su uvrede na račun žena u politici, medijima i nevladinom sektoru skoro po pravilu zasnovane na degradiranju njihovih stavova i postupaka zbog njihovog roda. Nakon što je u julu objavljen spisak botova, odnosno osoba koje su na društvenim mrežama organizovano pružale podršku Srpskoj naprednoj stranci i učestvovale u deljenju prorežimske propagande, korisnici su brzo krenuli u misiju razotkrivanja identiteta svih onih koji su se našli iza

ovih naloga. Naravno, nije neobično da je pored oštrih uvreda koje su bile upućene svima na spisku, i ovde bila uočljiva njihova rodna dimenzija. Javnost je mnogo oštrije kritikovala žene koje su bile na spisku - delile su se njihove fotografije, često uz komentare koji bi se u najmanju ruku mogli okarakterisati kao seksualno uznemirujući i rodno diskriminišući. Stiče se utisak da je njihov prekršaj bio ne samo to što su odlučile da podršku pruže vlasti, već i njihov rod. Iako se često ponavlja da političke ili bilo kakve nesuglasice nisu opravdanje za napad na neistomišljenike na osnovu rodnih karakteristika ili seksualne orijentacije, ovo nažalost ne znači da se sa ovakvim slučajevima i dalje ne susrećemo redovno.

Zloupotreba intimnih sadržaja bez saglasnosti takođe je jedan od najpotresnijih i potencijalno najopasnijih problema sa kojima se žene u Srbiji sve učestalije susreću u digitalnom prostoru. Jedan od najčešćih oblika ovakve vrste zlostavljanja je zloupotreba intimnih sadržaja od strane bivših partnera, poznatiji i pod nazivom osvetnička pornografija. Iako ovaj naziv sam po sebi može biti problematičan, jer implicira nekakvu pornografsku komponentu intimnog sadržaja koji je bez saglasnosti objavljen (u nekim slučajevima i napravljen), to je termin koji je trenutno najzastupljeniji u razgovorima o ovom fenomenu. Iako su neke zemlje počele sa uvođenjem odvojenog krivičnog dela koji se bavi zloupotrebom intimnog sadržaja (uključujući i Hrvatsku), daleko smo od društvenog konsenzusa oko štete koja se nanosi osobama koje ovakvo nasilje prežive. Srbija se ne razlikuje preterano od drugih zemalja po tom pitanju, jer deluje da svuda problem leži u simultanom nedostatku razumevanja i saosećanja od strane nadležnih organa i nedovoljne tehnološke pismenosti, kao i letargičnog odgovora pravosuđa i odsustva političke volje da se bliže pozabavi ovim rastućim problemom.

Kao što se da zaključiti iz analize slučajeva, tehnološki izvršeno rodno zasnovano nasilje ne podleže ni socio-ekonomskom statusu, godinama niti političkom opredeljenju i samim tim je skoro nemoguće obuhvatiti sve incidente. Česta anonimnost izvršitelja neretko pruža

dodatan vetar u leđa za dalje napade i maltretiranje, a nedovoljna zakonska regulisanost ovakvih incidenata može biti obeshrabrujuća za one koje se nađu na oštećenoj strani. Drugi problem predstavlja (ne)poverenje da će na ovakve slučajeve reagovati policija i tužilaštvo, kao i same kompanije koje su vlasnice društvenih platformi. Neretko se događa da od Fejsbuka, Instagrama, Tiktoka ili Telegrama ili nema odgovora ili su u pitanju opšti odgovori na prijave u kojima se navodi da su njihovi kapaciteti preopterećeni brojem prijava koje dobijaju i da nemaju procenu kada će pristupiti slučaju. Čak i kada do reakcije dođe i u najvećem broju slučajeva ovi nalozi budu ugašeni, ne postoji nikakav sistem zaštite koji sprečava kreiranje novih naloga i ponovnog upadanja u ciklus zlostavljanja od strane izvršilaca.

U martu prošle godine, skoro 30 žena podelilo je svoja iskustva nakon što su saznale da su se njihove intimne fotografije i video snimci našli na nekim od mnogobrojnih Telegram grupa koje su otkrivene 2021. godine. Svrha ovih grupa bilo je deljenje intimnih sadržaja, uglavnom bivših partnerki, među više od 50.000 ljudi, koliko je brojala jedna od najvećih grupa. Prema BIRN-ovom istraživanju, otkriveno je čak 16 grupa od kojih su neke bile aktivne čak i dve godine nakon što je javnost saznala za njih. Jedan od glavnih problema je to što osvetnička pornografija i dalje nije prepoznata kao krivično delo u Srbiji i samim tim je ove slučajeve ponekad nemoguće procesuirati. Trenutno je potrebno da se utvrde elementi ucene, uznemiravanja ili proganjanja kako bi državni ograni preduzeli odgovarajuće mere i pokrenuli postupke protiv počinilaca. Uprkos velikoj prašini u javnosti povodom ovog slučaja, bilo kakvo sistemsko rešenje je izostalo, a žene i devojke su i dalje izložene riziku od nekažnjivog zlostavljanja u digitalnom prostoru.

Uz rast popularnosti generativne veštačke inteligencije, rastu i zloupotrebe u polju rodno zasnovanog onlajn nasilja. Na raskrsnici tehnologija koje omogućavaju generisanje veštačkih sadržaja uz pomoć autentičnih slika i snimaka, poznatih kao dipfejk (deepfake) tehnologija, i osvetničke pornografije, postavljaju se mnoga pitanja

na koja je i dalje teško pronaći odgovore. Ni državni organi, ni tehnološke platforme nisu još pronašli adekvatan način da se suoče sa ovim rastućim trendom, i sve dok se to ne dogodi veliki broj žena i devojaka naći će se u nemogućim situacijama. Ovo je svakako potvrđeno kada je prošle godine nepoznata osoba otvorila naloge na različitim društvenim mrežama radi targetiranja devojaka iz beogradskog naselja Batajnica. Na ovim nalozima objavljene su slike i snimci devojaka, uključujući seksualno eksplicitne, koji su najvećem broju slučajeva bili praćeni uvredljivim i zlostavljačkim komentarima. Sa tih naloga su objavljivani i eksplicitni snimci devojaka napravljeni posredstvom generativne veštačke inteligencije. Mnoge objave pratili su i lični podaci devojaka, njihova imena, adrese na kojima rade, pa čak i kućne adrese. U sličnom scenariju, nalozi su prijavljivani više puta ali su ili ostajali aktivni ili, u slučaju da jesu deaktivirani, pojavljivali su se novi koji su samo nastavljali tamo gde su prethodni stali. Iz policije je izostala hitna reakcija, a ni Tužilaštvo za visokotehnološki kriminal nije bilo preterano ažurno u obaveštavanju devojaka o razvoju slučaja. Doduše, ovaj slučaj je delimično dobio zaključak pozitivan za oštećene devojke, ali je malo verovatno da će se incident poslužiti kao motiv institucijama da razmotre odgovarajuće sistemske promene.

Teodora Uzelac, prebroditeljka rodno zasnovanog onlajn nasilja u slučaju Batajnica

VEŠTAČKI SADRŽAJ, PRAVE OPASNOSTI

„Ne drami, nije tako strašno.“ „On se šali.“ „Ti si kriva.“ „Izazvala si ga.“ „Zašto uopšte imaš društvene mreže?“ „Zaslužila si.“ „Prija ti.“ „Zašto nisi prijavila do sad?“ Ljudi zaključuju i pitaju, a ti uplakana, preplašena i postiđena tražiš način da se opravdaš i odgovoriš. „Možda i nije tako strašno.“ „Možda ja ne razumem šalu.“ „Šta ako ga jesam izazvala?“ Počneš da preispituješ sebe, jer koliko god glasno da vičeš - društvo ne želi da te čuje. Tako su se osećale devojke iz Batajnice, čiji su privatni podaci i fotografije objavljivani na Instagramu i TikToku, u najgnusnijem kontekstu.

Svaka nova objava je još jedan šamar. Ne znaš ko te udara. Modrica nema. Sve što ti se dešava je neopipljivo, neuhvatljivo i nestvarno. A to radi stvarna osoba, kojoj je za dva dana, na TikToku, podršku pružilo 13 hiljada stvarnih ljudi. Za sve njih, ti nisi stvarna - ti si seksualizovani objekat, predmet ismevanja i odvratnih komentara. Šamar postaje 13 hiljada puta jači, a tvoje modrice su i dalje nevidljive.

Kada se profil prvi put pojavio, bila sam četrnaestogodišnja devojčica. Sada sam dvadesetogodišnja devojka. „Stvaralac“ je postajao „kreativniji“, a sadržaj sve ogavniji i izopačeniji. U julu 2023. godine, setio se veštačke inteligencije. Videla sam sebe kako izgovaram rečenice, koje ne mogu ni da smislim. Videli su i moji roditelji, prijatelji, kolege sa fakulteta, komšije i poznanici. Tada srastete sa sramom. Njegova senka vas prati gde god da idete. „Zašto ćutiš?“ Nijednim

odgovorom nisam mogla da se opravdam ni sama sebi. Podnela sam krivičnu prijavu. Obratila sam se medijima. Prvi su ćutali, a većina drugih je o ovome izveštavala kao o skandalu u rijaliti programu.

Posle dva meseca, pozvana sam da dam izjavu. „Konačno", pomisliš. Odeš u MUP, a tamo te dočeka dvoje ljudi, gomila papira, koje si priložila kao dokaz i reči „Nemoguće da ga ne poznaješ". Sa knedlom u grlu, objašnjavaš da si žrtva, a ne nasilnik. Tako dobiješ odgovor na pitanje „Zašto nisi prijavila?". Optuže te da sarađuješ sa nekim ko te šest godina maltretira. Vratiš se kući. Pokušavaš da živiš normalno, dok se na ulici osvrćeš za sobom, ne bi li nekako uočila lice, koje stoji iza tog profila. Mnogo hiljada ljudi zna ko si, kako izgledaš i gde živiš. Ne znaš šta nekome od njih može da padne na pamet, kada te vidi - jer „ti to voliš" i „ti si to zaslužila". Nisam. Ni ako nosim kratku suknju, ni ako se u njoj slikam - nisam. Mnogo vremena mi je trebalo da to shvatim, jer mi je društvo govorilo suprotno. Početkom novembra, drugarica mi je poslala link. „Mladić uhapšen zbog sumnje da je proganjao i polno uznemiravao devojke u Batajnici", piše RTS. Čitala sam desetinama puta, ne bih li ubila nevericu. Neko je ipak video moje modrice. B.B. (24). Borba protiv vetrenjača dobijala je sve više smisla. Dve nedelje kasnije, dobila sam poziv iz Višeg javnog tužilaštva, gde sam dala iskaz. Pridružila sam se procesu suđenja, zajedno sa još nekim devojkama. Ubrzo sam dobila poziv za glavni pretres. Nestrpljivo sam iščekivala taj dan, ali svakim korakom ka Palati pravde, disanje je postajalo sve teže. Sedela sam ispred sudnice, kada ga je doveo policajac. B.B. (24) ima lice. To je lice nasilnika. To je osoba koja stoji iza moje šestogodišnje patnje.

Koliko god mislili da ste spremni za suočavanje, nikada niste dovoljno spremni. Otišla sam sama. Bez roditelja, bez advokata. Druge devojke nisu došle. Sedela sam tri mesta od njega. Mislila sam da neću moći da skinem pogled sa njegovog lica, a nisam mogla ni da ga pogledam. Glavni pretres je odložen. B.B. (24) je podneo žalbu na pritvor. Možda mu je pravo na slobodu kretanja neosnovano uskraćeno i to mu smeta. Razumem - zaista smeta kada

neko gazi vaša prava. Pre nego što smo izašli iz sudnice, policajac mu je stavio lisice. Simbolično, ruke koje su stajale iza tog profila, ipak nisu neuhvatljive. To me raduje, lično, ali i kao devojku koja je deo ovog društva. Možda posle ovog slučaja shvatimo da digitalno nasilje nikada ne ostaje u sferi „neopipljivog". Ono nije šala, nije samo jedan komentar ili fotografija - to je nasilje. Ono se uliva i preplavljuje „stvaran" život žrtve. Zbog toga je važno da i nasilnik, koji se krije iza lažnog korisničkog imena i profilne fotografije, „u stvarnosti" i odgovara. Digitalno nasilje je stvarno nasilje.

Teodora Uzelac godinama vodi borbu protiv nasilnika koji je anonimno preko mreže naloga seksualno zlostavljao i uznemiravao nju i mnoge druge devojke iz Batajnice. Uprkos brojnim preprekama s kojima se susrela, Teodora nije odustajala od svoje borbe. Nakon šest godina, počinilac je konačno uhvaćen i procesuiran. Teodorina priča personifikuje ovakve slučajeve nasilja i može služiti kao podsetnik da, iako smo svesni da su te slike i snimci lažni, trauma koju izazivaju je veoma stvarna.

Ako se vi, ili bilo ko koga poznajete nađete na meti ovakvih zloupotreba, na raspolaganju su vam brojne organizacije u Srbiji koje se bave zaštitom ženskih prava i pružanjem svih vrsta pomoći, od psihološke do pravne. Iako distribucija intimnih sadržaja bez saglasnosti i dalje nije posebno krivično delo u Srbiji, postoje druga dela po kojima se to može goniti. Zbog toga je važno svaki slučaj prijaviti.