SHARE@ WORK 2016

MONITORING DIGITALNIH PRAVA I SLOBODA U SRBIJI

SHARE FOUNDATION

SHARE@ WORK 2016

MONITORING DIGITALNIH PRAVA I SLOBODA U SRBIJI

SHARE FOUNDATION

IMPRESUM:

SHARE@WORK 2016 - MONITORING DIGITALNIH PRAVA I SLOBODA U SRBIJI
SHARE FONDACIJA, MAJ 2017.
UREDNICI: ĐORĐE KRIVOKAPIĆ, VLADAN JOLER
AUTORI: ĐORĐE KRIVOKAPIĆ , JELENA ADAMOVIĆ, PETAR KALEZIĆ, DANILO KRIVOKAPIĆ, NEVENA KRIVOKAPIĆ, SONJA MALINOVIĆ, BOJAN PERKOV, ANDREJ PETROVSKI
OBRADA TEKSTA: MILICA JOVANOVIĆ
DIZAJN I PRELOM: OLIVIA SOLIS VILLAVERDE

ŠTAMPARIJA: NS PRESS DOO NOVI SAD
TIRAŽ: 200

PODRŠKA PROJEKTU:

Kingdom of the Netherlands

Министарство трговине, туризма и телекомуникација

Ovaj projekat je finansiran od strane Evropske unije.

Ovaj dokument je proizveden u okviru granta koji finansira Evropska unija. Sadržaj dokumenta je isključiva odgovornost SHARE Fondacije i ni u kom slučaju ne odražava stavove Evropske unije.

CIP - Каталогизација у публикацији

Библиотека Матице српске, Нови Сад

004.738.5:351.083.8(497.11)

SHARE@ work 2016 : monitoring digitalnih prava i sloboda u Srbiji / [autori Đorđe Krivokapić ... [et al.] ; urednici Đorđe Krivokapić, Vladan Joler]. - Novi Sad : Share fondacija, 2017 (Novi Sad : NS press). - 149 str. : ilustr. ; 24 cm

Tiraž 200. - Napomene i bibliografske reference uz tekst.

ISBN 978-86- 89487-10- 7

1. Кривокапић, Ђорђе

а) Интернет - Заштита података - Србија

COBISS.SR-ID 314217991

1. Úvod

1.1. O SHARE FONDACIJI

Posle serije uspešnih SHARE konferencija o internet kulturi i aktivizmu, sa više od 1000 učesnika u Beogradu (2011, 2012) i Bejrutu (2012), saradnja i zajedničko iskustvo stečeno na ovim događajima inicirali su osnivanje zajednice koja će se kontinuirano baviti istraživanjem i zagovaranjem standarda ljudskih prava u digitalnom okruženju. Kao neprofitna organizacija, SHARE Fondacija je osnovana 2012. godine, s ciljem unapređenja ljudskih prava i sloboda u digitalnom okruženju i promovisanja pozitivnih vrednosti otvorenosti i decentralizacije Mreže, kao i slobodnog pristupa informacijama, znanju i tehnologiji. Primarne oblasti delovanja SHARE Fondacije su sloboda izražavanja na internetu, informaciona privatnost, digitalna bezbednost i otvoren pristup znanju.

Naš multidisciplinarni tim čine pravnici, umetnici, novinari i IT stručnjaci. Fondacija je od osnivanja organizovala desetine konferencija, skupova i radionica u Srbiji i inostranstvu, kojima su pristustvovali vodeći aktivisti i stručnjaci za digitalna prava i slobode. Kao deo civilnog društva, SHARE Fondacija redovno učestvuje u javnim raspravama povodom svih relevantnih propisa koji mogu imati uticaj na digitalna prava i slobode građana Srbije. U okviru izdavačke delatnosti, Fondacija je objavila više od deset info-vodiča i drugih besplatnih publikacija. Tokom prethodne dve godine istraživačka laboratorija, SHARE Lab, objavila je niz istraživanja o nevidljivim infrastrukturama interneta u Srbiji, informacionom ratovanju, metapodacima mejl komunikacije, izborima u onlajn okruženju, Fejsbukovim ,,algoritamskim fabrikama'', itd. Kako bi široj javnosti ukazala na značaj poštovanja ljudskih prava u digitalnom okruženju, SHARE Fondacija je u završnoj fazi produkcije dokumentarne TV serije od 10 epizoda u kojoj o ključnim pitanjima, poput slobode izražavanja, zaštite privatnosti, novih medija i digitalne bezbednosti, govori više od 50 domaćih i međunarodnih stručnjaka.

Od marta 2017. godine, SHARE Fondacija je članica Evropske mreže za digitalna prava (European Digital Rights, EDRi), evropske koalicije od preko 30 organizacija za zaštitu ljudskih prava u digitalnom okruženju iz Evrope, ali i prekookeanskih država. SHARE Fondacija je i deo #newmednet neformalne mreže pravnika, novinara, aktivista i akademika iz 14 zemalja Centralne i Jugoistočne Evrope, osnovane 2013. godine, kao i Globalne koalicije za mrežnu neutralnost (Global Net Neutrality Coalition). Posle tri godine pružanja besplatne pravne i tehničke pomoći onlajn medijima i organizacijama civilnog društva u Srbiji, SHARE Fondacija je u aprilu 2017. osnovala prvi Poseban centar za prevenciju bezbednosnih rizika u informaciono komunikacionim sistemima (CERT) u Srbiji.

Doprinos SHARE Fondacije afirmisanju oblasti od značaja za digitalna prava i slobode prepoznao je i Poverenik za informacije od javnog značaja i zaštitu podataka o ličnosti, koji je krajem januara 2017. Fondaciji uručio zahvalnicu za izuzetan doprinos afirmisanju prava na zaštitu podataka o ličnosti. Upravitelj Vladan Joler primio je zahvalnicu u ime Fondacije.

1.2. UPOTREBA IKT U SRBIJI

PREPORUKE

Izrada i usvajanje strateških dokumenata u oblasti razvoja širokopojasnog pristupa i digitalne uključenosti, sprovođenje kontinuiranih, sveobuhvatnih istraživanja upotrebe i primene IKT u opštoj i segmentiranoj populaciji. Uspostavljanje ,,digitalnog dijaloga'' javne uprave, akademije, industrije i civilnog sektora, u pravcu identifikacije problema i utvrđivanja razvojnih prioriteta, kao i modela primene domaćeg prava na internetu.

1.2.1. OPŠTA POPULACIJA: DIGITALNO RASLOJAVANJE I USPOREN RAST

Prema poslednjim istraživanjima Republičkog zavoda za statistiku, od oko sedam miliona stanovnika Srbije[1] nešto više od 64% ima pristup internetu, dok oko 86% od ukupnog broja građana sa pristupom, koristi internet svakog ili skoro svakog dana.[2] Ponašanje, navike i trendovi u korišćenju interneta, međutim, retko su predmet istraživanja. Zainteresovanoj javnosti su na raspolaganju uglavnom samo periodične statistike globalnih merenja internet saobraćaja ili povremene sondaže privatnih aktera na domaćoj sceni, o čijoj se metodologiji malo zna. Najređa su naučna istraživanja fokusirana na pojedine slojeve zajednice, koja prevazilaze standardne anketne upitnike.

Zvanične statistike nesumnjivo ukazuju da se u Srbiji poslednjih godina produbljuje tzv. digitalni jaz, socioekonomski rizik koji ugrožava slobodan i ujednačen pristup digitalnim tehnologijama. Unutar društva, ove razlike najizraženije su u odnosu na marginalizovane i ranjive grupe: osobe sa invaliditetom, romsku populaciju, stanovništvo ruralnih sredina. Istovremeno, usporen rast i razvoj u oblasti informaciono-komunikacionih tehnologija Srbiju drže u položaju žrtve globalnog digitalnog jaza.

U regionalnom izveštaju Svetske banke za Evropu i Centralnu Aziju, predstavljenom početkom marta 2017, Srbija je smeštena u grupu zemalja sa

1 Procena broja stanovnika, od 01.01.2016: 7.076.372, RZS http://www.stat.gov.rs/WebSite/Public/PageView.aspx?pKey=2

2 Upotreba informaciono-komunikacionih tehnologija u Republici Srbiji, 2016. http://webrzs.stat.gov.rs/WebSite/repository/documents/00/02/25/89/ICT2016s.pdf

najvišom cenom fiksnog interneta (više od 25 dolara po paritetu kupovne moći).[3]

Vlada Srbije je 2009. godine donela Strategiju razvoja širokopojasnog pristupa u Republici Srbiji do 2012. godine, zajedno sa pratećim akcionim planom. Ovim dokumentima predviđene su mere za povećanje socijalne uključenosti: izrada katastra i plana za efikasno korišćenje telekomunikacione infrastrukture, izrada modela za podsticanje razvoja tržišta širokopojasnog pristupa, integracija osnovnih i srednjih škola u jedinstvenu mrežu, povezivanje ustanova kulture na akademsku mrežu, obezbeđivanje javne dostupnosti širokopojasnog pristupa korisnicima u prostorijama javnih ustanova i organima državne uprave. Predviđene mere nisu realizovane. Nadležno ministarstvo je krajem 2013. izradilo nacrt nove strategije razvoja širokopojasnog pristupa, ali ona nije usvojena. Na tribini održanoj početkom 2017. godine u Privrednoj komori Beograda, saopšteno je da država nema novca, ali da se traže načini za podsticaj provajderima da ulažu sopstvena sredstva u razvoj širokopojasne veze, s neposrednim ciljem od 70% pokrivenosti teritorije.[4]

Podaci Republičkog zavoda za statistiku govore da računar poseduje 65,8% domaćinstava u Srbiji, što čini povećanje od 1,4% u odnosu na 2015, a 2,6% u odnosu na 2014. godinu.[5] Zastupljenost računara u domaćinstvima varira u zavisnosti od teritorijalne celine: u Beogradu iznosi 75,9%, u Vojvodini 67,7%, a u centralnoj Srbiji 59,4%. Razlike se mogu uočiti i kada se uporedi zastupljenost računara u urbanom i ruralnom delu Srbije: 73,3% naspram 54%. Statistika govori da se u odnosu na 2015. godinu ovaj jaz neznatno povećao, na šta ukazuju i stope rasta zastupljenosti računara u urbanom (2,2%) i ruralnom (0,1%) delu Srbije.

Najdrastičniji digitalni jaz izražen je kod populacije sa invaliditetom koja, prema popisu iz 2011, čini 8% stanovništva u Srbiji. Podaci iz Izveštaja o digitalnoj uključenosti govore da računar i internet ne koristi 90,2% od ukupnog broja osoba sa invaliditetom. Od ukupne populacije sa invaliditetom u Srbiji, računarski pismene osobe čine svega 5%, dok internet koristi nešto manje od 9%.[6]

Kada je reč o opštoj populaciji, po podacima Republičkog zavoda za statistiku, 64,7% domaćinstava poseduje internet priključak, što čini povećanje od 0,9% u odnosu na 2015, a 1,9% u odnosu na 2014. godinu.[7] Zastupljenost internet priključka najveća je u Beogradu i iznosi 73,1%. U Vojvodini ona iznosi 68,7%, a u centralnoj Srbiji 57,9%.

3 ,,Ubiranje digitalne dividende: Doprinos interneta razvoju u Evropi i Centralnoj Aziji'', str 62. https://openknowledge.worldbank.org/bitstream/handle/10986/26151/9781464810251.pdf

4 Upotreba računara u Srbiji http://rs.n1info.com/a224076/Sci-Tech/Upotreba-racunara-u-Srbiji.html

5 Upotreba informaciono-komunikacionih tehnologija u Republici Srbiji, 2016. http://webrzs.stat.gov.rs/WebSite/repository/documents/00/02/25/89/ICT2016s.pdf

6 Izveštaj o digitalnoj uključenosti u Republici Srbiji u periodu 2011-2014. godine http://socijalnoukljucivanje.gov.rs/wp-content/uploads/2015/03/Izvestaj-o-digitalnoj-ukljucenosti.pdf

7 Broj korisnika interneta povećao se za 1,4 u odnosu na 2015, za 3,9 u odnosu na 2014, a za 12,3 u odnosu na 2013. godinu.

Poređenja radi, granicu od 55% domaćinstava sa internet priključkom EU je prešla 2007. dok je 2014. ovaj procenat iznosio 83%.[8] Najviša stopa zabeležena je u Luksemburgu i Holandiji (97%) a najniža u Bugarskoj (64%), Grčkoj (69%) i Rumuniji (72%).[9]

Ekonomski jaz u Srbiji čini značajan faktor za pristup internetu. Internet priključak većinom poseduju domaćinstva koja imaju mesečni prihod iznad 600 evra (94,7%), dok učešće domaćinstava sa prihodom do 300 evra iznosi svega 46,1%. Za pristup internetu, građani Srbije najčešće koriste mobilni telefon (76,5%), 72% domaćinstava pristupa internetu koristeći personalni računar, dok 49,3% domaćinstava u tu svrhu koristi laptop. Broj domaćinstava koja pristupaju internetu pomoću mobilnog telefona povećao se za 8,6% u odnosu na 2015. godinu. Od ukupnog broja domaćinstava koja poseduju internet priključak, DSL (ADSL) poseduje 45,5%, kablovski internet 45,3%, a modemsku konekciju 1,2% domaćinstava.

Širokopojasnu internet konekciju ima 57,8% domaćinstava što, prema statistici, čini povećanje od 1,8% u odnosu na 2015, a 2,7% u odnosu na 2014. godinu. Zastupljenost ove vrste internet konekcije najveća je u Beogradu i iznosi 68,5%, u Vojvodini 61%, a najmanja je u centralnoj Srbiji i iznosi 50,4%. Na nivou EU, 2016. je 83% domaćinstava imalo fiksnu i/ili mobilnu širokopojasnu konekciju.[10]

Rezultati istraživanja Republičkog zavoda za statistiku među preduzećima pokazuju da 99,8 % preduzeća na teritoriji Republike Srbije koristi računar u svom poslovanju. 98,6% preduzeća koristi elektronske servise javne uprave, što čini povećanje od 4,1% u odnosu na 2015, a 6,6% u odnosu na 2014. godinu. Tu mogućnost ne koristi 1,4% preduzeća. Tokom 2015. godine 41% preduzeća u Republici Srbiji naručivalo je proizvode/usluge putem interneta, što čini smanjenje od 0,7% u odnosu na 2014. godinu, a povećanje od 0,6% u odnosu na 2013. godinu. Statistika Republičkog zavoda pokazuje da je samo 23,3% preduzeća tokom 2015. primalo porudžbine (izuzev imejl-porudžbina) putem interneta. 9,3% preduzeća plaća usluge klaud (cloud) servisa.

1.2.2. SAOBRAĆAJ, TRENDOVI I TOKOVI

Jasno je da građani Srbije značajan deo vremena na internetu provode na nekoliko većih medijskih portala i društvenih mreža, ali nije poznato šta tamo rade - da li radije čitaju tekstove ili gledaju snimke pojedinih vesti; da li ih više zanimaju komentari čitalaca, forumi ili druge, komercijalne sekcije medijskog sajta; ne zna se, konačno, koliko se jedinstvenih poseta ovim

8 Digitalna ekonomija i društvo, statistika - domaćinstva i pojedinci http://ec.europa.eu/eurostat/statistics-explained/index.php/Digital _ economy _ and _ society _ statistics _ - _ households _ and _ individuals

9 Internet pristup i upotreba, statistika - domaćinstva i pojedinci http://ec.europa.eu/eurostat/statistics-explained/index.php/Internet _ access _ and _ use _ statistics _ - _ households _ and _ individuals

10 Internet pristup i upotreba, statistika - domaćinstva i pojedinci http://ec.europa.eu/eurostat/statistics-explained/index.php/Internet _ access _ and _ use _ statistics _ - _ households _ and _ individuals

sajtovima zapravo generiše preko inficiranih uređaja, podešenih za tzv. botovanje.[11]

Treba imati u vidu da nešto više od tri miliona građana Srbije koristi internet svakog ili skoro svakog dana.[12] Po metrici kompanije Aleksa (alexa.com), koja obuhvata globalne servise i njihove lokalizovane verzije, tri najpopularnija internet servisa su Gugl pretraga, Jutjub video platforma i društvena mreža Fejsbuk. Blic.rs je prvi domaći sajt na ovoj listi (peto mesto), a slede Vikipedija i globalni porno servis Bongakams.[13] U okviru 20 najposećenijih sajtova nalaze se 2 pretraživača, 3 društvene mreže, 5 onlajn medija, 5 platformi za kolaborativnu razmenu sadržaja i znanja, te 4 platforme za elektronsku trgovinu.[14]

Kompanija ''Gemius Audience'' mesečno objavljuje listu najposećenijih sajtova u Srbiji prema nepouzdanom sistemu merenja[15], ali se lista delimično poklapa sa statistikom globalnog indeksa Aleksa. Računajući samo posete upućene sa desktop uređaja, prve tri najposećenije domaće adrese u januaru 2017. pripadale su sajtovima medija - Blic.rs (1.837.924 realnih korisnika), Kurir.rs (1.511.200) i B92.net (1.089.862).[16] Prema Gemijusovoj listi, sajt za onlajn posredovanje u trgovini, kupujemprodajem.com, u januaru ove godine nalazio se na četvrtom mestu sa 1.001.838 realnih korisnika. Sledeći ove vrste bio je polovniautomobili.com (sedmo mesto, 679.079 realnih korisnika). Među prvih deset nalaze se još i Telegraf.rs i sajt dnevnog lista Večernje novosti.

Usled nedostatka podataka za prethodne godine[17] nije moguće pratiti posećenost sajtova u kontekstu različitih vektora uticaja, rasta upotrebe interneta, na primer, novih zakonskih rešenja koja regulišu različite onlajn aktivnosti ili masovnije pojave astroturfinga[18], usmerenog na veće medijske portale.

Kada je reč o korišćenju društvenih mreža u opštoj populaciji, prema nezvaničnim statistikama koje računaju na oko 4,7 miliona korisnika interneta

11 Repetitivne operacije poput automatskog 'lajkovanja', postovanja i ocenjivanja komentara, i slično.

12 Upotreba informaciono-komunikacionih tehnologija u Republici Srbiji, 2016. http://webrzs.stat.gov.rs/WebSite/repository/documents/00/02/25/89/ICT2016s.pdf

13 Najposećeniji sajtovi u Srbiji http://www.alexa.com/topsites/countries/RS

14 Gugl se pojavljuje u okviru 20 sajtova 2 puta pod domenima .rs i .com, te stoga zbir po kategorijama iznosi 19.

15 Početkom marta 2017. nacionalno udruženje digitalnih oglašivača ,,IAB Serbia'' javno je upozorilo kompaniju Gemijus na nepravilnosti prilikom merenja internet saobraćaja, zahtevajući ispravku počev od decembra 2014. Relevantni podaci za mobilni i ukupan saobraćaj očekuju se tek u maju 2017, dok se desktop posete mogu tretirati kao relativno pouzdane http://iab.rs/en/saopstenje-iab-serbia-komiteta-za-audience-measurement/

16 Gemius Audience http://www.audience.rs/; poseta nije geografski raslojena.

17 U prvoj polovini 2015. Gemijusova lista više liči na nasumični popis, bez merljivih indikatora.

18 Prikrivena promocija političkih, verskih, reklamnih i drugih poruka u vidu autentičnog mišljenja građana; u internet okruženju podrazumeva organizovano komentarisanje, šerovanje, glasanje.

u Srbiji, gotovo 3,5 miliona koristi Fejsbuk.[19] Za ovu platformu opredeljeno je 91,52% korisnika društvenih mreža dok Tviter, koji u javnoj sferi zauzima posebno mesto zbog brzine komunikacije i pretraživosti, okuplja svega 4,06% korisnika društvenih mreža u Srbiji.[20]

Mada je danas praćenje cirkulacije tema i ključnih pojmova znatno olakšano različitim digitalnim alatima, i dalje nedostaju podaci koji se tiču samog sadržaja javne komunikacije na internetu. Neke indicije o javnom diskursu mogu se izvesti iz godišnjih statistika globalnih servisa ili uz pomoć alata integrisanih u ove servise, kao što je Gugl pretraga: ,,Na prvom mestu tražimo zabavu i način da popunimo slobodno vreme (dominiraju igrice i sajtovi za zabavu sa ukupno 20 pojmova pretrage). Na drugom mestu su alati komunikacije i rada (17 pojmova). Na trećem mestu su mediji i informisanje sa ukupno 15 pojmova.''[21]

1.2.3. NADLEŽNOST SRBIJE NA INTERNETU

Regulatorni domet države na internetu može se praktično ispitati analizom 100 sajtova koje građani Republike Srbije najčešće posećuju, prema podacima globalnog servisa za analitiku mrežnog saobraćaja, Aleksa.

Najpre se može uočiti da se samo jedna četvrtina (24 sajta) nalazi na srpskom .rs domenu, dok su ostali sajtovi uglavnom na top level domenima (59 .com, osam na .net, dva na .org, itd).

Kada je reč o registrovanim vlasnicima domena, uočava se da 15 sajtova ima zaštitu privatnosti vlasnika, dok je od poznatih vlasnika 35 sa teritorije Srbije, 29 sa teritorije SAD, po dva sa teritorije pet dodatnih jurisdikcija (Irska, Hrvatska, Malta, Kosovo, Britanija), dok su ostali sa teritorije još 11 zemalja.

Ukoliko se posmatra ko je na veb stranici označen kao lice koje upravlja samom platformom, ispostavlja se da 10 sajtova nema naznačeno niti jedno lice u tom pogledu, 40 ima označeno isto lice koje je vlasnik domena, dok kod 50 postoji razlika u manjoj ili većoj meri, to jest ili je reč o odnosu ,,majka–ćerka'' firma ili ne postoji jasna veza između registrovanog vlasnika domena i lica označenog na sajtu. Pregledom poznatih lica koja stoje iza veb platformi može se zaključiti da jedna trećina potiče iz SAD (34) i Srbije (33), dok su ostali raspoređeni u Britaniji (4), Malti, Kanadi, Kosovu, Kipru (2) i drugim državama.

Pregledom hosting kompanija čije usluge koristi 100 najposećenijih sajtova u Srbiji, gotovo polovina je odabrala hosting kompanije iz SAD (48), oko jedne četvrtine ima poverenje u srpske hosting kompanije (23), dok su sledeće po izboru kompanije u Nemačkoj i Holandiji (po 7).

19 Internet korisnici, statistika http://www.internetworldstats.com/stats9.htm

20 Statistika društvenih medija u Srbiji http://gs.statcounter.com/social-media-stats/all/serbia/#monthly-201702-201702-bar

21 ,,Šta je Srbija guglala u 2016.'' http://genuine.rs/sta-je-srbija-guglala-u-2016

Na kraju, korišćenjem dijagnostičkih alata za praćenje tranzita (traceroute) može se utvrditi na čijoj se teritoriji nalaze serveri koji sadržaj ovih veb stranica čine dostupnim na Mreži. Rezultati pokazuju da se dve petine sajtova nalazi na serverima koji se fizički nalaze u SAD (40), nešto više od četvrtine je u Srbiji (27), dok su Holandija (9) i Nemačka (8) i u ovoj kategoriji popularne za internet kompanije sa sedištem izvan matične teritorije.

Dakle, 60% sajtova ne poseduje nikakvu vezu sa Srbijom, dok sajtovi koji po jednom od navedenih kriterijuma imaju vezu sa Srbijom obično imaju vezu i po drugim kriterijumima. Tako u odnosu na 40% sajtova Srbija ima neku vrstu suverenosti nad licem koje je vlasnik domena, licem koje upravlja veb stranicom, hosting kompanijom na čijim serverima se veb stranica nalazi ili samim serverima koji sadržaj čine dostupnim. Na taj način se domaći organi mogu osetiti pozvanim i efikasnim prilikom regulisanja sadržaja koji se na njima nalaze. Detaljnijom analizom 60 sajtova koji nemaju uspostavljene veze sa Srbijom po opisanim kriterijumima, pokazaće se da dve trećine (41 od 60) ne poseduje nikakvu dodatnu vezu sa Srbijom, dok se za jednu trećinu (19 od 60) može reći da poseduje poslovno prisustvo na domaćoj teritoriji (sajt je dostupan na srpskom, postoji registrovan .rs domen pored glavnog domena, postoje partneri na srpskoj teritoriji). U odnosu na ovu trećinu, Republika Srbija bi mogla da uspostaviti određenu vrstu nadležnosti, ali bi za sprovođenje svojih odluka verovatno bila prinuđena da koristi instrumente međunarodne saradnje. U pogledu 40 sajtova koji ni po jednom kriterijumu ne poseduju vezu sa Srbijom, svaka vrsta regulisanja i sprovođenja određene politike zavisila bi od kooperacije mreže međunarodnih partnera.

Dakle, od 100 najposećenijih, 40% sajtova na određeni način jasno potpada pod suverenitet Republike Srbije, te se stoga može razumno očekivati da poštuju propise Srbije; 20% ima poslovno prisustvo, pa je razumno očekivati poštovanje srpskog prava u određenim situacijama. Preostalih 40% nalaze se isključivo pod regulativom drugih država. Ukratko, domet suvereniteta Republike Srbije na globalnu informacionu mrežu je ograničen, kao i njen uticaj na internet na sopstvenoj teritoriji.

U kontekstu ograničenog suvereniteta značajno je pozabaviti se izazovima i modelima primene prava na internetu, kao i mogućnostima direktne primene nacionalnog prava na Mreži, potencijalima za kreiranje nadnacionalnog foruma, značajem unifikovanih pravila međunarodnog prava i osnovama rešavanja sukoba zakona i nadležnosti na internetu.

1.3. MONITORING: OPŠTI PREGLED

PREPORUKE

Neodložna primena mera iz Sporazuma MUP-a, tužilaštva, novinarskih i medijskih udruženja, unapređenje kapaciteta organa nadležnih za istragu i procesuiranje dela visokotehnološkog kriminala u pravcu jačanja pravne sigurnosti učesnika u javnom informisanju. Jačanje medijskih udruženja, samoregulatornih tela i medija u pogledu upoznavanja sa rizicima, prepoznavanja incidenata i podizanja opšte bezbednosne kulture.

SHARE Fondacija od sredine 2014. godine prati digitalna prava i internet slobode u Srbiji, dokumentujući povrede prava građana, novinara, medija i drugih društvenih aktera. Neposredan povod za pokretanje stalnog monitoringa na internetu bio je veliki broj uklonjenih sadržaja, nedostupnih sajtova, ali i privedenih građana za vreme i nakon poplava u maju 2014. godine.[22] Tokom tri godine monitoringa obrađeno je više od 300 slučajeva.[23]

Tokom prikupljanja podataka o incidentima, monitoring tim SHARE Fondacije izradio je metodologiju za obradu i klasifikaciju slučajeva povreda digitalnih prava i sloboda u Srbiji. Povrede se obrađuju u odnosu na konkretne podatke o incidentu:

1. Meta ili akteri (ako je više meta ili učesnika slučaja)
2. Napadač (ako je poznato)
3. Sredstvo (npr. maliciozni softver) ili pravna posledica (npr. krivična prijava)
4. Kategorija (vrsta povrede, npr. tehnički napad na integritet sadržaja)
5. Datum početka / završetka
6. Dodatne stavke (slika, linkovi, opis povrede)

22 „Internet sve pamti"; SHARE Fondacija, 2014 http://www.shareconference.net/sh/defense/internet-sve-pamti

23 Monitoring baza http://monitoring.labs.rs/

Kategorije povreda u monitoringu su osmišljene tako da obuhvate sve vrste potencijalnih povreda, sadašnjih i budućih. Recimo, blokiranje i filtriranje internet sadržaja nije tipično za Srbiju, ali to ne znači da takvih povreda neće biti ubuduće.

KATEGORIJE POVREDA:

A. TEHNIČKI NAPADI NA INTEGRITET SADRŽAJA

1. Onemogućavanje pristupa sadržaju
2. Uništavanje podataka i programa, krađa podataka, izmena sadržaja (neovlašćeno brisanje, izmena i činjenje neupotrebljivim podataka i programa, sabotaža - unos, uništavanje, brisanje, oštećenje, prikrivanje ili na drugi način činjenje neupotrebljivim podataka ili programa sa namerom da se onemogući ili znatno oteža pristup sadržaju ili sistemu)
3. Računarska prevara - unošenje netačnih podataka ili neunošenje tačnih podataka sa namerom da se utiče na rezultat elektronske obrade i prenosa podataka.

B. NADZOR ELEKTRONSKIH KOMUNIKACIJA, NARUŠAVANJE PRAVA NA PRIVATNOST I ZAŠTITU PODATAKA O LIČNOSTI

1. Elektronski nadzor
2. Narušavanje privatnosti komunikacije od strane privatnih aktera
3. Povrede regulative zaštite podataka o ličnosti

C. PREKORAČENJE SLOBODE IZRAŽAVANJA I PRITISCI ZBOG AKTIVNOSTI I IZRAŽAVANJA NA MREŽI (NOVINARI, ONLAJN MEDIJI, BLOGERI, AKTIVISTI, POJEDINCI)

1. Iznošenje neistina
2. Uvrede i vrednosni stavovi
3. Ugrožavanje privatnosti
4. Pritisci, pretnje i ugrožavanje sigurnosti
5. Sloboda izražavanja na internetu i radni odnos

D. MANIPULACIJE U DIGITALNOM OKRUŽENJU

1. Lažno predstavljanje i krađa identiteta
2. Zloupotreba mehanizama digitalnog okruženja (između ostalog i astroturfing, botovi, itd.)

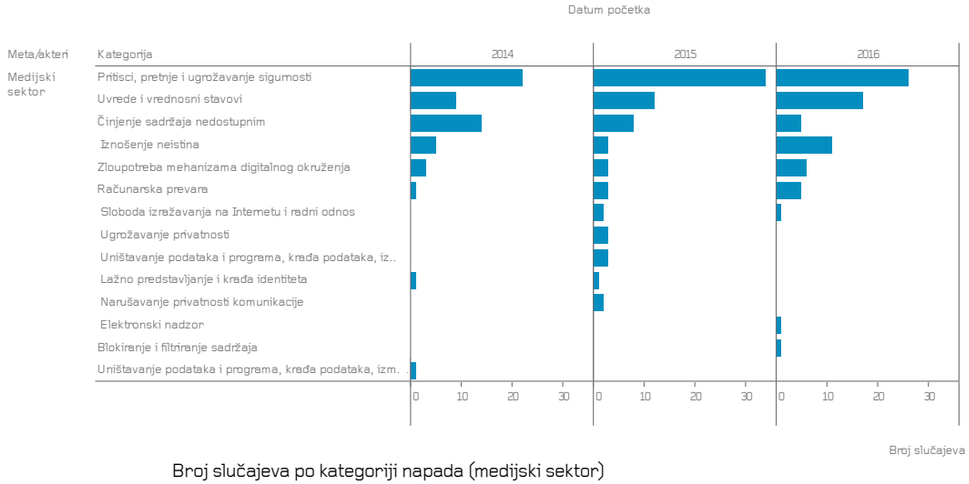
E. POZIVANJE POSREDNIKA NA ODGOVORNOST

F. BLOKIRANJE I FILTRIRANJE SADRŽAJA

G. OSTALO

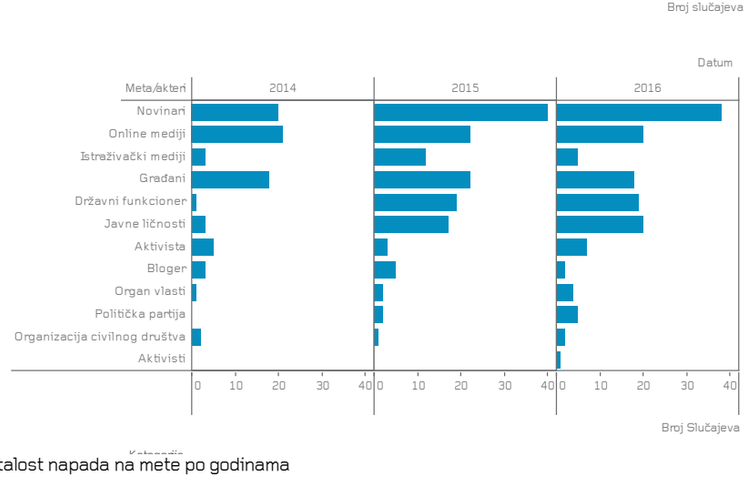
TRENDOVI

Mediji i novinari, naročito oni koji se bave istraživačkim radom, tokom prethodne tri godine najviše se susreću sa pretnjama, pritiscima i ugrožavanjem sigurnosti, dok su tehnički napadi kojima je cilj da onlajn sadržaj učine nedostupnim, u trendu opadanja.



Broj slučajeva po kategoriji napada (medijski sektor)

Najčešće mete povreda digitalnih prava i sloboda su novinari, onlajn mediji i građani, s tim da su napadi na istraživačke medije, aktiviste, javne ličnosti i državne funkcionere u porastu.



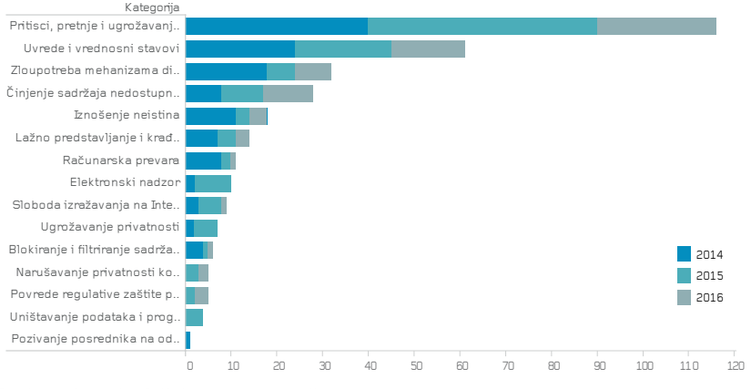
Učestalost napada na mete po godinama

1.3.1. POŠTOVANJE DIGITALNIH PRAVA I SLOBODA U 2016.

Incidenti su u monitoring bazi klasifikovani prema vrsti povreda, od tehničkih napada, povreda privatnosti, do pritisaka, uvreda i ugrožavanja sigurnosti. Od početka monitoringa do danas, kategorija ,,Pritisci, pretnje i ugrožavanje sigurnosti'' obuhvata gotovo trećinu od ukupnog broja zabeleženih incidenata. Tokom 2016. uočljiv je pad u odnosu na prethodnu godinu, ali je broj ovih slučajeva i dalje visok u poređenju sa drugim kategorijama povreda.[24]

Prvu polovinu godine svakako su obeležili aprilski parlamentarni izbori. Društveni mediji i platforme za onlajn razmenu su u 2016. po prvi put odigrali značajnu ulogu u promovisanju političkih ideja tokom kampanje. Pojedini politički akteri (Dveri, Dosta je bilo, SRS) na ovaj način su ostvarili svoje izborne ciljeve, odnosno prešli su cenzus i osvojili mesta u parlamentu.[25] Borba nedozvoljenim sredstvima preneta je iz oflajn kampanje i na internet, gde digitalni alati u znatnoj meri olakšavaju aktivnosti u cilju manipulacije javnim mnjenjem, kao što su lažna predstavljanja, negativne poruke, i slično. Tokom kampanje plasirani su sadržaji vizuelno ili na drugi način slični autentičnim porukama pojedinih aktera, na osnovu kojih su u javnosti stvarane pogrešne asocijacije političkih stavova i stranaka u izbornoj trci. Poseban je trud uložen u izradu video-priloga lažno pripisanih pokretu Dveri, uz odgovarajući kanal na platformi Jutjub, s ciljem diskreditacije aktera, odnosno obmanjivanja javnosti.

Za razliku od prve dve godine monitoringa, u 2016. nije zabeležen rast slučajeva kompromitovanja onlajn sadržaja tehničkim sredstvima, što je u domaćoj sajber sferi najčešće DDoS napad (Distributed Denial of Service). Tokom 2014. i 2015. upravo su tehnički napadi na sajtove koji objavljuju kritičke tekstove (Peščanik, CINS, Teleprompter) privukli značajnu pažnju javnosti. Do danas ovi slučajevi nisu rešeni sudskim putem.



Broj zabeleženih slučajeva po kategorijama

24 Stanje digitalnih prava i sloboda u Srbiji - pregled za 2016. godinu; SHARE Fondacija, 2016 http://www.shareconference.net/sites/default/files/u742/godisnji _ monitoring _ izvestaj _ 2016 _ za _ sajt.pdf

25 ,,#izbori2016: Kampanja na mrežama se isplati'', SHARE Fondacija, 2016 http://www.shareconference.net/sh/defense/izbori2016-kampanja-na-mrezama-se-isplati

Tokom 2016. SHARE tim je registrovao petnaestak tehničkih slučajeva povreda prava u onlajn okruženju. Najmanje dva slučaja vezana su za medije (Danas, Pištaljka), na koje je napad lansiran neposredno nakon objave izveštaja vezanih za najviše državne funkcionere i njihovo neposredno okruženje.

Na društvenim medijima učestali su slučajevi zaključavanja i suspenzije naloga, međutim, nedostatak podataka onemogućava jasnu kvalifikaciju većine ovih incidenata. Slučajeve su najčešće prijavljivali korisnici koji su smatrali da im je pristup uskraćen zbog iznošenja kritičkih stavova ili njihove uloge u društvu, kao što su novinari, odbornici u lokalnoj vlasti, akteri iz nevladinog sektora i onlajn aktivisti. Zasad ostaje nejasno u kojim se situacijama aktivira automatski servis platforme za zaključavanje naloga, ,,usled neuobičajenih aktivnosti'', pokušaja pristupa sa drugog uređaja ili većeg broja prijava koje upućuju politički oponenti, po raznim osnovama navodne povrede pravila korišćenja (govor mržnje, kršenje autorskih prava, i slično).

Iskustva govore da je, bar kada je reč o mikroblogerskoj platformi Tviter, zaključan nalog relativno lako otključati ako nije bilo stvarne povrede pravila - pod uslovom da se korisnici sećaju mejl adrese sa koje su se inicijalno prijavili, ili stare lozinke.

Netransparentne procedure suspenzije, brisanja pojedinih statusa i čitavih naloga na društvenim medijima, pre svega na Fejsbuku i Jutjubu, sve češće su u fokusu globalne javnosti. Patroliranje granicama slobode govora u onlajn sferi preuzele su gigantske korporacije, čiji ljudski i algoritamski cenzori preuzimaju ovlašćenja da uređuju javni prostor i sprovode selekciju informacija koje razmenjujemo.

Granice između slobode govora i govora mržnje, verbalnih napada i pretnji, s druge strane, i dalje su jedna od ključnih tema globalne onlajn sfere, pa i u domaćim okvirima. Brojni slučajevi povreda prava, zabeleženi u monitoringu SHARE Fondacije tokom 2016. čine različite vrste prekoračenja slobode izražavanja i pritisaka zbog aktivnosti i iznošenja stavova na Mreži - neistine, uvrede, omalovažavanje, pretnje i ugrožavanje sigurnosti, i slično. U poređenju sa 2015. godinom, kada je tokom monitoringa zabeleženo 104 slučaja iz ove kategorije, SHARE Fondacija je tokom protekle godine registrovala 91 slučaj, što govori o blagom padu. Međutim, utisak je da su u 2016, kao i prethodnih godina, različiti oblici pritisaka i dalje brojni pre svega usled izostanka pravnih posledica, posebno u slučajevima gde su na meti novinari ili aktivisti civilnog društva.

Ključne posledice ugrožavanja digitalnih prava i internet sloboda ogledaju se u pravnoj nesigurnosti, jer počinioci retko budu otkriveni i procesuirani. Uprkos osetnom padu u broju tehničkih napada zabeleženih tokom protekle godine, jasna je potreba za unapređenjem odbrambenih kapaciteta zajednice u domaćoj sajber sferi. Jedan od osnovnih preduslova onlajn bezbednosti, za opštu populaciju, svakako čini sistemsko digitalno opismenjavanje.

Takođe, u sajber prostoru, odbrana je uobičajeno skuplja nego napad, što prilično obeshrabruje male i nezavisne onlajn i građanske medije koji ne

mogu sebi da priušte skupe stručnjake za sajber bezbednost ili tehnička rešenja za zaštitu. Smanjenje broja tehničkih napada većih razmera ne znači da ne treba raditi na unapređenju odbrambenih kapaciteta. Osvajanje višeg nivoa digitalne bezbednosti, međutim, često podrazumeva složene procedure, promenu uobičajenih navika pri korišćenju tehnologije, što može umanjiti efikasnost novinara i organizacija.

Napadi i pritisci na novinare i pojedince zbog blogova, komentara ili drugih oblika onlajn izražavanja ima za posledicu efekat zebnje (chilling effect)[26] ne samo kod novinara i medijskih organizacija, već i kod šire onlajn zajednice, koja danas čini 60% stanovništva Srbije. Stoga se može reći da se građani ne osećaju osnaženo i zaštićeno u digitalnom okruženju, što umanjuje potencijale za primenu novih tehnologija.

Jasno je da nadležni organi vlasti imaju ograničene tehničke i organizacione kapacitete za efikasniju reakciju u pojedinim situacijama. Međutim, reakcije tužilaštva, policije i sudstva sve češće znatno variraju od slučaja do slučaja - nekada su veoma efikasne, a nekada spore i bez pravog odgovora. Vrlo spore reakcije, ili njihovo potpuno odsustvo, u najvećem broju slučajeva uočene su kod sajber napada i pretnji onlajn medijima, istraživačkim novinarima i građanskim medijima, kritičnim prema postupcima vlasti. Takva praksa obeshrabruje poverenje građana i onlajn medijskih organizacija u zaštitu države, koja treba da preuzme aktivniju ulogu u obezbeđivanju poštovanja prava u digitalnom okruženju.

1.3.2. MONITORING DIGITALNIH PRAVA I SLOBODA - ODABRANI SLUČAJEVI

Iz vizure tradicionalnih medija, internet kao javni prostor često se asocira s odsustvom odgovornosti i različitim oblicima povreda prava, podstaknutim skrivanjem identiteta počinilaca. S druge strane, incidenti koji testiraju granice privatnog i javnog, ugrožavanje sloboda pojedinaca suočenih sa nesrazmernom moći globalnih korporacija i državnih institucija neprilagođenih novom okruženju, digitalni alati koji su tehnike manipulacije javnim mnjenjem unapredili do neslućenih razmera, samo su neka od gorućih pitanja na koje javne politike, ali i čitava zajednica, moraju neodložno obratiti pažnju. Pet odabranih slučajeva obrađenih tokom 2016. godine poslužiće kao primeri novih izazova za slobodu govora u onlajn sferi.

1. JUTJUB PROTIV ZAŠTITNIKA GRAĐANA

Pitanje uticaja onlajn platformi kroz kontrolu nad sadržajem koji postavljaju korisnici, u Srbiji je otvoreno u avgustu 2016. kada je Jutjub blokirao zvanični kanal Zaštitnika građana.[27] Na kanalu su se nalazili snimci tele-

26 Efekat zebnje (Chilling Effect) je pravna kovanica koja se može tumačiti kao obeshrabrivanje legitimnog i dozvoljenog ispoljavanja nekog prava pretnjom ili stavljanjem u izgled neke pravne sankcije: http://www.shareconference.net/sh/blog/ciling-efekat-presude-protiv-dva-forumasa-u-slucaju-malagurski-da-li-je-sloboda-izrazavanja-na

27 ,,Kako mreže uređuju javni prostor: YouTube protiv Ombudsmana'', SHARE Fondacija, 2016. http://www.shareconference.net/sh/defense/kako-mreze-uredjuju-javni-prostor-youtube-protiv-ombudsmana

vizijskih nastupa Saše Jankovića, a moderatori globalne platfrome za razmenu video sadržaja su ga suspendovali po prijavama korisnika zbog kršenja pravila. Jutjub, u vlasništvu Gugla, odbio je žalbu koju su uložili saradnici Ombudsmana, a u međuvremenu je blokiran i mejl korišćen za postavljanje video-snimaka na kanal. Pristup kanalu je, bez objašnjenja i obaveštenja, posle izvesnog vremena ponovo omogućen.

SHARE Fondacija je uz pomoć evropske koalicije za zaštitu digitalnih prava EDRi, stupila u kontakt sa predstavnicima evropskog sedišta Gugla, tražeći objašnjenje procedura za suspenziju i povraćaj kanala. Prema njihovom uveravanju, nalozi ili pojedinačni video-klipovi se ne uklanjaju automatski, bez obzira na broj upućenih prijava korisnika. Kako se navodi, pregledom sadržaja i prijava bave se ljudi a ne mašine, te se svakim pojedinačnim slučajem odgovarajući tim bavi posebno. Odluka o suspenziji dostavlja se vlasniku kanala, kao i obaveštenje o ponovnoj dostupnosti, dok je izostanak odgovarajućeg obaveštenja Zaštitniku građana ocenjen kao nenameran propust.

S obzirom na količinu sadržaja, opisani postupak moderacije na Jutjub platformi deluje teško sprovodiv, a procedure nedovoljno transparentne. Problem algoritamskih cenzora i mašinskog uređivanja javnog prostora, odnosno selekcije dostupnih sadržaja, sve češće je u fokusu globalne zajednice.

2. TRI GODINE DO OSLOBAĐAJUĆE PRESUDE ZA FORUMAŠE

Krajem marta 2016. advokat Ognjen Rašuo, pravni zastupnik trojice članova foruma ,,Parapsihopatologija'', objavio je na Tviteru da su forumaši konačno oslobođeni optužbi za pretnje i ugrožavanje sigurnosti reditelja Borisa Malagurskog.[28] Sudski proces, pokrenut zbog izjava u zatvorenom delu internet foruma, trajao je tri godine da bi, posle odluke Vrhovnog kasacionog suda po zahtevu za zaštitu zakonitosti, članovi foruma Rastislav Dinić, Marko Nikolić i Nemanja Paleksić bili oslobođeni krivice. Uprkos neopravdano dugom procesu, okončanje slučaja u korist optuženih forumaša značajno je za slobodu govora na internetu i donekle ublažava efekat zebnje koji netizene odvraća od slobodnog izražavanja stavova na Mreži, iz straha od potencijalnih pravnih posledica.[29]

Krivični postupak pokrenut je zbog izjava u diskusiji o filmu Borisa Malagurskog, ,,Pretpostavka pravde'', vođenoj na delu foruma kojem pristup imaju samo registrovani članovi. U filmu snimljenom tri godine posle ubistva francuskog navijača Brisa Tatona u Beogradu 2009, autor predstavlja incident kao nesrećan slučaj, a istragu i sudske presude okrivljenima za ubistvo kao rezultat političkih pritisaka na pravosuđe. Komentari forumaša na film bili su oštri i vulgarni, što je autor doživeo kao ugrožavanje

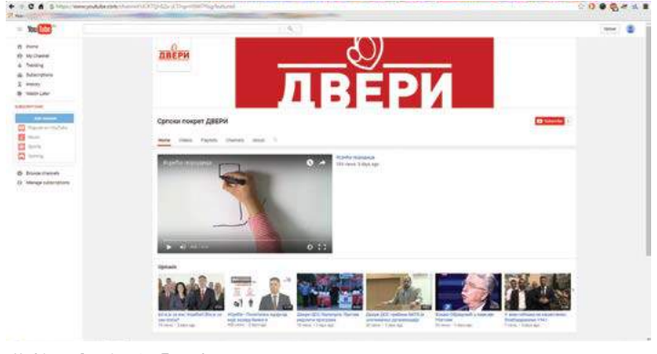
28 Tvit advokata optuženih: ,,Vrhovni kasacioni sud je preinacio presudu u predmetu Malagurski protiv PPP. Forumasi oslobodjeni. :)'' https://twitter.com/ORasuo/status/715538553141379073

29 ,,Čiling efekat presude protiv dva forumaša u slučaju Malagurski - da li je sloboda izražavanja na Internetu ugrožena'', SHARE Fondacija, 2014. http://www.shareconference.net/sh/blog/ciling-efekat-presude-protiv-dva-forumasa-u-slucaju-malagurski-da-li-je-sloboda-izrazavanja-na

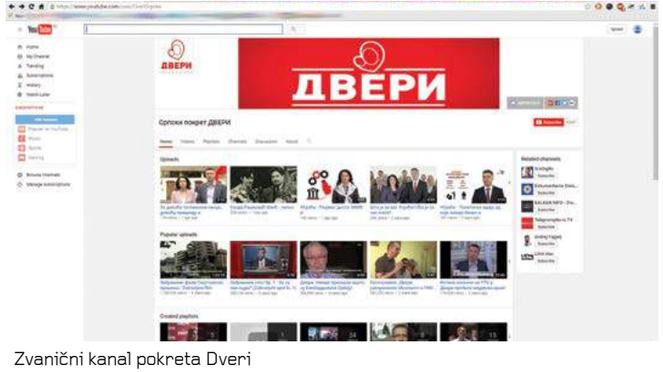
bezbednosti. Prvostepena presuda stala je na stranu tužitelja, da bi zatim bila oborena na Apelacionom sudu zbog niza povreda postupka.[30] Na ponovljenom suđenju, forumaši su ponovo proglašeni krivim, dok je na apelaciji izmenjena pravna kvalifikacija dela i smanjena uslovna kazna zatvora. Vrhovni kasacioni sud, konačno, ocenjuje da je ,,primenjen zakon koji se ne može primeniti'' i oslobađa optužene.[31]

3. LAŽNI KANAL DVERI

Serija promotivnih spotova, navodno u produkciji desničarskog pokreta ,,Dveri'', pojavila se na platformi za deljenje video sadržaja u vreme predizborne kampanje za parlamentarne izbore 2016. U spornim klipovima, pokret i njegovi lideri su diskreditovani tako što su im pripisivane ideje koje su u suprotnosti sa njihovom zvaničnom politikom i podmetani sadržaji koje nisu kreirali (npr. video posvećen 8. martu koji bio je veoma uvredljiv za žene).[32] Početkom aprila, u jeku kampanje, na Jutjubu je napravljen kanal koji je vizuelno podsećao na zvanični kanal Dveri, sa kog su deljeni spotovi.



Lažni kanal pokreta Dveri



Zvanični kanal pokreta Dveri

30 ,,Vaspitavanje javnosti strahom'', oktobar 2014. http://www.autonomija.info/milica-jovanovic-vaspitavanje-javnosti-strahom.html

31 Vrhovni kasacioni sud, Kzz 1203/2015 http://www.vk.sud.rs/sr/K33-12032015

32 Vesti o spotovima u tabloidima: http://informer.rs/vesti/izbori/65644/VIDEO-NEVIDJENA-PREDIZBORNA-BRUKA-Dveri-otcepili-Kosovo-Metohiju-Srbije, http://www.alo.rs/u-dverima-ovako-tretiraju-zene-video/38613

Inače, pokret Dveri se tokom kampanje u najvećem delu svojih promotivnih aktivnosti okrenuo internetu i slobodnim platformama što ih, uz pokret ,,Dosta je bilo'' sa sličnom strategijom, praktično čini pionirima u primeni slobodnih onlajn resursa za političku propagandu u Srbiji. Uprkos inicijalnim prognozama i slabom prisustvu u tradicionalnim medijima, dva pokreta su prešla cenzus i osvojila mesta u Parlamentu.[33]

4. SUSPENZIJA NALOGA NA TVITERU

Odgovorni urednik magazina NIN, Nikola Tomić, u junu 2016. ostao je bez pristupa svom dotadašnjem tviter nalogu @N _ Tomic.[34] Sumnje da je nalog hakovan pokazale su se neosnovanim kada se ispostavilo da je reč o automatskoj suspenziji naloga usled nepoznate sumnjive aktivnosti, kako je navedeno u automatskom obaveštenju. Suspenzija naloga podudarila se sa objavljivanjem teksta u NIN-u, o političkoj odgovornosti ministra unutrašnjih poslova Nebojše Stefanovića za noćno rušenje objekata u Hercegovačkoj ulici u Beogradu, zbog čega je ministar kasnije podneo i tužbu.[35]

U ovom slučaju nije bilo moguće sprovesti tehničku analizu, niti je utvrđeno koji je mehanizam popularne mikroblogerske platforme pokrenut za suspenziju naloga iz bezbednosnih razloga. Da li zbog pokušaja nasilnog preuzimanja naloga, korisničkih prijava ili nečeg drugog, procedure zaključavanja naloga su najčešće u potpunosti automatizovane, a suspenzija traje sve dok pravi vlasnik ne otključa nalog putem pristupnog mejla.

Složene, različite lozinke za naloge na društvenim medijima i mejlovima, povremena promena lozinki i njihovo bezbedno čuvanje, osnovne su preporuke za zaštitu integriteta ličnih naloga.

5. DR TATJANA MRAOVIĆ PROTIV BLOGERKE ,,VITKI GURMAN''

Tužba zbog teksta na blogu još uvek je retkost u Srbiji, a jedan od prvih sudskih slučajeva tim povodom odigrao se kada je dr Tatjana Mraović podnela privatnu krivičnu tužbu zbog uvrede, protiv Maje Petrović koja vodi blog o zdravoj ishrani ,,Vitki gurman''.[36] Povod je bio tekst iz 2015. godine u kom blogerka kritikuje promociju margarina kao sastojka zdrave ishrane.[37] Prvostepenom presudom Prvog osnovnog suda u Beogradu Maja Petrović je oslobođena optužbi za uvredu, a dr Mraović je naloženo da blogerki nadoknadi troškove postupka. Kako je tužilja uložila žalbu na presudu, postupak nije pravosnažno okončan, te se na epilog slučaja još uvek čeka.

U vreme objave teksta o ,,doktorki za margarin'' blogerka je najpre bila na

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

34 Tvit: ,,...dok mi cenjeni @twitter ne osposobi hakovani @n _ tomic. Širi dalje'' https://twitter.com/blablaTomiccc/status/745206034235555840?ref _ src=twsrc%5Etfw

35 Tvit: ,,Kako je Nebojša Stefanović smenio svog najboljeg inspektora'' https://twitter.com/N _ Tomic/status/743763398702182400/photo/1?ref _ src=twsrc%5Etfw

36 Vitki gurman na sudu http://vitkigurman.com/vitki-gurman-na-sudu/

37 Sramna saradnja – kompanija ,,Dijamant'' i dr Tatjana Mraović http://vitkigurman.com/tatjana-mraovic-doktorka-za-margarin/

meti povrede reputacije[38], a zatim je od hosting provajdera njenog bloga zahtevano da mu se onemogući pristup zbog ,,govora mržnje'' i ,,kršenja osnovnog pravila ponašanja na internetu''.[39]

1.3.3. ALGORITAMSKO UPRAVLJANJE SADRŽAJEM

Obilje informacija koje se objavljuju na internetu zahteva posebne mehanizme upravljanja sadržajem i njegovom distribucijom ciljanoj publici. Kako korisnici interneta provode sve više vremena na platformama koje posreduju u distribuciji između kreatora i konzumenata sadržaja (Gugl, Fejsbuk i Jutjub su tri najpopularnija internet servisa u Srbiji), mehanizmi distribucije dobijaju sve veći značaj u digitalnoj medijskoj sferi.

Bez obzira da li se medij, organizacija ili pojedinac pojavljuju u ulozi kreatora, odnosno distributera sadržaja preko internet platformi, na putu do publike sadržaj prolazi kroz niz različitih prepreka i filtera. Platforme najčešće upravljaju procesom distrubucije uz pomoć automatizovanih mehanizama zasnovanih na matematičkim algoritmima, a ređe koristeći procene ljudi, odnosno svog osoblja angažovanog na procesu.

Životni ciklus onlajn sadržaja započinje postavljanjem na određenu platformu, što je uslovljeno automatskom proverom kroz takozvani ,,upload'' filter. Svaka platforma može imati drugačiji mehanizam provere, u zavisnosti od tehnologije koju koristi i utvrđenim politikama o nedozvoljenom i štetnom sadržaju ali su, u načelu, filteri trovrsni:

1. Filtriranje sadržaja koji je već označen kao nedozvoljen i štetan, poređenjem hash vrednosti[40] i ključnih reči (terorizam, govor mržnje, dečija pornografija, itd.).
2. Filtiranje ,,spam''[41] sadržaja kroz upoređivanje ,,hash'' vrednosti i analizu kanala distribucije.
3. Filtriranje sadržaja kroz vizuelno, video i audio prepoznavanje, na osnovu kataloga dela zaštićenih autorskim pravima.

Ukoliko interni sistem prepoznavanja, odnosno provere označi sadržaj kao nedozvoljen, platforma automatski sprečava objavu ili uklanja sadržaj nakon objave. U određenim slučajevima (autorska prava) povratak sadržaja može biti omogućen na osnovnu naknadne saglasnosti nosioca autorskih prava. Interesantno je primetiti da administratori određenih vrsta kanala komunikacije imaju na raspolaganju mogućnost da, u okviru zajednice kojom upravljaju, unesu i dodatne vrste filtriranja (prema posebno definisanim

38 ,,Ustanem ja jutros i otkrijem..'' https://www.facebook.com/VitkiGurman/posts/759608117477916?hc _ location=ufi%20htt

39 ,,Kako mali perica zamišlja internet'' https://www.facebook.com/notes/sibin-gra%C5%A1i%C4%87/kako-mali-perica-zami%C5%A1lja-internet/10153795172603092

40 Jednosmerna, ireverzibilna funkcija pomoću koje se vrši transformacija informacije proizvoljne veličine u ,,hash'' vrednost fiksne veličine

41 Neželjeno, nasrtljivo oglašavanje, plasiranje sadržaja, isl.

ključnim rečima i već kreiranim bazama vulgarnog govora).[42] Treba imati u vidu da ova vrsta upravljanja sadržajem nije dovoljno fleksibilna da uzme u obzir sve standarde slobode izražavanja, te zbog previše rigidnog automatskog odlučivanja često dolazi do povreda slobode govora i slobode informisanja.[43] Doduše, algoritam omogućava da, umesto uklanjanja, sadržaj posle provere bude označen određenom oznakom kao neprilagođen za pojedine grupe korisnika (decu, mlade, osetljive potrošače, itd).

Kada sadržaj preživi automatske filtere prilikom postavljanja na platformu, i dalje nije izvesno da li će i u kom obimu biti dostupan željenoj publici. Različiti faktori utiču na odlučivanje o tome koji sadržaj će biti automatski prikazan pojedinim korisnicima, pri čemu lista nije konačna:

- karakter lica koje želi da distribuira sadržaj (korisnik, stranica, grupa, kompanija, itd);
- forma sadžaja (tekst, video, audio, foto, itd);
- interesovanje za sadržaj među korisnicima platforme;
- automatski generisan profil korisnika;
- direktni zahtevi korisnika (sakriti, označiti, uvek prikazati, itd);
- posebne relacije između sadržaja i korisnika (tagovanje, itd);
- bustovanje, oblik onlajn promocije, odnosno sponzorisanja sadržaja na platformi.

Tako se ispostavlja da nisu svi akteri, svaka vrsta sadržaja i svaki korisnik u okviru digitalne medijske sfere u jednakom položaju. Platforme koje poseduju obilje sadržaja (Fejsbuk, Jutjub i drugi), uz pomoć automatske obrade, sprovode uredničko oblikovanje sadržaja koji će korisnicima biti dostupan.

Nakon što sadržaj postane dostupan korisnicima - kroz automatske prikaze, kao rezultat pretrage ili direktnim pristupom kanalima komunikacije (profil, kanal, stranica, grupa) - sadržaj se dalje proverava po prijavama korisnika u skladu sa pravilima zajednice (smernice, uslovi korišćenja, itd). Prijavu nedozvoljenog i štetnog sadržaja može podneti svaki zainteresovani korisnik, čime se pokreće postupak ispitivanja osnovanosti prijave i primene eventualnih sankcija. Preispitivanje osnovanosti prijava vrše specijalizovani timovi ljudi koje platforma namenski angažuje, ali se sve više zagovara potreba da se ovaj posao poveri ekspertskim organizacijama.[44] Moguće sankcije po prihvaćenoj prijavi nedozvoljenog sadržaja, obuhvataju uklanjanje samog sadržaja, kao i privremeno i trajno blokiranje naloga sa kog je sadržaj distribuiran. Ekspertska javnost je stava da su mehanizmi

42 Primer: https://www.facebook.com/help/131671940241729?helpref=related

43 Primeri: Parodija i autorska prava: odbranimo remiks kulturu! http://www.shareconference.net/sh/defense/parodija-i-autorska-prava-odbranimo-remiks-kulturu; Kako mreže uređuju javni prostor; YouTube protiv Ombudsmana http://www.shareconference.net/sh/defense/kako-mreze-ureduju-javni-prostor-youtube-protiv-ombudsmana; Monitoring predsedničke onlajn kampanje 2017 https://labs.rs/sr/izbori2017/

44 Dobar primer je nemačka neprofitna istraživačka organizacija Correctiv angažovana da na nemačkom govornom području spreči distribuciju lažnih vesti na Fejsbuku https://correctiv.org/en/correctiv/

upravljanja sadržajem po prijavama korisnika nedovoljno transparentni, kako u pogledu procesa tako i u pogledu kriterijuma za uspostavljanje ravnoteže između slobode izražavanja i suprostavljenih vrednosti, te da su „pravni lekovi" u okviru ove procedure nedovoljno razvijeni.

Dodatno, posebni vidovi uklanjanja sadržaja nastaju kao rezultat saradnje određene platforme sa državnim organima i međunarodnim organizacijama koje se bave upravljanjem sadržajem. Tako platforme pružaju mogućnost za uklanjanje sadržaja obično na osnovu nacionalnih sudskih odluka ili prijava specijalizovanih organizacija koje štite interese određenih kategorija stanovništva, poput Agencije EU za mrežnu i informacionu bezbednost.[45]

1.4. EU INTEGRACIJE

PREPORUKE

Hitna izrada novog zakona o zaštiti podataka o ličnosti, predvidenog Akcionim planom za Poglavlje 23, koji će biti u skladu sa novom Opštom uredbom EU o zaštiti podataka o ličnosti i novim predlogom Modela zakona Poverenika za informacije od javnog značaja i zaštitu podataka o ličnosti. Primena mera iz Akcionog plana za Poglavlje 24 obuhvata povećanje kapaciteta u oblasti visokotehnološkog kriminala (VTK), gde je kao značajna prepreka identifikovano donoše-nje nove sistematizacije radnih mesta u okviru Ministarstva unutrašnjih poslova, odnosno sektora za VTK na operativnom nivou, kao i na nivou komunikacije sa međunarodnim telima (Interpol, Europol, Eurojust, itd).

45 ENISA https://www.enisa.europa.eu/about-enisa

1.4.1. POGLAVLJE 23

Dva ključna poglavlja za tok pregovora Srbije o pristupanju Evropskoj uniji, Poglavlja 23 i 24, otvorena su u julu 2016. godine. Akcioni plan za pregovaranje Poglavlja 23, koje se tiče pravosuđa i osnovnih prava, usvojen je na sednici Vlade Srbije 27. aprila 2016.[46]

SHARE Fondacija je u ovom procesu posebno zainteresovana za segment koji se odnosi na zaštitu podataka o ličnosti, gde su Akcionim planom predviđena ustavna i legislativna usklađivanja sa pravnim tekovinama EU. U dokumentu se ističe da regulativi EU u ovoj oblasti predstoji usvajanje nove opšte uredbe o zaštiti ličnih podatka, te da će Srbija uskladiti svoje zakonodavsto nakon njenog donošenja. Takođe se navodi da će biti donet novi zakon o zaštiti podataka o ličnosti, u skladu sa tabelama usklađenosti sa postojećim tekovinama EU, Opštom Uredbom EU o zaštiti podataka o ličnosti koja je doneta u maju 2016. godine i Modelom zakona koji je predložio Poverenik za informacije od javnog značaja i zaštitu podataka o ličnosti.

Akcionim planom je donošenje novog zakona bilo predviđeno do kraja 2016. godine, dok je kao rok za usvajanje podzakonskih akata za njegovu primenu označen 4. kvartal 2017. godine. Budući da novi zakon nije donet po planu, i podzakonska akta očekuju drugi rokovi.

Značajna mera predviđena Akcionim planom jeste jačanje kadrovskih i finansijskih resursa kancelarije Poverenika za informacije od javnog značaja i zaštitu podataka o ličnosti. Planom je definisano da se u 1. i 2. kvartalu 2017. godine sprovede analiza kadrovskih potreba Poverenika, da bi se do 2019. postepeno povećavao broj sa 64 zaposlenih, koliko ih sada ima, do krajnjeg cilja od 94 zaposlenih.

Po usvajanju Opšte Uredbe EU o zaštiti podataka o ličnosti, naglašeno je u Akcionom planu, biće potrebno uneti adekvatne izmene u nadležnosti Poverenika za informacije od javnog značaja i zaštitu podataka o ličnosti, kao i izraditi novi pravilnik o unutrašnjem uređenju i sistematizaciji radnih mesta.

1.4.2. POGLAVLJE 24

Izveštaj o skrinigu za Poglavlje 24[47], kao i izveštaji Evropske komisije o napretku Srbije za 2013. i 2014. upućuju na činjenicu da je borba protiv sajber kriminala u Srbiji u svojoj početnoj fazi. Izveštajem o napretku iz 2016. Srbija je obavezana da usvoji strategiju o visokotehnološkom kriminalu. U izveštaju o skriningu utvrđeno je da je Srbija ustanovila posebnu jedinicu nadležnu za borbu protiv visokotehnološkog kriminala u Ministarstvu unutrašnjih poslova, kao i Specijalno tužilaštvo za borbu protiv visokotehnološkog kriminala, potvrdila Konvenciju Saveta Evrope o

46 Akcioni plan za pregovaranje Poglavlja 23, Ministarstvo pravde RS http://www.mpravde.gov.rs/files/Akcioni%20plan%20PG%2023.pdf

47 Izveštaj o skriningu: Srbija, Poglavlje 24 - Pravda, sloboda i bezbednost http://www.bezbednost.org/upload/document/izvestaj _ o _ skriningu _ pg24.pdf

visokotehnološkom kriminalu („Sl. glasnik RS“, br. 19/2009) i u velikoj meri uskladila propise sa Direktivom 2013/40/EU o napadima na informacione sisteme, uz zaključak da su neophodne izmene i dopune propisa, naročito u pogledu sankcija, kako bi se u potpunosti uskladile sa pravnim tekovinama EU u oblasti borbe protiv sajber kriminala. U preporukama nakon skrininga, Komisija je utvrdila da je potrebno obezbediti nastavak specijalizovanih obuka kao i unapređenje kapaciteta organa za sprovođenje zakona u oblasti sajber kriminala.

Akcionim planom za Poglavlje 24 preporučen je niz mera za unapređenje aktivnosti:[48]

1. Pružiti dalju specijalizovanu obuku i unaprediti kapacitet organa za sprovođenje zakona zaduženih za suzbijanje sajber kriminala.
   - Izraditi predlog relevantnih podzakonskih akata kako bi se unapredili organizacioni, kadrovski i tehnički kapaciteti protiv sajber kriminala.
   - Osnažiti kapacitete Specijalnog tužioca za visokotehnološki kriminal.
   - Osnažiti kapacitete Specijalnog državnog tužioca za visokotehnološki kriminal, Specijalne policijske jedinice za visokotehnološki kriminal, sudova i drugih relevantnih institucija putem obuka.
   - Osnovati specijalizovanu Jedinicu za istragu zloupotreba kreditnih kartica, trgovine putem interneta i elektronskog bankarstva unutar Ministarstva unutrašnjih poslova, tj. Službe za suzbijanje organizovanog kriminala te Odeljenja za suzbijanje visokotehnološkog kriminala.
   - Osnovati specijalizovanu Jedinicu za suzbijanje nezakonitog i štetnog sadržaja na internetu unutar Ministarstva unutrašnjih poslova – Službe za suzbijanje organizovanog kriminala – Odeljenja za suzbijanje visokotehnološkog kriminala (ova jedinica bi se takođe bavila istragama u oblasti dečije pornografije, uspostavljanjem sistema automatizovane podrške za ovu Jedinicu – kompjuterski sistem za analizu foto i video materijala koji sadrže dečiju pornografiju).

2. Usklađivanje domaćih zakona sa pravnom tekovinom Direktive 2013/40 i standardima Evropske unije u oblasti borbe protiv sajber kriminala.
   - Analizirati trenutni zakonodavni okvir kako bi se odredio nivo njegove usklađenosti sa pravnom tekovinom i standardima Evropske unije.
   - Izraditi predlog zakona i podzakonskih akata na osnovu sprovedene analize.

3. Jačanje saradnje između državnih organa i institucija civilnog društva u oblasti borbe protiv sajber kriminala.

4. Izraditi i potpisati sporazume o saradnji između državnih organa i institucija civilnog društva u oblasti borbe protiv sajber kriminala.

48 Akcioni plan za Poglavlje 24 – pravda, sloboda i bezbednost (treći nacrt, 2015) http://www.bezbednost.org/Svi-dokumenti/5758/Akcioni-plan-za-Poglavlje-24--pravda-sloboda.shtml

Evropska komisija je u izveštajima o napretku Srbije za 2013. i 2014. prepoznala uložene napore Srbije u oblasti borbe protiv sajber kriminala, poboljšavanjem saradnje sa tužilaštvom, kao i organizovanjem obuka za policijske službenike i više rukovodioce, uključujući i obuke za sprovođenje istraga na nacionalnom nivou i u saradnji sa drugim zemljama. Međutim, Komisija je upozorila na potrebu za strukturiranim obukama i adekvatnim resursima. Naime, postoji potreba za jačanjem kapaciteta Odeljenja za borbu protiv visokotehnološkog kriminala u Ministarstvu unutrašnjih poslova, u cilju efikasnijeg upravljanja rastućim obimom kompleksnih kriminalnih aktivnosti nad kojima treba sprovoditi istragu, kao i uvođenjem specijalizovanih tehnika kako bi Odeljenje bilo usklađeno sa modernim operativnim međunarodnim standardima. Komisija je u preporukama takođe prepoznala neophodnost uspostavljanja bliske saradnje sa privatnim i javnim sektorom i akademskom zajednicom. Dakle, za sveobuhvatnu borbu protiv sajber kriminala u Srbiji potrebne su dodatne specijalizovane obuke, bolja koordinacija između institucija i adekvatna budžetska sredstva.

2. SLOBODA IZRAŽAVANJA

PREPORUKE

Osnaživanje samoregulatornih tela i mehanizama, uspostavljanje modela reputacionih sistema medija (žig poverenja, etičko ponašanje u onlajn prostoru), provere i analize činjenica u internet sferi (fact-checking); promocija prednosti registracije medija, digitalno opismenjavanje onlajn i građanskih medija, dece i mladih, kao i opšte javnosti; budućim zakonom o elektronskom dokumentu, elektronskoj identifikaciji i uslugama od poverenja u elektronskom poslovanju, predvideti obavezu identifikacije registrovanih onlajn medija putem autentifikacije.

2.1. ONLAJN MEDIJI U SRBIJI

2.1.1. DEFINICIJA I PRAVNA ZAŠTITA NOVINARA

S obzirom na okruženje u kom već samo prisustvo podrazumeva mogućnost učešća u javnom informisanju, onlajn i građanski mediji posebno su na udaru zahteva za nekim oblikom licenciranja, odnosno formalnog regulisanja ,,prava'' na bavljenje novinarstvom. Internet se u tom smislu najčešće označava kao okruženje u kom ne važe pravila kvalitetnog novinarstva i gde ,,svako može da piše šta mu padne na pamet'' - s podjednakim šansama za uticaj na javno mnjenje kao i školovano, uredrički oblikovano novinarstvo koje dosledno poštuje zakonske i etičke norme. Osim u kontekstu samoregulatornih mehanizama, ovo pitanje se naročito postavlja s obzirom na dva posebna oblika pravne zaštite koju uživaju novinari: zaštite novinarskih izvora i zaštite bezbednosti novinara. Takođe, do diskriminacije građanskih novinara može doći prilikom ostvarivanja prava na ravnopravan pristup informacijama, posebno kada je reč o organima javne vlasti koji mogu različito tretirati novinare registrovanih medija i građanske novinare.

Čini se da u pravosuđu preovlađuje tumačenje prema kom se dva posebna prava odnose samo na profesionalne novinare, članove strukovnih udruženja, odnosno angažovane u nekom od postojećih medija upisanih u Registar. Međutim, s obzirom na drastične promene medijskog okruženja poslednjih godina, značajnu pažnju treba obratiti na usklađivanje standarda istrage i sudske prakse sa načelom da novinarska zaštita pripada i učesnicima u javnoj komunikaciji koji nemaju formalni status novinara, ali stalno ili povremeno preduzimaju novinarski čin, odnosno izveštavaju javnost o pitanjima od javnog interesa.

Ukoliko postoji namera da se postavi nova definicija medija i novinara, Preporuke ministarskog saveta EU činile bi dobru osnovu.[1] Takođe, izveštaj koji je raniji specijalni izvestilac UN za slobodu izražavanja Frank La Ru objavio 2012. godine, predviđa da se novinari definišu kao pojedinci koji posmatraju, opisuju, dokumentuju i analiziraju događaje, izjave, politike i svaki stav koji može da utiče na društvo, sa svrhom sistematizovanja takvih informacija, sakupljanja činjenica i analize radi informisanja delova društva ili društva u celini.[2]

Dobra praksa ukazuje da se na ovo pitanje može odgovoriti sa dva aspekta - statusnog i delatnog. Naime, građani i organizacije mogu steći posebna prava ili kroz profesionalnu vezu sa medijskom organizacijom, udruženjem novinara i samoregulatornim instrumentima, ili kroz novinarski čin, odnosno prikupljanje i širenje informacija u javnom interesu i vršenje kontrole vlasti.

U situaciji kada postoji funkcionalna veza, podrazumevana je pretpostavka da građani, odnosno organizacija imaju posebna novinarska prava i zaštitu, dok se kod kontekstualne veze čini da je na građanima teret dokazivanja da u konkretnoj situaciji vrše novinarski akt koji im omogućava novinarske beneficije.

Odgovori na niz značajnih pitanja predstavljaju moguće repere za budući (samo)regulatorni model koji nadilazi okvire sektorskih propisa. U kom trenutku pojedinac ili organizacija počinju profesionalno da se bave medijskom delatnošću i na koji način to utiče na njihov regulatorni status? Da li uopšte ima smisla regulisati male medije sa neznatnom tržišnom snagom? Koji kriterijum bi bio odgovarajući za potencijalno regulisanje u slučaju medijskog aktera sa velikim uticajem na određene zajednice i koji ostvaruje značajne prihode? Da li postoji potreba za automatskom primenom medijske regulative u slučaju neregistrovanog onlajn medija? Kada se aktiviraju pravila oglašavanja i zaštite potrošača?

2.1.2. STATISTIKA IZ REGISTRA

Od uspostavljanja Registra medija pri Agenciji za privredne registre (ranije: Registar javnih glasila) do kraja februara 2017, u Registar je ukupno upisano 539 onlajn medija, od čega je svega 14 podnelo zahtev za brisanje.

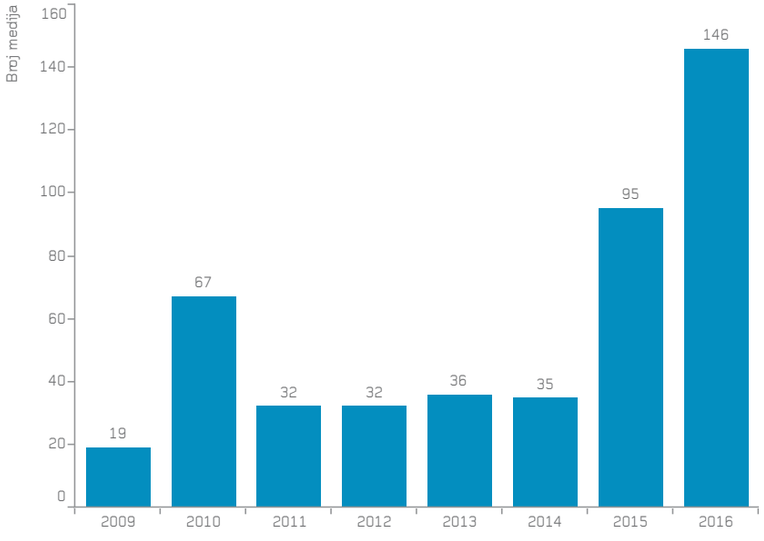
Broj registrovanih onlajn medija se povećava: 2014. se upisalo 35, naredne se broj novoregistrovanih popeo na 95, dok se tokom 2016. registrovalo čak 146 onlajn medija. Ovaj trend se može objasniti usvajanjem novog Zakona o javnom informisanju i medijima, čije odredbe ne obavezu-

1 Preporuka CM/Rec(2011)7 o novoj odrednici medija https://search.coe.int/cm/Pages/result _ details.aspx?ObjectID=09000016805cc2c0

2 Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session20/A-HRC-20-17 _ en.pdf

ju onlajn medije na registraciju ali upis u Registar postavljaju kao uslov, između ostalog, za projektno finansiranje iz javnih izvora.[3]

Ne računajući period pre usvajanja novih medijskih zakona, najveći skok u broju novoregistrovanih medija zabeležen je 2015. godine (više od dva puta veći broj u odnosu na prethodnu godinu). Rast je tokom 2016. godine usporen.



Broj registrovanih onlajn medija po godinama

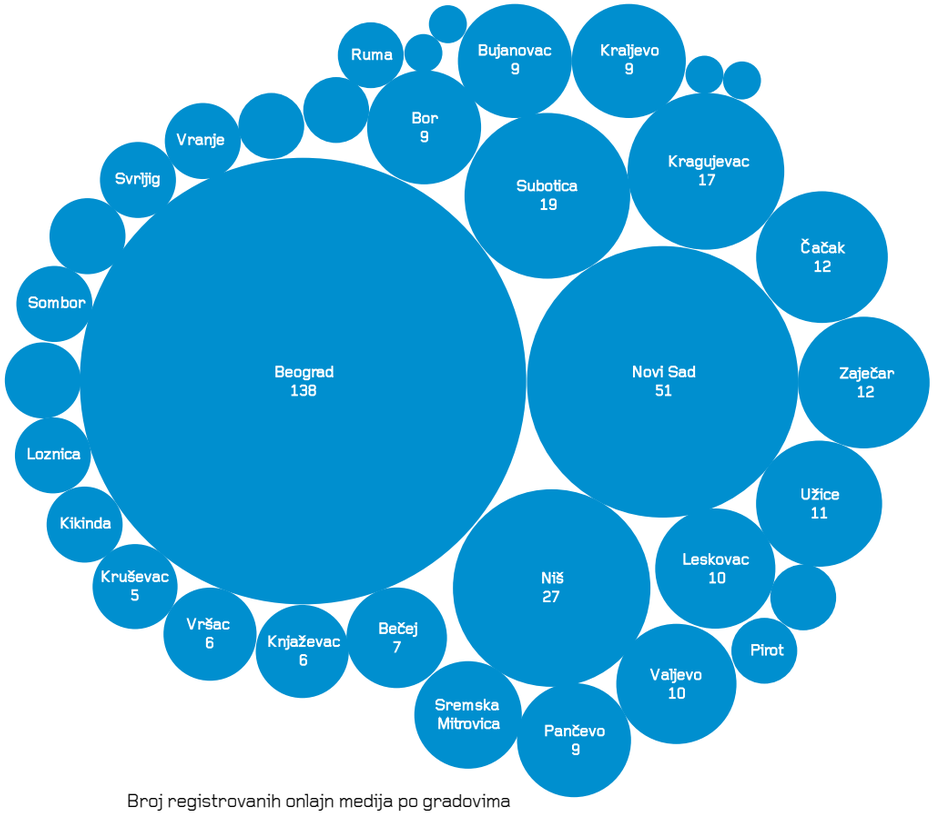
Po broju registrovanih onlajn medija očekivano prednjače veliki gradovi poput Beograda (132), Novog Sada (49) i Niša (25), kao i regionalni centri (Kragujevac, Zaječar, Subotica, Čačak).

U prva dva meseca 2017. godine u Registar se upisalo novih 65 onlajn medija, što govori o nastavku trenda rasta registracije ove vrste medija.

Zanimljiv uvid u ponašanje zajednice u okruženju onlajn medija pruža istraživanje Share Labs sprovedeno tokom predizborne kampanje u proleće 2016. godine, u okviru kog je analiziran relevantan sadržaj desetak najuticajnijih domaćih informativnih portala - mada treba imati u vidu da je reč o periodu svojevrsnog vanrednog stanja u društvu, koji može i znatno oduda-rati od ponašanja u svakodnevnim prilikama.[4] Prema ovom istraživanju, prosečan životni vek jedne vesti u onlajn medijima u Srbiji traje između jednog i dva sata. Tokom prva dva sata vest se komentariše na matičnom sajtu i deli na mrežama, a onda joj se najčešće gubi trag u gomili novih sadrža-

3 Zakon o javnom informisanju i medijima, Službeni glasnik RS, br. 83/2014, 58/2015 i 12/2016 http://www.paragraf.rs/propisi/zakon _ o _ javnom _ informisanju _ i _ medijima.html

4 Analiza onlajn medija i društvenih mreža tokom izbora 2016. u Srbiji; SHARE Labs, 2016 https://labs.rs/sr/analiza-onlajn-medija-i-drustvenih-mreza-tokom-izbo-ra-2016-u-srbiji/



Broj registrovanih onlajn medija po gradovima

ja. Brzi tempo produkcije diktiraju tri najveće novinske agencije u Srbiji (Tanjug, Beta, FoNet) koje zajedno proizvode više od 60% vesti na onlajn medijima. Originalni sadržaji onlajn medija čine svega jednu četvrtinu vesti vezanih za izbornu kampanju, a koje su u ovom istraživanju činile korpus analiziranih tekstova u predizbornom periodu 2016.

Tradicionalni i onlajn mediji održavaju svoje prisustvo na društvenim mrežama u različitim oblicima - od jednosmernog saopštavanja linkova za nove sadržaje na matičnom sajtu do pune iskorišćenosti specifičnih mogućnosti platformi za deljenje raznovrsnog sadržaja, dvosmernu komunikaciju i dublje angažovanje publike. Razlike među pojedinim medijima u pristupu društvenim mrežama vidljive su već i iz podataka o broju pratilaca. Tako stranica javnog servisa na Fejsbuku ima svega osam hiljada lajkova, dok na Tviteru ista kuća ima više od 80.000 pratilaca. S druge strane, onlajn istraživački medij KRIK ima gotovo četvorostruko više angažovanih korisnika na Fejsbuku nego na Tviteru.

Fejsbuk je primarni kanal neformalne distribucije sadržaja za većinu tradicionalnih medija: u stotinama hiljada lajkova mere se stranice dnevnih listova kao što su Politika (109.000), Večernje novosti (356.000), Kurir (748.000) ili Blic (892.000), te novosadskog radija 021 (126.000), TV Pink (341.000) ili TV B92 (499.000). Za većinu je Tviter platforma od manjeg

značaja: dnevni list Blic ima dvostruko manje pratilaca na ovoj mreži, dok TV Pink ima čak pedeset puta manje (6.000).

2.1.3. PRAVNI POLOŽAJ ONLAJN MEDIJA

Zakon o javnom informisanju i medijima[5] definiše šta se i pod kojim uslovima smatra medijima (članovi 29-31), obuhvatajući elektronska izdanja tradicionalnih medija (štampe, agencija, radio i tv stanica) i samostalna elektronska izdanja, odnosno urednički oblikovane internet stranice ili internet portale, za koje je naznačen uslov upisa u Registar medija. Iz svoje definicije Zakon izričito isključuje internet forume, društvene mreže i slične platforme, pri čemu se ostali oblici proizvodnje i distribucije informativnog sadržaja na internetu (blogovi, veb prezentacije, onlajn portali) ne smatraju medijima ukoliko nisu upisani u Registar medija.

Dakle, zakonodavac je građanskim i onlajn medijma ostavio izbor da se, ukoliko to žele, registruju kao mediji i da na taj način steknu odgovarajući status sa svim pravima i obavezama. Neregistrovani građanski i onlajn mediji ostaju van opsega ovog Zakona.

Ovakav pristup ograničava posebne oblike pravne zaštite i druge beneficije koje uživaju mediji, uslovljavajući zaštitu registrovanjem elektronskog izdanja. S druge strane, neregistrovani onlajn i građanski mediji nisu dužni da poštuju posebne obaveze koje su Zakonom propisane medijima.

Posebne odgovornosti koje snose registrovani mediji, između ostalog, uključuju obavezu novinarske pažnje, proširenu odgovornost urednika, novinara i izdavača, te transparentnost vlasništva. Status registrovanog medija omogućava zaštitu izvora informacija, nesporan režim krivično-pravne zaštite bezbednosti novinara, poseban osnov za isključenje krivičnog kažnjavanja novinara, kao i neposredniji pristup informacijama i privilegovan položaj prilikom izveštavanja, posebna ograničenja autorskih prava, te pristup javnim fondovima koji su namenjeni finansiranju projekata u oblasti javnog informisanja.[6]

Registrovani medij je dužan da u okviru svog sajta ima stalno dostupan impresum, odnosno podatke o nazivu, sedištu izdavača, imenima urednika i slično, dok sadržaj koji objavljuje podleže i posebnim obavezama kojima se reguliše medijski diskurs, kao što su zabrana podsticanja diskriminacije i mržnje. Sadržaj medija takođe ne sme da naškodi moralnom, intelektualnom, emotivnom ili socijalnom razvoju maloletnika. Drugim rečima, u procesnom tretmanu prekršaja i krivičnih dela, otežavajuću okolnost čini ukoliko su počinjena na sajtu koji ima status medija, odnosno sredstva javnog informisanja.

5 Zakon o javnom informisanju i medijima http://www.paragraf.rs/propisi/zakon _ o _ javnom _ informisanju _ i _ medijima.html

6 N. Krivokapić, O. Colić, M. Maksimović, Pravni položaj online medija u Srbiji: vodič namenjenonline i građanskim medijima kao korisnicima, SHARE Fondacija, 2015. http://www.shareconference.net/sites/default/files/u742/vodic-pravnipolozaj _ onlajn _ medija _ u _ srbiji _ - _ preview _ .pdf

Registar medija vodi Agencija za privredne registre[7], dok je za pokretanje postupka registracije potrebno da medij ima izdavača (pravno lice ili preduzetnik, registrovan za obavljanje delatnosti), odgovornog urednika i verifikovane podatke o vlasnicima koji neposredno ili posredno imaju više od 5% udela u osnivačkom kapitalu izdavača medija koji se registruje i drugih izdavača postojećih medija. Naknada za upis u Registar iznosi 2.800 dinara, odnosno nešto više od 10% minimalne neto zarade u januaru 2017.

PREDNOSTI REGISTRACIJE MEDIJA

- Zaštita izvora informacija
- Poseban režim krivično-pravne zaštite ličnog integriteta novinara
- Posebni osnovi isključenja krivičnog kažnjavanja
- Pristup informacijama i akreditacije za izveštavanje
- Pristup državnim fondovima - sufinansiranje projekata u oblasti javnog informisanja radi ostvarivanja javnog interesa
- Posebna pravila o slobodnoj upotrebi autorskih dela za medije

ODGOVORNOSTI REGISTROVANOG MEDIJA

- Obaveza novinarske pažnje – ,,odgovorno novinarstvo''
- Proširena odgovornost urednika, novinara i izdavača
- Pravila koja se tiču preuzetih informacija
- Ostala posebna pravila: impresum, oglašavanje, autorska prava, itd.
- Obaveza prijavljivanja sredstava iz javnih fondova

7 Registar medija, APR http://apr.gov.rs/Регистри/Медији/Медији-ОРегистру.aspx

PREPORUKE

Unaprediti pravila vodenja Registra medija u pogledu detaljnijih podataka koji se prikupljaju, obima njihove javne dostupnosti, definisanja mehanizama kontrole ažuriranja podataka i sankcija u slučaju nepoštovanja obaveza. Obezbediti da podaci iz Registra medija, bez naknade, budu dostupni za ponovnu upotrebu, zajedno sa metapodacima, u mašinski čitljivom i otvorenom obliku. Stvoriti preduslove za formiranje registra audio-vizuelnih medijskih usluga koje se pružaju putem interneta i audio-vizuelnih medijskih usluga na zahtev.

2.2. MEDIJSKA STRATEGIJA 2011-2016

Strategija razvoja sistema javnog informisanja u Republici Srbiji do 2016. godine doneta je u jesen 2011. i praktično označava početak reformskog ciklusa u medijskoj sferi.[8] Okosnica Strategije bila je izlazak države iz vlasništva u medijima te transparentnost vlasništva, novi modeli finansiranja iz javnih prihoda i slično, u skladu sa proklamovanim načelom sprečavanja neposrednog uticaja javne vlasti na rad medija. Fokusirana na javne medijske servise (RTS i RTV) i lokalne medije čiji su osnivači organi javne vlasti, Strategija je trasirala put za usvajanje medijskih zakona tri godine kasnije, koji će bliže regulisati ove oblasti.

S obzirom na urgentnost rešavanja državnog vlasništva u medijima, Strategija je dobrim delom zanemarila niz drugih pitanja koja izviru iz, tada već očiglednih, radikalnih promena u realizaciji javnog informisanja u digitalnom okruženju. Značajnija pažnja je u ovom dokumentu posvećena samo procesu digitalizacije televizijskog signala, sprovedenom 2015. godine.

U drugom poglavlju (Analiza stanja u oblasti javnog informisanja u Republici Srbiji), Strategija razlikuje tradicionalna elektronska javna glasila od sredstava javnog informisanja koja sadržaj emituju posredstvom interneta, konstatujući nedostatak propisa kojima se uređuje ta oblast. Strateškim dokumentom je iskazana namera države da podstiče tehnološke inovacije u medijskom prostoru i razvoj novih medijskih platformi. Međutim, Strategija nije dala smernice za neku buduću regulativu ni modele podsticaja, izuzev obaveze da se medijski sadržaji od javnog značaja koji su proizvedeni na novim tehnološkim platformama, tretiraju ravnopravno u pogledu mogućnosti projektnog finansiranja.

Strategija se poziva na Digitalnu agendu EU po kojoj se svim građanima mora obezbediti pristup internetu velikog protoka, pogodnog za razvoj i korišćenje širokopojasnih servisa. Konačno, Strategijom se potvrđuje da država Srbija ,,priznaje internet kao osnovno ljudsko pravo, kao javno dobro koje je lako dostupno svima i otvoreno u smislu slobode izražavanja i informisanja'', što je ključno političko opredeljenje na kom treba insistirati i u budućim dokumentima ove vrste, a koje treba imati u vidu i prilikom izrade odgovarajućih propisa.

Paket medijskih zakona usvojen je u Skupštini Srbije 2. avgusta 2014. godine kako bi se omogućio izlazak države iz vlasništva u medijima tokom narednih godinu dana, prelazak na projektno finansiranje medija iz javnih prihoda i transformaciju regulatornog tela za elektronske medije. Zakon o javnom informisanju i medijima, Zakon o elektronskim medijima i Zakon o javnim servisima stupili su na snagu desetak dana kasnije. Sva tri zakona trpela su naknadne izmene.

Mada se očekivalo da će rad na novoj medijskoj strategiji započeti i pre formalnog isteka stare, nadležno ministarstvo se ovim povodom još nije oglasilo. Deo medijske zajednice i građanskih organizacija samostalno je pokrenuo seriju javnih debata krajem 2016. godine, u nastojanju da se formulišu neki od ključnih problema koji bi trebalo da se nađu u novom strateškom dokumentu.[9] U ovom dijalogu je, kao jedno od važnijih pitanja buduće strategije, prepoznata potreba digitalnog opismenjavanja medija i publike, te bliže uređenje odnosa države prema onlajn medijima.[10]

Krajem marta 2017. Vlada Srbije usvojila je izmene[11] Uredbe o prenosu kapitala bez naknade zaposlenima kod izdavača medija iz 2015. kojom je prema novom Zakonu o javnom informisanju i medijima trebalo rešiti situacije u kojima medij nije privatizovan do postavljenog roka. Dva novinarska udruže-nja, NUNS i NDNV, upozorila su da se na ovaj način omogućava prenos akcija medija u kojima je privatizacija poništena na lokalne samouprave, što nije u skladu sa medijskim zakonima, te da je ovo znak da je država ,,definitivno odustala od medijskih reformi i najavila reetatizaciju medija u Srbiji''.[12]

Nadležno ministarstvo je odbacilo ove optužbe, navodeći da se izmenama Uredbe sprečava gašenje medija u kojima je raskinuta privatizacija, do kojeg bi došlo stečajem ili likvidacijom: ,,Ministarstvo kulture i informisanja uverava NUNS i NDNV da nije odustalo od medijskih reformi. Naprotiv, na ovaj način jedino želimo da štitimo kako pravo građana da budu

8 Strategija razvoja sistema javnog informisanja http://nuns.rs/reforma-javnog-informisanja/strategija.html

9 Konferencija iz serije SpeakUp!, ,,U susret savremenoj medijskoj politici'', TACSO i OEBS, novembar 2016. http://www.tacso.org/news/events/?id=14590

10 Seriju debata o novoj medijskoj strategiji organizovao je i Novi magazin, uz podršku Fonda za otvoreno društvo http://www.novimagazin.rs/vesti/onlajn-informisanje-digitalna-prava-i-vestine-medijska-pismenost-brzi-razvoj-brzi-i-problemi

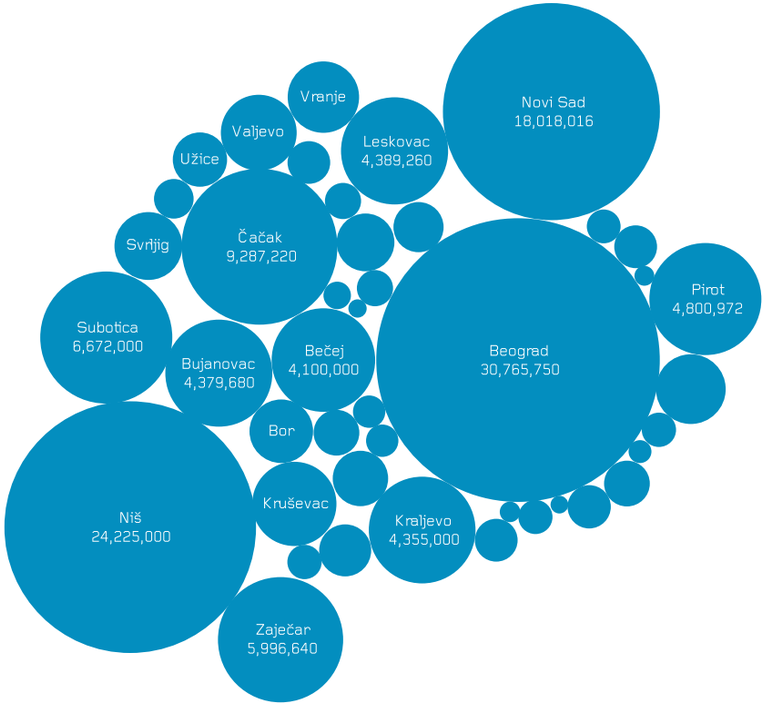
11 Uredba o izmeni Uredbe http://www.srbija.gov.rs/extfile/sr/289619/uredba-prenos-kapitala-zaposleni-mediji046 _ cyr.zip

12 NUNS i NDNV: Država ponovo postaje vlasnik medija http://nuns.rs/info/statements/30565/nuns-i-ndnv-drzava-ponovo-postaje-vlasnik-medija.html

informisani tako i da pružimo mogućnost novinarima i medijskim radnicima da nastave da rade u interesu javnosti.''[13]

2.3. PRIMENA MEDIJSKIH ZAKONA: PROJEKTNO FINANSIRANJE

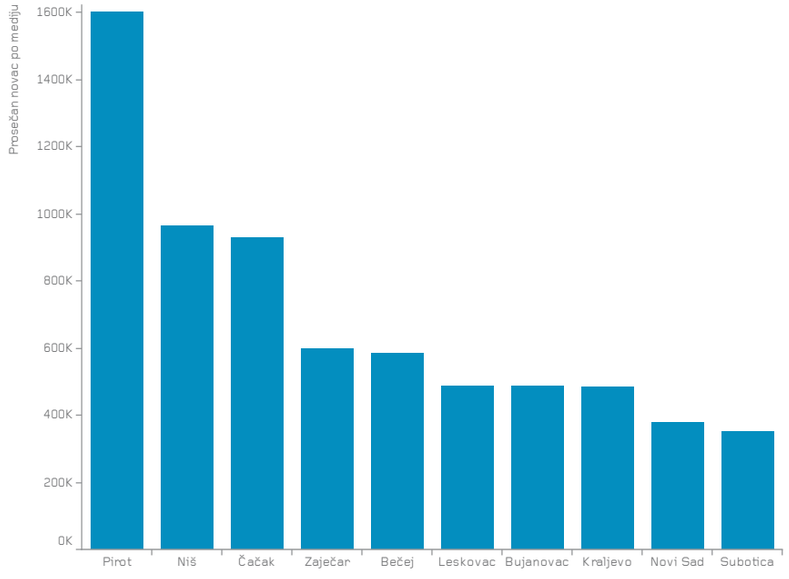
Prema podacima dostupnim u Registru medija pri Agenciji za privredne registre, koji obuhvata finansiranje iz javnih fondova na republičkom, pokrajinskom i lokalnom nivou, budžetska izdvajanja usmerena su u gradove koji su sedišta najvećem broju registrovanih onlajn medija. Zbirno, najviše sredstava iz javnih budžeta opredeljeno je za onlajn medije u najvećim gradovima (Beograd, Niš, Novi Sad) ali i drugim gradovima prema kojima pojedini regioni gravitiraju (Zaječar, Čačak, Bujanovac, Subotica).



Izdvojena sredstva za onlajn medije po gradovima (RSD)

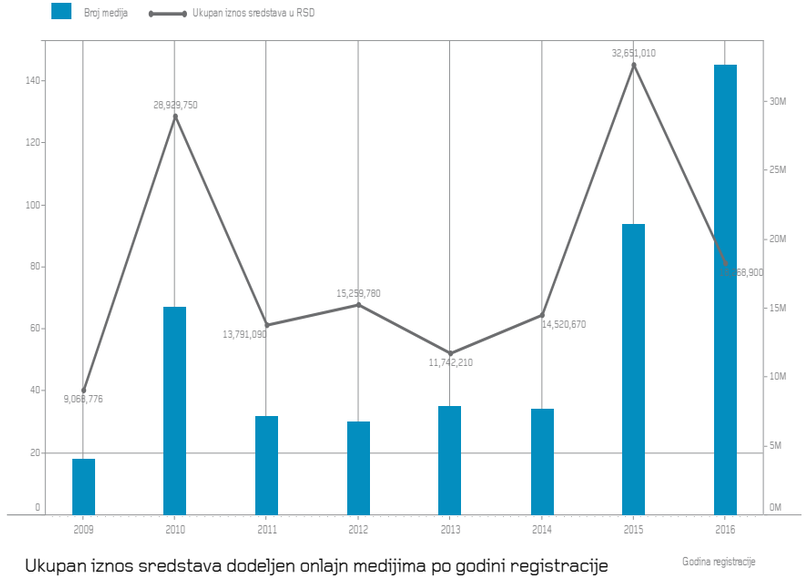
13 Ministarstvo kulture i informisanja: NUNS i NDNV za gašenje, Vlada za opstanak medija http://www.kultura.gov.rs/lat/aktuelnosti/ministarstvo-kulture-i-informisanja:-nuns-i-ndnv-za-gasenje--vlada-za-opstanak-medija

Pojedinačno, najviše novca po onlajn mediju dodeljeno je u Pirotu gde su tri onlajn medija dobila ukupno nešto više od 4.800.000 dinara, odnosno svaki onlajn mediji je u proseku dobio 1.600.000 dinara.



Prosečan iznos sredstava dodeljen onlajn medijima po gradovima

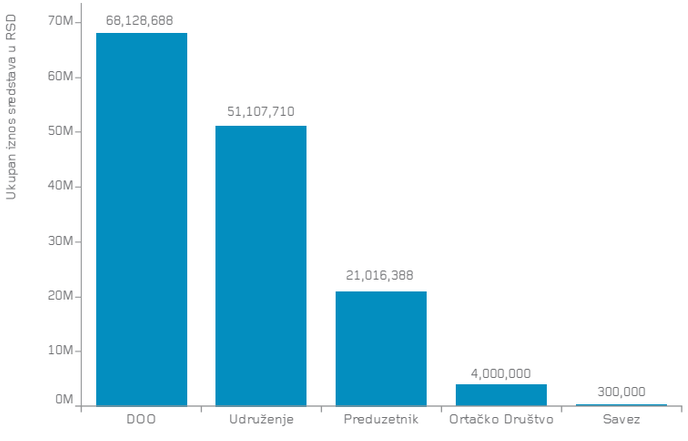
Među onlajn medijima koji su dobili novac iz javnih budžeta, najviše je onih koji su registrovani 2015. godine, kada je projektno finansiranje počelo da se primenjuje.



Ukupan iznos sredstava dodeljen onlajn medijima po godini registracije

Od 520 obrađenih registrovanih onlajn medija (zaključno sa januarom 2017. godine) 133 je primilo sredstva po ovom osnovu projektnog finansiranja, odnosno 26%. U odnosu na broj registrovanih onlajn medija u pojedinoj godini, izdvajanja iz budžeta relativno su ujednačena i retko prelaze trećinu:

- 2009 - 36.8%
- 2010 - 20.9%
- 2011 - 25%
- 2012 - 28.1%
- 2013 - 30.5%
- 2014 - 45.7%
- 2015 - 33.6%
- 2016 - 22.6%



Broj onlajn medija koji su dobili novčana sredstva prema formi osnivača

Najveći procenat medija koji su dobili sredstva iz javnih izvora registrovani su 2009. i 2014. godiine, a odmah za njima su mediji registrovani 2015, nakon donošenja nove regulative i uspostavljanja sistema projektnog sufinansiranja.

Budući da su po novom zakonu svi registrovani mediji dužni da prijavljuju sredstva primljena iz javnih fondova, sa republičkog, pokrajinskog i lokalnog nivoa, podaci o sufinansiranju projekata su dostupni u bazi Registra medija. Prema ovim podacima, za 81 onlajn medij je 2015. godine ukupno izdvojeno 68.579.196 dinara, dok je 2016. godine novcem iz javnih fondova finansirano 106 onlajn medija, sa ukupnim iznosom od 75.739.280 dinara.

Kao javni izvor koji pojedinačno raspolaže sa najviše sredstava namenjenih javnom informisanju, Ministarstvo kulture i informisanja značajno je za analizu i kao najviši nivo uprave na kom se donose presudne političke odluke i u značajnoj meri usmerava nacionalni kurs. Prva raspodela sredstava namenjenih medijima po novom budžetskom modelu u ovom Ministarstvu, realizovana je kroz šest konkursa tokom 2015. godine, od kojih je konkursom za sufinansiranje projekata proizvodnje medijskih sadržaja iz oblasti javnog informisanja, u dva polugodišnja ciklusa, raspodeljeno najviše novca: 164 miliona dinara.

Ukupno je odabrano 228 projekata štampanih, elektronskih medija i produkcija, dobrim delom u realizaciji lokalnih medija. U prvom ciklusu, od 161 odabranog projekta, 25 kandidovali su onlajn i građanski mediji koji sadržaj distribuiraju na internetu, za koje su izdvojena sredstva u rasponu od 72.000 do dva miliona dinara.[14] Od toga, za 12 projekata izdvojeno je do pola miliona dinara pojedinačno, oko 700-800 hiljada dobilo je pet projekata, koliko je odabrano i za iznos subvencije od po milion dinara. Jednom projektu dodeljeno je oko 1,5 miliona a dva su dobila 1,9 odnosno 2 miliona dinara.

Drugim konkursnim ciklusom iz 2015. opredeljeno je znatno manje sredstava za 67 odabrana projekta, od čega su 13 kandidovali onlajn i građanski mediji.[15] U ovom navratu, izdvojena sredstva za informisanje javnosti na internetu bila su ujednačena, u rasponu od 450.000 do 600.000 dinara.

Ukupno, Ministarstvo je u 2015. za javno informisanje na internetu izdvojilo oko 25 miliona dinara, dok je naredne godine ova suma iznosila nešto manje od 28 miliona.

U 2016. sproveden je jedan konkurs iz oblasti javnog informisanja na kom je podržano 176 projekta sa 151.410.000 dinara.[16] Među ukupno 36 projekata onlajn i građanskih, odnosno medija koji su kandidovane projekte realizovali na internetu, 20 je finansirano sumama od po pola miliona dinara. Sledećih osam projekata dobilo je iznose manje od milion, za četiri je izdvojeno po milion dinara, dva su dobila po 1,5 a jedan 1,7 miliona. Jedan projekat sufinansiran je sumom od 2,5 miliona dinara.

Ukoliko sprovodi evaluaciju realizovanih projekata, Ministarstvo kulture i informisanja takve procedure i eventualne rezultate ne objavljuje.

Ni medijska zajednica se ne bavi posebno analizom rezultata projektnog finansiranja kroz realizovane projekte i njihove efekte. Jedno istraživanje nacionalne organizacije za razvoj medija iz regionalne mreže BIRN, posvećeno prvoj godini primene novog modela finansiranja, obuhvatilo je 30 projekata koji većinom predstavljaju primere dobro izvedenih programskih sadržaja.[17]

14 Rešenje o raspodeli sredstava, 11.05.2015. http://www.kultura.gov.rs/docs/konkursi/19919583532220160079/RESENJE%20OPSTI%20KONKURS.pdf

15 Rešenje o raspodeli sredstava, 20.11.2015. http://www.kultura.gov.rs/docs/konkursi/15328113138329153612/RESENJE,kona%C4%8Dno.pdf

16 Rešenje o raspodeli sredstava, 22.07.2016. http://www.kultura.gov.rs/docs/konkursi/82925044729285405888/Resenje,%20proizvodnja%20medijskih%20sadrzaja.pdf

17 Projektno finansiranje medija: Rezultati prve godine primene novog budžetskog modela, BIRN Srbija 2016. http://birnsrbija.rs/wp-content/uploads/2016/12/Projektno-finansiranje-medija-Ministarstvo-kulture-i-informisanja.pdf

Među analiziranim projektima nalazi se i šest koje su realizovali onlajn mediji - Jug press, Južne vesti, Vojvođanski istraživačko-analitički centar (VOICE), portal Udruženja novinara Srbije, istraživački portal Pištaljka udruženja Eutopija i sajt Udruženja novinara za poljoprivredu Agropress.

Izuzev projekta UNS, koji je realizovan kroz informativni sadržaj usmeren pre svega ka samoj medijskoj zajednici i stručnoj javnosti, i projekta Agropressa čiji je rezultat u analizi ocenjen kao nezadovoljavajući, ostali projekti onlajn medija iz analizirane grupe opravdali su svoju ulogu u informisanju javnosti o pitanjima od opšteg značaja. Bavili su se istraživanjem poslovanja javnih preduzeća, transparentnim programskim budžetiranjem, partijskim zapošljavanjem u javnoj administraciji i korupcijom na lokalnom nivou.

Sličnu analizu za 2015. godinu BIRN Srbija sproveo je i prema izdvajanju iz budžeta Vojvodine, odnosno medijske konkurse Pokrajinskog sekretarijata za kulturu, javno informisanje i odnose sa verskim zajednicama, gde je za privatna preduzeća i organizacije civilnog društva predviđeno ukupno oko 53 miliona dinara. Međutim, dodeljeno je tek oko 34,3 miliona jer prema proceni komisije nije bilo dovoljno kvalitetnih projekata da se ostatak raspodeli. U 2016. godini budžet Sekretarijata za podršku javnom informisanju smanjen je šest puta - na svega 8,5 miliona dinara. Tim novcem je podržano 48 projekata, za razliku od 2015. kada je više od 100 projekata dobilo finansijsku podršku. Kao problem se ističe činjenica da ne postoje javno dostupni podaci o proizvedenim sadržajima i namenskom trošenju novca, kao ni o tome u kojoj meri je kroz finansiranje projekata unapređeno javno informisanje.[18]

U 2015. godini, onlajn mediji privatnih preduzeća i civilnog društva su na konkursu Pokrajinskog sekretarijata[19] dobili ukupno oko 2.900.000 dinara. Na konkursu sprovedenom 2016. godine[20] situacija je daleko drugačija u pogledu dodeljenih sredstava, pa su tako onlajn mediji za projekte sufinansiranja dobili svega nešto više od 1.200.000 dinara, tj. u proseku oko 135.000. Kada je reč o sufinansiranju projekata onlajn informisanja na manjinskim jezicima, novčana sredstva od AP Vojvodine je 2016. dobio samo portal ,,Vajdasag ma'', koji objavljuje sadržaj na mađarskom, i to 168.000 dinara. Poređenja radi, isti portal je na konkursu godinu dana ranije dobio više nego dvostruko veću sumu (366.000 dinara).

U medijskoj i srodnim zajednicama sve češće se kao problem ističe činjenica da se iz javnih fondova subvencionišu projekti medija koji kontinuirano krše Kodeks novinara Srbije, odnosno da građani silom prilika finansiraju, između ostalog, objavljivanje neistina i spekulacija, kršenje pretpostavke nevinosti i ugrožavanje privatnosti. Savet za štampu je predložio da se izmenama odgovarajućeg Pravilnika[21] propiše da su odluke Komisije za žalbe Saveta za štampu obavezujuće prilikom razmatranja projekata, odnosno da mediji koji krše Kodeks ne mogu da računaju na novac iz budžeta. Početkom 2017. godine, državni sekretar za informisanje u Ministarstvu kulture izjavio je da je taj predlog Saveta za štampu prihvatljiv, kao i da Ministarstvo radi na izmenama Zakona o javnom informisanju i Zakona o elektronskim medijima.[22]

PREPORUKE

Podsticati javne konkurse za projektno sufinansiranje onlajn medija, posebno u oblastima izveštavanja u lokalnoj zajednici, kao i informativnog, naučno-obrazovnog i kulturnog sadržaja, te sadržaja na jezicima nacionalnih manjina. Onlajn mediji su ekonomičniji a značajno doprinose pluralizmu u oblasti javnog informisanja. Kao poseban, obavezan kriterijum uključiti pitanje prihvatanja i poštovanja Kodeksa novinara Srbije prilikom usvajanja projekata za sufinansiranje.

18 Rezultati prve godine primene novog budžetskog modela - Pokrajinski sekretarijat za kulturu i javno informisanje AP Vojvodine, BIRN Srbija http://birnsrbija.rs/wp-content/uploads/2016/08/Projektno-finansiranje-medija-AP-Vojovodina.pdf

19 Pokrajinski sekretarijat za kulturu i javno informisanje AP Vojvodine, rezultati konkursa za 2015. godinu http://www.kultura.vojvodina.gov.rs/Konkursi/rez _ inform _ 15/rezul _ inform _ 15.htm

20 Pokrajinski sekretarijat za kulturu i javno informisanje AP Vojvodine, rezultati konkursa za 2016. godinu http://www.kultura.vojvodina.gov.rs/Konkursi/rez _ inform _ 16/rezultat _ inform _ 16.htm

21 Pravilnik o sufinansiranju projekata za ostvarivanje javnog interesa u oblasti javnog informisanja http://www.kultura.gov.rs/docs/dokumenti/propisi-iz-oblasti-medija/pravilnik-o-sufinansiranju-projekata-za-ostvarivanje-javnog-interesa--u-oblasti-javnog-informisanja--.docx

22 Građani će opet finansirati i medije koji iznose neistine, Insajder https://insajder.net/sr/sajt/tema/2927/Gra%C4%91ani-%C4%87e-opet-finansirati-i-medije-koji-iznose-neistine.htm

VODIČ:

PRAVNI POLOŽAJ ONLINE MEDIJA U SRBIJI

Vodič „Pravni položaj online medija u Srbiji“ predstavlja nova rešenja iz Zakona o javnom informisanju i medijima važna za onlajn i građanske medije. Digitalne platforme poput blogova, foruma, društvenih mreža i samostalnih internet portala po zakonu se ne smatraju medijima, osim ako odluče da se registruju. Vodič daje pregled svih prava i obaveza koje bi onlajn mediji stekli ukoliko se registruju, razlika u odgovornosti za objavljene sadržaje u medijskom i opštem režimu i samog procesa registracije.

Iako sticanje statusa medija u pravnom smislu podrazumeva mnoga dodatna prava, poput zaštite identiteta izvora informacija, višeg standarda zaštite ličnog integriteta novinara ili pristupa državnim fondovima, istovremeno se preuzimaju i određene obaveze. Neke od tih obaveza su novinarska pažnja, tj. proveravanje porekla, istinitosti i potpunosti informacija pre objavljivanja, čuvanje medijskih zapisa i isticanje impresuma, dok izdavač medija, urednik i novinar imaju proširenu odgovornost za sadržaje u skladu sa Zakonom o javnom informisanju i medijima.

(Vodič objavljen u martu 2015.)

2.4. ONLAJN MEDIJI I SAMOREGULACIJA

Onlajn izvori, poput internet portala, blogova i društvenih mreža, omogućavaju raznovrsniji spektar dostupnih informacija, nelinearno praćenje povezanih sadržaja i neposrednije učešće publike u stvaranju i deljenju vesti. Međutim, brzina kojom se informacije šire na internetu, kao i odsustvo selekcije učesnika u javnom informisanju, između ostalog, uslovili su nekontrolisan prodor kršenja etičkih i profesionalnih standarda novinarstva u javni prostor, pronošenja neistina, ugrožavanja privatnosti, kršenja pretpostavke nevinosti, širenja diskriminacije i slično. Ako građanski novinari i slobodne platforme žele da istinito, blagovremeno i potpuno izveštavaju javnost, neophodno je da poštuju odredbe Kodeksa novinara Srbije, bez obzira da li su profesionalni novinari ili ne.

Savet za štampu je u Srbiji osnovan 2009. godine, kao nezavisno, samoregulatorno telo koje prati poštovanje Kodeksa novinara Srbije. U punoj nadležnosti Saveta do skoro su bili samo štampani mediji i njihova onlajn izdanja, da bi nedavno ovo telo uspostavilo instrument ograničene nadležnosti i u odnosu na medije koji nisu prihvatili njegovu punu nadležnost. Time je omogućeno da se protiv svakog štampanog medija, novinske agencije ili informativnog portala može podneti žalba, ukoliko se smatra da je povređen Kodeks novinara Srbije.[23]

Internet okruženje je pred medije i profesionalne novinare postavilo nove etičke izazove, pa nije uvek jednostavno primeniti odredbe Kodeksa na sadržaj objavljen na onlajn platformama. Stoga su tokom 2016. godine pripremljene Smernice za primenu Kodeksa novinara Srbije u onlajn okruženju, prvi zvanični dokument ove vrste u regionu, koje omogućavaju shodnu primenu etičkih principa novinarske profesije na novonastalo tehničko okruženje.[24] Smernice pružaju jasne upute novinarima, urednicima i medijima, čitaocima, oglašivačima i Komisiji za žalbe Saveta za štampu kako da izađu na kraj sa novim izazovima.

„Ovaj dokument je prevashodno namenjen novinarima i medijima koji su dostupni onlajn, ali je primenljiv i na druge forme izražavanja na internetu, gde se na različitim platformama plasiraju uredrnički oblikovani medijski sadržaji. Cilj je da se razjasne brojne nedoumice koje se odnose na primenu standarda dužne novinarske pažnje, odnosa prema izvorima informacija, načina na koji se prenose medijski sadržaji, poštovanja privatnosti, poštovanja autorstva i na druga važna pitanja uređena Kodeksom", navodi se u Preambuli smernica Saveta za štampu.

23 SHARE Fondacija je u ime Sajmona Vilsona krajem oktobra 2013. godine podnela žalbu protiv internet portala „Teleprompter", koji nije registrovan kao javno glasilo, niti je član relevantnih udruženja. Savet za štampu je prihvatio nadležnost i izrekao javnu opomenu portalu: http://www.shareconference.net/sh/defense/savet-za-stampu-portal-teleprompter-prekrsio-kodeks-novinara-srbije

24 Smernice za primenu Kodeksa novinara Srbije u onlajn okruženju http://www.savetzastampu.rs/latinica/smernice-za-primenu-kodeksa-novinara-srbije-u-onlajn-okruzenju

Svako od 10 poglavlja Kodeksa novinara Srbije interpretirano je za internet okruženje i prošireno specifičnim odrednicama onlajn medijima, dok su pojedine oblasti, poput sadržaja koji generišu korisnici, preuzimanja informacija sa društvenih mreža i poštovanja autorstva, nešto detaljnije opisane. Smernice su značajno sredstvo u procesu daljeg digitalnog opismenjavanja novinara i publike.

Između ostalog, načelo istinitosti izveštavanja, primenjeno na medije koji informacije skladište i dele na internetu, podrazumeva zabranu fabrikovanja digitalnih tragova, naknadne izmene sadržaja bez naznake karaktera, uzroka i vremena izmene, odnosno antidatiranja objavljenog sadržaja. Novinarska pažnja u onlajn okruženju primenjuje se na društvene mreže i druge platforme neformalne razmene informacija, dok se zvanični nalozi medija na ovim mrežama takođe smatraju uredrnički oblikovanim sadržajem. Nalog poštovanja autorstva i integriteta autorskog sadržaja na snazi je i u onlajn okruženju, posebno s obzirom na digitalne alate za obradu, agregatore vesti i slično.

PREPORUKE

Podsticati razvoj samoregulacije, primenu Kodeksa novinara Srbije i prihvatanje nadležnosti Komisije za žalbe Saveta za štampu. Pružiti podršku daljem razvoju etičkih pravila u oblasti informisanja u digitalnom okruženju. Podsticati onlajn medije, organizacije koje održavaju prisustvo na internetu, gradanske novinare i ostale aktere koji se bave izveštavanjem javnosti o pitanjima od javnog značaja, a koji ne žele da budu registrovani kao mediji, da prihvate Kodeks novinara Srbije i nadležnost Komisije za žalbe Saveta za štampu. Promovisati primenu mehanizama samoregulacije sadržaja u zajednici. Jačati princip postmoderacije sadržaja koji postavljaju treća lica. Promovisati mehanizme brzog i jasnog prijavljivanja štetnog i nedozvoljenog sadržaja.

VODIČ:

DOBRE PRAKSE I REGULATORNI MODELI ZA ODGOVORNO OBJAVLJIVANJE ONLAJN KOMENTARA

Digitalno medijsko okruženje, pored onlajn izdanja štampe, radija i televizije, danas čine i brojne druge platforme kao što su informativni portali, blogovi, servisi za pretraživanje, društvene mreže, onlajn prodavnice, sajtovi za deljenje video-sadržaja, agregatori vesti i slične. Okosnicu ovih servisa predstavljaju sadržaji koje kreiraju sami korisnici (user-generated content), koji doprinose interakcijama (šerovanje, lajkovanje, retviti, fejvanje) i od kojih zavisi prihod platforme. Sadržaji sa više interakcija će privući više korisnika, te će oglašivači biti više zainteresovani da plasiraju reklame na ovakvim onlajn platformama.

Onlajn komentari omogućavaju sajtovima medija i drugim informativnim platformama donekle ravnopravnu utakmicu sa društvenim mrežama u privlačenju korisnika, tj. uvećanju saobraćaja. Prakse koje umanjuju vidljivost komentara i onemogućavaju njihovo trenutno objavljivanje, znatno usporavaju interakcije među korisnicima, ograničavaju rasprave i slobodan protok informacija, što snižava atraktivnost sajtova za oglašivače. S druge strane, sekcija komentara bez moderatorske kontrole izlaže medije pravnim rizicima.

(Vodič objavljen u oktobru 2015.)

2.5. SPORAZUM O SARADNJI MEDIJA, POLICIJE I TUŽILAŠTVA

PREPORUKE

Operacionalizovati saradnju policije i tužilaštva sa onlajn portalima koji su česta meta hakerskih napada, u pravcu efikasnijeg suzbijanja pretnji po informacionu bezbednost. Otkloniti pravnu neizvesnost pitanja ko ima pravo na posebnu zaštitu novinara i pravo na zaštitu novinarskih izvora.

Kao važan korak u poboljšanju zaštite novinara, krajem decembra 2016. potpisan je sporazum o saradnji i merama za podizanje nivoa bezbednosti novinara, između predstavnika Ministarstva unutrašnjih poslova, Republičkog javnog tužilaštva i sedam novinarskih i medijskih udruženja (Udruženje novinara Srbije, Nezavisno udruženje novinara Srbije, Udruženje novinara Vojvodine, Nezavisno društvo novinara Vojvodine, ANEM, Asocijacija medija i Asocijacija onlajn medija).[25] Tehnički napadi na portale onlajn medija i pretnje novinarima na društvenim mrežama već neko vreme ugrožavaju slobodu izražavanja. Dodatni problem na koji SHARE Fondacija ukazuje jeste selektivna zaštita od pretnji koje nadležni organi pružaju novinarima i aktivistima.[26] Slučajevi brze i efikasne reakcije policije i tužilaštva na pretnje upućene državnim funkcionerima, u sve većoj su disproporciji sa slučajevima u kojima novinari, posebno oni sa istraživačkih i kritičkih portala, i posle više prijavljenih pretnji dugo čekaju na ishode istraga. Formalna saradnja novinarskih udruženja i nadležnih državnih organa predstavlja značajnu kariku u obezbeđivanju pravne sigurnosti i izvesnosti u istragama napada na novinare i medije.

Sporazumom je predviđeno da se ustanovi sistem mera za ,,obezbeđivanje efikasnije krivičnopravne zaštite novinara''. Usaglašeno je 10 aktivnosti, od kojih su među najvažnijima formiranje radne grupe za sprovođenje sporazuma čiji će članovi biti ovlašćeni predstavnici potpisnika, određivanje kontakt osoba, vođenje evidencija krivičnih dela na štetu novinara, formiranje registra o krivičnim delima protiv novinara, medija i informativnih internet portala, kao i obuke novinara i vlasnika medija o osnovama informacione bezbednosti. Sporazumom je takođe predviđena edukacija zaposlenih u Ministarstvu i tužilaštvu.

Već i samo unapređenje mera zaštite kroz neposrednu saradnju medijske zajednice i nadležnih institucija, doprinosi prevenciji povreda prava. Za dosledno sprovođenje zakona u slučajevima kada dođe do pretnji, pritisaka, fizičkih napada i različitih dela iz oblasti visokotehnološkog kriminala, neophodan je element efikasnog postupanja. MUP i Republičko javno tužilaštvo su se sporazumom obavezali da svojim internim aktima uspostave obavezu hitnog postupanja u predmetima krivičnih dela protiv novinara, najkasnije u roku od tri meseca od potpisivanja sporazuma. Usvajanjem obaveze hitnog postupanja slučajevi pretnji u digitalnom okruženju i sajber-napadi na novinare i informativne portale trebalo bi da postanu prioritet policije i tužilaštva, naročito s obzirom na to da prethodni slučajevi tehničkih napada na sajtove poput Peščanika ili CINS-a ni gotovo tri godine kasnije nisu rešeni. Istrage brojnih slučajeva pretnji upućenih novinarima na društvenim mrežama i komentarima na tekstove, takođe su ostale bez pravnog epiloga.

25 Sporazum o saradnji i merama za podizanje nivoa bezbednosti novinara http://www.aom.rs/wp-content/uploads/2016/12/Sparazum-o-saradnji.pdf

26 Selektivna zaštita, SHARE Fondacija, 2015. http://www.shareconference.net/sh/blog/selektivna-zastita

VODIČ:

ZAŠTITA TAJNOSTI IZVORA INFORMA-CIJA

Pravo na zaštitu anonimnosti izvora od ključnog je značaja za izveštavanje o pitanjima od javnog interesa, s kojima društvo na drugi način ne bi bilo upoznato. Neke od najznačajnijih reportaža u istoriji novinarstva (npr. afera „Votergejt" u SAD) nastale su upravo zahvaljujući saznanjima dobijenim iz izvora čiji je identitet skriven od javnosti. S druge strane, izmišljanje i zloupotreba anonimnih izvora predstavljaju grube prekršaje profesionalnih i etičkih standarda.

U eri digitalnih komunikacija, informisanje javnosti više nije rezervisano samo za novinare tradicionalnih medijskih organizacija - brojne internet platforme, poput blogova, foruma, društvenih mreža i nezavisnih onlajn portala, omogućavaju građanima da učestvuju u izveštavanju javnosti o društvenim pojavama i problemima. Pošto se može reći da korisnici društvenih medija obavljaju ulogu sličnu novinarima, da li u određenim slučajevima treba da uživaju i prava profesionalnih novinara, kao što je zaštita identiteta izvora informacije? Odgovor na ovu i slične nedoumice nalazi se u odgovarajućim propisima, preporukama, međunarodnim iskustvima i sudskoj praksi.

(Vodič objavljen u oktobru 2015.)

2.6. PRAVNI POSTUPCI I SUDSKE ODLUKE

PREPORUKE

Unaprediti kapacitete pravosuda za primenu regulatornog okvira na onlajn medije. Kroz obrazovanje policije, tužilaštva, sudstva i advokature, ustanoviti praksu sistemskog usvajanja znanja o karakteristikama digitalnog okruženja, rizicima i zaštiti slobode govora u kontekstu komunikacije koja preovladava na internetu. Obezbediti ujednačenu efikasnost pravosuda u procesuiranju povreda i pretnji po prava građana na internetu, bez obzira na to ko je ugrožena strana, kako bi se izbegla pravna nesigurnost selektivne zaštite.

SHARE Fondacija prati procesni razvoj pojedinih slučajeva iz monitoringa, njihovu pravnu kvalifikaciju i sudske odluke. Incidenti iz sajber prostora retko ulaze u sudsku proceduru, njihov pravni tretman nije uvek odraz razumevanja povreda u onlajn okruženju, dok sami procesi, bilo parnični ili krivični, traju prilično dugo, čak i po nekoliko godina.

1. ZORAN PERIŠIĆ V. JUŽNE VESTI

Bivši gradonačelnik Niša Zoran Perišić tužio je portal Južne vesti za povredu časti i ugleda zbog teksta „Spasić: vlast ukrala pare radnika EI" iz septembra 2014. godine. Viši sud u Beogradu je u prvostepenom postupku presudio[27] u korist Perišića, ali je redakcija Južnih vesti uložila žalbu na presudu.[28]

2. TUŽILAŠTVO V. RADOMIR POČUČA

Bivši portparol Protivterorističke jedinice MUP-a Srbije Radomir Počuča prvostepeno je oslobođen odgovornosti da je izvršio krivično delo ugrožavanja sigurnosti. Presuda je izrečena u Višem sudu u Beogradu, a pisani otpravak će biti naknadno izrađen. Krivični postupak protiv Počuče je pokrenut jer je 2014. na svom Fejsbuk profilu pozivao na nasilje prema članicama nevladine organizacije Žene u crnom.[29]

27 Presuda Višeg suda u Beogradu http://niskevesti.rs/wp-content/uploads/2016/11/Presuda-1.pdf

28 Presuda u korist Perišića protiv Južnih vesti, novembar 2016. http://niskevesti.rs/presuda-u-korist-perisica-protiv-juznih-vesti/

3. TUŽILAŠTVO V. JELENA POPOVIĆ IVANOVIĆ

Profesorka Srednje mašinske škole u Novom Sadu Jelena Popović Ivanović pravnosnažno je osuđena na uslovnu kaznu od tri meseca zatvora, sa rokom provere od godinu dana, zbog njene Fejsbuk objave iz 2011. u kojoj je širila mržnju i netrpeljivost prema LGBT populaciji. Apelacioni sud u Beogradu je potvrdio prvostepenu presudu Višeg suda u Beogradu iz maja 2016. za krivično delo rasne i druge diskriminacije.[30] Presuda još uvek nije dostupna.

4. FUNKCIONERI V. GRAĐANI

Prema pisanju portala „Pištaljka", policija iz Bogatića je krajem 2016. saslušavala najmanje jednog građanina kako bi utvrdila ko je na Fejsbuk stranici „Mačva zdravog razuma" vređao trojicu lokalnih funkcionera, među kojima je i predsednik opštine Nenad Beserovac. Osnovno javno tužilaštvo u Šapcu je posle prijave funkcionera navelo da nema elemenata krivičnog dela za koje se gonjenje preduzima po službenoj dužnosti, ali je takođe navelo da policija u Bogatiću treba da preduzme sve mere i radnje u cilju pronalaženja lica koje je vređalo funkcionere, kako bi oni mogli da ga tuže.[31]

UGROŽAVANJE SIGURNOSTI PUTEM INTERNETA

Presude donete tokom 2016. godine, koje su od značaja za razumevanje ljudskih prava u onlajn okruženju, pružaju uvid u rezon sudova prilikom primene zakona na platforme za deljenje sadržaja i društvene medije.

1. BORIS MALAGURSKI V. FORUMAŠI

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

ETAPE PROCESA

1. Prvostepeni postupak: Viši sud u Beogradu 11.03.2014. donosi osuđujuću presudu protiv trojice optuženih i izriče krivične sankci-

29 Počuča oslobođen za pretnje Ženama u crnom i vraćen mu oduzeti pasoš, decembar 2016. http://www.kurir.rs/crna-hronika/izrecena-presuda-pocuca-oslobodjen-za-pretnje-zenama-u-crnom-i-vracen-pasos-clanak-2588901

30 Profesorki Srednje mašinske uslovna kazna za širenje mržnje protiv LGBT populacije, septembar 2016. http://www.021.rs/story/Novi-Sad/Vesti/144105/Profesorki-Srednje-masinske-uslovna-kazna-za-sirenje-mrznje-protiv-LGBT-populacije.html

31 Policija istražuje ko je uvredio funkcionere, decembar 2016. https://pistaljka.rs/home/read/578

je izdržavanja kazne zatvora u trajanju od godinu dana, s tim da utvrđene kazne neće biti izvršene ukoliko okrivljeni u roku od tri godine od pravnosnažnosti ne izvrše neko novo krivično delo. Ovaj postupak se ponavlja zbog procesnih grešaka pa Viši sud u prvom stepenu ponovo donosi osuđujuću presudu 24.03.2015. kojom izriče iste kazne.

2. Drugostepeni postupak po žalbi okrivljenih: Apelacioni sud u Beogradu 09.09.2015. godine delimično uvažava žalbe branioca okrivljenih i preinačuje presudu Višeg suda u Beogradu, tako da dvojicu optuženih osuđuje na 6 meseci zatvora, uslovno 2 godine, a jedno lice na 4 meseca zatvora, uslovno 2 godine. Žalba je, dakle, bila uspešna u delu smanjenja kazne.

3. Postupak po vanrednom pravnom leku: Okrivljeni su iskoristili zahtev za zaštitu zakonitosti, vanredni pravni lek, nakon čega Vrhovni kasacioni sud 20.01.2016. donosi oslobađajuću presudu.

ANALIZA PRESUDE VRHOVNOG KASACIONOG SUDA KZZ 1203/2015 OD 20.01.2016. GODINE

Vrhovni kasacioni sud je naveo da se u zahtevu za zaštitu zakonitosti osnovano ističe da je primenjen zakon koji se nije mogao primeniti, što bi značilo da se radnje koje su okrivljeni preduzeli ne mogu smatrati krivičnim delom ugrožavanja sigurnosti.

Sud je zaključio da u izreci pravnosnažne presude nedostaje bitan element krivičnog dela ugrožavanja sigurnosti, a to je pretnja da će se napasti na život i telo oštećenog. Da bi bila element krivičnog dela, pretnja mora biti ozbiljna i mora se odnositi na napad na život ili telo oštećenog lica. Posebno kada je reč o verbalnoj pretnji kojom se najavljuje napad, što je ovde slučaj, ona mora biti jasna i nedvosmislena, odnosno da se iz pretnje može zaključiti da će izvršilac zaista i napasti oštećeno lice, bez obzira da li on to namerava da učini.

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

Sud je konstatovao da izreka sporne presude sadrži samo želje okrivljenih da se oštećenom desi neko zlo, ali ne i izjavu da će okrivljeni oštećenom takvo zlo i naneti. Stoga su okrivljeni oslobođeni.[32]

2. JUŽNE VESTI V. KOMENTATORI

Sudski epilog dobila je i krivična prijava onlajn medija Južne vesti, protiv lica koje je na portalu ostavilo komentar: ,,Južne vesti su najveća medijska go...a u Nišu, treba zapaliti da ne postoje, lažljive, iskompleksirane degenerike koji tamo rade''.[33]

32 Vrhovni kasacioni sud, Kzz 1203/2015 http://www.vk.sud.rs/sr/K33-12032015

33 Sud: ,,Treba zapaliti novinare'' nije pretnja, već sloboda govora, juli 2016. https://www.juznevesti.com/Drushtvo/Sud-Treba-zapaliti-novinare-nije-pretnja-vec-sloboda-govora.sr.html

Pravnosnažnom presudom Višeg suda u Nišu potvrđena je prvostepena oslobađajuća presuda Osnovnog suda u Nišu u korist okrivljenog. Sud je i u ovom slučaju došao do zaključka da se ne može govoriti o pretnji, iz razloga što okrivljeni ,,niti jednog momenta nije izrazio lične namere za preduzimanjem bilo kakve radnje koje bi kod oštećenih ugrozila sigurnost. Samo u situaciji da je okrivljeni izrazio lične namere u pogledu delovanja prema oštećenima, pri čemi je bez uticaja da li bi te namere bile stvarne, moglo bi se govoriti o postojanju krivičnog dela ugrožavanje sigurnosti''.

Razmatranje presuda nadležnih sudova u Srbiji navodi na utisak da u procesima pokrenutim zbog navodnog ugrožavanja sigurnosti, uglavnom nema bitnog elementa ovog krivičnog dela, odnosno ozbiljne, jasne i nedvosmislene pretnje, kao i lične namere da se napadne na život i telo pojedinca ka kom je pretnja usmerena. U svakom pojedinačnom slučaju mora se uzeti u obzir i celokupan kontekst u kojem su informacije objavljene, uz tumačenje svih iskazanih reči.

3. UVREDE SA DRUŠTVENIH MREŽA - SUDSKA PRAKSA U SUKOBU

Do Vrhovnog kasacionog suda došao je i predmet okrivljenog I.P. koji je podneo zahtev za zaštitu zakonitosti protiv pravnosnažnih presuda Osnovnog suda u Novom Sadu K 266/15 od 21.12.2015. godine i Višeg suda u Novom Sadu Kž1 110/16 od 24.06.2016. godine.[34] U ovom slučaju osuđeno je lice zbog produženog krivičnog dela uvreda koje je učinjeno putem društvene mreže Fejsbuk, iz člana 170. stav 2. KZ, na novčanu kaznu od 250.000,00 dinara, zbog toga što je uvredio privatnu tužilju objavljivanjem više tekstova na svojoj stranici.

Sud je ipak nakon razmatranja slučaja došao do zaključka da je zahtev neosnovan i potvrdio je presudu kojom je okrivljeni proglašen krivim. Navodi okrivljenog u zahtevu da se Fejsbuk stranica ne može smatrati sredstvom javnog informisanja nisu prihvaćeni. ,,[...] po nalaženju Vrhovnog kasacionog suda facebook stranica kao deo društvenih mreža, upravo zbog dostupnosti iste korisnicima ovih mreža na internetu predstavlja sredstvo slično sredstvima štampe, radija ili televizije i sledstveno tome putem ovog sličnog sredstva - facebook stranice se može uputiti uvredljiva izjava i samim tim izvršiti krivično delo uvreda.''

Rezonovanje Vrhovnog kasacionog suda da je Fejsbuk sredstvo ,,slično sredstvima štampe, radija ili televizije'' odudara od zaključka Višeg suda u Beogradu donetog u pravosnažnoj presudi od 25.08.2015. u predmetu u kojem je razmatrana uvreda upućena preko Tvitera.[35] Naime, u prvostepenom postupku, Osnovni sud u Beogradu je optuženog oglasio krivim za krivično delo uvrede iz čl. 170 stav 2, tj. za kvalifikovani oblik dela koje je učinjeno putem štampe, radija, televizije ili sličnih sredstava ili na javnom skupu. Međutim, Viši sud je ovu presudu preinačio, pozivajući se na odredbu

34 Vrhovni kasacioni sud, Kzz 1058/2016 http://www.vk.sud.rs/sr-lat/kzz-10582016

35 Presuda Kž1 br. 465/15

člana 11 Zakona o javnom informisanju, koji je bio na snazi u vreme izvršenja krivičnog dela. Ovom odredbom je propisano da su javna glasila ''novine, radio programi, televizijski programi, servisi novinskih agencija, internet i druga elektronska izdanja navedenih javnih glasila […] namenjene javnoj distribuciji i neodređenom broju korisnika''. Viši sud je stao na stanovište da društvena mreža Tviter ,,predstavlja grupu individualno određenih internet korisnika koji su međusobno povezani radi interpersonalne komunikacije i međusobne ramene informacija, mišljenja i ideja njenih članova'', te da se stoga ova mreža ne može smatrati sličnom štampi, radiju ili televiziji ,,koji predstavljaju sredstva javnog informisanja i namenjeni su javnoj distribuciji i neodređenom broju korisnika''.

Ovakvo tumačenje Višeg suda odgovara i smislu važećeg Zakona o javnom informisanju i medijima koji u članu 30, stav 2, nedvosmisleno propisuje šta nisu mediji, odnosno iz definicije medija izričito isključuje forume i društvene mreže.[36] Uzimajući u obzir celokupni pravni okvir, definicije koje su bile u osnovi i starog i novog zakona, odluka Vrhovnog kasacionog suda predstavlja presedan koji direktno ugrožava slobodu mišljenja i izražavanja.

Osim što je jasno da se na društvene mreže ne može primenjivati član 170, stav 2, Krivičnog zakonika, posebno u svetlu novih, jasnih odredbi Zakona o javnom informisanju i medijima, trebalo bi skrenuti pažnju i na samu uvredu, koja je i dalje krivično delo u Krivičnom zakoniku, iako se u svetu teži dekriminalizaciji klevete i uvrede. Republika Srbija je 2013. dekriminalizovala klevetu, ali je uvreda iz nejasnih razloga ostala u krivičnom sistemu. Krivično delo uvrede predstavlja izjavu ili drugu radnju kojom se, po objektivnoj oceni, izražava omalovažavanje određenog lica. Međutim, ovako široko definisan, ovaj pojam se praktično može primeniti na bilo koju izjavu izrečenu na društvenim mrežama. Ukoliko bi odluka Vrhovnog kasacionog suda uspostavila novu praksu, odnosno da se Tviter i Fejsbuk tretiraju kao štampa ili televizija, svaka od tih izjava mogla bi dobiti i svoj kvalifikovani oblik dela učinjenog putem sredstva javnog informisanja.

Budući da su mogućnosti i rizici interneta kao novog medijskog okruženja, još uvek nedovoljno poznati, čini se da u praksi domaćih sudova nedostaje razumevanje komunikacije, tehničkih karakteristika i načina primene zakona u onlajn sferi. Uz unapređenje znanja i usvajanje novih standarda u radu nadležnih institucija, ali i podizanje odgovornosti među samim korisnicima interneta, treba očekivati razvoj sudske prakse u dobrom smeru.

36 Zakon o javnom informisanju i medijima, Službeni glasnik RS, br. 83/2014, 58/2015 i 12/2016 http://www.paragraf.rs/propisi/zakon _ o _ javnom _ informisanju _ i _ medijima.html

3. INFORMACIONA PRIVATNOST

Na osnovu zahteva za pristup informacijama od javnog značaja poslatih Povereniku za informacije od javnog značaja i zaštitu podataka o ličnosti, SHARE Fondacija je aprila 2014. došla u posed 2000 stranica dokumenata i izveštaja, u vezi sa Poverenikovim izveštajem o izvršenom nadzoru nad sprovođenjem i izvršavanjem Zakona o zaštiti podataka o ličnosti od strane operatora mobilne i fiksne telefonije u Srbiji. Ta dokumenta su poslužila kao osnova za analizu zadržavanja metapodataka i arhitekture elektronskog nadzora.

Tehnička i pravna analiza, predstavljena kroz infografike, ilustruje različite načine na koje četiri operatora mobilne i fiksne telefonije u Srbiji omogućavaju državnim organima direktan pristup korisničkim metapodacima. Bitno je napomenuti da svaki uređaj, bez obzira na to da li je pametan telefon ili mobilni telefon starije generacije, generiše metapodatke. Jedina značajna razlika između ovih uređaja je u tome što stariji telefoni nemaju pristup internetu, stoga je ovo istraživanje sprovedeno sa fokusom na pametne telefone.

U svrhu povezivanja na Mrežu, uređaj koristi dva identifikaciona broja. Prvi je IMEI broj uređaja (International Mobile Station Equipment Identity - Međunarodni identitet mobilne opreme), a drugi je IMSI broj SIM kartice (International Mobile Subscriber Identity - Međunarodni identifikacioni broj korisnika). Oba ova broja su jedinstvena i unapred definisana za svaki uređaj i SIM karticu. Mrežnu infrastrukturu mobilnih operatora čine bazne stanice (BS), geografski raspoređene po području koje pokriva pojedini mobilni operator.

Prilikom iniciranja poziva, uređaj s kojeg se poziva kontaktira najbližu baznu stanicu koja dalje prosleđuje poziv centrali mobilne telefonije (Mobile Switching Centre, MSI). Centrala zatim obaveštava baznu stanicu najbližu uređaju koji se poziva, s kojim se zatim uspostavlja veza. Kada je veza uspostavljena, tj. kada se pozvani korisnik javi, metapodaci se generišu u mobilnoj centrali. Centrala skladišti metapodatke u data centru operatora. Sam sadržaj poziva se ne arhivira, ali takođe prolazi kroz centralu.

KOJA VRSTA METAPODATAKA SE ARHIVIRA?

Različite centrale prikupljaju različite vrste metapodataka, ali postoji opšti tip metapodataka koje arhiviraju svi operatori, kao što su identifikacioni broj koji poziva, pozvani broj, IMEI, detalji bazne stanice, datum i vreme poziva, količina podataka (za internet), tip usluge, identitet obe strane u komunikaciji, spisak svih SIM kartica koje su korišćene u tom uređaju, i obrnuto, spisak svih uređaja u kojima je korišćena ta određena kartica.

KAKO SE PODACI SKLADIŠTE?

Operatori u Srbiji su obavezani zakonom da metapodatke svakog korisnika čuvaju 12 meseci. Nije striktno definisano da li operatori moraju da poseduju sopstvene, ili mogu da koriste servere druge kompanije.

KAKO SE MOŽE PRISTUPITI OVIM PODACIMA?

Mobilni operatori u Srbiji su formirali odeljenja koja se bave procedurama zadržavanja podataka, a zaposleni na tim odeljenjima su prošli posebne obuke. Pravo pristupa zadržanim podacima pripada organima pravosuđa, policiji, kao i civilnim i vojnim obaveštajnim službama.

Najveći operatori u Srbiji su implementirali dva mehanizma za pristup zadržanim podacima. Prvi mehanizam podrazumeva proceduru upućivanja zahteva operatoru, koji zatim razmatra zahtev i dostavlja odgovor: državni organi ovlašćeni za pristup metapodacima u svom zahtevu navode kojim podacima žele da pristupe, kako bi operator obradio zahtev i dostavio odgovarajući izveštaj. Zahtev državnih organa nužno sadrži i pravno obrazloženje ovlašćenja, odnosno sudski nalog.

Drugi mehanizam pristupa zadržanim podacima je sporan sa pravnog stanovišta, budući da podrazumeva aplikacije za samostalno pristupanje zadržanim podacima. Pojedini operatori su implementirali ovaj softver kako bi državnim organima olakšali pristup zadržanim podacima, pre svega u proceduralnom smislu, s obzirom na to da omogućavaju pristup zadržanim podacima bez odluke suda, što je u suprotnosti sa Ustavom.

Poslednjih godina doneti su brojni podzakonski akti koji definišu prava i obaveze operatora i državnih organa u vezi sa presretanjem elektronskih komunikacija. Ovom regulativom su operatori obavezani da kupe opremu (hardver i/ili softver) kojom će komunikacija biti presretana i dostaviti je u monitoring centar, čiji štab vodi BIA.

FIZIČKO PRAĆENJE U REALNOM VREMENU

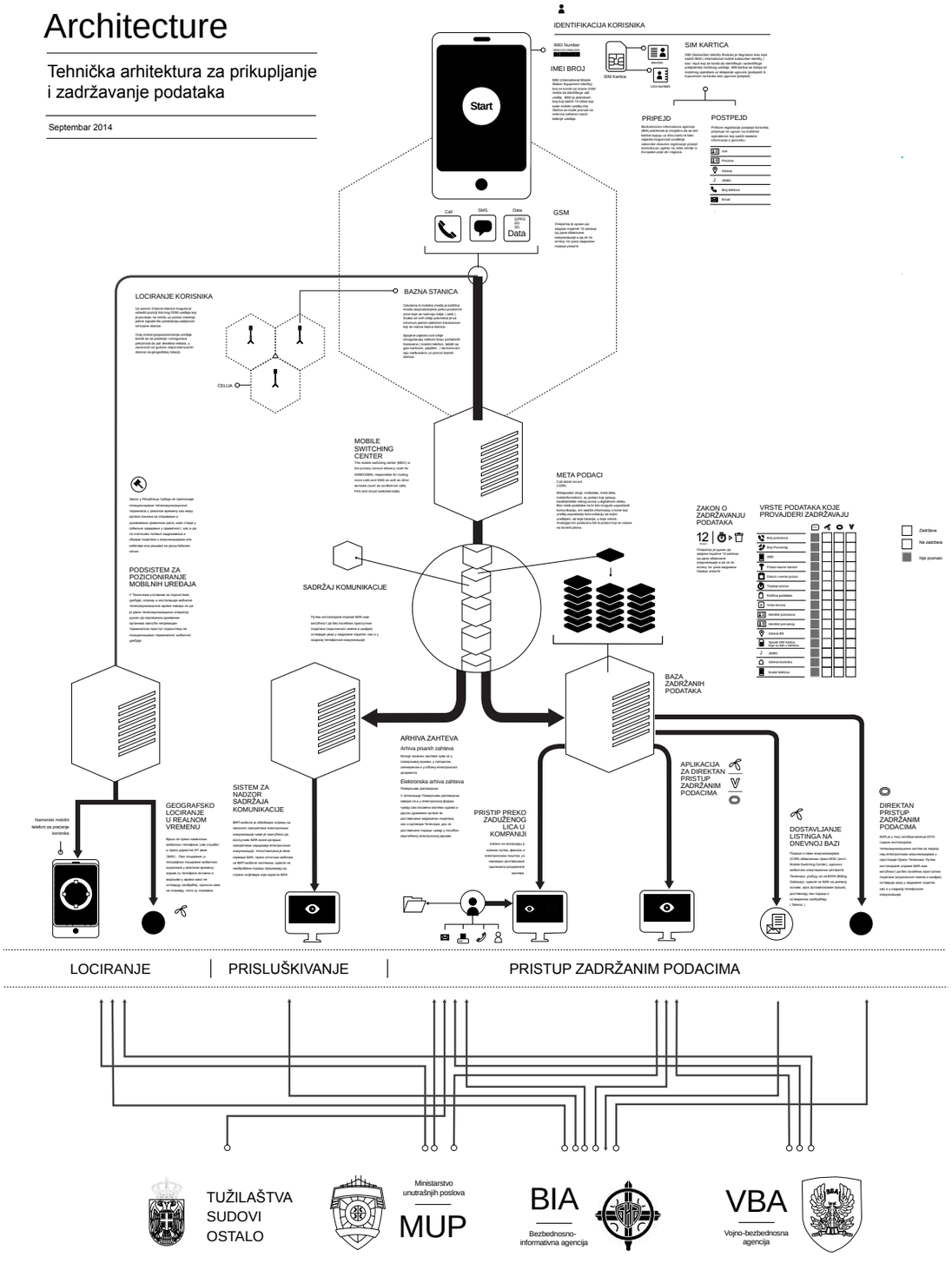
Bazne stanice predstavljaju "ćelije" infrastrukture operatora, koje međusobnim povezivanjem stvaraju celularnu, odnosno ćelijsku mrežu. Ćelija je zapravo geografsko područje koje pokriva jedna bazna stanica. Svaki pojedinačni uređaj je, u svakom trenutku, povezan sa tri bazne stanice radi kontinuiranosti signala – to znači da tri stanice neprestano razmenjuju dolazne i odlazne signale sa uređajem. Bazne stanice su tako postavljene da kroz nekoliko parametara u signalu registruju udaljenost uređaja, tj. određuju njegovu lokaciju. Neki od tih parametara su ugao prijema (AOA, Angle of Arrival), razlika vremena polaska i prijema (TDOA, Time Difference of Arrival) i vreme prijema (TOA, Time of Arrival). To znači da svako ko ima pristup baznoj stanici može u bilo kom trenutku, s visokim stepenom preciznosti, odrediti fizičku lokaciju svakog uređaja povezanog na mrežu.

U Srbiji, u skladu sa odgovarajućim podzakonskim aktima, pristup specijalnim terminalima opreme za praćenje uređaja ima Bezbednosno-informativna agencija. U upotrebi su, takođe, mobilni uređaji napravljeni po posebnim specifikacijama koji su konfigurisani na takav način da omogućavaju geo-praćenje u realnom vremenu. Ove mobilne uređaje izdaju operatori državnim organima na njihov zahtev. Svako ko ima pristup terminalu ovakve opreme, može tačno da locira bilo koji uređaj povezan na mrežu u Srbiji.

Surveillance Architecture

Tehnička arhitektura za prikupljanje i zadržavanje podataka

Septembar 2014

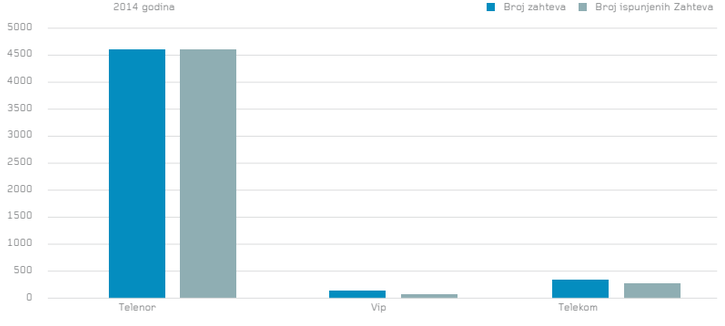


3.1. ELEKTRONSKI NADZOR: STATISTIKA

Osnovni oblik nadzora koji država sprovodi nad građanima, ne samo u Srbiji već i na globalnom nivou, još uvek je elektronski nadzor zadržanih podataka. Evropski sud pravde (ECJ) je u aprilu 2014. proglasio Direktivu Evropske unije o zadržanim podacima ništavnom[1], nakon čega je više država članica u okviru svojih legislativa proglasilo zakone o zadržanim podacima neustavnim.[2] Srbija zasad ne razmatra ukidanje regulative koja obavezuje operatore telekomunikacionih usluga, odnosno fiksne i mobilne telefonije i interneta, da zadržavaju podatke o svojim korisnicima kako bi bili dostupni istražnim i drugim organima.

Prema izveštajima koje su Povereniku za pristup informacijama od javnog značaja i zaštitu podataka o ličnosti, dostavili operatori za 2014. i 2015. godinu, nastavlja se trend zahteva za pristup zadržanim podacima, ali i samostalnog pristupa zadržanim podacima pri čemu se ne primenjuju sve zaštitne mere propisane Zakonom o elektronskim komunikacijama.

Drugi po veličini operator telekomunikacionih usluga u Srbiji, Telenor, registrovao je znatno više zahteva za pristup koje su tokom 2014. i 2015. uputili državni organi (MUP, BIA, VBA, sudovi) nego državni Telekom, koji je po broju korisnika najveći operator u zemlji. Tokom 2014. Telenor je registrovao 4611 zahteva, od čega je ispunio 4599, dok je od 2287 zahteva primljenih tokom naredne godine, ispunjeno 2257. Za to vreme, prema navodima Telekoma, ova kompanija je primila samo 344 zahteva za pristup zadržanim podacima drugoj polovini 2014. godine[3] od kojih je 280 ispunjeno. Naredne godine, Telekom je primio 745 zahteva i ispunio njih 546. Treći operator, Vip, prijavio je najmanje zahteva - 109 u 2014. (58 ispunjeno) i 147 u 2015. (69 ispunjeno).

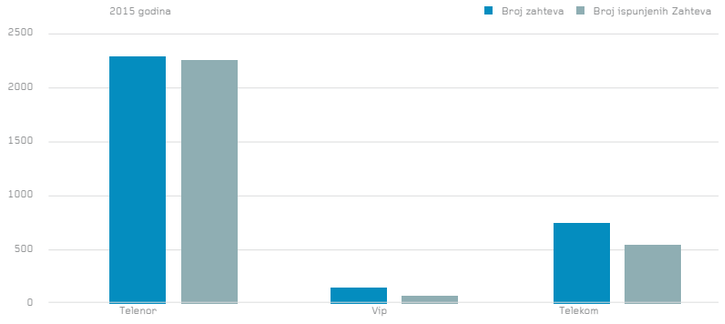


Broj podnetih i ispunjenih zahteva za pristup zadržanim podacima u 2014. godini

1 ECJ poništio direktivu o zadržanim podacima https://www.loc.gov/law/help/eu-data-retention-directive/eu.php

2 Regulativa o zadržavanju podataka u različitim državama https://www.goldenfrog.com/blog/global-data-retention-laws

3 Podaci koje je Telekom dostavio za 2014. godinu se odnose na period posle 21.06.2014., od kad je na snazi regulativa o izveštavanju o zahtevima za zadržane podatke.



Broj podnetih i ispunjenih zahteva za pristup zadržanim podacima u 2015. godini

Od velikih operatora koji su dostavili podatke Povereniku, samo je Telenor registrovao neposredne pristupe organa javne vlasti u IKT sistem kompanije, u svrhe pretrage zadržanih podataka. Broj samostalnih pristupa je višestruko veći u odnosu na dostavljene zahteve, što sugeriše mogućnost nasumičnog pretraživanje svih zadržanih podataka u potrazi za potrebnim podacima.

Tokom 2014. Telenorov IKT sistem registrovao je 201.879 samostalnih pristupa zadržanim podacima, i to: MUP 199.818, BIA 993, VBA: 1068. Naredne godine ukupno je ostvareno 300.845 samostalnih pristupa.

3.2. REFORMA OKVIRA ZA TELEKOMUNIKACIJE

Ministarstvo trgovine, turizma i telekomunikacija je 14. novembra 2016. objavilo javni poziv za učešće u javnoj raspravi o Nacrtu zakona o elektronskim komunikacijama, koja je trajala do 3. decembra 2016.[4] Nacrt novog zakona[5] ima za cilj da zameni trenutno važeći propis donet 2010. godine.[6] U tekstu Nacrta dve su oblasti od značaja za digitalna prava građana.

3.2.1. ZADRŽANI PODACI

Nacrtom Zakona je predviđeno da će odredbe trenutno važećeg Zakona o elektronskim komunikacijama koje se odnose na tajnost elektronskih komunikacija, zakonito presretanje i zadržavanje podataka, nastaviti da se primenjuju i nakon donošenja novog zakona i to sve do izrade posebnog zakona koji bi uredio ova pitanja. To znači da su predlagači Nacrta odlučili da u ovom trenutku ne menjaju pravni okvir u ovoj oblasti, odnosno da i nakon eventualnog stupanja na snagu novog zakona, presretanje elektronskih komunikacija kojim se otkriva sadržaj komunikacije, kao i pristup zadržnim podacima - ne bi bilo dopušteno bez pristanka korisnika, osim na određeno vreme i na osnovu odluke suda, ako je to neophodno radi vođenja krivičnog postupka ili zaštite bezbednosti Republike Srbije, na način predviđen zakonom.

Ipak, činjenica da je predviđeno donošenje posebnog zakona koji bi regulisao ova pitanja, otvara nove mogućnosti, naročito u pogledu usklađivanja domaćeg pravnog okvira sa najnovijim trendovima u okviru EU, ali i rizik snižavanja nivoa garantovanog prava na privatnost građana.

3.2.2. REGISTRACIJA PRIPEJD BROJEVA

Član 144 Nacrta zakona o elektronskim komunikacijama predviđa obaveznu „registraciju pretplatnika pre početka pružanja usluge preko javne mobilne komunikacione mreže" (st. 1). Međutim, nije definisano na koje će se tačno korisnike odnositi ova obaveza, iz čega se može zaključiti da bi registracija bila obavezna i za pripejd korisnike mobilne telefonije, što u važećem Zakonu nije slučaj.

Na osnovu iskustava zemalja u kojima su usvojena slična rešenja, kao i analize domaćeg pravnog okvira, SHARE Fondacija zastupa stav da bi uvođenje obavezne registracije pripejd SIM kartica korisnika mobilne telefonije u Srbiji predstavljalo intruzivnu meru, bez garancija da će ovakva mera zaista pomoći u borbi protiv kriminala i zaštiti nacionalne bezbednosti. Posebno brine činjenica da se obavezna registracija predlaže bez adekvatne analize društvenih i ekonomskih efekata, koja bi pružila argumente zašto je takva mera neophodna. U vezi s tim, značajno je pomenuti da se u najnovijem izveštaju GSM Asocijacije ističe da ne postoje empirijski dokazi da ova praksa direktno utiče na smanjenje stope kriminala.[7]

U okviru javne rasprave, SHARE Fondacija je nadležnom Ministarstvu uputila komentare na predloženu registraciju pretplatnika, sa stavom da bi član 144 Nacrta zakona o elektronskim komunikacijama trebalo izbrisati iz konačne verzije Nacrta.[8]

4 Javna rasprava o Nacrtu zakona o elektronskim komunikacijama http://mtt.gov.rs/vesti/javna-rasprava-o-nacrtu-zakona-o-elektronskim-komunikacijama/?lang=lat

5 Nacrt zakona o elektronskim komunikacijama http://mtt.gov.rs/download/Nacrt 20zakona 20o 20elektronskim 20komunikacijama.pdf?lang=lat

6 Zakon o elektronskim komunikacijama ("Sl. glasnik RS", br. 44/2010, 60/2013 - odluka US i 62/2014) http://www.paragraf.rs/propisi/zakon _ o _ elektronskim _ komunikacijama.html

7 Obavezna registracija pripejd SIM kartica, april 2016. http://www.gsma.com/publicpolicy/wp-content/uploads/2016/04/GSMA2016 _ Report _ MandatoryRegistrationOfPrepaidSIMCards.pdf

8 Komentari SHARE Fondacije na Nacrt zakona o elektronskim komunikacijama, decembar 2016. http://www.shareconference.net/sites/default/files/u742/komentari _ na _ nacrt _ zek _ share _ fondacija.pdf

3.3. ZAŠTITA PODATAKA O LIČNOSTI

3.3.1. ČEKAJUĆI NOVI ZAKON O ZAŠTITI PODATAKA O LIČNOSTI

PREPORUKE

Donošenje novog zakona o zaštiti podataka o ličnosti nalazi se u vrhu prioriteta u ovoj oblasti. Proces izrade teksta zakona mora uključiti odgovarajuću javnu raspravu, kako bi se našla optimalna rešenja u ravnoteži interesa privatnosti i zaštite ličnih podataka građana sa interesima razvoja ekonomije podataka i poslovanja domaćih i međunarodnih kompanija.

Trenutno važeći Zakon o zaštiti podataka o ličnosti donet je sada već davne 2008. godine. Iako je to prvi propis koji je regulisao ovu oblast u Srbiji, te su već na samom početku uočene brojne nelogičnosti i problemi u primeni, izuzev sitnih izmena Zakon je na snazi u integralnom obliku. Tako su do danas ostali neuređeni neki od ključnih segmenata ove oblasti, kao što su video-nadzor, biometrija, bezbednosne provere, privatni sektor bezbednosti, i drugi. Gotovo je suvišno govoriti koliko se svet promenio od kada je Zakon napisan, u kojoj meri su, kao posledica korišćenja informaciono-komunikacionih tehnologija i razvoja ekonomije podataka, pitanja zaštite podataka o ličnosti postala kompleksnija, što domaći pravni okvir uopšte ne prepoznaje.

Nakon četvorogodišnjeg procesa, u aprilu 2016. godine Evropski parlament i Savet su usvojili Opštu Uredbu o zaštiti podataka o ličnosti.[9] Usklađivanje domaćeg pravnog okvira sa ovom Uredbom svakako je glavni prioritet u ovoj oblasti. S jedne strane, to je obaveza Srbije u procesu pregovora sa Evropskom unijom, što je i predviđeno Akcionim planom za poglavlje 23. S druge, značajnije strane, treba istaći da Uredba predstavlja novi standard privatnosti građana i zaštite podataka o ličnosti, ali i u poslovanju kompanija koje na bilo koji način obrađuju podatke o ličnosti.

Poverenik za informacije od javnog značaja i zaštitu podataka još je sredinom 2014. godine izradio Model novog zakona i dostavio ga Vladi Srbije.

9 Direktiva (EU) 2016/680 Evropskog parlamenta i Saveta od 27. aprila 2016. o zaštiti pojedinaca u vezi s obradom ličnih podataka http://eur-lex.europa.eu/legal-content/HR/TXT/?uri=CELEX:32016L0680

Akcionim planom za poglavlje 23 je bilo predviđeno da će novi zakon biti izrađen u skladu sa ovim Modelom. Međutim, kada je radna grupa Ministarstva pravde, u novembru 2015. godine, oglasila javnu raspravu o Nacrtu novog zakona, ispostavilo se da tekst gotovo uopšte ne odgovora Modelu. Bitna odstupanja detaljno je obrazložio Poverenik[10], dok se o nizu problematičnih predloga iz ovog Nacrta SHARE Fondacija i formalno izjasnila u svom komentaru, uz podršku brojnih organizacija civilnog društva.[11] Kritika zajednice je očigledno uzeta u obzir, te se nakon završene javne rasprave o novom zakonu više nije govorilo.

U međuvremenu, Poverenik je javnosti predstavio novi Model zakona o zaštiti podataka o ličnosti, „usklađen sa aktuelnim standardima relevantnih evropskih dokumenata, a prvenstveno sa Opštom uredbom o zaštiti podataka o ličnosti, i otvorio javnu raspravu o njemu".[12] SHARE Fondacija je tokom aprila 2017. organizovala konsultativni sastanak i pozvala relevantne organizacije civilnog društva da predstave svoje komentare na novi Poverenikov Model zakona o zaštiti podataka o ličnosti, kao i da zajedničkim pismom pozovu Vladu Srbije da novi Zakon o zaštiti podataka o ličnosti bude usvojen u najkraćem roku.

S ove vremenske distance, čini se da zadovoljavajuća reforma pravnog okvira zaštite podataka o ličnosti i nije bila moguća pre donošenja evropske Opšte Uredbe o zaštiti podataka ličnosti. Stoga je neizbežno konstatovati da je drugu polovinu 2016. trebalo iskoristiti za uporednu analizu Opšte Uredbe i domaćeg pravnog okvira zaštite podataka ličnosti, budući da postoje svi elementi za kvalitetnu reformu ove oblasti.

Propušteno vreme nalaže da se u što kraćem roku izradi nacrt novog zakona o zaštiti podataka o ličnosti, koji će biti u skladu sa Opštom Uredbom, uz učešće stručne i zainteresovane javnosti u okviru svrsishodne javne rasprave.

10 Slab nacrt zakona o zaštiti podataka o ličnosti http://www.poverenik.rs/yu/saopstenja-i-aktuelnosti/2228-slab-nacrt-zakona-o-zastiti-podataka-o-licnosti.html

11 Komentari na Nacrt zakona o zaštiti podataka o ličnosti, SHARE Fondacija, novembar 2015. http://shareconference.net/sites/default/files/u742/share _ fondacija _ komentari _ na _ nacrt _ zakona _ o _ zastiti _ podataka _ o _ licnosti.pdf

12 Model zakona o zaštiti podataka o ličnosti http://www.poverenik.org.rs/sr/2017-03-06-09-09-59.html

VODIČ ZA ORGANE VLASTI

ZAŠTITA PODATAKA O LIČNOSTI

Analiza najboljih praksi i procedura zaštite podataka koje se primenjuju u nekoliko odabranih institucija, sprovedena prema principima ustanovljenim tokom višegodišnjeg iskustva službe Poverenika te znanjima SHARE Fondacije iz oblasti zaštite privatnosti u digitalnom okruženju.

Vodič je namenjen pre svega organima vlasti, ali s obzirom na to da je zaštita podataka o ličnosti uređena zakonom koji se tiče svih aktera, analize i preporuke iz istraživanja SHARE Fondacije od koristi su i rukovaocima podataka iz privatnog sektora. Značajan doprinos boljem razumevanju podataka o ličnosti i njihove zaštite, kao i dužnosti rukovaoca i obrađivača podataka, te tehničkih i organizacionih mera koje su im na raspolaganju ili koje su u obavezi da primene kako bi zaštitili podatke o ličnosti građana Srbije.

(Vodič objavljen u martu 2016.)

3.3.2. UREDBA GDPR

Opsežna reforma propisa o zaštiti podataka o ličnosti u EU, finalizovana je 2016. godine usvajanjem Opšte uredbe o zaštiti podataka o ličnosti (GDPR).[13] Uredba je stupila na snagu 24. maja 2016, a njena primena počinje 25. maja 2018. godine, kada prestaje da se primenjuje Direktiva o zaštiti podataka o ličnosti 95/46.[14] Odredbe GDPR u suštini uvode nova, stroža pravila za obrađivače i rukovaoce podacima, što će dovesti do revizije poslovnih modela mnogih kompanija. Teritorijalna primena GDPR proširena je u odnosu na Direktivu iz 1995. godine, te se ona primenjuje i na obradu podataka lica iz EU koju vrše kompanije izvan EU.

Druge značajnije novine u odnosu na postojeću Direktivu uključuju zahtev da saglasnost za obradu podataka bude eksplicitna, nove obaveze za obrađivače i rukovaoce podacima, regulisanje prava na prenos podataka (data portability), prava na zaborav (right to be forgotten), regulisanje instituta integrisane zaštite privatnosti (privacy by design) i instituta podrazumevane privatnosti (privacy by default), obaveze izrade studija uticaja na privatnost (privacy impact assessment). Kazne koje mogu biti izrečene za nepoštovanje odredbi GDPR su značajne: do 4% celokupnog godišnjeg prometa (dakle, ne samo u EU, već u celom svetu).

3.3.3. BUDUĆNOST JEDINSTVENOG MATIČNOG BROJA GRAĐANA

PREPORUKE

Kompromitovan a intruzivan sistem dodele jedinstvenih matičnih brojeva trebalo bi zameniti sistemom nasumično kreiranog ličnog broja, koji u sebi ne sadrži podatke o ličnosti. Centralni registar obaveznog socijalnog osiguranja već je uspostavio ovakav sistem, dodelom ličnog broja osiguranika (LBO) koji ne sadrži lične podatke; poseduje ga skoro sedam miliona građana Srbije i već ga upotrebljava više organa javne vlasti.

Još decembra 2014. godine javnost je saznala za najmasovniju povredu privatnosti i prava na zaštitu podataka o ličnosti građana Srbije. Tih dana je, naime, SHARE Fondacija utvrdila da je na sajtu Agencije za privatizaciju dostupan dokument koji sadrži lične podatke o 5.190.396 građana Srbije - njihovo ime i prezime, srednje ime i jedinstveni matični broj (JMBG).[15] U postupku nadzora koji je potom sprovela služba Poverenika za informacije od javnog značaja i zaštitu podataka o ličnosti, ustanovljeno je da je sporni dokument 10 meseci bio javno dostupan na sajtu Agencije za privatizaciju sa kog je, po rečima nadležnih iz Agencije, preuzet ,,više'' puta. Posledice ovog slučaja teško da se mogu u potpunosti sagledati i čini se da još uvek nedostaje puno razumevanje ozbiljnosti incidenta. O tome govori i činjenica da je postupak, koji je zbog povrede privatnosti i zaštite ličnih podataka vođen pred Prekršajnim sudom protiv Agencije za privatizaciju, odnosno odgovornih lica, zastareo početkom januara 2017.[16]

Nema informacija o tome ko sve poseduje ovaj dokument, ni da li se on prodaje na crnom tržištu, međutim, JMBG se nalazi pohranjen u svakoj evidenciji koju vode državni organi o građanima, te se i dalje koristi kao kontrolni identifikator za potvrdu identiteta prilikom školovanja, poslovanja, sklapanja ugovora, prijave boravka, otvaranja računa. Čini se da je suvišno govoriti o mogućim zloupotrebama neovlašćeno objavljene zbirke ličnih podataka više od pet miliona građana Srbije. Lažno predstavljanje u elektronskoj komunikaciji – phishing, vishing, SmiShing, u zavisnosti od toga da li se odvija mejlom, telefonom ili sms porukama – u doba globalne umreženosti čini deo zasebne discipline sociooloških i kriminoloških istraživanja, pod zajedničkim nazivom ,,društveni inženjering'', a koja podrazumeva lakoću stupanja u ličnu komunikaciju bez fizičkog prisustva. Poznavanje bar jednog ličnog podatka žrtve društvenog inženjeringa, prvi je korak za prevaru zasnovanu na poverenju. Jedinstveni matični broj građana idealan je primer: predstavlja podatak koji je čvrsto asociran uz državne organe i, uopšte, ovlašćene rukovaoce ličnim podacima, a pritom je kompromitovan u meri koja obesmišljava odredbe Zakona o zaštiti podataka o ličnosti.

Dodatno treba istaći da JMBG otkriva daleko više informacija o građanima nego što je to potrebno. Ovaj broj je sastavljen od nekoliko numeričkih elemenata koji svaki za sebe bliže određuju osobu na koju se odnose. Prvih sedam cifara označavaju dan, mesec i godinu rođenja, dok su naredne dve obeležje područja registracije prema administrativnoj podeli u Jugoslaviji, u vreme uvođenja ovog sistema 1976. godine (Srbija koristi brojeve od 70 do 89, uz narednu dekadu za rođene na Kosovu).[17] Ovaj deo JMBG na taj način doslovno preslikava osnovne činjenice o rođenju građana. Uz sve to, JMBG se nalazi u svakoj evidenciji o građanima, replicira se u beskrajnim nizovima dosijea, papirnim i elektronskim, objavljuje se u javno dostupnim bazama državnih organa, balansirajući na granici koju Ustav postavlja za svrsishodnost obrade ličnih podataka.

Čini se, međutim, da je moguće relativno jednostavno rešenje za ovaj

13 Uredba (EU) 2016/679 Evropskog parlamenta i Saveta od 27. aprila 2016. o zaštiti građana u vezi s obradom ličnih podataka i o slobodnom kretanju takvih podataka te o stavljanju van snage Direktive 95/46/EZ (Opšta uredba o zaštiti podataka) http://eur-lex.europa.eu/legal-content/HR/TXT/?uri=CELEX:32016R0679
(U daljem tekstu koristi se izraz Opšta uredba i međunarodna skraćenica 'GDPR').

14 Direktiva Evropskog parlamenta i Saveta 95/46/EC od 24.10.1995. o zaštiti građana u vezi sa obradom ličnih podataka i slobodnim kretanjem tih podataka http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML

15 Neovlašćeno objavljeni podaci o ličnosti više od 5 miliona građana Srbije http://www.shareconference.net/sh/defense/neovlasceno-objavljeni-podaci-o-licnosti-vise-od-5-miliona-gradana-srbije

16 Zastareo postupak za curenje podataka iz Agencije, N1 http://rs.n1info.com/a220880/Vesti/Vesti/Curenje-podataka-iz-Agencije-za-privatizaciju-zastarelo.html

17 Zakon o uvođenju jedinstvenog matičnog broja građana http://www.paragraf.rs/propisi/zakon _ o _ uvodjenju _ jedinstvenog _ maticnog _ broja _ gradjana.html

problem. Unikatan broj sačinjen od niza nasumičnih cifara koje, za razliku od JMBG, ne otkrivaju lične podatke građana, zapravo već postoji u Srbiji i u širokoj je upotrebi. Dodeljen je svim državljanima i osobama sa prebivalištem na teritoriji države, koji su osigurani po bilo kom osnovu, kao zaposleni, deca, supružnici i drugi. Prema nepotpunim podacima, poseduje ga blizu sedam miliona građana, a zove se Lični broj osiguranika (LBO). Broj dodeljuje Centralni registar za obavezno socijalno osiguranje (CROSO), najmlađi organ državne uprave koji je, kao takav, od početka građen u digitalnom okruženju.[18] Broj sadrži 11 cifara od kojih poslednja predstavlja kontrolni broj, a sve ostale cifre se određuju slučajnim izborom. Dodeljuje se svakom osiguranom licu samo jednom, trajan je i nepromenljiv, pa se može koristiti kao jedinstveni numerički identifikator osobe. Za razliku od jedinstvenog matičnog broja, LBO nema nikakve veze sa ličnim svojstvima građana, sam po sebi ne otkriva nijedan podatak, dok algoritamski izbor otklanja mogućnost pogrešnih dodela.

3.3.4. KIČMA DRŽAVNOG IT & DATA SISTEMA

Slučaj Agencije za privatizaciju (vidi: poglavlje 3.2.3.) otkrio je razmere rizika kojem su izloženi podaci građana, ali je ukazao i na nedostatak pouzdanih saznanja o praktičnim i tehničkim uslovima u kojima se podaci građana prikupljaju, obrađuju i čuvaju. SHARE Fondacija je stoga rešila da istraži koji se podaci o ličnosti građana prikupljaju u javnom sektoru, gde se čuvaju, kako se obrađuju, ko ima pristup podacima i koje su organizacione i tehničke mere zaštite podataka implementirane. Istraživanje je sprovedeno tokom 2015. i 2016. godine, a njime je obuhvaćeno je šest javnih institucija: Agencija za privredne registre, Centar za socijalni rad u Beogradu, Centralni registar obaveznog socijalnog osiguranja, Republički fond za zdravstveno osiguranje, Republički fond za penzijsko i invalidsko osiguranje i Poreska uprava.

Istraživanje je pokazalo da se lični podaci državljana Srbije bespotrebno umnožavaju, odnosno da identične podatke poseduje više institucija. Na ovaj način raste rizik da podaci budu netačni i neažurni, što može otežati rad državnih institucija ili uticati na prava građana. Što je još bitnije, ovakvo umnožavanje podataka uvećava rizik po bezbednost ličnih podataka građana, s obzirom na to da se identični podaci čuvaju na različitim serverima, pod potpuno drugačijim tehničkim i organizacionim merama zaštite.

Utvrđeno je i da sve analizirane institucije imaju u svom vlasništvu servere i druge uređaje koji služe za čuvanje podataka, te da se svi ovi uređaji nalaze u Srbijii, uglavnom u sedištima samih institucija. To znači da ove institucije ne iznose podatke građana iz Srbije i da imaju osnovne preduslove za kontrolu nad podacima. S druge strane, međutim, to znači da se mogu osloniti samo na svoje kapacitete kada su mere zaštite podataka u pitanju, što će u mnogome zavisiti od resursa sa kojima institucija raspolaže.

18 Centralni registar za obavezno socijalno osiguranje http://www.croso.gov.rs/cir/index.php

Sve institucije, osim Centra za socijalni rad u Beogradu, imaju centralizovan informacioni sistem, odnosno svi uređaji za obradu podataka (serveri, kompjuteri) unutar jedne institucije predstavljaju jedinstven sistem, što znatno olakšava uspostavljanje sigurnosnih mehanizama. Čuvanje svih događaja u okviru sistema, takozvanih logova, pojedinim institucijama i dalje predstavlja izazov. Poseban problem s kojim su suočene javne ustanove jeste zadržavanje kvalitetnog kadra koji je zadužen za razvoj i održavanje informacionih sistema.

Ustanovljeno je da se razmena podataka između ovih organa vrši preko infrastrukture Uprave za zajedničke poslove republičkih organa, i to preko VPN-a, dakle, mimo uobičajenih kanala internet komunikacije, što je izuzetno značajno za bezbednost podataka.

Uprkos pozitivnim tendencijama uočenim tokom istraživanja, treba reći da je analiza sprovedena u institucijama koje spadaju među najbolje sisteme u Srbiji i raspolažu sa znatnim resursima. U Srbiji, međutim, postoji više od 11.000 javnih institucija i njihovih ogranaka, sa daleko slabijim kapacitetima, zbog čega se stanje u ustanovama, odabranim prema značaju za elementarno funkcionisanje društva, ni u kom slučaju ne može uzeti kao reprezentativno u nacionalnim okvirima.

3.4. REGULISANJE ELEKTRONSKOG POSLOVANJA

Elektronsko poslovanje u Srbiji bi uskoro moglo da bude regulisano novim zakonskim tekstom. Početkom septembra 2016. godine javnosti je predstavljen Nacrt zakona o elektronskom dokumentu, elektronskoj identifikaciji i uslugama od poverenja u elektronskom poslovanju.[19] Ovaj zakon bi trebalo da zameni dva trenutno važeća zakona: Zakon o elektronskom potpisu (Službeni glasnik RS, br. 135/04) i Zakon o elektronskom dokumentu (Službeni glasnik RS, br. 51/2009).

Cilj zakona je da omogući da se poslovanje odvija brže i efikasnije, smanjenje troškova poslovanja, kao i razvoj tržišta od poverenja i ubrzanje procesa rada organa javnih vlasti i privrednih subjekata, a da se korisnicima javnih i drugih servisa olakša pristup uslugama.[20]

Svrha budućeg zakona svakako je i usaglašavanje propisa sa Uredbom EU o elektronskoj identifikaciji i uslugama od poverenja u elektronskim transakcijama, koja je zamenila Direktivu o elektronskom potpisu iz 1999. godine.

19 Nacrt zakona o elektronskom dokumentu, elektronskoj identifikaciji i uslugama od poverenja u elektronskom poslovanju http://mtt.gov.rs/download/Nacrt.pdf

20 Održan treći sastanak Ekonomskog kokusa http://www.parlament.gov.rs/Одржан_трећи_састанак_Економског.30840.43.html

Materija koja treba da bude regulisana novim zakonom uključuje pojam elektronskog dokumenta, elektronsku identifikaciju, usluge od poverenja, elektronski potpis i elektronski pečat, vremenski žig, preporučenu elektronsku dostavu, autentifikaciju veb sajtova i elektronsko čuvanje dokumenata.

Stručna javnost načelno se složila u oceni da predloženi tekst predviđa moderna rešenja koja će doprineti unapređenju elektronskog poslovanja u Srbiji, ali i da postoji prostor za poboljšanja u pogledu pojedinih odredbi prepisanih iz postojećih zakona o elektronskom potpisu i elektronskom dokumentu, koji nisu trpeli nijednu izmenu od usvajanja.[21]

Javna rasprava povodom ovog zakonskog teksta je trajala do 30. septembra 2016. Zasad nisu javno dostupne informacije o rokovima koje Vlada Republike Srbije ima za izradu konačnog predloga.

21 Komentari na Nacrt zakona o elektronskom dokumentu, elektronskoj identifikaciji i uslugama od poverenja u elektronskom poslovanju, Naled, januar 2017. http://www.naled-serbia.org/upload/CKEditor/Komentari 20na 20Nacrt 20zakona 20o 20elektronskom 20dokumentu 20potpisu 20i 20uslugama 20od 20poverenja.pdf

4. DIGITALNA BEZBEDNOST

Srbija je 2010. godine usvojila Strategiju razvoja informacionog društva u Republici Srbiji do 2020. godine, kojom je borba protiv visokotehnološkog kriminala definisana kao jedan od četiri prioriteta u razvoju informacione bezbednosti, prioritetne oblasti razvoja informacionog društva.[1] Strategija donosi preporučene aktivnosti u okviru prioriteta informacione bezbednosti:

- Potrebno je doneti propise iz oblasti informacione bezbednosti kojima će se dodatno urediti standardi informacione bezbednosti, područja informacione bezbednosti, kao i nadležnosti i zadaci pojedinih institucija u ovoj oblasti.
- Potrebno je formirati instituciju koja u oblasti informacione bezbednosti obavlja poslove verifikacije i sertifikacije metoda, softverskih aplikacija, uređaja i sistema, kao i istraživanje i razvoj. Ova institucija treba da nadzire i primenu standarda informacione bezbednosti u državnim organima.
- Potrebno je formirati nacionalni CSIRT (Computer Security Incident Response Team), s ciljem da preventivno deluje i koordinira rešavanje incidenata u oblasti računarske bezbednosti na internetu.
- Potrebno je razvijati i unapređivati zaštitu od napada primenom informacionih tehnologija na kritične infrastrukturne sisteme, što pored IKT sistema mogu biti i drugi infrastrukturni sistemi kojima se upravlja korišćenjem IKT, poput elektro-energetskog sistema.
- Potrebno je dodatno urediti kriterijume za utvrđivanje kritične infrastrukture sa stanovišta informacione bezbednosti, kriterijume za karakterizaciju napada primenom informacionih tehnologija na takvu infrastrukturu u odnosu na klasične oblike napada, kao i uslove zaštite u ovoj oblasti.
- Potrebno je usvojiti nova i unaprediti već postojeća zakonodavna rešenja, kako bi se omogućila veća usklađenost, a samim tim i efikasnija primena Konvencije o visokotehnološkom kriminalu čime bi se, u zajedničkom dejstvu i drugih državnih i vandržavnih činilaca koji sprovode javni interes za suzbijanje visokotehnološkog kriminala, omogućilo postizanje optimalnih rezultata u ovoj oblasti.

1 Strategija razvoja informacionog društva u Republici Srbiji do 2020. godine http://www.paragraf.rs/propisi/strategija _ razvoja _ informacionog _ drustva _ u _ republici _ srbiji.html

4.1. IMPLEMENTACIJA ZAKONA O INFORMACIONOJ BEZBEDNOSTI

Zakon o informacionoj bezbednosti je usvojen krajem januara 2016. kao prvi propis iz ove oblasti u pravnom sistemu Republike Srbije, kojim su privatni i javni akteri obavezani da primene odgovarajuće mere zaštite informacionih sistema. Zakon definiše IKT sisteme od posebnog značaja kao sisteme koji se koriste za poslove državnih organa, obradu naročito osetljivih podataka o ličnosti i obavljanje delatnosti od opšteg interesa, što između ostalog podrazumeva i elektronske komunikacije.

U eri sofisticiranih tehničkih napada i ubrzanog razvoja sajber oružja[2], od presudne važnosti je da informacioni sistemi koji kontrolišu kritičnu infrastrukturu,[3] dakle snabdevanje vodom, električnom energijom, imaju odgovarajući nivo zaštite propisan zakonom.

Među najvažnijim institutima novog Zakona svakako je Nacionalni centar za prevenciju bezbednosnih rizika u IKT sistemima (CERT), čije su uloge pre svega prevencija i koordinacija komunikacije između relevantnih aktera u Srbiji i inostranstvu.

Zakonom su predviđeni i posebni CERT-ovi, koji bi trebalo da doprinesu prevenciji i zaštiti od bezbednosnih rizika informacionih sistema u okviru određene oblasti poslovanja, pa čak i posebnih kompanija ili grupe kompanija. Primer posebnog CERT-a je CERT republičkih organa. Članom 7 Zakona propisano je 28 mera zaštite informacionih sistema od posebnog značaja, a zakon nalaže i niz obaveza, poput donošenja akta o bezbednosti koji se mora usklađivati sa promenama u digitalnom okruženju ili samom sistemu.

Operatori IKT sistema od posebnog značaja su dužni da bar jednom godišnje izvrše proveru usklađenosti mera zaštite informacionog sistema u odnosu na akt o bezbednosti i o tome napišu izveštaj. Obaveštavanje Ministarstva trgovine, turizma i telekomunikacija o incidentima koji mogu značajno da utiču na bezbednost informacionih sistema još jedna je obaveza operatora.

Vlada Srbije je 17. novembra 2016. usvojila podzakonske akte neophodne za početak primene Zakona o informacionoj bezbednosti. Niz propisanih mera zaštite na koje su operatori informacionih sistema obavezani, dodatno su razjašnjene ovim uredbama. Ustanove i kompanije koje upravljaju informacionim sistemima od posebnog značaja, kao što su državni organi, operatori elektronskih komunikacija ili banke, morali su da do početka marta 2017. usvoje akt o bezbednosti informacionog sistema. Prijavljivanje svakog incidenta na infrastrukturi informacionog sistema Ministarstvu trgovine, turizma i telekomunikacija, Narodnoj banci Srbije i RATEL-u obavezno je već od poslednje nedelje novembra 2016.

2 Ratovanje u 21. veku http://www.bbc.co.uk/guides/zq9jmnb

3 Kritična infrastruktura http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/crisis-and-terrorism/critical-infrastructure/index _ en.htm

VODIČ ZA IKT SISTEME OD POSEBNOG ZNAČAJA

INFORMA-CIONA BEZBEDNOST

Zaštita informaciono - komunikacionih sistema konačno je našla svoje mesto u pravnom poretku Srbije, usvajanjem prvog Zakona o informacionoj bezbednosti početkom 2016. godine. Ovaj vodič namenjen je pre svega Operatorima IKT sistema od posebnog značaja:

- Rukovodiocima operatora IKT sistema od posebnog značaja koji moraju imati osnovna znanja o značaju informacione bezbednosti, naročito s obzirom na to da su upravo oni prekršajno odgovorni u slučaju nepoštovanja odredbi Zakona i uredbi, ali i da u slučaju ozbiljnijih propusta mogu građanski i krivično odgovarati.
- Tehničkim ekspertima koji su zaduženi za informacionu bezbednost IKT sistema od posebnog značaja, te je u tom smislu posebno obrađena svaka mera zaštite koje se moraju primeniti.
- Rukovodiocima pravnih službi u čijoj su nadležnosti izrada i donošenje akta o bezbednosti.

(Vodič objavljen u januaru 2017.)

4.2. SHARE CERT ZA ONLAJN I GRAĐANSKE MEDIJE

Usvojen početkom 2016. godine, Zakon o informacionoj bezbednosti predvideo je osnivanje posebnih centara za prevenciju bezbednosnih rizika u informaciono-komunikacionim sistemima u različitim sektorima. Prvi Poseban CERT u Srbiji osnovala je SHARE Fondacija, aprila 2017, kao organizacija koja se bavi sistemskim istraživanjem pravnih, društvenih i tehničkih rizika kojima su ljudska prava izložena u novom komunikacionom okruženju.

Zvanično uručivanje rešenja o registraciji SHARE CERT-a

SHARE CERT prati i analizira pretnje po bezbednost u infrastrukturi onlajn i građanskih medija u Srbiji, pruža pomoć u prepoznavanju i prevenciji pretnji, osnažuje aktere za adekvatne odgovore na napad, obezbeđuje pravnu asistenciju u procesuiranju sajber incidenata, održava komunikaciju sa nadležnim institucijama, i drugo.

Aktivnosti SHARE CERT-a uključuju naučna istraživanja, edukaciju opšte javnosti, građanskih i onlajn medija, zagovaranje javnih politika u pravcu unapređenja standarda poštovanja ljudskih prava na internetu i zaštite bezbednosti, tehničke usuge u oblasti zaštite informacionih sistema, pravnu i tehničku analizu incidenata, te stručnu pomoć u njihovom saniranju i procesuiranju.

USLUGE SHARE CERT-A SE MOGU PODELITI U TRI KATEGORIJE:

- **PREVENCIJA** je primarna usluga SHARE CERT-a i podrazumeva uspostavljanje mera prevencije od napada na informacione sisteme. Osnovna preventivna mera je revizija informacionih sistema od strane ISO 27001 sertifikovanih auditora, koja omogućava identifikovanje slabosti sistema, a zatim i definisanje procesa njihovog proaktivnog rešavanja. Ova usluga podrazumeva i pružanje saveta u oblasti bezbednosti sistema, prepoznavanja rizika i ublažavanja posledica napada na informacione sisteme.
- **REAKCIJA** uključuje pružanje brzog i preciznog odgovora u slučaju realizacije bezbednosnog incidenta u IKT sistemu. Tim SHARE CERT-a stupa u aktivnu komunikaciju sa administratorom napadnutog sistema, u cilju što bržeg uspostavljanja normalnog funkcionisanja sistema, vrši prikupljanje digitalnih dokaza i uspostavlja ponovnu zaštitu integriteta sistema. Nakon toga, eksperti SHARE CERT-a sprovode forenzičku analizu digitalnih dokaza i, ukoliko je potrebno, pokreću krivično-pravnu proceduru.
- **EDUKACIJA** je usko povezana sa prevencijom i podrazumeva realizaciju posebnog seta usluga - održavanje treninga za različite ciljne grupe prilagođene njihovim specifičnim potrebama, kao i diseminaciju edukativnog sadržaja u različitim formatima koji su dostupni i široj javnosti. Edukativni program je kreiran na osnovu dugogodišnjeg ekspertskog iskustva u ovoj oblasti, kao i na podacima o incidentima iz države i regiona.

SHARE CERT čine stručnjaci različitih profila, od sajber forenzičara, pravnika, organizacionih i tehničkih stručnjaka, do novinara i aktivista. Sarađujemo sa organima javne uprave, predstavnicima industrije, internet i građanskim aktivistima i akademskom zajednicom, u cilju razvoja naprednih metoda i tehnologija sajber zaštite.

VODIČ:

OSNOVE DIGITALNE BEZBEDNOSTI

Postoji čitav niz faktora koji utiču na to da li će sistem biti bezbedan ili ne. Pre svega, to su tehnološki faktori: da li je sistem tehnološki kompromitovan ili ranjiv i koji je nivo bezbednosti koji sami uređaji i instalirani programi pružaju. Zatim, postoje i netehnološki faktori, odnosno određene navike korisnika, koji su takođe veoma bitni. Opšte pravilo jeste da bezbednost nije urođena karakteristika digitalnih sistema, te da bi sistem bio bezbedan moraju se preuzeti konkretni koraci.

Svaki korisnik tokom svojih onlajn aktivnosti ostavlja određene tragove, „senku" koja ga prati dok se kreće kroz sajber prostor. U digitalnom okruženju, slično kao i u nedigitalnom, ove senke otkrivaju neke karakteristike fizičkog lica. Analizom senke može se doći do određenih informacija, od značaja za napadače koji imaju za cilj da udu u određeni sistem. Prednost digitalne sredine je u tome što korisnici donekle mogu da kontrolišu oblik svoje senke, ukoliko povedu računa o svojoj digitalnoj bezbednosti.

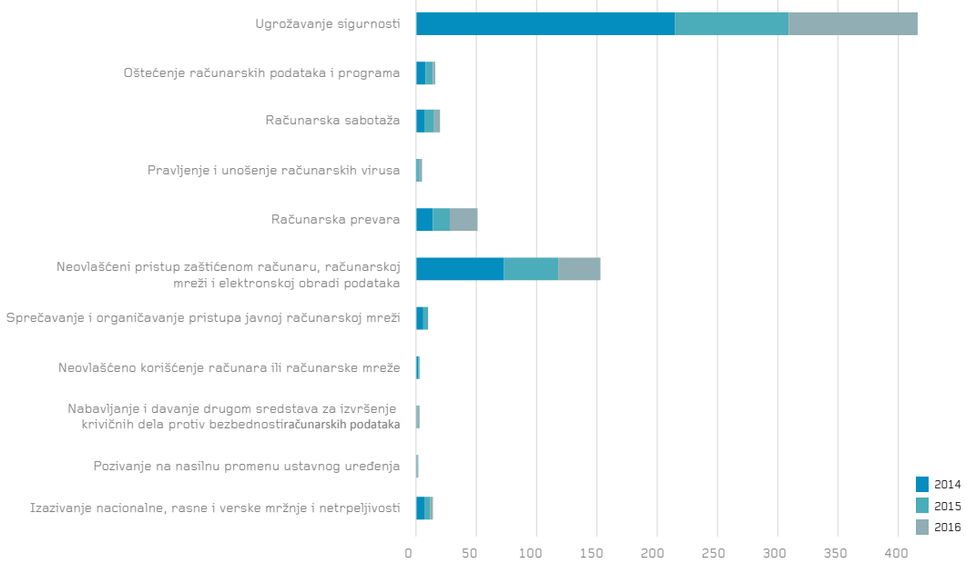
(Vodič objavljen u martu 2015.)

4.3. SAJBER KRIMINAL: ISTRAGE, PRIJAVE, PROCESI

Sajber kriminal predstavlja jedno od prioritetnih polja za tužilaštvo i policiju, naročito kada su u pitanju sofisticirani tehnički napadi. Stoga je SHARE Fondacija od Višeg javnog tužilaštva u Beogradu, u čijem se sastavu nalazi Posebno tužilaštvo za visokotehnološki kriminal, zatražila statističke podatke o broju krivičnih prijava za određena dela iz Krivičnog zakonika, u periodu od 2014. do 2016. godine.

Podaci se odnose na krivična dela koja predstavljaju sajber kriminal u najužem smislu, ali i druga krivična dela u kojima se kao sredstvo izvršenja koristi računar ili računarska mreža. Upravo je za jedno krivično delo iz te kategorije tužilaštvo postupalo u najviše slučajeva - reč je o ugrožavanju sigurnosti. Pod pretpostavkom da je zapravo reč o pretnjama upućenim preko društvenih mreža, u trogodišnjem periodu primetan je trend opadanja postupanja za ugrožavanje sigurnosti, ali je broj i dalje visok: od čak 215 krivičnih prijava tokom 2014. do nešto više od stotinu u 2016. godini.

Još jedno krivično delo sajber kriminala koje se ističe po broju krivičnih prijava jeste računarska prevara. Tokom 2014. i 2015. tužilaštvo je po ovom osnovu postupilo po 14 puta, dok je u 2016. preduzelo radnje u 23 slučaja. Tužilaštvo takođe često postupa po krivičnim prijavama za neovlašćeni pristup zaštićenom računaru, računarskoj mreži i elektronskoj obradi podataka, ali je broj postupaka u 2016. skoro duplo manji (35) u odnosu na 2014. godinu (74).



Statistika krivičnih dela visokotehnološkog kriminala 2014-2015

PREPORUKE

Organizovati edukacije nosilaca pravosudnih funkcija o sajber napadima u cilju efikasnijeg odgovora sudova na hakerske napade. Unaprediti kapacitete državnih organa koji se bave napadima i drugim bezbednosnim pretnjama u onlajn okruženju, kako bi bili u stanju da se adekvatno suprotstave sve većem broju vrlo kompleksnih oblika ugrožavanja slobodne razmene informacija.

4.4. LIČNA I ORGANIZACIONA BEZBEDNOST

Usled sve brojnijih slučajeva ugrožavanja bezbednosti novinara i medijskih organizacija, tehničkim sredstvima i u onlajn prostoru, SHARE Fondacija je izradila posebne priručnike posvećene ovim pitanjima.

Digitalna bezbednost novinara se retko posmatra iz persprektive njihove mreže ljudi, odnosno kruga osoba sa kojima komuniciraju, među kojima su izvori i kolege svakako najvažniji. Dovoljna je samo jedna slaba karika u komunikacionom lancu, da bi privatnost i bezbednost bili izloženi riziku, stoga se organizaciona bezbednost takođe nameće kao pitanje prioriteta za medije.

U PRAKSI JE IDENTIFIKOVANO VIŠE PROBLEMA DIGITALNE BEZBEDNOSTI NA KOJE TREBA OBRATITI PAŽNJU:

1. Tehnički upadi u privatne komunikacije i pristup podacima.
2. Krađa i oduzimanje opreme.
3. Nadzor elektronskih komunikacija koji vrše državni organi.
4. Socijalni inženjering.
5. Onemogućavanje pristupa sadržaju.
6. Ugrožavanje sigurnosti u onlajn prostoru.

1. TEHNIČKI UPADI U PRIVATNE KOMUNIKACIJE I PRISTUP PODACIMA

Opšti bezbednosni rizici obuhvataju neovlašćene pristupe putem hakovanja, ubacivanja malicioznog softvera (malware), korišćenja tehnologije za nadzor digitalnih komunikacija u privatne svrhe ili takozvano curenje podataka usled neadekvatne zaštite infrormacionog sistema.

Glavne tačke napada, odnosno primarne mete na koje napadači ciljaju jesu mejl serveri, uređaji (računari, mobilni telefoni, tableti), nalozi na onlajn platformama (društvene mreže, kolaborativni alati, čet aplikacije…), nosači informacija (fizički hard diskovi, fleš memorije, cloud platforme - Dropbox, Google Drive).

Cilj ovih napada je da se otkriju informacije i podaci koje bi novinari, blogeri, aktivisti i medijske organizacije svakako želeli da zaštite. To može da podrazumeva sledeće informacije:

- Na čemu radite - planovi i nacrti istraživačkih priča ili kampanja, dokumenta, snimci, beleške itd.
- Podaci koje posedujete - poverljive informacije dobijene od izvora, potencijalni dokazi zloupotreba državnih službenika ili privatnih aktera (kompanije, kriminalci, itd)
- Ko su vam saradnici - informacije o vašoj mreži kolega, izvora, urednika itd.
- Kuda se krećete - informacije o kretanju, dnevnim rutinama, planovima za putovanja u inostranstvo itd.
- Da li nešto krijete - informacije iz privatne sfere koje drugi mogu da zloupotrebe.

KONFLIKT: Privatnost i poverljivost komunikacije v. tehnički napadi v. digitalna sigurnost kompanija koje čuvaju podatke.

SREDSTVA ZAŠTITE: Digitalna pismenost, krivično-pravna zaštita kroz domaći pravni poredak i instrumente Budimpeštanske konvencije o visokotehnološkom kriminalu, pouzdani pružaoci i kvalitetne usluge informacionog društva, enkripcija sadržaja.

KO JE ODGOVORAN:, Internet i telekomunikacione kompanije, pružaoci usluga informacionog društva, organizacije nadležne za upravljanje internetom (Internet governance), države, organizacija i IT podrška, pojedinci za vlastiti sadržaj.

2. KRAĐA I ODUZIMANJE OPREME

Jedan od mogućih scenarija čine krađa ili oduzimanje opreme po nalogu državnih organa (policije, tužilaštva, suda). Mada policijsko pretresanje redakcija na domaćem terenu još nije zabeleženo u praksi, slučaj portala Klix.ba iz susedne Bosne i Hercegovine, čije je prostorije pretresla policija da bi oduzela i uništila deo opreme, ukazuje da rizik uvek postoji.[4] U Srbiji je neovlašćeno oduzimanje opreme zabeleženo kada su novinari istraživačkog portala Krik pokušali da postave pitanja gradonačelniku Beograda.[5]

U slučaju krađe uređaja poput laptopova, tableta, telefona ili kamera, počiniocu s dovoljnim tehničkim znanjima neće predstavljati problem da dođe do informacija zaštićenih običnom šifrom. Enkripcija hard diskova je stoga veoma važna za zaštitu poverljivih podataka, čak i u slučaju krađe uređaja.

KONFLIKT: Zaštita novinarskih izvora v. onemogućavanje izveštavanja

SREDSTVA ZAŠTITE: Napredne tehnike enkripcija, pravljenje rezervnih kopija podataka (data backup)

KO JE ODGOVORAN: Korporacije, IT podrška, pojedinci za svoje uređaje i podatke

3. NADZOR ELEKTRONSKIH KOMUNIKACIJA KOJI VRŠE DRŽAVNI ORGANI

Rizik koga treba biti svestan prilikom rada sa poverljivim informacijama jeste moguće presretanje komunikacije od strane državnih organa (policija i bezbednosne službe). Prema pravnom okviru Srbije, tajnost sredstava komunikacije je zagarantovana Ustavom, a od te garancije se može odstupiti samo u slučajevima vođenja krivičnog postupka ili zaštite nacionalne bezbednosti, na način predviđen zakonom i uz odluku suda. Nadzor putem video-kamera i sličnih sredstava u fizičkom prostoru takođe može predstavljati kritično narušavanje privatnosti, dok sama oblast video-nadzora nije regulisana postojećim zakonima.

Posebno treba istaći odsustvo kontrole tržišta opreme za nadgledanje i presretanje elektronskih komunikacija u Srbiji. Privatni akteri lako mogu doći do sofisticiranih uređaja i programa potrebnih za nadzor, čija je instalacija i upotreba prilično jednostavna.

Nadzor i praćenje, kao najčešći oblici narušavanja privatnosti, u popularnim predstavama uglavnom se vezuju za prisluškivanje sadržaja komunikacije. Međutim, podaci o komunikaciji, tzv. metapodaci, otkrivaju daleko više informacija od samog razgovora. U slučaju, na primer, telefonskog razgovora to bi bili podaci o tome koji broj ste zvali, ko je vas zvao, u koje vreme, koliko je trajao razgovor i slično. Pažljivim kombinovanjem velike količine metapodataka može se dobiti kompletan digitalni profil određene ličnosti: lokacija, dnevne rutine, mreža ljudi, izvori informacija, interesovanja. Prema Zakonu o elektronskim komunikacijama, koji ove podatke naziva zadržani podaci, operatori su dužni da ih čuvaju 12 meseci i stave na uvid ovlašćenim licima, u skladu sa zakonom. Pristup ovim podacima predstavlja veoma intruzivnu meru kojom se odstupa od garancije tajnosti sredstava komunikacije, te se zbog toga akteri u javnom i privatnom sektoru koji čuvaju ove podatke moraju pridržavati procedura propisanih Zakonom o zaštiti podataka o ličnosti.

Podsetimo da je Poverenik za informacije od javnog značaja i zaštitu podataka o ličnosti u postupku nadzora nad operatorima mobilne i fiksne

4 Ko su glavni akteri koji su naredili i odobrili pretres portala Klix.ba, decembar 2014: http://www.klix.ba/vijesti/bih/ko-su-glavni-akteri-koji-su-naredili-i-odobrili-pretres-portala-klix-ba/141230118

5 Obezbeđenje gradonačelnika sprečilo KRIK da Malom postavi pitanja, oktobar 2015: https://www.krik.rs/obezbedenje-gradonacelnika-sprecilo-krik-da-malom-postavi-pitanja/#sthash.k3u72Mr5.dpuf

telefonije, sprovedenom 2012. godine, došao do zabrinjavajućih podataka o nezakonitom pristupanju državnih organa metapodacima. Tada je utvrđeno da je kod samo jednog operatora, tokom jedne godine, MUP direktno pristupio podacima o komunikaciji korisnika više od 270.000 puta.[6] Kako su operatori u međuvremenu obavezani da dostavljaju statistike o broju zahteva, javno dostupni podaci otkrivaju da su državni organi tokom 2015. godine ostvarili ukupno 300.845 pristupa, samo kod jednog operatora.

KONFLIKT: Privatnost v. bezbednost

SREDSTVA ZAŠTITE: Međunarodni standardi ljudskih prava, watchdog inicijative[7]

KO JE ODGOVORAN: Države, policija, tajne službe, pravosuđe, operatori elektronskih komunikacija

4. SOCIJALNI INŽENJERING

Taktika koja se takođe može koristiti za prikupljanje poverljivih informacija od novinara ili njihovih izvora jeste socijalni inženjering, odnosno manipulacija kako bi se prikupile informacije ili na prevaru pristupilo informacionom sistemu. Često je to jedan od mnogih koraka u okviru složenijih planova za prevaru. Na primer, novinar može dobiti mejl sa adrese koja naizgled deluje kredibilno, sa ,,dokumentom poverljive sadržine'' u prilogu, a koji zapravo predstavlja virus; ili mejl od lažnog izvora koji želi da sazna informacije od novinara u vezi s njegovim radom. Anonimnost i neverifikovani kontakt podaci omogućavaju čak i da se pojedinac lažno predstavi kao novinar[8] u cilju ispunjavanja skrivenih agendi. Neretko zbog niza različitih okolnosti može doći i do zloupotrebe poverenja (npr. ,,curenje'' informacija od bivšeg nezadovoljnog kolege) što može da izazove posebne probleme.

KONFLIKT: Poverenje v. anonimnost

SREDSTVA ZAŠTITE: Nacionalno krivično pravo, verifikacija identiteta (enkripcija/potpisivanje mejlova)

KO JE ODGOVORAN: Države, korporacije, IT podrška, pojedinci

5. ONEMOGUĆAVANJE PRISTUPA SADRŽAJU

U većini slučajeva, sigurnost sadržaja objavljenog na nekoj onlajn platformi zavisi od bezbednosnih praksi same platforme. Najčešći rizici su opterećivanje servera DDoS (Distributed Denial of Service) napadima, tj. zagušivanje servera na kome je sajt onlajn medija hostovan, slanjem ogromnog broja zahteva za pristup u isto vreme.[9] Još jedan od načina da se naruši integritet sadržaja njegovom izmenom ili uklanjanjem jesu napadi na baze podataka sajta onlajn medija ubacivanjem malicioznog koda, kako bi se kompromitovao sadržaj baze (tzv. SQL Injection[10]).

Legalni načini da se određeni sadržaj donekle učini nedostupnim, jesu podnošenje zahteva po osnovu ,,prava na zaborav'' (right to be forgotten) ili procedure za uklanjanje sadržaja po prijavi (notice-and-takedown). Pravo na zaborav se za sada primenjuje na teritoriji Evropske unije, u skladu sa odlukom Evropskog suda pravde u predmetu Gugl protiv Španije.[11] Ova presuda omogućava građanima EU da od servisa za pretraživanje zatraže uklanjanje informacija koje nisu istinite ili više nisu relevantne, doduše samo iz rezultata pretrage a ne sa samih sajtova na kojima su objavljene. Kada je reč o proceduri za uklanjanje sadržaja po prijavi, ona se najčešće primenjuje u slučajevima kada se od platforme traži da ukloni određeni sadržaj po nekom pravnom osnovu (npr. kršenje autorskih prava).

KONFLIKT: Slobodan pristup informacijama v. arhitektura mreže

SREDSTVA ZAŠTITE: Budimpeštanska konvencija o visokotehnološkom kriminalu, nacionalni pravni okvir

KO JE ODGOVORAN: Organizacije nadležne za upravljanje internetom, države, korporacije, hosting & IT podrška

6. UGROŽAVANJE SIGURNOSTI U ONLAJN PROSTORU

Ugrožavanje sigurnosti novinara, koje se u oflajn svetu manifestuje pretnjama, sve više uzima maha na internetu, a posebno na društvenim mrežama, usled mogućnosti da se pretnje upute anonimno. Procenjuje se da se više od četvrtine pretnji i zastrašivanja novinarima upućuje onlajn, dok su novinarke tri puta više izložene verbalnom nasilju na internetu od svojih kolega.[12] Ranija predstavnica OEBS za slobodu medija Dunja Mijatović pozvala je zemlje članice da preduzmu ozbiljne korake za stvaranje bezbednijeg okruženja za rad onlajn novinarki.[13] Glavni ciljevi ove vrste napada jesu zastrašivanje radi odvraćanja od izveštavanja o određenim temama, javno izlaganje poruzi i podsticanje ili opravdavanje fizičkih napada na novinare. To se može postići otvorenim pretnjama, objavljivanjem privatnih informacija, poput adrese, imena ili fotografija članova porodice, govorom mržnje, uvredama koje podstiču na nasilje, uznemiravanjem na društvenim mrežama i slično. Kada je reč o nešto suptilnijim taktikama, treba pomenuti narušavanje reputacije novinara i angažovanje hakera.

KONFLIKT: Sloboda izražavanja i anonimnost v. prava ličnosti i kvalitet informacija

SREDSTVA ZAŠTITE: Međunarodni standardi ljudskih prava, nacionalni pravni okvir, samoregulacija

KO JE ODGOVORAN: Internet zajednica, države, korporacije, pojedinci

6 Nevidljive infrastrukture, SHARE Labs, juni 2015. http://labs.rs/sr/nevidljive-infrastrukture-elektronski-nadzor-i-zadrzavanje-podataka-sa-mobilnih-telefona/

7 12 međunarodnih principa primene standarda ljudskih prava na nadzor komunikacija podržalo je više od 400 organizacija širom sveta, među kojima je i SHARE Fondacija https://en.necessaryandproportionate.org/

8 U slučaju novinarke Dragane Pećo, nepoznato lice je u njeno ime slalo zahteve za pristup informacijama od javnog značaja sa lažne mejl adrese http://www.cins.rs/srpski/news/article/saopstenje-za-javnost-783

9 Razumevanje DDoS napada http://www.digitalattackmap.com/understanding-ddos/

10 SQL Injection napadi https://www.acunetix.com/websitesecurity/sql-injection/

11 Odluka Suda: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX-:62012CJ0131&from=EN

12 IWMF, Nasilje i maltretiranje žena u medijima: Globalna slika / Intimidation, Threats, and Abuse: http://www.iwmf.org/intimidation-threats-and-abuse/

13 Komunike predstavnice OEBS za slobodu medija o porastu ugrožavanja sigurnosti novinarki u onlajn okruženju: http://www.osce.org/fom/139186?download=true

VODIČ:

KROZ RIZIKE I MEHANIZME ZAŠTITE NEZAVISNOSTI I BEZBEDNOSTI ONLAJN MEDIJA

HOD PO DIGITALNOJ IVICI

Sajber napadi na onlajn medije i novinare u Srbiji postaju sve učestaliji. Veb portali najčešće su meta DDoS napada kojima se onemogućava pristup sadržaju, ali i napada u kojima se utiče na integritet baza podataka. Novinari se suočavaju sa izazovima društvenog inženjeringa, oduzimanja i lažiranja onlajn identiteta i neovlašćenog pristupanja privatnim komunikacijama. Gradanski novinari i aktivni učesnici u javnim debatama nalaze se na meti manipulacije javnim mnjenjem, zastrašivanja putem anonimnih pretnji, ali i dvostrukih aršina nadležnih prilikom procesuiranja slučajeva eventualnog prekoračenja slobode izražavanja. Da bismo bolje pojasnili i predstavili ove probleme, procenićemo trenutnu poziciju onlajn medija i novinara u digitalnom okruženju, uzimajući u obzir činjenicu da oni čuvaju naročito poverljive i osetljive informacije, ne samo na svojim uredajima već i širom Mreže. Stoga ćemo posebnu pažnju posvetiti digitalnim rizicima, kao što su gubitak ili otkrivanje podataka, kao i mehanizmima za smanjenje i izbegavanje rizika, odgovornim akterima ali i odnosu izmedu suprostavljenih načela privatnosti i bezbednosti.

(Vodič objavljen u oktobru 2015.)

4.5. TEHNIČKI MONITORING: ODABRANI SLUČAJEVI

Tokom 2016. značajno je smanjen broj registrovanih tehničkih napada na onlajn medije u odnosu na prethodne dve godine. Smanjenje je svakako posledica daljeg unapređenja zaštite informacionih sistema onlajn medija, ali i sve šire primene drugih oblika zlonamernih pritisaka mimo sajber napada.

Specifični slučajevi kojima se tehnički tim SHARE Fondacije bavio u 2016. predstavljaju ilustraciju opšte klime u oblasti internet bezbednosti.

1. SLUČAJ I

VRSTA NAPADA: Promena izgleda sajta istraživačkog medija (defacement)

VREME RESTAURACIJE: Nakon tri sata na domen je podignuta verzija samo za čitanje (read-only) iz sigurnosne kopije. Za uspostavljanje pune funkcionalnosti sajta sa editovanjem i objavljivanjem novih članaka, bilo je potrebno četiri dana.

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

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

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

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

S obzirom na to da je napadač imao potpuni pristup sistemu, pošlo se od pretpostavke da su kompromitovane sve lozinke, uključujući i one koje se koriste za pristup bazi podataka. Ove lozinke su odmah promenjene, dok su ostale lozinke generisane pre vraćanja sajta u punu funkcionalnost (write-read). Kada je sajt u potpunosti restauriran, sledećeg jutra je nastavljeno istraživanje tačnog vektora koji je omogućio pristup sa administratorskim ovlašćenjima.

PREPORUKE: Potpuni pristup za čitanje i editovanje (read-write) treba da je moguć samo u direktorijumima gde je to nephodno za njihovo korišćenje. Potpuni pristup drugim direktorijumima bi trebalo ukinuti. Pokretanje PHP skripti u tim direktorijumima ne treba da bude moguće. Protokoli za autentifikaciju SSL/TLS bi trebalo da budu obavezni za sve pristupe, i korisničke i administratorske. Akreditacije za sve sajtove treba promeniti, ukloniti sve suvišne naloge i promeniti slabe lozinke.

2. SLUČAJ II

VRSTA NAPADA: DDoS napad na veb sajt istraživačkog medija

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

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

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

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

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

S obzirom na okolnosti, malo je verovatno da je došlo do upada na server, jer su svi bezbednosni standardi ispunjeni. Za napad je odabrana poplava ogromnim brojem zahteva spolja, koji praktično onemoguće rad servera. Serverski log generisan tokom napada je jako veliki (130 GB), a analizom njegovih segmenata utvrđeno je da IP zahtevi dolaze iz celog sveta, najviše iz SAD.

REŠENJE: Nakon migracije, sajt je prebačen na novi server sa svežim

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

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

3. SLUČAJ III

VRSTA NAPADA: DoS/DDoS napad na medijski veb sajt

VREME RESTAURACIJE: Nekoliko sati

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

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

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

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

4. SLUČAJ IV

VRSTA NAPADA: DoS napad na veb sajt organizacije civilnog društva

VREME RESTAURACIJE: Nekoliko sati

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

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

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

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

VODIČ:

BEZBEDNOST ORGANIZA - CIJA U DIGITALNOM OKRUŽENJU

KAKO SAČUVATI PRIVATNOST I POVERLJIVOST DIGITALNE KOMUNIKACIJE

Novinarski posao i gradansko organizovanje u zajednici, u cilju blagovremenog i tačnog informisanja javnosti i zaštite javnog interesa u digitalnoj eri, nisu mogući bez odgovarajuće tehničke zaštite osetljivih podataka. Od internog poslovanja, organizacionih planova i komunikacije sa poverljivim izvorima, sve do objavljenog sadržaja na internetu, čitav informacioni sistem medija i organizacija civilnog društva sačinjen je od podataka čiji je integritet neophodno sačuvati. Na prvoj liniji fronta u borbi za javni interes, novinarima i aktivistima na mreži pridružili su se administratori i veb-masteri.

Ovaj vodič je namenjen upravo tehničkim službama informacionih sistema u medijskim i gradanskim organizacijama, koje imaju potrebu da svoja uobičajena znanja o hardveru i softveru dopune lekcijama o njihovoj zaštiti.

(Vodič objavljen u oktobru 2015.)

5. OTVOREN PRISTUP ZNANJU

5.1. UVOĐENJE OPEN DATA U SRBIJU

Tokom 2016. godine započela je s radom radna grupa za otvorene podatke, osnovana u skladu sa Strategijom razvoja elektronske uprave u Republici Srbiji za period od 2015-2018. godine i Akcionim planom za sprovođenje strategije za period 2015-2016. godine. SHARE Fondacija ima svoja dva predstavnika u ovoj radnoj grupi, u podgrupi za pravna pitanja, čiji je zadatak da analizira pravni okvir Republike Srbije u kontekstu otvaranja podataka i predlaže buduća zakonska rešenja u ovoj oblasti. U tom smislu, poseban fokus stavlja se na primenu Direktive 2013/37/EU o ponovnoj upotrebi informacija iz javnog sektora iz 2013. godine (Public Sector Information Directive, PSI Direktiva).[1]

Uzimajući u obzir da pozitivno pravo Republike Srbije trenutno ne poznaje pojam otvorenih podataka, potrebno je prvo taj pojam definisati i staviti u odgovarajući kontekst. Naime, ,,otvoreni podaci'', ,,otvaranje podataka'' i ,,pravo na ponovnu upotrebu informacija'' usko su povezani i međusobno uslovljeni. U cilju adekvatnog zakonskog regulisanja ovih instituta potrebno ih je prethodno definisati, odnosno razgraničiti.

Otvoreni podaci imaju sličan izvor kao i ,,informacije od javnog značaja'': oba koncepta utemeljena su u zahtevu da rad državnih organa treba da bude transparentan i da javnost treba da ima uvid u dokumenta koja u svom radu ,,proizvode'' državni organi (sem u slučaju jasno definisanih izuzetaka, kao što su bezbednost zemlje, interes sudskog i drugih postupaka, isl). Međutim, otvoreni podaci, za razliku od informacija od javnog značaja, imaju određene specifičnosti jer je (pored transparentnosti) naglasak na tome da su u pitanju podaci koje javnost dalje može koristiti za neke druge svrhe, različite od onih koju su imali kod nadležnih organa koji su ih prikupili, odnosno proizveli (dalja komercijalna ili nekomercijalna upotreba). Stoga otvoreni podaci imaju određene kvalitete: u otvorenim su formatima i mašinski čitljivom obliku, da bi bili pogodni za dalju upotrebu, što ne mora biti slučaj sa informacijama od javnog značaja.

Pošto je pokret za otvaranje podataka utemeljen u idejama transparentnosti i korisnosti za privatni sektor, s jedne strane postoji zahtev za države da proaktivno otvaraju svoje podatke, tj. da u otvorenim formatima objavljuju informacije koje prikupljaju u svom radu. Tako javno objavljene informacije može da koristi bilo koje lice iz privatnog ili javnog sektora. Međutim, ovog trenutka na nivou Evropske unije ne postoje propisi koji bi regulisali minimum pravila koje države članice moraju da poštuju prilikom aktivnog otvaranja podataka, niti pravila o tome koji krug, vrsta i obim podataka mora biti otvoren tj. objavljen. U tom smislu, svaka država članica ima pravo da svojim nacionalnim propisima reguliše ovo pitanje. Kada bi država proaktivno objavljivala sve podatke koji su joj u posedu u otvorenom obliku, imperativ transparentnosti bi bio u potpunosti zadovoljen. Međutim, kako to za sada nije realno, potrebno je prvenstveno privatnom sektoru obezbediti pravo da od države zahteva da mu budu dostavljeni tačno određeni podaci koji odgovaraju njegovim konkretnim potrebama. To je teren ,,prava na ponovnu upotrebu informacija'' gde država postupa pasivno, tj. tek po zahtevu.

Pravo na ponovnu upotrebu informacija pretpostavlja da je građanima određenim propisom zagarantovao pravo da od nadležnog organa zahteva-ju i dobiju konkretne informacije odgovarajućeg kvaliteta, odnosno otvorene podatke - ukoliko su ti podaci već javno objavljeni, tražilac informacije može da im pristupi bez podnošenja posebnog zahteva. Moglo bi se reći da je pravo na ponovnu upotrebu informacija jedno od sredstava pritiska na državu da otvara svoje podatke, odnosno da ih objavljuje u otvorenom obliku, te da poštuje principe transparentnosti. U evropskom pravu na snazi su pravila o tome kako organi države članice moraju da postupe ako prime zahtev od pojedinačnog lica (pravnog li fizičkog) da mu budu dostavljeni tačno određeni otvoreni podaci, što su zapravo pravila PSI Direktive.

Dakle, proaktivan aspekt otvorenih podataka, odnosno javno objavljivanje određenih setova podataka u otvorenom obliku, podrazumeva skup pravila u kome ne postoji minimum zahteva u EU, sem jednog člana u PSI Direktivi, dok pasivan aspekt, tj. dostavljanje podataka u otvorenom obliku na ponovnu upotrebu tek po konkretnom zahtevu tražioca, podrazumeva drugi skup pravila (primenjuje se PSI Direktiva).

5.1.1. ZAKON O ELEKTRONSKOJ UPRAVI

Regulisanje obaveze organa javne uprave da objavljuju setove podataka u otvorenom obliku, usko je povezano sa uspostavljanjem i upravljanjem elektronskim podacima i dokumentima, odnosno njihovom razmenom kroz elektronsku komunikaciju u okviru elektronskog upravnog postupanja (elektronska uprava). Ova materija bi trebalo da bude obuhvaćena novim zakonom koji bi regulisao elektronsku upravu Republike Srbije.

S obzirom na to da otvaranje podataka nužno podrazumeva elektronsku komunikaciju koja bi morala biti u skladu sa regulativom elektronske uprave, predmetni zakon, čini se, omogućava više nego odgovarajući kontekst za regulisanje obaveze države da određene setove podataka objavljuje u otvorenoj formi.

Kako je nacrt zakona o elektronskoj upravi u kasnoj fazi izrade, u saradnji sa radnom grupom koja radi na izradi predloga zakona potrebno je postići zajedničko razumevanje o načinu na koji bi mogle biti obuhvaćene odredbe o otvaranju podataka. Pravna podgrupa radne grupe za otvorene podatke je krajem 2016. godine pripremila predlog zakonskih odredbi za ovu materiju, koju će prezentovati na prvom sledećem sastanku radne grupe za zakon o elektronskoj upravi.

1 Direktiva 2003/98/EC http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:02003L0098-20130717; nezvaničan prevod na srpski jezik: http://www.poverenik.rs/yu/pravni-okvir-pi/medjunarodni-dokumenti-pi/1644-nezvanican-prevod-direktiva-201337eu-evropskog-parlamenta-i-saveta-od-2662013-.html

5.1.2. ZAKON O SLOBODNOM PRISTUPU INFORMACIJAMA OD JAVNOG ZNAČAJA

Stav radne grupe za otvorene podatke jeste da je najbolje rešenje za implementaciju PSI Direktive putem odgovarajućih izmena Zakona o slobodnom pristupu informacijama od javnog značaja. Ovaj stav zauzet je zahvaljujući istraživanjima SHARE Fondacije u okviru radne grupe, a koje se odnosilo i na analizu načina na koje je ova Direktiva implementirana u EU zemljama.

Naime, PSI Direktiva iz 2003. godine nije obavezivala države članice da dostavljaju podatke za ponovnu upotrebu, niti je menjala opšti režim pristupa informacijama od javnog značaja država članica. Izmenama Direktive iz 2013. godine je uvedena obaveznost dostavljanja informacija za ponovnu upotrebu, u skladu sa uslovima iz same Direktive, i dodatno je proširen krug dokumenata na koje se Direktiva odnosi. Države članice su u vreme donošenja Direktive bile na različitom regulatornom nivou po pitanju koncepta ponovne upotrebe, neke su ga već poznavale i imale svoje nacionalne zakone, a neke su obavezu ponovne upotrebe uvele tek u cilju implementacije Direktive. Takođe je postojala razlika i u tome što su neke države obavezu dostavljanja podataka za ponovnu upotrebu direktno vezivale za pravo slobodnog pristupa informacijama, a kod nekih ta veza nije bila jasna što je izazivalo pravnu nesigurnost. Razlike u stepenu razvoja, stanju i režimu nacionalne zakonske regulative, dovele su do toga da su pravila iz Direktive implementirana na različite načine:

- Donošenje ili izmena ranije donetih zakona i ostalih propisa koji su već regulisali obavezu dostavljanja informacija za ponovnu upotrebu.
- Izmena postojećih zakona o slobodnom pristupu informacijama od javnog značaja (ili sličnih zakona) radi dodavanja obaveze dostavljanja informacija za ponovnu upotrebu u odgovarajućem formatu.

U Srbiji trenutno ne postoje propisi koji bi zabranjivali dostavljanje informacija za ponovnu upotrebu po zahtevu korisnika, ali ni oni koji to pitanje regulišu. Regulativa ovog pitanja bi, u principu, mogla da ide u jednom od dva glavna pravca evropskih zemalja. Ipak, ovog trenutka se čini da postoje opravdani razlozi da se institut otvaranja podataka za ponovnu upotrebu u domaći pravni sistem uvede kroz već ustaljena pravila o slobodnom pristupu informacijama od javnog značaja.

U tom smislu je važno napomenuti da pokreti za otvaranje podataka za ponovnu upotrebu informacija (open government data, OGD) i za slobodan pristup informacijama od javnog značaja (right-to-information, RTI) imaju dosta sličnosti i dodirnih tačaka, ali i neke različitosti. Razlike su uglavnom istorijske, postojale su tokom nastanaka oba pokreta i danas sve više blede. Naime, pokret za slobodan pristup informacijama istorijski je zasnovan na pravu građana na informisanost i smanjivanju asimetrije informacija, odnosno na ideji da država prikuplja i čuva informacije radi koristi građana a ne svoje sopstvene (ideološki porivi), dok je pokret za otvaranje podataka za ponovnu upotrebu stavljao akcenat na tehnološku korisnost takvih podataka za dalje korišćenje u cilju inovacija i ekonomskog napretka, pa tek onda na odgovornost države i transparentnost (tehnološki porivi).[2] Još jedna razlika je u tome da slobodan pristup informacijama nikad nema zahtev za odgovarajućim licencama za uvid i/ili upotrebu, što sa otvorenim podacima ne mora biti slučaj.

Ipak, u literaturi i stručnoj javnosti stav je da su sličnosti brojnije i sušastvenije te da, iako nemaju potpuno identičan sadržaj, oba instituta imaju toliko veliko i značajno polje preseka da ima smisla regulisati ih zajedno. Dakle, mogu se tumačiti u odnosu komplementarnosti, a ne međusobnog sukoba ili isključivanja.

Sličnosti se najpre vide u identičnosti zahteva zagovarača oba prava za transparentan rad državnih organa i slobodu pristupa svim informacijama koji su u njihovom posedu, osim podataka koji su po nekom posebnom režimu izuzeti. Zagovarači prava na ponovnu upotrebu otvorenih podataka mogli bi da se oslone na već razvijenu i izgrađenu svest o važnosti transparentnog rada države dok bi, s druge strane, zagovarači prava na slobodan pristup mogli imati koristi ukoliko bi pod pritiskom zahteva za ponovnu upotrebu bio povećan kvalitet informacija koje se dostavljaju po zahtevima za pristup, zbog činjenice da su zahtevi za slobodnu upotrebu po pravilu detaljniji i konkretniji.[3] Drugim rečima, već sada ustanovljeno pravo na slobodan pristup ispunjava svoju svrhu tek ukoliko su informacije koje se daju tačne i jasne. To, nažalost, često nije slučaj zbog toga što sami državni organi ne prikupljaju i ne čuvaju informacije na odgovarajući način, informacije nisu sistematizovane niti proverene, a nije retkost ni da organi imaju duplirane informacije koje se ne podudaraju. Filozofija u osnovi otvorenih podataka mogla bi da bude motiv državnim organima da se pozabave ovim problemima, s kojima su se već susretali tokom primene Zakona o slobodnom pristupu informacijama od javnog značaja.

Dodatno, paralelnim postupanjem i po zahtevima za slobodan pristup i zahtevima za ponovnu upotrebu, državni službenici bi razvijali znanja i veštine u oblasti transparentne e-uprave, što bi indirektno doprinelo poboljšanju i u nekim drugim oblastima, od kojih se kao najvažnija ističe kompetentnost u postupanju sa podacima o ličnosti.[4]

U slučaju Srbije, ono što ide u prilog regulisanju otvorenih podataka u okviru Zakona o slobodnom pristupu informacijama od javnog značaja, jeste činjenica da se taj Zakon već godinama primenjuje i da su državni organi, stručna javnost i građani dobro upoznati sa pravima na informacije koja su na njemu zasnovana. Zbog izuzetno visoko postavljenih standarda postupanja po zahtevima za slobodan pristup informacijama, koji se izgrađuju pre svega zahvaljujući angažovanosti Poverenika za informacije od javnog značaja i zaštitu podataka o ličnosti, ne bi trebalo da postoji opasnost, uočena u stručnoj javnosti, da bi fokus državnih organa lako mogao da sklizne na tehnički aspekt otvaranja podataka, umesto na suštinski zahtev

2 A.Yannoukakoua, I. Araka, Pristup informacijama vlasti: Sinergija prava na informaciju i otvorenih podataka vlasti: http://www.sciencedirect.com/science/article/pii/S187704281404018X

3 WWW Foundation Blog, Open data + Pravo na informaciju = Pravo na podatke: http://webfoundation.org/2015/06/open-data-right-to-information-right-to-data/;

4 Ibid.

transparentnosti.[5] Naprotiv, unošenje dodatnih zahteva da se informacije koje su dostupne moraju dostaviti u odgovarajućem formatu i služiti za ponovnu upotrebu, može pozitivno uticati na održavanje visokih standarda, uz odgovarajući oprez u slučajevima kad priroda otvorenih podataka to nalaže.

U tom smislu, važno je imati u vidu da bi postojeće razlike između ova dva instituta potencijalno mogle da dovedu do toga da sam pristup otvorenim podacima može biti u određenim slučajevima ograničen iz razloga koji ne važe za slobodan pristup informacijama, te je zato u delu koji se tiče ograničenja prava potrebno posvetiti posebnu pažnju prilikom regulisanja oba instituta.

Regulisanje prava na slobodan pristup otvorenim podacima u okviru već postojećih propisa o slobodnom pristupu informacijama od javnog značaja, nije bez izazova ali, ukoliko bude pažljivo isplanirano, može značajno doprineti povoljnom razvoju i efikasnoj praktičnoj primeni oba prava, i omogućiti Srbiji da možda čak bude među istaknutijim zemljama u ovom smislu u svetskim razmerama, naročito s obzirom na to da su otvoreni podaci nova i izazovna tema za najveći broj zemalja sveta.[6]

PREPORUKE

Neophodno je dopuniti pravni okvir koji reguliše pristup informacijama od javnog značaja kako bi se uredilo pitanje otvorenih podataka u Srbiji i u skladu s tim, kao prioritet u organima vlasti, započeti praksu otvaranja podataka. Neophodno je sprovesti edukaciju zaposlenih u organima vlasti, pre svega tehničku, u pogledu praksi otvaranja podataka, kako bi podaci bili objavljeni u mašinski čitljivom obliku i ispunjavali ostale uslove za obradu i analizu.

5 K. Janssen, Otvoreni podaci vlasti i pravo na informaciju: Mogućnosti i prepreke http://ci-journal.net/index.php/ciej/article/view/952/954.

6 Open Data Barometar: http://opendatabarometer.org/3rdEdition/report/; Freedominfo.org, http://www.freedominfo.org/2016/04/open-data-barometer-reads-low-and-steady-study-says/

5.2. PRAVA INTELEKTUALNE SVOJINE

5.2.1. STRATEGIJA INTELEKTUALNE SVOJINE

Predlog strategije intelektualne svojine za period od 2016. do 2020. godine podnelo je Ministarstvo prosvete, nauke i tehnološkog razvoja vladinom Odboru za privredu i finansije. Predlog je 3. novembra 2016. godine stavljen na javnu raspravu, uz nedostatak informacija o tome ko je i kada učestvovao u njegovoj izradi.

SHARE Fondacija je pozvala biblioteke, IT zajednicu, kreativni sektor, organizacije civilnog društva, i druge zainteresovane aktere da učestvuju u pripremi komentara na Predlog strategije, koje je bilo neophodno dostaviti do 22. novembra, upozoravajući javnost na netransparentnost procesa izrade dokumenta.[7]

Pisanje komentara trajalo je manje od sedam radnih dana, a konačnu verziju je podržalo 29 organizacija.[8] Opšti zaključak Komentara ukazuje da je Predlog strategije izrađen mimo zainteresovane javnosti, bez konsultacija sa javnim i privatnim akterima čije će poslovanje trpeti neposredan uticaj predložene strategije. Pojedina rešenja Predloga nalaze se u koliziji sa ustavnim i zakonskim okvirom Republike Srbije, te odstupaju sa puta harmonizacije domaćeg pravnog poretka sa evropskim tekovinama.

Predloženi strateški tekst potpuno izostavlja čitav spektar delatnosti i načela od javnog interesa, kao što su slobodan pristup znanju i zajedničkom nasleđu, sloboda izražavanja u onlajn okruženju, informaciona privatnost te razvoj inovacija, kreativnih industrija i IT preduzetništva. Autori Predloga promovišu mere za zaštitu intelektualne svojine koje bi mogle ugroziti Ustavom i zakonima zaštićena prava građana i narušiti odnose na slobodnom tržištu. Ne uzimajući u obzir prirodu poslovanja na internetu ni tehničke mogućnosti za izvršenje predloženih mera, Predlog potencijalno ugrožava poslovanje pružalaca usluga informacionog društva, a pravosudnom sistemu najavljuje zatrpavanje zahtevima za odlučivanje. Sporne mere obuhvataju blokiranje i filtriranje sajtova, oduzimanje domena, kreiranje baze „sumnjivih lica" i prikupljanje obaveštajnih podataka, što nije u skladu sa domaćim i evropskim pravnim sistemom. Očekivanje rasta prihoda po osnovu intelektualne svojine (u najvećoj meri velikih internacionalnih kompanija, van granica Republike Srbije) sprovođenjem ovakvih

7 Strategija za ograničavanje onlajn sloboda, inovacija i pristupa znanju, novembar 2016. http://www.shareconference.net/sh/defense/strategija-za-ogranicavanje-onlajn-sloboda-inovacija-i-pristupa-znanju

8 Komentar na Predlog strategije intelektualne svojine za period od 2016. do 2020. godine, SHARE Fondacija http://www.shareconference.net/sites/default/files/u742/komentari_na_predlog_strategije_ip2016-2020_share_fondacija.pdf

mera ne odražava iskustva razvijenih zemalja niti relevantna istraživanja, dok bi troškovi primene i održavanja predloženih mera predstavljali dodatni finansijski teret za internet provajdere, a koji bi na kraju snosili građani Srbije.

Upozoravajući da, ukoliko ovaj Predlog strategije bude usvojen i implementiran, internet u Srbji više nikada neće biti isti, SHARE Fondacija i srodne organizacije građanskog društva ocenile su da predloženi dokument direktno gura Srbiju u režim neusaglašenosti zakonodavnih rešenja sa pravom Evropske unije. Predložene mere su nepotrebno komplikovane i skupe, pritom bez izgleda da budu uspešne.

Po predaji komentara Zavodu za intelektualnu svojinu, Fondacija je zatražila uvid u sve ostale prispele komentare na Predlog strategije. Prema rečima vd direktora Zavoda za intelektualnu svojinu, komentari SHARE Fondacije su najobimniji i biće pažljivo razmotreni.

PREPORUKE

Izmenama regulative iz oblasti autorskog i srodnih prava, redefinisati izuzetke i ograničenja, odnosno koncept fer upotrebe (fair use) predmeta prava intelektualne svojine bez potrebe pribavljanja saglasnosti nosioca tog prava i bez potrebe plaćanja naknade, u cilju uspostavljanja ravnoteže izmedu zaštite prava intelektualne svojine i drugih važnih prava i interesa, poput prava na slobodu izražavanja, kulturnih prava, prava na obrazovanje i drugih.

5.2.2. SLOBODNA UPOTREBA AUTORSKIH DELA

Nove tehnologije omogućile su radikalne promene u proizvodnji, skladištenju i distribuciji informacija. Digitizacija sadržaja pohranjenih na tradicionalnim, analognim nosačima posebno je značajna za oslobađanje pristupa znanju u oblastima od opšteg interesa, kao što su obrazovanje, nauka, javno informisanje ili kulturno nasleđe. Početak realizacije procesa digitizacije pre svega je vezan za ograničenje autorskog prava, odnosno definisanje privatnog i javnog domena u pogledu zaštite autorskih prava.

SHARE Fondacija je krajem 2015, u saradnji sa beogradskom kancelarijom Fondacije Heinrich Boll, započela pripremnu fazu projekta ,,Pravno istaživanje i razvijanje onlajn alata u skladu sa javnim domenom, u saradnji sa Narodnom bibliotekom Srbije (NBS)''. Nakon serije sastanaka i razgovora sa predstavnicima uprave i članovima pojedinih organizacionih jedinica u Narodnoj biblioteci, metodološki su popisani pravni problemi bibliotečke delatnosti u procesu digitizacije. Stručni savet NBS prihvatio je ovaj dokument kao prilog Sporazumu o razumevanju koji su potpisali Narodna biblioteka Srbije, SHARE Fondacija i ,,Heinrich Boll Foundation'' - Predstavništvo u Beogradu.

Projekat je započet u julu 2016. godine kada je sprovedeno kompleksno istraživanje u oblasti oslobađanja sadržaja i stvaranja slobodnog sadržaja u bibliotečkoj građi NBS. Istraživanje se posebno bavilo pitanjima utvrđivanja da li je autorsko delo u javnom domenu ili ne; da li postoji mogućnost korišćenja izuzetaka u skladu sa Zakonom o autorskom i srodnim pravima; na koji način se dobija dozvola od autora; kako se primenjuju posebna pravila, ako je autor nepoznat, kako bi se oslobodila građa i omogućio slobodan pristup znanju.

Na osnovu rezultata istraživanja, kao optmalno rešenje predložena je izrada vodiča o autorskim pravima i onlajn alata koji analizira status autorskog dela i upućuje na zakonske izuzetke koji se mogu primeniti pri upotrebi dela u zavisnosti od potreba korisnika alata (vidi: odeljak 5.6).

Stručni vodič o autorskim pravima, ,,Slobodna upotreba autorskih dela'', namenjen je institucijama kulture, kreativnoj industriji, medijima, ali i široj javnosti, i sadrži dodatna pojašnjenja o mogućnostima za slobodno korišćenje autorskih dela, u skladu sa izuzecima predviđenim domaćim Zakonom o autorskom i srodnim pravima i odgovarajućim međunarodnim konvencijama. Priručnik pojašnjava zakonske definicije, vrste prava i ograničenja, kao i upotrebu autorskih dela koja su u javnom domenu, dakle slobodna za korišćenje bez dozvole autora i obavezne naknade. Kao i drugi vodiči SHARE Fondacije, i ovaj je slobodno dostupan javnosti.[9]

Programski direktor SHARE Fondacije Đorđe Krivokapić i advokat Jelena Adamović održali su radionice za zaposlene u Narodnoj biblioteci Srbije u Beogradu, kao i u Narodnoj biblioteci ,,Stevan Sremac'' u Nišu za zaposlene u bibliotekama na jugu Srbije, gde su predstavili onlajn alat za autorska prava i vodič o autorskim pravima. Na radionici je bilo reči i o tehnološkim inovacijama, digitizaciji i autorskim pravima, kao i o slobodnoj upotrebi dela bez ugrožavanja autorskih prava.

Narodna biblioteka Srbije u Beogradu

Narodna biblioteka ,,Stevan Sremac'' u Nišu

9 Vodič o autorskim pravima: Slobodna upotreba autorskih dela, SHARE Fondacija, 2017. http://www.shareconference.net/sites/default/files/u742/vodic _ o _ autorskim _ pravima _ final.pdf

VODIČ O AUTORSKIM PRAVIMA

SLOBODNA UPOTREBA AUTORSKIH DELA

Digitalne komunikacione tehnologije su nam otvorile ne samo pristup gotovo beskonačnoj količini sadržaja, već i mogućnost da sami kreiramo nova dela i obrađujemo postojeća. Usled brzine razmene sadržaja i razvoja remiks kulture, korisnici interneta često ne vode računa o tome da li su fotke, video-snimci ili tekstovi zaštićeni autorskim pravom, odnosno da li je i u kojoj meri ograničeno pravo njihovog korišćenja i prerade. Iako u našem pravnom sistemu postoje brojni izuzeci koji omogućavaju slobodnu upotrebu autorskih dela, ponekad nije jednostavno protumačiti zakon na pravi način. Samostalnim umetnicima, novinarima, naučnicima i predavačima često nedostaje poznavanje pravničke terminologije iz ove oblasti ili resursa za angažovanje pravnog savetnika.

Ovaj vodič je namenjen svakome ko želi da sazna nešto više o mogućnostima za slobodno korišćenje autorskih dela, u skladu sa izuzecima predvidenim domaćim Zakonom o autorskom i srodnim pravima i odgovarajućim medunarodnim konvencijama. Razjasnićemo zakonske definicije, vrste prava i ograničenja, kao i upotrebu autorskih dela koja su u javnom domenu, dakle slobodna za korišćenje bez dozvole autora i obavezne naknade.

(Vodič objavljen u martu 2017.)

5.2.3. COPYRIGHT KALKULATOR

Regulatorni okvir kojim se autorska dela štite od neovlašćene upotrebe, predstavlja kompleksnu prepreku za slobodan pristup znanju i neometan protok ideja i informacija u onlajn okruženju. Stoga je tehnički tim SHARE Fondacije kreirao alat za informisanje digitalne zajednice o kriterijumima za slobodnu upotrebu dela i zakonskim izuzecima u slučajevima kada delo nije u javnom domenu. Alat je interaktivan i jednostavan za upotrebu: www.copyrightcalculator.rs

Izrađen na osnovu pravne analize za Vodič o slobodnoj upotrebi autorskih dela, kao i istraživanja o oslobađanju pristupa sadržajima iz bibliotečkog fonda NBS, ,,kalkulator'' u formi upitnika vodi korisnike kroz zakonski lavirint autorskih prava, pružajući konkretne odgovore na moguće nedoumice prilikom upotrebe autorskog dela. Godina izdanja, na primer, rešava pitanje da li je istekla zakonska zaštita, odnosno da li je delo ušlo u javni domen; dilema o autorstvu vodi ka razjašnjenju zakonskog tretmana dela čiji autor nije poznat; praktični primeri ilustruju zakonske izuzetke koji omogućavaju specifične upotrebe dela pod punom zaštitom, kao što su obrazovanje, javno informisanje, citiranje, ili slično.

Informativni alat razjašnjava pojmove i pravne kriterijume za regulisanje autorskih prava i izuzetaka, kao što su vrsta dela, korisnik, namena i način korišćenja, a predstavlja i savremeni sistem licenciranja upotrebe dela pod međunarodnim oznakama ,,creative commons''.

5.2.4. AUTENTIČNIM TUMAČENJEM PROTIV FOTOGRAFIJE KAO AUTORSKOG DELA

Serija tužbi protiv medija zbog neovlašćenog korišćenja fotografija dovela je do neobične inicijative u Skupštini Srbije. Naime, predlog ,,autentičnog tumačenja'' odredbi Zakona o autorskim i srodnim pravima koje se odnose na fotografiju kao autorsko delo, dospeo je početkom januara 2016. na Odbor za ustavna pitanja i zakonodavstvo. Tekst predloženog autentičnog tumačenja trebalo je da ukine zaštitu autorskog prava svakoj ,,rutinski'' izrađenoj fotografiji, ,,koja se pojavljuje i preuzima u elektronskom obliku, bez obzira da li je originalna duhovna tvorevina autora''.[10] Da je usvojeno, ovakvo autentično tumačenje bi u praksi značilo da se svaka fotografija objavljena na internetu može slobodno koristiti bez dozvole. Autentično tumačenje na kraju ipak nije prošlo Odbor[11], ali je ,,odbrana fotografije''[12] svakako ostala jedan od značajnijih napora stručne zajednice i javnosti u zaštiti digitalnih prava tokom 2016. godine.

10 ,,Od petka fotografije bez pravne zaštite: sa vašim selfijem svako će moći da radi šta hoće'', SHARE Fondacija, 2016. http://www.shareconference.net/sh/defense/od-petka-fotografije-bez-pravne-zastite-sa-vasim-selfijem-svako-ce-moci-da-radi-sta-hoce

11 ,,Pobeda fotografa: Nije usvojen predlog zakona, ostaju im autorska prava'', januar 2016. http://www.newsweek.rs/srbija/68987-nije-usvojen-predlog-zakona-fotoreporterima-ostaju-autorska-prava.html

12 ,,Šta dalje posle odbrane fotografija'', SHARE Fondacija, 2016. http://www.shareconference.net/sh/defense/sta-dalje-posle-odbrane-fotografija

Apsurd predloga autentičnog tumačenja ogleda se već i u njegovom obrazloženju, u kome se kao problem postojećeg zakonskog rešenja ukazivalo da se autorskim delom smatra svaka, ,,rutinski'' izrađena fotografija, na kojoj može biti predstavljena ,,kobasica [...], rupe na putu''. Nejasno je ostalo kako su pisci predloga uspostavili objekat fotografije kao kriterijum autorstva, ili njenu umetničku vrednost, budući da se Zakonom reguliše nameravana upotreba dela, bez obzira šta se na njemu nalazi ili koliko je delo kvalitetno. Bernska konvencija o zaštiti književnih i umetničkih dela, koju je ratifikovala i Srbija, u članu 2, stav 1 predviđa da izraz ,,književna i umetnička dela'' obuhvata i dela iz oblasti fotografije, s kojima su izjednačena i dela izražena postupkom sličnom fotografiji.[13] Takođe, u Konvenciji se u članu 9, stav 1 jasno navodi da autori književnih i umetničkih dela uživaju isključivo pravo da daju odobrenje za reprodukovanje dela, bez obzira na koji način i u kom obliku.

Kada je reč o selfijima i drugim ličnim fotografijama koje se svakodnevno objavljuju na društvenim medijima, njihovim slobodnim preuzimanjem i korišćenjem se ne bi kršila samo autorska prava već i pravo na privatnost i pravo na lik. U tom smislu treba istaći i da praksa povodom ovog pitanja nije ujednačena. Kada svoje fotografije čine javno dostupnim na internetu, korisnici treba da pođu od pretpostavke da će svako moći da dođe u njihov posed i iskoristi ih u različite svrhe. Koliko god da se javno objavljena fotografija smatra privatnom, autor mora znati da ju je svesno objavio na internetu, da je upravo zahvaljujući njegovom radnjom (jednim običnim klikom) ona postala javno dostupna neodređenom broju ljudi. U zavisnosti od okolnosti svakog pojedinačnog slučaja, zaštita se može tražiti u slučaju kršenja prava trećeg lica, kada se lik osobe na preuzetoj fotografiji iskoristi za reklamu ili drugu komercijalnu svrhu bez dozvole, u kom slučaju osoba čiji je lik zloupotrebljen može tražiti naknadu zbog povrede prava na lik.

Problematičan je bio i pokušaj da se sistem zaštite autorskih prava, uzimajući u obzir sve karateristike onlajn medija i digitalnog okruženja, reformiše ,,autentičnim tumačenjima'', što je nedopustivo. Reforma sistema zaštite autorskih prava, naime, treba isključivo da se sprovodi izmenama i dopunama Zakona o autorskim i srodnim pravima, kojima prethodi ozbiljna javna rasprava. Pritom treba voditi računa da se svim akterima omogući adekvatna zaštita, ali i opravdano korišćenje autorskih dela u situacijama od javnog interesa (obrazovanje, nauka, javno informisanje itd) u skladu sa međunarodnim standardima ljudskih prava.

13 Bernska konvencija o zaštiti književnih i umetničkih dela http://www.zis.gov.rs/upload/documents/pdf _ en/pdf _ ap/bern.pdf

6. LABS.RS

6.1. NAŠA LABORATORIJA

SHARE Lab je sastavni deo SHARE Fondacije koji se bavi izučavanjem i istraživanjem podataka sa različitih tehničkih aspekata intersekcija društva i tehnologije.[1] Istražujemo nevidljive puteve elektronskih prostranstava, u svrhu boljeg razumevanja novih formi bezbednosnih rizika, kao i rizika po privatnost i neutralnost Mreže. U svojim istraživanjima takođe pokušavamo da odgonetnemo mnoge fenomene digitalnog doba, kao što su ,,crne kutije'' algoritamskih fabrika.

Korišćenjem različitih metoda za prikupljanje, ukrštanje, analizu i vizualizaciju podataka, tokom prethodne dve godine objavljeno je desetak obimnih istraživanja, koja otkrivaju različite tehničke aspekte svakodnevnog korišćenja tehnologije - internet istoriju, informacione ratove, mejl komunikaciju, političku kampanju na društvenim mrežama, ,,lokaciju'' srpskog interneta i tome slično.

6.2. INTERNET ATLAS PRIVATNOSTI

U istraživanju ,,Nevidljive infrastrukture''[2], koristili smo različite metode za analizu mrežne topologije, data mining i vizualizaciju podataka, kako bismo izradili jedinstveni internet atlas privatnosti i transparentnosti, koji predstavlja skup vizuelnih predstava i metodologija kreiranih za mapiranje, razotkrivanje, vizualizaciju i nezavisno praćenje različitih aspekata privatnosti i transparentnosti na internetu.

Ova serija tekstova se bavi ,,životnim putem'' jednog internet paketa[3], tj. delića informacije koji prolazi kroz Mrežu posredstvom internet protokola, kao i putanjama internet paketa[4] do 100 najposećenijih sajtova u Srbiji. Istraživanje se takođe bavilo internet mapom Srbije[5] - predstavili smo glavne linkove i servere koji čine nacionalnu infrastrukturu interneta.

Predstavili smo i onlajn pratioce[6], odnosno male programe koji prikupljaju ,,digitalne tragove'', tj. informacije o kretanju i ponašanju korisnika na internetu. Na osnovu zahteva za informacije od javnog značaja, od kancelarije Poverenika za informacije od javnog značaja i zaštitu podataka o ličnosti dobili smo statističke podatke o elektronskom nadzoru i zadržavanju podataka[7], to jest različitim načinima na koje četiri operatora mobilne i fiksne telefonije u Srbiji omogućavaju državnim organima direktan pristup podacima o komunikaciji. Na kraju, ukazali smo na dozvole[8] koje dajemo u zamenu za ,,besplatno'' korišćenje aplikacija na mobilnim uređajima. Neke od najčešće korišćenih aplikacija, posebno one u vlasništvu Fejsbuka i Gugla, prikupljaju mnogo više podataka korisnika od drugih sličnih aplikacija (npr. DuckDuckGo) te se dovodi u pitanje poštovanje privatnosti korisnika.

6.3. IZBORI

Izborne kampanje na internetu[9] su takođe bile tema istraživanja SHARE Lab-a. Politički akteri su prepoznali društvene mreže i onlajn medije kao značajno polje za osvajanje uticaja i prikupljanje podrške. Tokom poslednja dva izborna ciklusa, tj. za parlamentarne izbore aprila 2016. godine i predsedničke izbore u Srbiji koji su održani 2017, pratili smo angažovanje političkih partija i predsedničkih kandidata u onlajn okruženju, kao i potencijalne povrede digitalnih prava i sloboda.

Istraživanje iz 2016. godine obuhvata izveštavanje onlajn medija o parlamentarnim izborima na internetu, reakciju publike na tekstove, kao i aktivnosti političkih aktera i njihovih sledbenika, odnosno oponenata na društvenim mrežama. Rezultati su pokazali da su partije i pokreti koji su uložili više resursa u odnosu na ostale u Fejsbuk kampanju (Dveri, Dosta je bilo, Srpska radikalna stranka) uspeli da ostvare svoj izborni cilj i da osvoje mesta u nacionalnom parlamentu, čemu je u određenoj meri sigurno doprineo pojačan angažman na društvenim mrežama.

Predsedničke izbore 2017. godine pratili smo sa malo drugačijeg aspekta, pošto za razliku od parlamentarnih izbora, predsednički izbori podrazumevaju znatno veću interakciju kandidata i građana. Fejsbuk je tokom kampanje najviše koristio kandidat Luka Maksimović, odnosno njegov alter-ego Ljubiša Preletačević Beli, komično predstavljeni srpski političar čiji je poduhvat dospeo i do svetskih medija. Sa više od milion zabeleženih interakcija, lajkova i komentara na objave njegove zvanične Fejsbuk stranice, Beli je vodio najaktivniju onlajn kampanju i osvojio treće mesto na predsedničkim izborima.

1 Sva istraživanja su slobodno dostupna: labs.rs

2 Razumevanje autonomnih sistema https://labs.rs/sr/test/

3 Uzbudljiv život internet paketa https://labs.rs/sr/nevidljiva-infrastruktura-uzbudljiv-zivot-internet-paketa/

4 Tokovi podataka https://labs.rs/sr/nevidljiva-infrastruktura-tokovi-podataka/

5 Internet mapa Srbije https://labs.rs/sr/nevidljive-infrastrukture-internet-mapa-srbije/

6 Onlajn pratioci https://labs.rs/sr/nevidljiva-infrastruktura-onlajn-pratioci/

7 Elektronski nadzor i zadržavanje podataka sa mobilnih telefona https://labs.rs/sr/nevidljive-infrastrukture-elektronski-nadzor-i-zadrzavanje-podataka-sa-mobilnih-telefona/

8 Dozvole na mobilnim uređajima https://labs.rs/sr/nevidljive-infrastrukture-dozvole-na-mobilnim-uredajima/

9 Oba istraživanja deo su laboratorijskog monitoringa: https://labs.rs/sr/category/monitoring/

VODIČ:

O DIGITALNIM PRAVIMA I INTERNET SLOBODAMA U POLITIČKOJ KOMUNIKA-CIJI

Društvene mreže, portali, blogovi i ostale onlajn platforme za sadržaj koji kreiraju korisnici, pružaju brojne mogućnosti političkim strankama i njihovim aktivistima za dvosmernu komunikaciju sa simpatizerima i potencijalnim glasačima.

Razvoj digitalnih tehnologija otvorio je nove mogućnosti za komunikaciju, ali je stvorio i nove oblike kršenja osnovnih prava na slobodu izražavanja, prava na pristup i razmenu informacija, prava na privatnost, kao i nove oblike pritiska na pojedince i medijske organizacije. U cilju otklanjanja neizvesnosti u vezi sa ovakvim zloupotrebama tehnologije, sastavili smo vodič sa smernicama zasnovanim na važećoj regulativi, koje omogućavaju svim akterima komunikacije da ravnopravno učestvuju u onlajn političkoj debati bez kršenja pravnih i etičkih normi, poštujući osnove internet kulture.

(Vodič objavljen u martu 2016.)

6.4. ALGORITAMSKA FEJSBUK FABRIKA

Ispitivali smo i implikacije nematerijalnog rada, skrivenog u algoritamskim fabrikama velikih internet kompanija.[10] Svako ko ima nalog na Fejsbuku nesvesno radi za kompaniju u čijem je vlasništvu ova društvena mreža, svakodnevnim unosom podataka o sebi, detaljima koji stvaraju digitalni profil sve atraktivniji za monetizaciju, odnosno targetirano reklamiranje. Taj nevidljivi i nematerijalni rad se odvija u okviru crnih kutija čije smo funkcionisanje pokušali da otkrijemo.

Istraživanje je obuhvatilo mapiranje i prikazivanje kompleksnih i nevidljivih procesa eksploatacije sakrivenih iza najveće društvene mreže na svetu. Istraživanje o Fejsbuku podeljeno je na tri dela koja opisuju ključne procese algoritamskih fabrika: prikupljanje podataka, skladištenje i algoritamsku obradu podataka, kao i targetiranje korisnika. Takođe smo se dotakli procesa tihe kolonizacije života korisnika interneta, koju Fejsbuk sprovodi preuzimajući sve veću ulogu u definisanju društvenih procesa.

10 Istraživanja o Fejsbuku su dostupna samo na engleskom jeziku: https://labs.rs/en/category/facebook-research/

7. DRUŠTVO U NOVOM OKRUŽENJU

7.1. RADNA PRAVA I INTERNET

Korišćenje interneta za posao ili tokom radnog vremena je stvar svakodnevice, naročito imajući u vidu da poslodavci za sve veći broj poslovnih profila traže aktivno poznavanje tehnologije. Kako prava iz radnog odnosa sve više dobijaju digitalnu dimenziju, neophodno je skrenuti pažnju na probleme poput blokiranja pristupa određenim sajtovima na radnom mestu, nadzoru elektronskih komunikacija zaposlenih, ili disciplinovanje zbog izražavanja stavova na društvenim mrežama. Recimo, Evropski sud za ljudska prava doneo je sredinom januara 2017. presudu u slučaju Barbulesku protiv Rumunije, čim je dao odgovor na pravne nedoumice u vezi sa pravom na privatnost digitalnih komunikacija na poslovnim nalozima.[1]

Stav suda u slučaju Barbulesku bio je da nema povrede člana 8 Evropske konvencije o ljudskim pravima, koji garantuje pravo na privatni i porodični život, u slučaju kada poslodavci pristupaju nalozima za komunikaciju koji zaposleni treba da koriste u profesionalne svrhe, tj. za aktivnosti na kojima su radno angažovani. Preciznije, poslodavac prema mišljenju sudija nije narušio privatnost g. Barbuleskua proveravanjem njegovog profesionalnog Jahu mesindžer naloga kako bi utvrdio da li ispunjava poslovne obaveze tokom radnog vremena. Iako je stav Evropskog suda ljudskih prava o proporcionalnom pristupu poslovnim komunikacijama (npr. službeni mejl nalog) radi provere izvršavanja radnih obaveza razumljiv, teško je saznati da li poslodavci u Srbiji nadgledaju sve komunikacije zaposlenih tokom radnog vremena, odnosno i prepiske na njihovim privatnim nalozima. Postoje indicije[2] da i pojedine kompanije u Srbiji putem softvera pregledaju šta njihovi zaposleni pišu tokom radnog vremena na poslovnim kompjuterima, te se mogu postaviti brojna pitanja u vezi sa pravnim osnovom ovakvih mera. Slučajevi sa kojima su se susretali istraživači SHARE Fondacije, ali i šira javnost posredstvom medija, uglavnom se odnose na državne subjekte.

SHARE Fondacija u okviru svog monitoringa prati i beleži slučajeve povreda internet sloboda u radnom odnosu,[3] koji su uglavnom u vezi sa posledicama koje pojedinci trpe na poslu zbog svojih aktivnosti na Mreži. Tipičan slučaj koji dobro ilustruje ovu pojavu jeste mobing Jasminke Kocijan, novinarke koja vodi sudski postupak protiv svog poslodavca, agencije Tanjug. Problemi su počeli neposredno posle akcije spasavanja zavejanih građana u Feketiću početkom februara 2014, kada je Kocijan sa svog privatnog Fejsbuk naloga komentarisala taj događaj. Važno je napomenuti da Kocijan nije objavila post tokom obavljanja novinarskog zadatka, već dok je bila na bolovanju. Po povratku na posao, usledili su brojni problemi, poput novčanog kažnjavanja i premeštanja na niža radna mesta. Još jedan slučaj zabeležen je u julu 2015. godine, kada je bivši pripravnik Višeg suda u Beogradu, Radovan Nenadić, dobio otkaz nakon što je na društvenim mrežama i blogu objavio informaciju o postupku jednog od sudija, koji je on smatrao nedostojnim sudijske funkcije, prema važećim propisima. Nenadić je zatražio sudsku zaštitu kao uzbunjivač, ali je Viši sud u Novom Sadu krajem novembra 2016. odbio njegov tužbeni zahtev. U martu 2016, Apelacioni sud u Novom Sadu je doneo presudu prema kojoj Nenadić nema status uzbunjivača, te da u ovom slučaju nije utvrđeno uzbunjivanje u skladu sa Zakonom o uzbunjivačima.[4]

Poslodavci mogu bliže urediti pravila za korišćenje društvenih mreža i uređaja na radnom mestu, ali moraju da budu svesni da njihove interne procedure, politike, ugovori o radu i svi drugi dokumenti u vezi za zapošljavanjem i radnom disciplinom moraju biti u skladu sa važećim zakonodavnim okvirom, preciznije sa Ustavom i Zakonom o radu. Iako postoji mogućnost da se radnicima daju smernice za korišćenje onlajn platformi, poslodavci svojim zaposlenima ne mogu u potpunosti ograničiti zagarantovana prava, pa tako ni pravo na slobodu izražavanja ili pravo na privatnost.

Međutim, neetični ili neprihvatljivi postupci poslodavaca su sada vidljiviji zahvaljujući internetu. Zbog odsustva jasnih smernica koje treba bliže da urede aktivnosti radnika na Mreži i postupke poslodavca u slučaju da se smernice prekrše, kao i nedostatka poznavanja ljudskih prava i digitalnog okruženja, poslodavci često preduzimaju ishitrene korake koji mogu biti nekorektni po radnike, pa čak i nezakoniti. Kako stvari trenutno stoje, među zaposlenima u javnim institucijama i u privatnom sektoru, prisutan je efekat zebnje koji ugrožava njihova digitalna prava u radnom odnosu.

1 Slučaj Bărbulescu v. Rumunija (Zahtev br. 61496/08) http://hudoc.echr.coe.int/eng?i=001-159906

2 „Da li vas kompanija gde radite špijunira?" https://sadrzaj.ogledalofirme.com/2017/01/05/itevci-da-li-vas-kompanija-gde-radite-spijunira-2/

3 Đorđe Krivokapić, Bojan Perkov i Nevena Krivokapić, Digitalna prava na radnom mestu, GISWatch 2016. https://www.giswatch.org/sites/default/files/gw2016-serbia.pdf

4 Apelacioni sud u Novom Sadu: Nenadić nije uzbunjivač; 021.rs, 2016 http://www.021.rs/story/Novi-Sad/Vesti/158435/Apelacioni-sud-u-Novom-Sadu-Nenadic-nije-uzbunjivac.html#comm

VODIČ:

RADNICI NA LIZING

PRAVA RADNIKA PRIVREMENO ANGAŽOVANIH PREKO AGENCIJA ZA ZAPOŠLJAVANJE

Počelo je kao gorka šala: posle automobila, u Srbiji se od sada i radnici mogu uzeti na lizing. Razumljiva je ogorčenost, izazvana beskrajnom tranzicijom i pratećim potresima na domaćem tržištu, visokom stopom nezaposlenosti i teškim uslovima za rad.

Medutim, bez sve šale, lizing je decenijska praksa u svetu i nije nužno vezana za osiromašenje privrede. U najkraćem, reč je o zakupu ili, preciznije, pravu na korišćenje robe ili usluge na odredeno vreme, pri čemu se posao sklapa preko posrednika. Istorija poznaje ovaj oblik poslovanja od pamtiveka i, bilo da se radi o uslugama najamnih ratnika ili radnika, posrednik je bio taj čija je obaveza da brine o dužnostima ali i dobrobiti najamnika. Vodič daje pregled pravnog okvira rada na lizing u Srbiji i preporuke za efikasniju zaštitu prava „rentiranih radnika".

(Vodič objavljen u martu 2016.)

7.2. KOLABORATIVNA EKONOMIJA

Fuzija novih tehnologija koja briše granice između fizičkog, digitalnog i biološkog sveta, znak je početka Četvrte industrijske revolucije, smatra Klaus Švab, osnivač Svetskog ekonomskog foruma.[5] Za razliku od ranijih industrijskih revolucija, Četvrta se razvija eksponencijalnom brzinom, bez presedana u istoriji. Radikalni uticaj na gotovo svaku industriju, u svakoj državi sveta, uz fundamentalne promene koje nastaju u čitavim sistemima proizvodnje, poslovanja i javne uprave, jasno govore da smo zakoračili u nepoznate vode. To nas ne sprečava da već uveliko uživamo u spoju najlepših odlika svih utopijskih svetova o kojima je čovečanstvo sanjalo. Jedna od njih je ekonomija deljenja, ili kolaborativna potrošnja, novi socio-ekonomski model koji se razvija na temelju tehnoloških inovacija.[6]

Tržišta preplavljuju slobodnjaci, frilenseri, radnici koji biraju za koga će i pod kojim uslovima raditi, koji sami određuju svoje radno vreme i sami podmiruju svoje potrebe i obaveze. Ovi radikalni poremećaji na tržištu rada restrukturiraju finansijske transakcije, koje se sada vrše sa daleko manje posrednika. Ne posedovati ništa, a imati pristup svemu, novi je nalog autonomije života i ljudske slobode. Digitalnoj reinkarnaciji antičke agore, na kojoj slobodni građani slobodno diskutuju o pitanjima značajnim za zajednicu, upravo je nedostajao aspekt emancipacije neslobodnih – mogućnost uključivanja u stvaranje vrednosti, preuzimanjem sredstava proizvodnje i kontrole nad vlastitim radom.

Stalna povezanost korisnika i uređaja kojima se služi, sugeriše ne samo buduću pervazivnost virtuelne i proširene stvarnosti, već uključivanje virtuelnih aktivnosti u opseg identiteta. Učešće u umreženoj zajednici vrednuje se u neposrednoj interakciji sa članovima zajednice, neograničene geografskim ili kulturološkim poreklom, na osnovu složenog reputacionog sistema koji dalje narušava tradicionalne društvene hijerarhije. Mnoge od ovih promena zapravo su već na snazi, a uticaj koji vrše oseća se širom sveta, bez obzira na to u kojoj meri lokalna tržišta uspevaju da uhvate korak.

Poseban problem predstavlja činjenica da se novi industrijski preokret odigrava ne samo izvan tradicionalnih odnosa, već i unutar diskurzivnog polja čiji jezik većina još uvek ne govori. Ljudi nisu u mogućnosti da razluče kada su u poziciji klijenta, kada pružaju usluge a kada su oni proizvod. U kom trenutku pojedinac koji povremeno pruža određenu uslugu postaje profesionalac, subjekt pravne zaštite ali i obaveza koje izviru iz tradicionalno regulisanih radnih, trgovinskih i potrošačkih odnosa? Kada društvena razmena postaje ekonomska razmena koja ugrožava do tada uspostavljeno tržište? Kada društvena razmena postaje novostvorena vrednost podobna za oporezivanje? Da li se ,,šerovano'' mesto u automobilu, na putu od Beograda do Zagreba, tretira kao drugarska razmena, usluga informacionog društva ili usluga prevoza? Ko garantuje kvalitet usluge, internet servisi ili učesnici u transakcijama, i da li se na njih odnose pravila oglašavanja i poštenih trgovinskih praksi? Kome je svrsishodno uputiti žalbu kada smo prevareni, izmanipulisani ili nepravično vrednovani: domaćem pravosuđu ili korisničkim servisima?

Kako će se uopšte ispregovarati novi društveni ugovor, kad još nije jasna ni struktura novog društva, niti su postojeći regulatorni okviri sposobni da obuhvate sve nove odnose koji se stvaraju u ,,organizaciji umreženog rada''?

Konačno, ni sama ,,ekonomija deljenja'' nije ono za šta se predstavlja, budući da su glavni igrači na sceni korporacije koje posreduju razmeni među korisnicima. Bilo da kupuju robu ili uslugu, primarni motiv potrošača je utilitaran, a ne društveni.[7] Stoga bi bilo nužno osvestiti utopijski entuzijazam i vratiti pažnju na temeljna pitanja društva u Četvrtoj industrijskoj revoluciji. Jedna od osnovnih aporija socijalnih pokreta 19. i 20. veka zasad ostaje nerešena – ima li demokratije bez vlasništva?

7.3. DECA I MLADI SRBIJE NA INTERNETU

Nedostatak sveobuhvatnih i kontinuiranih istraživanja[8], uz pojmovne i metodološke nesuglasice, predstavlja ozbiljan izazov u prikupljanju kvalitetnih podataka o ponašanju dece i mladih u Srbiji na internetu i njihovu izloženost rizicima u onlajn okruženju. Svega je nekoliko novijih, naučnih ili anketnih istraživanja koja pružaju delimičan pogled na ovu osetljivu oblast.

U proseku, deca u Srbiji počinju da koriste internet u uzrastu od osam godina.[9] Istraživanja se slažu da sa godinama starosti raste i broj sati provedenih onlajn, sa prosekom od oko 3 i po sata dnevno. Četiri od pet mladih osoba koristi internet za pristup društvenim mrežama, dve trećine mladih zainteresovano je za muziku, svaka četvrta mlada osoba igra onlajn igrice, a najmanje je aktivnosti u vezi sa novčanim transakcijama. Gotovo polovina mladih (45,9%) na internetu se informiše o političkim događajima.[10]

5 Četvrta industrijska revolucija, januar 2016. https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond/

6 Rezolucija Evropskog parlamenta od 29. oktobra 2015. o novim izazovima i konceptima za podsticanje turizma u Evropi http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P8-TA-2015-0391+0+DOC+XML+V0//EN

7 Ekonomija deljenja nema veze sa deljenjem, januar 2016. https://hbr.org/2015/01/the-sharing-economy-isnt-about-sharing-at-all

8 Nacionalna strategija za mlade za period od 2015. do 2025. godine, str. 53 http://www.mos.gov.rs/wp-content/uploads/download-manager-files/Nacionalna 20strategija%20za%20mlade%20-%20SR.pdf

9 Popadić, D., Pavlović, Z., Petrović, D. and Kuzmanović, D., ,,Global kids online Serbia: Balansiranje između mogućnosti i rizika. Rezultati pilot studije'', Beograd, 2016 http://blogs.lse.ac.uk/gko/reportserbia/

10 Tomanović, S. i Stanojević, D. ,,Mladi u Srbiji 2015: Stanja, opažanja, verovanja i

Deset odsto dece i mladih od 9 do 17 godina, obuhvaćenih istraživanjem „Global Kids Online Serbia", ne poseduje vlastiti uređaj za pristup internetu bilo koje vrste (smartfon, tablet, kompjuter), a 44% poseduje jedan. Od ukupno ispitanih, 32% poseduje dva uređaja, 11% tri, 2% prijavilo je da ima četiri a 1% da ima pet uređaja.[11]

Isto istraživanje navodi da apsolutna većina (95%) koristi smartfon za pristup internetu, dok je personalni računar drugi na listi popularnih uređaja (76%). Ispitani radije biraju uređaj koji samo oni koriste, odnosno koji je u njihovom vlasništvu, zbog čega smartfoni imaju prednost, kao i zbog lakoće pristupa internetu na različitim mestima, mogućnosti da se povežu dok su nasamo, te radi kontrole nad sadržajima koje čuvaju na svom uređaju.

Podaci iz ankete koju je sproveo BIRODI (2453 učenika završnih razreda srednjih škola) govore da samo 5,1% ispitanih uopšte ne koristi društvene mreže.[12] Od onih koji ih koriste, na društvenim mrežama većina provodi od jednog do dva sata dnevno (34,8%). Oko četvrtine ispitanih provodi od 2 do 4 sata, dok 15,8% provodi više od 4 sata dnevno na društvenim mrežama.

Ispitivanja o mestu pristupa posredno sugerišu da se školsko okruženje, kao jedna od lokacija s koje se najčešće pristupa internetu, ne opaža kao bitno različito od kućnog. Ovaj utisak korelira sa percepcijom roditelja dece od 8 do 17 godina, prema kojoj igrice, muzički sadržaji i društvene mreže u najvećoj meri zaokupljaju dečiju pažnju na internetu, dok znatno manji deo internet aktivnosti ima veze sa informisanjem i obrazovanjem.[13]

Gotovo 79% dečaka i 63% devojčica smatra da poznaje internet bolje od svojih roditelja. U istraživanju Global Kids Online sa ovom tvrdnjom složiće se trećina dece u starosnoj grupi od 9 do 11 godina, dve trećine iz grupe 12-14 i gotovo sva deca u uzrastu od 15 do 17 godina. Deca i mladi obuhvaćeni ovim istraživanjem najbolje su ocenili svoje društvene veštine (prosečna ocena 3.7). Preko 90% njih smatra da zna koje informacije mogu da se dele sa drugima onlajn, dok 94% zna kako da izbriše nekog iz svojih kontakata na mrežama. Sledeće na listi su informatičke veštine (prosečna ocena 3.2), povezane sa snalaženjem u onlajn okruženju (ključne reči za pretragu, provera tačnosti informacija, itd). Veštine korišćenja mobilnih uređaja dobile su relativno visoku prosečnu ocenu (3.1) zahvaljujući poznavanju procedure za instalaciju novih aplikacija (95%), međutim samo nešto više od polovine ispitanih zna kako da prati troškove korišćenja mobilne aplikacije ili da preko nje obavi kupovinu. Operativne veštine su ocenjene nisko (2.8) jer samo trećina ispitanih zna, na primer, da postavi video na onlajn platformu ili da koristi neki programski jezik. Sa skidanjem i čuvanjem sadržaja na svom uređaju upoznato je tri četvrtine ispitanih, dok oko 77% smatra da zna kako da primeni opcije privatnosti na mrežama. Najlošiji

nadanja", Friedrich Ebert Stiftung & SeConS, Beograd, 2015. http://library.fes.de/pdf-files/bueros/belgrad/12065.pdf

11 Global kids online Serbia

12 Medijska pismenost u Srbiji, BIRODI, 2013, http://www.birodi.rs/medijska-pismenost-u-srbiji-rezultati-istrazivanja/

13 Istraživanje o nivou svesti o potencijalnim internet rizicima i zloupotrebama među roditeljima dece uzrasta 8 do 17 godina, UNICEF & Ipsos, 2016. https://drive.google.com/file/d/0B4WVugCwd1buWDlvQkJyaEwxWkU/view

ocenu deca i mladi dali su za svoje kreativne veštine (2.2) u pogledu stvaranja novih i prerade postojećih sadržaja na internetu.

7.4. ZAŠTITA DECE NA INTERNETU

Analiza medijskog tržišta u Srbiji iz 2015. ukazuje na trend među mlađom i publikom srednje dobi (15-29 i 30-39 godina starosti) koja sve manje vremena provodi pred televizorom, a sve više na internetu.[14] S obzirom na napuštanje tradicionalnih medija, regulisanje linearnog televizijskog programa u pogledu izlaganja dece i mladih štetnim sadržajima postaje periferno pitanje.

DECA I SLOBODA IZRAŽAVANJA - MEĐUNARODNA I DOMAĆA REGULATIVA

Ne umanjujući vrhunski značaj koji je potrebno dati sistemskoj zaštiti dece od objektivnih opasnosti na internetu, javne politike su dužne da zaštitu dece ne zasnivaju na ograničavanju njihovih prava na slobodu izražavanja[15], pristup znanju i učešće u društvu.[16]

Iako Univerzalna deklaracija o ljudskim pravima[17] i Međunarodni pakt o građanskim i političkim pravima[18] (član 19) garantuju pravo na slobodu izražavanja svakom ljudskom biću, član 13 Konvencije UN o pravima deteta posebno potvrđuje ovo pravo maloletnim osobama.[19] Primena ovog člana smatra se jasnim indikatorom mere u kojoj se deca tretiraju kao nosioci prava, posebno u pogledu omogućavanja deci da izraze i opišu načine na koje se njihova ukupna prava poštuju, odnosno krše.

Prepoznatljiva zloupotreba široke margine za interpretaciju ograničenja prava na slobodu izražavanja iz ključnih međunarodnih dokumenata, uobičajeno se temelji na interesima nacionalne bezbednosti. U slučaju dečijih prava, međutim, posebno otežavajuću okolnost predstavljaju patrijarhalni modeli u kojima, čak i u slučajevima kada je društvo posvećeno pravima i slobodama građana, tradicionalni društveni odnos prema detetu podrazumeva izuzimanje maloletnika iz učešća u javnom životu. Upravo je zaštita

14 Analiza medijskog tržišta u Srbiji, Ipsos Strategic Marketing, http://www.rra.org.rs/uploads/useruploads/PDF/6529-Analiza%20medijskog%20trzista%20u%20Srbiji%20-%20final.pdf

15 Član 13: Sloboda izražavanja (engl.), https://www.crin.org/en/home/rights/convention/articles/article-13-freedom-expression

16 S. Livingstone, Jedno od troje: Upravljanje internetom i dečija prava, LSE (engl.) http://blogs.lse.ac.uk/mediapolicyproject/2015/11/02/one-in-three-internet-governance-and-childrens-rights

17 Univerzalna deklaracija o ljudskim pravima, http://www.poverenik.rs/images/stories/Dokumentacija/54 _ ldok.pdf

18 Međunarodni pakt o građanskim i političkim pravima http://www.bgcentar.org.rs/bgcentar/wp-content/uploads/2013/02/Me%C4%91unarodni-pakt-o-gra%C4%91anskim-i-politi%C4%8Dkim-pravima.pdf

19 Zakon o ratifikaciji konvencije o pravima deteta, Sl. list SFRJ, br. 15/90 i Sl.i list SRJ, br. 4/96 2/97. http://www.paragraf.rs/propisi/zakon _ o _ ratifikaciji _ konvencije _ ujedinjenih _ nacija _ o _ pravima _ deteta.html

dece najčešći izgovor za ograničenje dečijih građanskih i političkih prava.

U okviru domaćeg pravnog okvira[20], dete ima pravo na obezbeđenje najboljih mogućih životnih uslova za svoj pravilan i potpun razvoj, pravo na obrazovanje u skladu sa svojim sposobnostima, željama i sklonostima, kao i pravo da blagovremeno dobije sva obaveštenja koja su mu potrebna za formiranje mišljenja.

Za ostvarivanje svakog od ovih prava detetu je neophodna sloboda informisanja i slobodan pristup informacijama. Rodite-lji mogu ograničiti ove slobode vršenjem roditeljskog prava u staranju o vaspitanju i obrazovanju deteta. Takođe se mogu ograničiti u skladu sa opštim Ustavnim pravilima za slobodu izražavanja, a koja se podudaraju sa uslovima koje nameće Konvencija UN o pravima deteta.

RIZICI

Poređenje različitih istraživanja otkriva priličan jaz između svedočenja dece i utisaka koji roditelji imaju o rizicima na internetu. Istraživači ukazuju na famu o internetu koja se u javnosti stvara senzacionalističkim izveštavanjem, što je verovatno pouzdaniji pokazatelj stvarne digitalne pismenosti u opštoj populaciji, uključujući i same medije.

Primera radi, rezultati istraživanja o potencijalnim internet rizicima pokazali su da je dostupnost neprikladnog materijala na internetu roditeljima izvor najvećeg stepena opšte zabrinutosti za decu - dvostruko više od ,,tradicionalnih'' briga o bezbednosti u saobraćaju i potencijalnog konzumiranja alkohola ili droge.[21] Kontakti sa nepoznatim ljudima na internetu zauzeli su drugo mesto na Unicefovom ,,brigometru'' (40.3%).

Istraživanja fokusirana na dečiju percepciju rizika ukazuju pre svega na onlajn agresiju, kao i uznemirujuće sadržaje ili situacije na internetu.[22] Takođe, zaraza uređaja virusom zauzima visoko mesto među onlajn rizicima, što se objašnjava materijalnim mogućnostima za nabavku boljih uređaja ili antivirusnih programa.[23]

7.4.1. ZAŠTITA OD ŠTETNIH SADRŽAJA - EVROPSKI OKVIR

Evropska Direktiva o audio-vizuelnim medijskim uslugama[24] sadrži posebna pravila za zaštitu maloletnika od neprimerenih sadržaja. Direktiva polazi od načela kontrole, odnosno da što korisnik medijskih usluga ima manju kontrolu nad sadržajem, to sadržaj može biti štetniji, te je stoga podložan primeni većih ograničenja. Pravila Direktive upotpunjena su preporukama iz 1998. i 2006. godine o zaštiti maloletnika i ljudskog dostojanstva.

Osnovni nedostatak Direktive se ogleda u njenoj ograničenoj primeni na sadržaje koji nisu u audio-vizuelnom formatu i koji se ne prikazuju putem tradicionalnih elektronskih medija, što danas predstavlja većinu sadržaja koji maloletnici prate putem platformi za razmenu. Reforma Direktive o audio-vizuelnim medijskim uslugama pokušava da se uhvati u koštac sa ovim problemom i da predvidi posebna pravila za zaštitu maloletnika od štetnog video sadržaja na internetu, uspostavljanjem sistema koregulacije platformi koje sadržaj čine dostupnim. Ishod ovakvog procesa je i dalje neizvestan iz više razloga, najpre usled činjenice da bi se takvim pravilima ugrozio institut ograničenja odgovornosti posrednika, na kome je zasnovana internet ekonomija, ali i usled okolnosti da je održavanje postojećih platformi postalo resursno izuzetno zahtevno.

Oglašavanje usmereno ka deci predmet je posebnih regulatornih mehanizama u okviru Evropske unije. Direktiva o nepoštenim komercijalnim praksama[25] utvrđuje zaštitu svih potrošača od nepoštenih praksi oglašavanja, posvećujući pažnju deci koja se smatraju ,,posebno osetljivom grupom'' potrošača. Plasiranje propagandnih poruka maloletnicima zahteva posebnu procenu rizika po njihov razvoj, kao i informisanje maloletnika da je u pitanju propagandni sadržaj, u skladu sa očekivanim nivoom medijske pismenosti dece.

7.4.2. ZAŠTITA OD ŠTETNIH SADRŽAJA - DOMAĆI OKVIR

Domaći sistem je zaštitu dece na internetu usmerio prvenstveno na zaštitu od nasilja, zlostavljanja i zanemarivanja. Na regulatornom nivou Vlada Republike Srbije donela je 30. juna 2016. godine Uredbu o bezbednosti i zaštiti dece pri korišćenju informaciono-komunikacionih tehnologija.[26] Uredba nalaže da Ministarstvo trgovine, turizma i telekomunikacija preduzima preventivne mere za bezbednost i zaštitu dece putem informisanja i edukacije i da uspostavi jedinstveno mesto za pružanje saveta i prijem prijava u vezi sa bezbednošću dece na internetu.

Mere koje su preduzimane u periodu pre donošenja Uredbe, usmerene su prvenstveno na podizanje svesti i obrazovanje u pogledu digitalnog nasilja kroz izradu istraživanja[27], priručnika[28] i posebnih kanala komunikacije za

20 Porodični zakon, Sl. glasnik RS, br. 18/2005, 72/2011 - dr. zakon i 6/2015, čl. 62, 63 i 65

21 Istraživanje o nivou svesti o potencijalnim internet rizicima i zloupotrebama među roditeljima dece uzrasta 8 do 17 godina, UNICEF & Ipsos, 2016. https://drive.google.com/file/d/0B4WVugCwd1buWDlvQkJyaEwxWkU/view, str 28

22 Global kids online Serbia

23 UNICEF/Ipsos, str. 40

24 Direktiva 2010/13/EU Evropskog parlamenta i Saveta od 10. marta 2010. o koordinaciji određenih odredaba utvrđenih zakonima i drugim propisima u državama članicama o pružanju audiovizuelnih medijskih usluga (Direktiva o audiovizuelnim medijskim uslugama) http://eur-lex.europa.eu/legal-content/HR/ALL/?uri=CELEX:32010L0013

25 Direktiva 2005/29/EZ Evropskog parlamenta i Saveta od 11. maja 2005. o nepoštenoj poslovnoj praksi poslovnog subjekta u odnosu prema potrošaču na unutrašnjem tržištu http://eur-lex.europa.eu/legal-content/HR/TXT/?uri=CELEX:32005L0029

26 Uredba o bezbednosti i zaštiti dece pri korišćenju informaciono-komunikacionih tehnologija, 30.06.2016 http://www.paragraf.rs/dnevne-vesti/040716/040716-vest17.html

27 Korišćenje digitalne tehnologije, rizici i zastupljenost digitalnog nasilja među učenicima u Srbiji, https://drive.google.com/file/d/0B4WVugCwd1buT0F2N3Y2U0lROFU/view?usp=sharing

28 Digitalno nasilje- prevencija i reagovanje, 2016, http://www.mpn.gov.rs/wp-content/uploads/2015/08/priru%C4%8Dnik-interaktivni.pdf

mlade koji dolaze u dodir sa digitalnim nasiljem.[29] Fond B92 je u saradnji sa institucijama razvio servis Net patrola[30], onlajn mehanizam putem kojeg se bezbedno i anonimno može prijaviti nezakonit i/ili štetan sadržaj na internetu, kao i portal Klikni bezbedno, na kome se javnost može informisati o rizicima i prednostima, kao i načinima odgovorne i bezbedne upotrebe informacionih i komunikacionih tehnologija, dok su za decu i mlade osmišljeni i dostupni onlajn edukativni alati, igre i kvizovi.[31] Takođe, veliki broj organizacija civilnog društva ponudio je baze znanja i resurse koji pomažu deci, roditeljima i vaspitačima da se suprotstave identifikovanim rizicima.

Nekoliko zakona u svojim odredbama tretira pitanje zaštite maloletnika od štetnih sadržaja, ali se oni odnose na tradicionalne, elektronske i štampane medije. Ovi okviri se primenjuju i kada mediji distribuiraju svoj sadržaj na internetu, međutim, treba imati u vidu da u onlajn okruženju ulogu medija i oglašivača obavlja i čitav niz drugih aktera koji ne spadaju ni u jednu od regulisanih kategorija, ne poseduju prisustvo u Republici Srbiji ali imaju i posebne osnove oslobođenja od odgovornosti. Upravo su to akteri koji maloletnicima pružaju najveći broj usluga na internetu.

7.4.3. ZAŠTITA PODATAKA DECE U EVROPSKOJ UNIJI

Jedna od najvažnijih novina Opšte uredbe o zaštiti ličnih podataka (GDPR), koja će u Evropskoj uniji početi da se primenjuje 2018, leži u odredbama koje se posebno bave zaštitom ličnih podataka dece. Izazov s kojim su se suočili pisci Opšte uredbe daleko je od beznačajnog, budući da uvodi pravila o zaštiti podataka generacija rođenih u digitalnoj eri. Za razliku od zakonodavaca, ova deca ne poznaju drugo socijalno okruženje osim onog koje se znatno oslanja na internet. Statistike procenjuju da je danas jedan od tri korisnika interneta u svetu mlađi od 18 godina, dok je jedan od pet internet korisnika u EU dete.

Sporovi oko pojedinih rešenja stoga nisu iznenađujući. Među njima je, svakako, član 8(1) kojim se postavlja čini se preterano visok prag za mogućnost davanja pristanka na obradu podataka (Članice EU imaju mogućnost da ovaj prag odrede u rasponu od 13-16 godina). Problem predstavlja i činjenica da GDPR ne uvodi obaveznu verifikaciju uzrasta, kao i veoma sužen krug osoba koje mogu dati pristanak u ime deteta.

Nova evropska regulativa nesporno je pionirski korak fokusiran na privatnost. Činjenica da se u Opštoj uredbi izričito prepoznaju dečija prava i potreba za njihovom posebnom zaštitom, već i u preambuli teksta, u osnovi predstavlja veoma značajan napredak.[32] Značajan pomak predstavlja i zahtev da, u situaciji kada se obrada odnosi na dete, svaka informacija i komunikacija treba da bude izražena tako jasnim i jednostavnim jezikom da ga dete može lako razumeti.

7.4.4. ZAŠTITA PODATAKA DECE U DOMAĆEM PRAVNOM OKVIRU

Jedina odredba važećeg Zakona o zaštiti podataka o ličnosti koji se tiče dece jeste član 10.[33] U stavu 6 ovog člana kao osobe koje mogu dati pristanak na obradu podataka o licu koje je umrlo, izričito se označavaju deca ,,sa navršenih 15 godina života'', što je granica primenjiva kod testamentalne i radne sposobnosti dece. U prethodnom, stavu 5, u kom se propisuje ko može dati pristanak za obradu podataka o ličnosti, deca se ne pominju izričito ali se iz formulacije ,,lice koje nije sposobno za davanje pristanka'' može pretpostaviti da zakonopisac izjednačava sposobnost davanja pristanka sa poslovnom sposobnošću, obuhvatajući ovom kategorijom i maloletnike.[34]

Očigledno je da legislativu Republike Srbije očekuje usaglašavanje propisa sa okvirom postavljenim novom Opštom uredbom Evropske unije o zaštiti ličnih podataka, već i na nivou određivanja starosne granice za pristanak na obradu podataka.

Pitanje razvoja onlajn okruženja i usmerenosti dece sve mlađeg uzrasta na digitalne tehnologije, odnosno stalnom izlaganju rizicima po privatnost i zaštitu ličnih podataka, neće biti moguće zaobići ni u lokalnim okvirima.

Teme značajne za budućeg zakonodavca u Srbiji biće i uspostavljanje sistema verifikacije starosne dobi, zatim pitanje vaspitača ili edukatora kao mogućih nosilaca prava na davanje pristanka na obradu, te zloupotrebe ovog prava u slučaju roditelja ili staratelja koji ne postupaju u najboljem interesu deteta. Tokom izrade novog zakona, stručna i zainteresovana javnost posebnu pažnju treba da obrate na odnos zaštite ličnih podataka dece sa univerzalnim pravima i slobodama deteta, kao što su pravo na izražavanje, pravo na pristup informacijama, pravo na učestvovanje u donošenju odluka, pravo na učenje i druga.

29 U okviru istog projekta pokrenuta je fejsbuk stranica ''Biraj reči hejt spreči'', gde svi zainteresovani mogu da nađu odgovore na dileme sa kojima se mladi susreću kada je digitalno nasilje u pitanju. https://www.facebook.com/BirajReciHejtSpreci/

30 Net patrola, http://www.netpatrola.rs/sr/naslovna.1.1.html

31 Klikni bezbedno, https://kliknibezbedno.wordpress.com/

32 GDPR: we all need to work at it!, https://www.betterinternetforkids.eu/web/portal/news/detail?articleId=694148

33 Zakono zaštiti podataka o ličnosti, ''Sl. glasnik RS'', br. 97/2008, 104/2009 - dr. zakon, 68/2012 - odluka US i 107/2012 http://www.paragraf.rs/propisi/zakon _ o _ zasti-ti _ podataka _ o _ licnosti.html

34 Poslovna sposobnost dece regulisana je članom 11 Porodičnog zakona, ''Sl. glasnik RS'', br. 18/2005, 72/2011 - dr. zakon i 6/2015) http://www.paragraf.rs/propisi/porodic-ni _ zakon.html

7.5. ISTRAŽIVANJA I PUBLIKACIJE SHARE FONDACIJE

PUBLIKACIJE

- Vodič XI: Vodič o autorskim pravima - slobodna upotreba autorskih dela
- Vodič X: Vodič za IKT sisteme od posebnog značaja - Informaciona bezbednost
- Vodič IX: Radnici na lizing
- Vodič VIII: Vodič za organe vlasti - Zaštita podataka o ličnosti
- Vodič VII: O digitalnim pravima i internet slobodama u političkoj ko-munikaciji
- Vodič VI: Zaštita tajnosti izvora informacija - pravni i tehnički aspekti
- Vodič V: Bezbednost organizacija u digitalnom okruženju
- Vodič IV: Kroz rizike i mehanizme zaštite nezavisnosti i bezbednosti onlajn medija - Hod po digitalnoj ivici
- Vodič III: Modeli za objavljivanje internet komentara
- Vodič II: Pravni položaj onlajn medija u Srbiji
- Vodič I: Osnove digitalne bezbednosti
- Vodič: Digitalni zaštitnici protiv Info-uljeza (prevod na srpski, izdavač EDRi)
- Share this book
- Izveštaj o obradi podataka o ličnosti - Poreska uprava
- Izveštaj o obradi podataka o ličnosti - Republički fond za zdravstveno osiguranje
- Izveštaj o obradi podataka o ličnosti - Gradski centar za socijalni rad Beograd
- Izveštaj o obradi podataka o ličnosti - Centralni registar obaveznog socijalnog osiguranja
- Izveštaj o obradi podataka o ličnosti - Agencija za privredne registre

MONITORING IZVEŠTAJI

- Monitoring predsedničke onlajn kampanje 2017 - trendovi i tenzije na internetu (14.3.2017)
- Poštovanje digitalnih prava i sloboda u 2016. godini (25.1.2017)
- Monitoring digitalnih prava: dvomesečni pregled za kraj 2016. godine (21.12.2016)
- Monitoring digitalnih prava u 2016: sukobi na društvenim mrežama (8.11.2016)
- #izbori2016: Kampanja na mrežama se isplati (26.04.2016)
- #izbori2016: Poslednji dan kampanje (21.4.2016.)
- #izbori2016: Zenit predizborne kampanje (12.4.2016)
- Tok predizborne kampanje na Internetu (5.4.2016)
- Izbori 2016 : Analiza socijalnih mreža i onlajn medija (26.3.2016)
- SHARE nadzire poštovanje Internet sloboda i digitalnih prava tokom izborne kampanje (24.3.2016)
- Monitoring stanja Internet sloboda u Srbiji za poslednji kvartal 2015. (7.4.2016)
- Monitoring izveštaj: porast verbalnog nasilja na Internetu u Srbiji (20.10.2015)
- Digitalna prava i slobode - prvi presek stanja u 2015. godini (1.6.2015)
- Internet slobode i digitalna prava u Srbiji - Monitoring izveštaj za period od 1. avgusta do 31. decembra 2014. (12.2.2015)
- Analiza Internet sloboda u Srbiji - Monitoring internet sloboda i digi-talnih prava u Srbiji za period jun i jul 2014. (8.8.2014)
- Internet sve pamti - Analiza Internet sloboda u toku vanredne situacije / Republika Srbija / maj 2014. godine (28.5.2014)

7.6. KONFERENCIJE, INICIJATIVE, SUSRETI

7.6.1. SERIJA RAZGOVORA O INFORMACIONOJ BEZBEDNOSTI

SHARE Fondacija je želela da iskoristi početak primene Zakona o informacionoj bezbednosti i da kroz seriju neformalnih susreta formira platformu za povezivanje i jačanje saradnje između ključnih aktera procesa implementacije Zakona - državnih organa kao donosilaca odluka, IT zajednice koja u praksi implementira rešenja iz Zakona o informacionoj bezbednosti, akademske zajednice koja je značajna zbog specifičnih znanja koje poseduje o informacionoj bezbednosti, organizacija civilnog društva i onlajn medija kao aktera na čije aktivnosti informaciona bezbednost ima značajan uticaj.

U ponedeljak, 28. novembra, 2016. godine, održan je prvi Cybersecurity meetup SHARE Fondacije. Tema događaja je bila Zakon o informacionoj bezbednosti i njegova implementacija. Na skupu se govorilo o važnosti ovog zakona, kao i podzakonskih akata, budući da informaciona bezbednost može biti ugrožena u svakom segmentu društva. Takođe je naglašeno da je potrebno raditi i na podizanju svesti o značaju informacione bezbednosti kako bi građani i sami mogli da štite svoje podatke.

Događaju je prisustvovalo više od 60 ljudi, a govorili su Sava Savić, pomoćnik ministra za informaciono društvo u Ministarstvu trgovine, turizma i telekomunikacija, Vladica Tintor, direktor Regulatorne agencije za elektronske komunikacije i poštanske usluge (RATEL), Adel Abusara, predstavnik misije OEBS-a u Srbiji, Slobodan Marković, savetnik za IKT politike i odnose sa internet zajednicom u RNIDS i Jovan Šikanja, administrator za bezbednost i zaštitu od prevara u kompaniji Limundo.

Prvi Cybersecurity Meetup

Drugi Cybersecurity meetup održan je 20. februara 2017. godine, u Startit centru, u Beogradu. Teme o kojima se govorilo na skupu bile su poboljšanje primene Zakona o informacionoj bezbednosti i pratećih podzakonskih akata, šta su problematične tačke i koje su uloge države, privrede i civilnog sektora. SHARE Fondacija je predstavila i Vodič za IKT sisteme od posebnog značaja, sa ciljem da razjasni nedoumice u vezi sa primenom zakona i predstavi dobre prakse informacione bezbednosti.

Susretu je prisustvovalo oko 60 ljudi, a govorili su Milan Vojvodić iz Ministarstva trgovine, turizma i telekomunikacija, glavni specijalista pravnik za mrežnu i informacionu bezbednost MUP CERT-a Aleksandar Maksimović, predstavnik kompanije Unikom telekom Viktor Varga, Milan Sekuloski iz Ženevskog centra za demokratsku kontrolu oružanih snaga i Danilo Krivokapić, koordinator SHARE Fondacije za privatnosti i zaštitu podataka o ličnosti. U okviru događaja održana je i radionica posvećena rizicima i problemima sa kojima se mediji susreću u pogledu informacione bezbednosti, kojoj su prisustvovali novinari, predstavnici civilnog sektora i medijskih udruženja.

Cybersecurity meetup seriju SHARE Fondacija organizuje u saradnji sa Ministarstvom trgovine, turizma i telekomunikacija, Udruženjem eSigurnost, Startitom i Društvom za informatiku Srbije. Sledeći susret planiran je za maj 2017. godine.

7.6.2. OEBS KONFERENCIJA „GAINING A DIGITAL EDGE: FREEDOM OF EXPRESSION“

Konferencija posvećena slobodi izražavanja u onlajn sferi, u organizaciji Kancelarije predstavnika OEBS-a za slobodu medija, Misije OEBS u Srbiji, SHARE Fondacije i Centra za medije, informacije i društvo pri Školi javnih politika Centralno-evropskog univerziteta u Budimpešti, održana je u Beču, od 15. do 16. novembra i okupila oko 120 novinara, medija, advokata, predstavnika vlade, IT stručnjaka, profesora, umetnika i branitelja ljudskih prava iz Jugoistočne i Centralne Evrope. Na konferenciji se govorilo o izazovima i preispitivanju novinarstva u digitalnom okruženju, kao i regulaciji onlajn sfere. Ovo je bila četvrta po redu konferencija o slobodi medija. Do sada su ove konferencije održane u Kotoru (2013), Budimpešti (2014) i Beogradu (2015).

Konferenciju je otvorila Dunja Mijatović, predstavnica OEBS-a za slobodu medija, koja je naglasila da bez interneta danas nema slobode izražavanja i slobode medija. Ukazujući na međunarodne standarde koji u određenim slučajevima mogu ograničiti ove slobode, Mijatović je istakla značaj dijaloga o konfliktu interesa nacionalne sigurnosti i javnog reda i interesa zaštite sloboda. Publici su se obratili i Peter Burkhard, šef Misije OEBS-a u Srbiji, kao i ambasadorka Holandije pri OEBS-u Desire Kopmels.

Izlaganje Džejkoba Mekhangame, osnivača i direktora danske think-tank organizacije ,,Justitia'', bilo je posvećeno sve većim ograničenjima koje se nameću slobodama i pravima na internetu, u vidu cenzure, kriminalizacije izražavanja i nadzora. Usledila je panel diskusija o novom razumevanju novinarstva (,,Re-thinking journalism''), u kojoj su učestvovali prof. dr Natali Helberger sa Pravnog fakulteta Univeziteta u Amsterdamu, Igor Božić, izvršni producent televizije N1, Endru Finkel, član Platforme za nezavisno novinarstvo P24 iz Turske i Fredrik Laurin, urednik odseka za istraživačko novinarstvo švedske televizije SVT.

Predstavnik Hermes Centra za transparentnost i ljudska prava u digitalnom okruženju, govorio je o partnerstvu digitalnog novinarstva i hakera u javnom interesu, nakon čega su učesnici konferencije mogli da biraju između dve panel diskusije koje su se održavale u isto vreme - o ženama u medijskoj sferi ili o rapidnom rastu imersivnog novinarstva. Na narednom predavanju predstavljeno je istraživanje o minimizaciji nepoverenja i političke polarizacije, neophodnoj u cilju postizanja i jačanja vizionarske političke debate, te ključnoj ulozi koju u tome igra konstruktivno novinarstvo.

Završni deo prvog dana konferencije sastojao se iz dva predavanja koja su se održavala u isto vreme - predavanje ,,The Page View is a Zombie'' Dejana Nikolića, osnivača Content Insights i predavanje ,,Inside the Facebook Algorithmic Factory'' Vladana Jolera, osnivača SHARE Fondacije - nakon čega je održana panel diskusija o algoritmima i novim oblicima cenzure, u kojoj su učestvovali Husein Derakšan, nezavisni istraživač iz Irana, Ben Vagner, direktor Centra za internet i ljudska prava Evropskog univerziteta Viadrina iz Nemačke, dr Radim Polčak, direktor Centra za prava i tehnologiju Masaryk Univerziteta iz Češke i Lenart Kučić, novinar iz Slovenije.

Drugog dana konferencije su predstavnici OEBS-a održali panel posvećen aktivnostima ove organizacije u zaštiti i promociji bezbednosti novinara, a zatim je održana diskusija o regulisanju sadržaja na internetu, u kojoj su učestvovali Danijel Ber, američki ambasador pri OEBS-u, Džo Meknami, izvršni direktor mreže EDRi, Marijus Dragomir, direktor Centra za medije, podatke i društvo - CEU u Mađarskoj i Đorđe Krivokapić, programski direktor SHARE Fondacije.

Drugi dan konferencije ,,Gaining the Digital Edge: Freedom of Expression''

Usledila su četiri bloka sa po dva istovremena predavanja na različite teme, od krize novinarstva kao problema javnih politika, značaja neutralnosti Mreže za slobodu govora, regionalnih prilika za onlajn novinarstvo, do razvoja novih medijskih biznis modela i uspostavljanja saradnje novinarstva i umetnosti. Završni panel posvećen stanju medija na Balkanu okupio je istraživače medija, naučnike i predstavnike medijskih organizacija.

7.6.3. KONFERENCIJA ,,EUROPEAN YOUTH CONFERENCE ON INTERNET AS A COMMONS AND THE NEW POLITICS OF COMMONING''

U organizaciji Hajnrih Bel Fondacije, SHARE Fondacije, Instituta za političku ekologiju iz Zagreba i Zelene evropske fondacije, od 19. do 21. maja 2016. u Beogradu, održana je omladinska konferencija o internetu kao javnom dobru. Tokom tri dana organizovano je više od 20 panela, otvorenih diskusija i drugih aktivnosti, uz prisustvo više od stotinu učesnika iz zemlje i inostranstva.

Konferenciju je otvorio Andreas Polterman, predsednik Hajnrih Bel Fondacije, a uvodno predavanje o načelu otvorenog pristupa održao je prof. dr Rajner Kulen sa Univerziteta u Konstancu, Odsek za kompjuterske i informatičke nauke u Nemačkoj. Usledila je regionalna premijera dokumentarnog filma ,,Democracy - Data Fever'', u kom autori prate lobiranje i nadmetanja oko novog zakona Evropske unije o prikupljanju i čuvanju podataka o ličnosti, kao i posledice koje složeni zakonski procesi imaju u evropskim i svetskim demokratijama.

O briselskim procedurama potom su razgovarale Julia Reda, poslanica Evropskog parlamenta iz Nemačke, Asta Helgadotir, poslanica Piratske partije u parlamentu Islanda, Nevena Ružić iz službe Poverenika za informacije od javnog značaja i zaštitu podataka o ličnosti Republike Srbije i Nataša Pirc Musar, advokatica i ranija Poverenica za informacije Slovenije. Moderator diskusije je bio Đorđe Krivokapić, direktor za pravne politike SHARE Fondacije.

Panel diskusija ,,How Brussels operates and what can we learn from it?''

U nastavku programa, učesnici su prema svom interesovanju mogli da izaberu jednu od tri panel diskusije, dok su završna predavanja Julije Rede i Vedrana Horvata, izvršnog direktora Instituta za političku ekologiju, bila posvećena reformi kopirajt regulative, odnosno značaju javnih dobara u društvenom i građanskom razvoju.

Drugog dana konferencije održane su tri istovremene panel diskusije, o ulozi javnih biblioteka, arhiva i muzeja u administriranju digitalnih javnih dobara, o pravnim pitanjima posrednika na interentu, kao i o javnim prostorima u doba virtuelne i proširene stvarnosti. Usledila su predavanja o

umetnosti i javnom dobru (Kristian Lukić sa Instituta za fleksibilne kulture i tehnologije iz Novog Sada), izazovima i ograničenjima internet aktivizma (Peter Sunde, jedan od osnivača torent pretraživača The Pirate Bay), ekonomiji podataka na internetu i rizicima po privatnost (Džema Galdon Clavel, direktorka organizacije Eticas Research & Consulting iz Barselone), kao i autsorsovanju u ekonomiji podataka (Fike Jansen, izvršna direktorka Tactical Tech organizacije iz Berlina). Dan je okončan blokom panel diskusija na različite teme od značaja za onlajn saradnju, zaštitu privatnosti i programiranje, dok su istraživanje SHARE Labs posvećeno algoritamskim fabrikama Fejsbuka predstavili Vladan Joler, osnivač SHARE fondacije, Kristian Lukić sa Instituta za fleksibilne kulture i tehnologije iz Novog Sada i Jan Krasni, saradnik SHARE Fondacije.

Treći dan konferencije počeo je predavanjem Žanete Hofman, direktorke Humbolt instituta za Internet i društvo u Berlinu, na temu poverenja u institucije i mehanizme upravljanja internetom, nakon čega je Đorđe Krivokapić, direktor za pravne politike SHARE Fondacije, održao predavanje o reputacionim sistemima. Na panel diskusiji o samoupravljanju zajednica na internetu učestvovali su Žaneta Hofmann i Peter Sunde, posle koje je usledio blok tri istovremena panela o algoritamskom odlučivanju, uzbunjivačima u digitalnoj eri, te seksualnim i rodnim pravima na internetu.

Posebno za ovu konferenciju razvijena je pervazivna igra kartama ,, Deck-Laration'', sa proglašenjem pobednika i uručenjem nagrada na završnom događaju.

7.6.4. MOKRIN: KONSULTATIVNI SASTANAK U OKVIRU PROJEKTA „MAPIRANJE INFRASTRUKTURE ZA OBRADU PODATAKA O LIČNOSTI U JAVNOM SEKTORU“

U okviru projekata ,,Mapiranje infrastrukture za obradu podataka o ličnosti u javnom sektoru'' koji je realizovan uz podršku USAID JRGA projekta, SHARE Fondacija je organizovala dvodnevni konsulatativni sastanak u Mokrinu, od 25. do 28. februara 2016. Sastanku su prisustvovali predstavnici Kancelarije Poverenika za informacije od javnog značaja i zaštitu podataka o ličnosti, Centralnog registra obaveznog socijalnog osiguranja, Fonda za penzijsko i invalidsko osiguranje, Gradskog centra za socijalni rad u Beogradu, Agencije za privredne registre, organizacije Partneri za demokratke promene, JRGA projekta i predstavnici SHARE Fondacije.

SHARE Fondacija je ovom prilikom predstavila publikaciju ,,Vodič za organe vlasti - zaštita podataka o ličnosti'' namenjenu pre svega organima vlasti, ali i predstavnicima privatnog sektora koji koriste podatke o ličnosti. Cilj okupljanja je bio da učesnici daju svoje komentare i primedbe na tekst vodiča kako bi se on još dodatno unapredio.

Vodič je nastao kao rezultat obimnog istraživanja o vrstama obrade i načinima zaštite podataka o ličnosti u javnom sektoru, a istraživanje je obuhvatilo šest državnih istitucija: Republički fond za zdravstveno osiguranje, Republički fond za penzijsko i invalidsko osiguranje, Centralni registar obaveznog socijalnog osiguranja, Poresku upravu, Agenciju za privredne registre i Gradski centar za socijalni rad iz Beograda. SHARE je kao deo projekta kreirao i posebnu internet stranicu - www.mojipodaci.rs - na kojoj se, pored elektronske verzije Vodiča, mogu naći i najčešća pitanja vezana za obradu podataka o ličnosti, kao i najčešći propusti državnih organa u ovoj oblasti i preporuke za njihovo otklanjanje.

7.7. DOKUMENTARNA TV SERIJA „U MREŽI“

DOKUMENTARNA TV SERIJA „U MREŽI“

SHARE Fondacija, Beograd 2017.

SCENARIO I REŽIJA: Dr Mirko Stojković

IZVRŠNI UREDNICI: Dr Đorđe Krivokapić, Dr Vladan Joler

DISTRIBUCIJA: TBA

Nakon višegodišnjih istraživanja, konferencija, brojnih publikacija i tribina, SHARE Fondacija je 2016. započela proizvodnju naučno-obrazovne TV serije, posvećene temama koje poslednjih godina okupiraju pažnju svetske javnosti. Priče o strukturi interneta, virtuelnoj realnosti, novim medijima, privatnosti i elektronskom nadzoru, slobodi izražavanja na internetu i drugim pitanjima, prilagođene su prosečno informisanim građanima koji tek ulaze u svet digitalnih tehnologija. Istovremeno, serijal se obraća i publici iz privatnog sektora i javne uprave, kojoj je novo okruženje postalo radna svakodnevica, sa svim rizicima i novim mogućnostima koje donosi internet.

Vladan Joler, Ana Martinoli i Đorđe Krivokapić, voditelji i urednici TV serije ,,U mreži''

Teme su razrađene u deset emisija, uz istorijat tehnološkog razvoja, popularne kulture, globalnih i nacionalnih tokova, koji zajedno čine okvir za razumevanje svakog od odabranih fenomena digitalnog doba. Aktuelni problemi predstavljeni su kroz razgovor sa domaćim i stranim stručnjacima, aktivistima i autorima, među kojima su Julia Reda, poslanica nemačke Piratske partije u Evropskom parlamentu, Džo Meknami, izvršni direktor Evropske mreže za digitalna prava (EDRi), Dunja Mijatović, ranija predstavnica OEBS za slobodu medija, Din Starkmen, novinar i publicista, dobitnik Pulicerove nagrade, Peter Sunde, jedan od osnivača sajta ,,The Pirate Bay'', i na desetine drugih.

Program namenjen emitovanju na televiziji sa nacionalnom frekvencijom, dopunjen je multimedijalnim sadržajima koji su objedinjeni u jedinstvenu, slobodno dostupnu, interaktivnu bazu znanja. Na portalu će se nalaziti publikacije, istraživanja, vizuelni i video materijali, te obrazovni alati SHARE Fondacije, koji gledaocima TV serije pružaju dodatna pojašnjenja, podatke i detaljne analize. Ova baza znanja, jedinstvena u regionu, namenjena je i stručnjacima, kreatorima javnih politika i donosiocima odluka.

Kerolajn Benok, Gardijan

Džo Meknami, Evropska mreža za digitalna prava (EDRi)

Asta Helgadotir, Piratska partija Islanda

SINOPSIS TV SERIJE

1. I 2. EPIZODA – ,,KOMUNIKACIJA''

Iako je svaka generacija ljudske civilizacije uverena u svoju posebnost, pod utiskom da se mnoge stvari iznenada i po prvi put u istoriji dešavaju baš njoj, to obično nije slučaj. Ponekad trendovi traju i hiljadama godina, da bi se materijalizovali u pojedinim fazama tehničkog napretka. Vreme u kom se stiču preduslovi potrebni da bi se preduzeo taj odlučujući korak napred, najčešće ostaje u senci. Prve dve epizode serije posvećene su istinski uzbudljivom, istorijskom kontekstu razvoja komunikacije, te najvažnijim trenucima moderne istorije interneta osamdesetih i devedesetih godina 20. veka.

3. EPIZODA – ,,SLOBODA GOVORA''

Načelo slobode govora, kao jednog od temeljnih ljudskih prava, istorijski se proteže sve do prvih političkih struktura na tlu Evrope, poput Rimskog carstva. U početku veoma sporo, a od Gutenbergovog pronalaska štamparske prese sve brže, razvoj komunikacionih tehnologija neposredno oblikuje već i samo razumevanje slobode govora, utiče na društvenu dinamiku, uslovljava granice javnog i privatnog – koje se u eri interneta prepliću na neočekivan način.

4. EPIZODA – ,,PAKET''

Šta se zapravo dešava tokom jednog delića sekunde, koliko protekne od klika kojim hoćemo da reagujemo na nečiji status na Fejsbuku - do trenutka kada se na ekranu pojavi očekivani emotikon? Paket o kom razgovaramo u četvrtoj epizodi sadrži sve informacije koje su potrebne za jedan običan lajk na fejsu. Njegovo putovanje, od rutera do servera i hostova, odvija se nezamislivom brzinom a trasa paketa, odabranog za našu priču, proteže se od Novog Sada, preko Beograda, Frankfurta, Kornvola i Nju Džerzija, sve do Forest Sitija u Sjedinjenim Američkim Državama, gde se nalaze serveri kompanije Fejsbuk. Ovo putovanje ujedno je i priča o složenoj arhitekturi globalne Mreže.

5. EPIZODA – ,,PRIVATNOST''

Na talasu informatičke revolucije nastale su čitave nove industrije, za koje informacije predstavljaju ,,novu naftu'', kako to stručnjaci obično kažu. To znači da danas svaki, pa i najbanalniji privatni ili javni podatak ima određenu vrednost, dok je vlasništvo nad uslugama koje pružaju kompanije Gugl ili Fejsbuk, nalik nekadašnjem vlasništvu nad naftnim poljima. Kako je nastala ekonomija podataka, o kojim je vrednostima reč, kojim se trikovima služe korporacije kako bi se domogle informacija, kako zakon gleda na sve to - i kakve sve to posledice ima po našu privatnost, pitanja su o kojima razgovaramo u petoj epizodi.

6. EPIZODA – ,,OTPOR NADZORU''

Rizici po privatnost građana sve su veći i složeniji, ali se rađaju i nove strategije za odbranu od invazije: od savremenih ludista, koji u potpunosti odbacuju upotrebu novih tehnologija, do aktivista koji stvaraju nove digitalne alate za odbranu, zagovaraju zakonske promene i učestvuju u slobodnoj razmeni znanja u svojoj zajednici. Načelo privatnosti trpi drastične promene pod uticajem novih tehnologija, koje omogućavaju masovno prikupljanje ličnih podataka i gotovo neograničen prostor za njihovo skladištenje. Obaveza je društva da ponovo promisli granice privatnog i javnog, jer građanske slobode osvojene u ,,analognoj'' prošlosti ne prestaju u digitalnom okruženju. Digitalna pismenost za sve postaje novi ideal prosvetitelja internet generacije.

7. EPIZODA – ,,MEDIJI''

Uz komercijalno dostupne tehnologije, internet je omogućio svakom pojedincu da bude vlastiti medij i aktivni učesnik u medijskom okruženju, s podjednakim šansama za uticaj na javno mnjenje kao i urednički oblikovano novinarstvo koje dosledno poštuje zakonske i etičke norme. Poplava infomacija s jedne strane predstavlja rizik po tačnu, važnu i blagovremenu vest, dok demokratizacija pristupa podriva odgovornost za javno izgovorenu reč. Interesi tradicionalne medijske industrije ozbiljno su ugroženi narušavanjem monopola, ne samo u proizvodnji i distribuciji sadržaja, već i u selekciji učesnika u javnom diksursu. S druge strane, izazovi s kojima se suočavaju građani zadiru u temelje prava i sloboda, kao što su slobodan pristup znanju, pluralizam i kvalitet dostupnih informacija. Danas se više ne

može biti ni pasivan korisnik medija bez znanja o tehnološkim inovacijama i mehanizmima pristupa sadržajima i uslugama na internetu.

8. EPIZODA – „BEZBEDNOST“

Svakodnevno slušamo o brojnim prednostima, ali i opasnostima koje vrebaju u sajber svetu. Internet je znatno olakšao mnoga krivična dela koja srećemo i u „analognom“ prostoru – prevare, pljačke, krađu identiteta, i slično. Međutim, nove tehnologije donele su i neke specifične načine povreda prava, koje ranije nismo poznavali. Na udaru su naš identitet, reputacija, bankovni račun, ali i čitavi komunalni sistemi koji su u međuvremenu digitalizovani. U ovoj epizodi razgovaramo o rizicima na internetu i zaštiti naše bezbednosti. Sagovornici će nam objasniti zašto je važno imati kvalitetne lozinke, šta znači dvostepena verifikacija i kako se održava „digitalna higijena“. Takođe, razgovaramo i o onim slučajevima koji prevazilaze mogućnost obične zaštite, kada je u pomoć potrebno pozvati službe nadležne za istragu i suzbijanje visokotehnološkog kriminala.

9. EPIZODA – „LIKOVI I LIČNOSTI“

Ne postoje dve iste osobe na planeti, čak se i blizanci među sobom razlikuju. Naš identitet je jedinstvena mešavina nasleđa, genetskog i kulturološkog, svakodnevnih slučajnosti koje su nam odredile pravac i tok razvoja, odluka koje smo doneli slobodno ili pod pritiskom sredine, kao i odluka koje su drugi doneli umesto nas. Internet nam je omogućio neposrednu komunikaciju sa ljudima širom planete, ostavljajući nam pritom prostor da sami podesimo parametre svog učešća. Ponekad nam to može izgledati kao šansa da napravimo novu, bolju verziju nas. U onlajn igricama možemo izabrati avatar koji čak nije ni istog pola kao naša „stvarna“ ličnost, na društvenim mrežama možemo izgraditi potpuno novi lik, zaštićeni osećajem prividne anonimnosti. U devetoj epizodi razgovaramo o psihološkim i društvenim aspektima susreta dva identiteta, slučajevima u kojima je „lik“ pobedio vlastitu ličnost, kao i prednostima i rizicima koje donose fluidni identiteti digitalnog doba.

10. EPIZODA – „INTERNET STVARI I VEŠTAČKA INTELIGENCIJA“

Mada se generacijama rođenim pre digitalne revolucije čini da već živimo u budućnosti opisanoj u starim naučno-fantastičnim romanima, tek nam sledi zaista korenita promena. Razvoj veštačke inteligencije, „Interneta stvari“, virtuelne realnosti i sličnih ideja, još uvek je u ranoj fazi prelaska iz puke teorije u široku upotrebu, ali su znanja i potrebne tehnologije već uveliko tu. U završnoj epizodi razgovaramo o tehnološkom razvoju koji je doneo pametne telefone i pametne frižidere, stvarajući sve širu mrežu povezanih kućnih uređaja i komunalnih usluga, na kojoj nastaju pametni gradovi. Novi svet nezaustavljivo niče pred našim očima i, mada smo podjednako fascinirani raznim pronalascima – vreme je da porazgovaramo i o opasnostima koje se ukazuju na horizontu.

8. KONSULTACIJE I TRENINZI SHARE FONDACIJE

SHARE Fondacija pruža različite konsultacije i treninge iz oblasti digitalne bezbednosti i medijskog prava na internetu:

OSNOVE DIGITALNE BEZBEDNOSTI

Fokus ovog treninga je na različitim aspektima digitalne bezbednosti na osnovnom nivou. Upoznavanje sa rizicima koji nisu tehničke prirode ali ugrožavaju onlajn bezbednost, razvoj svesti o posledicama koje stare navike mogu imati u digitalnom okruženju, podjednako je važno kao i tehničko-tehnološki aspekt digitalne bezbedsnosti

ORGANIZACIONI ASPEKTI DIGITALNE BEZBEDNOSTI

Postoji čitav niz mera, protokola i politika koje organizacija može primeniti kako bi unapredila svoju digitalnu bezbednost. U tom smeru se analiziraju vrste hardvera i softvera u svakodnevnom radu organizacije, rizici i preventivne mere. Takođe, pažnja se posvećuje osnaživanju administratora i korisnika sistema u organizaciji za kontinuiranu edukaciju i samostalno korišćenje resursa koji će im ponuditi znanja o digitalnoj bezbednosti.

UPRAVLJANJE UZBUNJIVAČKIM PLATFORMAMA

Trening se odnosi na tehničke aspekte uspostavljanja i administriranja uzbunjivačke platforme. U posebanom fokusu treninga su znanja i veštine potrebne za odgovarajuću zaštitu privatnosti platforme i potencijalnih uzbunjivača, kao i za jednostavne modele upravljanja platformom.

PRAKTIČAN TRENING

Trening je osmišljen kao vežba praktične primene znanja o tehnologijama i alatima obuhvaćenim edukativnim treninzima SHARE Fondacije. Cilj treninga je da polaznici sami, uz pomoć trenera, instaliraju i testiraju softver koji unapređuje digitalnu bezbednost.

PRAVNI RIZICI U ONLAJN MEDIJIMA

Trening se sastoji od upoznavanja učesnika sa aktuelnim medijskim pravom koji reguliše rad onlajn medija, od objavljivanja i širenja informacija na internetu do zaštite privatnosti. Kroz tumačenje propisa i praktične primere, polaznici treninga se upoznaju sa zakonskom regulativom koja se tiče onlajn medija i digitalnih aktivista, njihovim pravima i obavezama.

ATLAS INTERNET PRIVATNOSTI - INTERNET MAPA SRBIJE

Predavanje je posebno osmišljeno da sa tehničkog aspekta predstavi strukturu interneta i prakse prikupljanja podataka, na način koji je razumljiv prosečnom korisniku, kao i da ukaže na neke posebno slabe tačke elektronskih komunikacija i njihov uticaj na društvene tokove. Polaznicima se internet predstavlja u svetlu njegovih fizičkih karakteristika, složene globalne mreže rutera, servera, data centaraa, kablova, satelita, kao i protokola koji omogućavaju svim ovim uređajima da međusobno komuniciraju, a podacima da se kreću. Mada se internet najčešće opaža kao prostor izvan fizičke realnosti, njegov materijalni aspekt donosi značajan uvid u geografske i pravne granice koje podaci prelaze putujući internetom, kao i slaba mesta u mreži u kojima su podaci, građanska prava i slobode, izloženi rizicima.