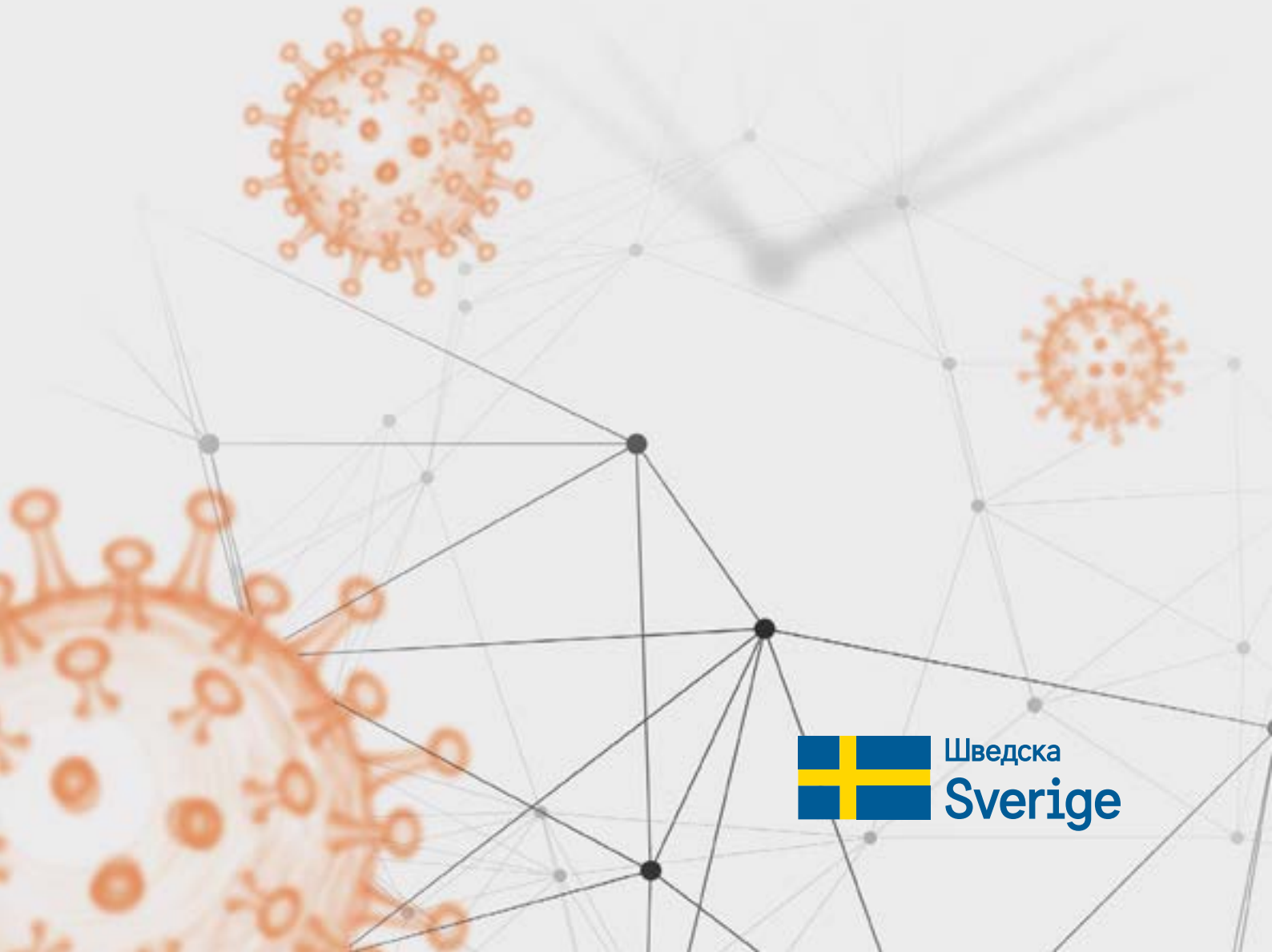
CIVIL RIGHTS DEFENDERS

LJUDSKA PRAVA U PANDEMIJI



Шведска
Sverige

IMPRESSUM

Izdavač
Civil Rights Defenders

Za izdavača
Goran Miletic

Autori
SHARE Foundation

Bojan Perkov
Kristina Ćendić
Filip Milošević
Andrej Petrovski
Milica Jovanović

Urednica
Neda Mirković

Dizajn
Marko Kovačevski

LJUDSKA PRAVA U PANDEMIJI

LJUDSKA PRAVA U PANDEMIJI

Pojačavajući već postojeće pritiske na ljudska prava i branitelje ljudskih prava širom sveta, pandemija COVID-19 donela je velike izazove zajednicama koje već trpe nejednakosti i nepravde u svojim državama, jer su mnoge od njih pribegle ekstremnim merama kako bi zauzdale izbijanje epidemije. „Slušajte svoje zajednice, osnažite ih i informišite“, upozorio je generalni direktor SZO u avgustu, skrećući pažnju na reakcije država i „štetu koju je socijalno, ekonomski i politički izazvao COVID-19“.[1]

Kako je rekao izvršni direktor Civil Rights Defenders Anders L. Peterson u maju: „Neke mere su možda neophodne, ali neke druge očigledno nisu – kada se jednom ovo sve okonča, svakako se sve mere moraju ukinuti. Osim toga, korišćenje pandemije da bi se uznemiravali branitelji ljudskih prava ili zloupotrebljavala vladavine prava u političke svrhe, čemu već sada svedočimo, jednostavno nije prihvatljivo“. On je naglasio i ulogu organizacija za ljudska prava u procesu praćenja i zahtevanja odgovornosti od predstavnika vlasti za prelazak preko linije između onoga što je stvarno nužno u jednom demokratskom društvu i zloupotrebe moći.[2]

Region Zapadnog Balkana deli slično iskustvo. U mnogim balkanskim zemljama predstavnici vlasti su svoje reakcije na pandemiju skovali na osnovu vojnih termina, te su pitanja javnog zdravlja postala pitanja diskursa državne bezbednosti gde se svaka različitost mišljenja i postavljanje pitanja posmatraju kao pobunjeništvo.

Dok je u nekim zemljama tradicionalni medijski prostor za izražavanje neslaganja već dosta ograničen, uz nametnutu potpunu ili delimičnu zabranu kretanja i policijski čas, većina društvenih i političkih aktivnosti premeštena je u onlajn sferu. Usledio je i pritisak na branitelje ljudskih prava.

Sprovođenje zvaničnih mera u borbi protiv pandemije često je podrazumevalo pojačani nadzor ili korišćenje tehnologije za praćenje kretanja. Takve okolnosti su ozbiljno uticale na privatnost rada koji su branitelji ljudskih prava obavljali u svakom domenu. Novinari, advokati i aktivisti koji se bave ljudskim pravima su se suočavali i sa teškoćama u izmeštanju svojih aktivnosti u zajednici, poput radionica, protesta i konferencija u onlajn sferu, a istovremeno su morali i da održe bezbednost svojih komunikacija.

Pored uvida u primere kršenja digitalnih prava i opisa vidljivih trendova u ograničavanju rada branitelja ljudskih prava u nekoliko zemalja u jugoistočnoj Evropi, u ovoj publikaciji nudimo i mogućnost za promišljanje internet servisa i alata koje koristimo u svakodnevnom radu. Postoje etički i bezbedni digitalni alati koji mogu zameniti velike komplekse za prikupljanje podataka poput Fejbsuka, Gugla i Amazona i ostalih svetskih IT giganata, a mogu nam pomoći i da izbegnemo cenzuru vlasti, nadzor bezbednosnih službi i tehničke napade sajber kriminalaca i zlonamernih hakera.

---

1 Uvodno obraćanje generalnog direktora SZO na medijskom brifingu povodom pandemije COVID-19 od 3. avgusta 2020. godine, Svetska zdravstvena organizacija, 3. avgust 2020.
2 COVID-19 nije izgovor vlastima da zloupotrebljavaju ljudska prava, Anders L. Peterson, Globe Post, 2. maj 2020.

REGIONALNI PREGLED

SHARE Fondacija još od 2014. godine prati kršenja digitalnih prava u Srbiji, a obim svog rada je prošle godine proširila kroz partnerstvo sa Balkanskom istraživačkom izveštačkom mrežom (BIRN) i prati ovu vrstu incidenata i u Bosni i Hercegovini, Hrvatskoj, Severnoj Makedoniji i Rumuniji.[3] Prvi zajednički rad je slučajno koincidirao sa globalnom pandemijom, razotkrivši zabrinjavajuće događaje i trendove u regionu.

Proces monitoringa zasniva se na praćenju različitih tipova kršenja na osnovu unapred definisane metodologije,[4] a svi slučajevi se razvrstavaju po određenim kategorijama. U ovoj metodologiji, postoji sedam različitih kategorija kršenja digitalnih prava i sloboda:

A. Narušavanje informacione bezbednosti: slučajevi u kojima je predmet povrede bezbednost informacionih sistema, npr. kroz upade u sistem, DDoS napadi (distribuirano odbijanje usluge) kako bi se onemogućio pristup nekom sadržaju, krađu i uništavanje podataka i tome slično.

B. Povrede informacione privatnosti i zaštite podataka o ličnosti: povrede kao što su curenje podataka, nedozvoljena obrada podataka ili nezakonit nadzor komunikacija.

C. Pritisci zbog izražavanja i aktivnosti na internetu: povrede digitalnih prava koje se odnose na čast i ugled, ugrožavanje sigurnosti, poruke diskriminacije i mržnje, pitanja slobode izražavanja u radnom okruženju, kao i pritiske na pojedince zbog objavljivanja informacija onlajn.

D. Manipulacija i propaganda u digitalnom okruženju: povrede koje obuhvataju različite oblike ciljanog širenja i manipulisanja sadržajem na internetu radi ostvarivanja određenih ciljeva, koji su često i ekonomske prirode.

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

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

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

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

U ovom izveštaju dati su podaci za četiri zemlje - Albaniju, Bosnu i Hercegovinu, Kosovo i Srbiju – na osnovu podataka koji su prikupljeni u periodu od 31. januara do 30. novembra 2020. godine.[5]

3 Baza podataka SHARE Fondacije i BIRN-a o monitoringu digitalnih prava: https://monitoring.bird.tools/
4 Možete saznati više o metodologiji monitoringa digitalnih prava SHARE Fondacije i BIRN-a na sledećem linku: https://monitoring.bird.tools/methodology
5 Napomena: podatke za Kosovo obezbedila je Balkanska istraživačka izveštačka mreža (BIRN), dok su podaci za Albaniju zasnovani na podacima koje smo dobili od zaposlenih iz CRD u Albaniji i na osnovu publikacije „Pravo na informisanje tokom prirodnih katastrofa u Albaniji 2020“, autora Doriana Matlije uz podršku zaposlenih iz centra Res Publica.

KATEGORIJA POVREDE	Srbija	Bosna i Hercegovina	Albanija	Kosovo
A. Narušavanje informacione bezbednost	4	1	1	0
B. Povrede informacione privatnosti i zaštite podataka o ličnosti	8	5	2	4
C. Pritisci zbog izražavanja i aktivnosti na internetu	30	9	2	3
D. Manipulacije i propaganda u digitalnom okruženju	15	6	2	4
E. Pozivanje posrednika na odgovornost	0	1	0	0
F. Blokiranje i filtriranje sadržaja	0	0	1	0
G. Ostalo	0	0	0	0
UKUPNO	**57**	**22**	**8**	**11**

Tokom perioda praćenja podataka, zabeleženo je 98 slučajeva kršenja digitalnih prava u Srbiji, Bosni i Hercegovini, Albaniji i Kosovu, koji su se kretali od hapšenja novinara i građana zbog informacija koje su delili na internetu i zaplenjivanja njihovih uređaja, pa sve do curenja podataka. Pored zabeleženih incidenata, zabeležen je i rastući broj slučajeva u kojima se na nepropisan način rukovalo osetljivim podacima o zdravstvenom stanju građana i namerno nezakonito objavljivanje takvih podataka u javnosti.

Najčešća vrsta kršenja u posmatranom periodu – oko polovine zabeleženih slučajeva – odnosila se na vršenje pritiska zbog izražavanja i aktivnosti na internetu, poput uvreda, pretnji, objavljivanja neistina sa namerom ugrožavanja reputacije i ostalo.

Na osnovu rezimea politika na Zapadnom Balkanu,[6] u nekim zemljama pandemija je razotkrila dugoročne probleme i poslužila „ubrzanju već postojećih trendova, kao što je kriza demokratije i nacionalizam“. U ostalim zemljama usledile su i izborne kampanje koje su izazvale „nevericu i bes usmerene na vlast i državu, prema kojoj postoji duboko ukorenjeno nepoverenje“. U svim državama u okviru ovog pregleda ugrožena je sloboda izražavanja.

Tokom kućne izolacije i zabrane kretanja, politički pritisci na medijski sektor u ovim državama doveli su do ozbiljnijih posledica poput centralizovanja informacija, širenja lažnih vesti i krivičnog gonjenja onih koji ne misle isto, bilo da su profesionalni novinari ili građani novinari. Istovremeno su javna glasila bliska vlastima bez uzdržavanja širila lažne vesti. U nekim slučajevima, vlasti su tako čvrsto zgrabile informacije da su pokušavale da uvedu zakone kojima bi se sve druge informacije osim zvaničnih proglasile nezakonitim. Na taj način sprovodili su svoja ovlašćenja i još više ometali demokratske procese u ovim državama, ograničavajući ljudska prava pod izgovorom borbe protiv pandemije.

6 Rezime politika: Zapadni Balkan u doba globalne pandemije, Savetodavna grupa za javnu politiku Balkan u Evropi (BiEPAG), april 2020. godine

REAKCIJE DRŽAVA NA COVID-19

U martu 2020. godine, predstavnici vlasti u nekim državama za koje se navode podaci u ovom izveštaju pribegli su proglašenju vanrednog stanja. U Srbiji je vanredno stanje uvedeno 15. marta i trajalo je do 6. maja, u Bosni i Hercegovini od 17. marta do 29. maja u Federaciji Bosne i Hercegovine, i od 28. marta do 21. maja u Republici Srpskoj; u Albaniji od 25. marta do 23. juna. Na Kosovu, vanredno stanje za javno zdravlje, pod nadzorom Ministarstva zdravlja, stupilo je na snagu 16. marta. U ove četiri države građani su se suočavali sa sličnim zabranama i izazovima tokom pandemije, i bez obzira na to što su se svi u javnosti gasno pobunili protiv zabrana, aktivizam za ljudskih prava morao je više nego ikada ranije da se osloni na internet.

Vanredno stanje u Albaniji trajalo je duže nego u ostalim državama iz ovog izveštaja. Vlasti su insistirale na nužnosti zaštite javnog zdravlja, ali je poštovanje prava građana postalo upitno, naročito u vezi sa vršenjem prava na slobodu izražavanja na internetu. Vlada je tokom krize još jače stegla svoj obruč nad informacijama naročito u pogledu širenja virusa, što je dovelo po pojačane zabrinutosti. Javni diskurs je bio prepun reči koje su ličile na ratne fraze, podgrevajući strah među građanima brojnim oklopnim vozilima na ulicama.[7] Kao i u drugim zemljama, građani Albanije su bili zbunjeni zbog uvedenih mera. Postojao je Tehnički odbor stručnjaka koji je osnovan da bi odlučivao o merama borbe protiv pandemije, „ali je rad ovog odbora bio obeležen ograničenim informacijama u javnosti o kompetentnosti odbora i razmerama na osnovu kojih su preporuke odbora preinačene u političke odluke. Do početka maja, nije bilo otkriveno ni ime predsedavajućeg ovog odbora“. U jednom trenutku, albanska policija za borbu protiv terorizma je tvrdila da desetoro ljudi koristi svoj Fejsbuk za širenje lažnih vesti i zatražila da budu osuđeni za krivično delo.[8]

Policija je navodno pratila Fejsbuk objave i komentare i pronašla neke tvrdnje izrečene u tom maniru. Ispostavilo se da je monopolizacija informacija jedan od najvećih problema sa kojima se Albanija suočila tokom krize. Osim njegovog dominantnog prisustva u javnom medijskom servisu, premijer je bio prisutan i na društvenim mrežama. U stvari, objavljeno je da je „tokom prvih meseca dana zabrane kretanja, premijer objavio 407 postova na Fejsbuku (13 dnevno) i 47 sati video materijala, što je predstavljalo prvo albansko iskustvo vladavine preko društvenih medija“.[9] Bilo je veoma problematično što je „većina odluka bila prvo objavljena na premijerovom Fejsbuku, a tek kasnije u Službenom glasniku, a 'konferencije za novinare' u stvari nisu bile otvorene za novinare“. Na taj način je javnosti onemogućen pristup tačnim informacijama, a „nacionalni mediji su imali ograničene mogućnosti da javnosti pruže dodatne informacije i da na taj način ponude drugačije informacije od onih koje je nudila vlast“[10]

Bosna i Hercegovina nije imala doslednu zvaničnu strategiju za borbu protiv pandemije, usled svojih administrativnih podela. Svaki entitet, i Federacija Bosne i Hercegovine i Republika Srpska, Brčko distrikt i deset kantona Federacije Bosne i Hercegovine uveli su različite mere kako bi zauzdali pandemiju. Takva situacija je naročito bila zbunjujuća za građana Sarajeva, jer linija podele između entiteta seče grad, pa su restrikcije i mere varirale u zavisnosti od ulice.[11] Javnost u Bosni i Hercegovini, uključujući i branitelje ljudskih prava, suočila se tokom krize sa problemom dezinformacija o lekovima koji su proizvedeni lokalno, nedostatkom testova, avionima koji raspršuju virus iznad gradova, itd. Trpela je i zaštita podataka o ličnosti: vlasti su razotkrile imena ljudi koji su prekršili naređenje o samoizolaciji a čak su razmišljali i o tome da javno objave imena zaraženih ljudi. Organi vlasti u Konjicu i Kantonu 10 objavili su lične podatke ljudi u samoizolaciji ali su ih povukli nakon što je Agencija za zaštitu ličnih podataka BiH objavila da je to kršenje.[12] Najveći udarac ljudskim pravima u Bosni i Hercegovini zadao je entitet Republike Srpske usvojivši Odluku kojom se zabranjuje izazivanje panike i nereda kroz objavljivanje navodno lažnih vesti.[13] Kako su lokalni branitelji ljudskih prava i međunarodni akteri kritikovali ovu Odluku kao štetnu, od nje se ubrzo odustalo, ali je već nekoliko građana bilo novčano kažnjeno ili uhapšeno.

7 G. Madhi, Albanija: javno informisanje postalo žrtva COVID-19, OBC Transeuropa, 11. jun 2020.
8 G. Emiri, Uznemirenost albanskih aktivista za ljudska prava u ratu sa „sejačima straha“, BIRN, 29. jul 2020.
9 G. Madhi, Albanija: javno informisanje postalo žrtva COVID-19, OBC Transeuropa, 11. jun 2020.
10 Ibid.
11 G. Sandić-Hadžihasanović, Entiteti i pandemija: Na jednoj strani ulice jedna pravila, na drugoj druga, Radio Slobodna Evropa/Radio Liberty, 14. maj 2020.
12 Bosna i Hercegovina i Crna Gora da poštuju pravo na privatnost građana u samoizolaciji, CRD, 25. mart 2020.
13 M. Milojević, Sprečavanje širenja panike ili 'disciplinovanje' doktora i novinara, Radio Slobodna Evropa/Radio Liberty, 12. april 2020.

Pored izazova koje je donela pandemija, Kosovo je prolazilo i kroz političku krizu, jer je vladi izglasano nepoverenje, što je doprinelo sveopštoj nebezbednosti i nepoverenju građana. Kao i u većini zemalja, vlasti su insistirale na tome da ljudi nose maske, da održavaju fizičku distancu uz uvedene mere ograničenja kretanja. U vezi sa tim, BIRN Kosovo i lokalna firma za razvoj softvera KUTIA, napravili su platformu „Tvojih 90 minuta“ („90 Minutëshi yt”) putem koje su građani mogli da provere kada im je dozvoljeno da napuste svoje domove, tako što bi ukucali pretposlednje brojeve svog matičnog broja ili brojeve pasoša.[14] Međutim, tokom krize građani su bili zabrinutiji zbog efekta zastrašivanja koji su izazvala hapšenja onih koji su govorili o stvarima od javnog interesa. Urednica iz Mitrovice je uhapšena, čime je stavljen veliki pritisak na slobodu izražavanja.[15] Efekat zastrašivanja se na Kosovu dodatno pojačao kada je kosovska policija odlučila da krivično goni osobu koja je navodno podelila tekstualnu poruku kojom je pozvala građane da se testiraju na korona virus na Kliničko-bolničkom univerzitetskom centru Kosova (KBUC), tvrdeći da su ljudi određene krvne grupe skloniji tome da se zaraze od ove bolesti.[16] Pored toga, informativni portal Sinjali objavio je imena, adrese i datume rođenja 210 građana koji su bili u karantinu u Severnoj Mitrovici i ostalim gradovima, što je ocenjeno kao narušavanje privatnosti.[17] Nakon snažne reakcije Udruženja srpskih novinara na Kosovu i Misije OEBS-a na Kosovu, podaci o ličnosti su zatamnjeni.

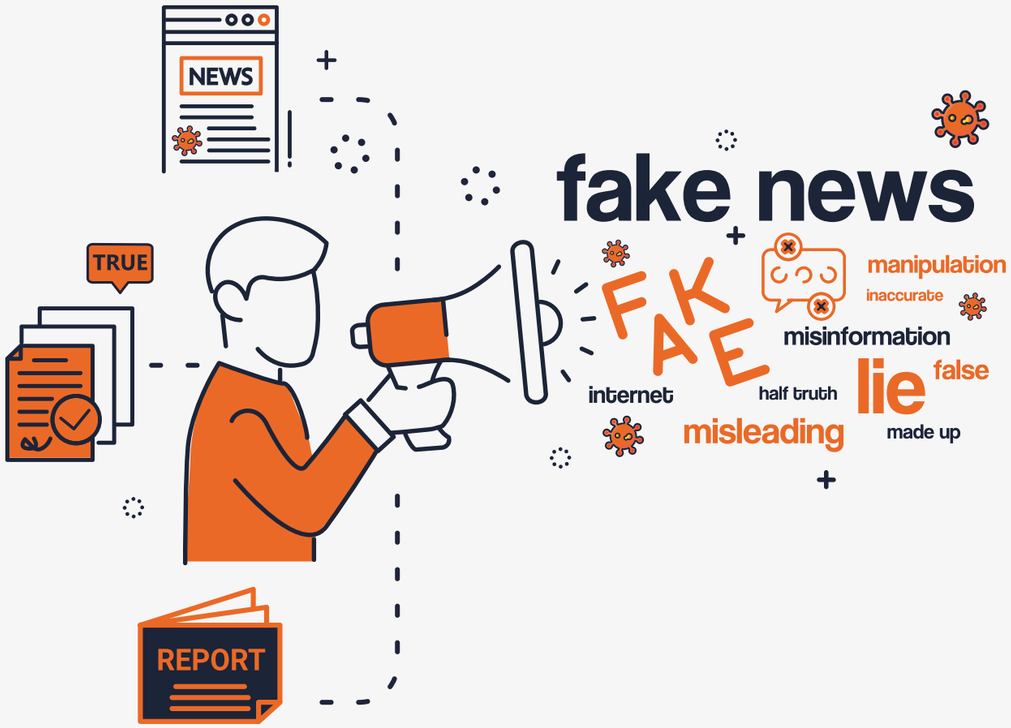
U Srbiji je izbijanje zarazne bolesti Covid-19 i uvođenje vanrednog stanja dovelo do problematičnih mera koje su predstavnici vlasti preduzeli kako bi se borili protiv pandemije. To je bilo vidljivo u pokušajima da se kontroliše tok informacija, uz favorizovanje provladinih medija, neprijateljstvo prema nezavisnim izdavačima medija i braniteljima ljudskih prava i kršenja zaštite podataka o ličnosti. Zbog situacije nastale usled pandemije, veliki broj aktera je više nego ikada ranije sve svoje aktivnosti prebacio na internet, zbog čega su postali još ranjiviji na digitalne pretnje i napade. Jedan od najozbiljnijih incidenata povezan je sa curenjem podataka kada su na internetu osvanuli korisničko ime i lozinka za COVID-19 informacioni sistem.[18] Oni su korišćeni za pristup sistemu za obradu osetljivih podataka građana u vezi sa pandemijom, a postali su i osam dana ostali javno dostupni na sajtu jedne zdravstvene ustanove. Bez obzira na to što su korisničko ime i lozinka uklonjeni nakon što su predstavnici civilnog društva upozorili predstavnike vlasti, Guglu je bilo dovoljno osam dana da indeksira informacije i da ih učini dostupnim prilikom pretrage. Osim toga, srpske vlasti su pokušale da centralizuju informacije o pandemiji tako što su doneli odluku kojom se pouzdanim informacijama smatraju samo one koje daju predstavnici vlasti, čime su sve ostale pretvorili u izvore navodno lažnih vesti. Novinari, aktivisti civilnog društva pa čak i građani koji su govorili o problemima kao što su nedostatak medicinske opreme, nestašice benzina, i drugom, bili su optuženi za širenje panike a neki od njih su čak i uhapšeni.

14 S. Todorović, BIRN platforma za pomoć građanima Kosova u praćenju restrikcija zbog pandemije COVID-19, BIRD, 16. april 2020.
15 Predstavnik OEBS-a za slobodu medija izražava zabrinutost zbog pritiska na internet portal KoSSev na Kosovu i njegovu urednicu, Organizacija za evropsku bezbednost i saradnju, 12. april 2020.
16 Pozivanje na testiranje na korona virus lažnim porukama, Kosovo online, 31. mart 2020.
17 COVID-19: političko mešanje u rad medija na Kosovu, Evropska federacija novinara, 4. april 2020.
18 Pandemija jedne lozinke. Kako je šifra za Covid-19 završila na internetu?, SHARE Fondacija, 24. april 2020.

Uticaj mera za borbu protiv virusa COVID-19

SLOBODA IZRAŽAVANJA

Pandemija je imala veliki uticaj na slobodu izražavanja širom sveta. Kada je javno zdravlje ugroženo i kada države uvedu vanredno stanje, građanima mogu biti nametnute određene restrikcije, ali ne smeju biti prekomerne. Na osnovu člana 19, mnoge države su izgleda iskoristile pandemiju da još jače utvrde svoje represivne mere i da ograniče slobodu izražavanja i informisanja.[19] Države Zapadnog Balkana uvele su ograničenja koja su ugrozila slobodu izražavanja i u velikoj meri uticala na rad aktivista i novinara.



Digitalne tehnologije promenile su način na koji mi ostvarujemo svoje pravo na slobodu izražavanja i isto tako omogućile različitim akterima da preuzmu ulogu novinara. Iz tog razloga sve više koristimo termine kao što su medijski akteri i građani novinari, jer svi oni učestvuju u raspravama o pitanjima od javnog značaja. Više nego ikada ranije, pandemija je izmestila ove rasprave u internet okruženje, ali se pored ovog preokreta, pojačao i pritisak na internetu na one koji ostvaruju svoju slobodu izražavanja ili izveštavaju o pitanjima od javnog značaja. Profesionalni novinari i ostali tradicionalni medijski akteri nisu jedine mete. Na osnovu Akcionog plana Ujedinjenih nacija za bezbednost novinara i pitanje nekažnjivosti i Opšteg komentara br. 34 Komiteta za ljudska prava UN-a, „definicija medijskih aktera je proširena kao rezultat novih oblika medija u digitalnom dobu. Stoga ona obuhvata i druge koji doprinose javnoj raspravi i koji obavljaju novinarsku delatnost ili ulogu javnog čuvara."[20] Međutim, na Zapadnom Balkanu svedoci smo pretnji i uvreda upućenih onima koji daju drugačije informacije od onih koje nam daju zvaničnici ili izražavaju svoje mišljenje o pandemiji, a u nekim slučajevima bili smo svedoci i hapšenja i izricanja novčanih kaznih.

19 Korona virus: uticaj na slobodu izražavanja, član 19.
20 Preporuka CM/Rec(2016)4 Komitet ministara Saveta Evrope državama članicama o zaštiti novinarstva i bezbednosti novinara i ostalih medijskih aktera, Savet Evrope, 13. april 2016.

Među prvim koracima koje su neke zemlje preduzele nakon što su proglasile vanredno stanje jeste bio pokušaj da se kontroliše protok informacija. Javnost ima pravo da ostvaruje ne samo pravo na slobodu izražavanja već i da dobije informacije. Međutim, Vlada Srbije je 28. marta zabranila da bilo koja osoba izvan Kriznog štaba daje informacije o pandemiji, jer se svaka informacija data javnosti iz drugih izvora ne može smatrati tačnom i proverenom. Tačnije rečeno, ako bi neko podelio takvu informaciju, ta osoba bi bila odgovorna i snosila bi zakonske posledice za širenje dezinformacija tokom vanrednog stanja.[21] Svedočili smo sličnim pojavama i u Bosni i Hercegovini, kada je u entitetu Republike Srpske doneta Odluka o zabrani izazivanja panike i nereda i putem društvenih mreža i medija.[22] Takva odluka nanela je štetu ostvarivanju prava na slobodu izražavanja, te su lokalni branitelji ljudskih prava i međunarodni akteri uticali na to na da se odluka što pre ukine. Od ove odluke se ubrzo odustalo, ali je već nekoliko građana bilo novčano kažnjeno ili uhapšeno. Za kršenje ove odluke predviđene su novčane kazne u iznosu od 500 do 1.500 evra za fizička lica i od 1.500 do 4.500 evra za pravna lica.

Jedan od najozbiljnijih slučajeva koji je izazvao efekat zastrašivanja bilo je hapšenje Ane Lalić, novinarke uhapšene zbog teksta o stanju u bolnici u Novom Sadu. Ana je uhapšena 1. aprila, samo nekoliko sati nakon što je objavljen njen članak „Klinički Centar Vojvodine pred pucanjem: bez zaštite za medicinske sestre". U ovom članku je govorila o pitanjima od javnog interesa – nedostatku zaštitne opreme kao što su maske i rukavice u Kliničkom Centru Vojvodine. Bolnica je podnela prijavu protiv nje navodeći da je njen članak narušio njihov ugled i uznemirio javnost zbog neproverene informacije. Nakon hapšenja, Ani su zaplenjeni laptop i telefoni i odvedena je u pritvor. Njeno hapšenje izazvalo je veoma burnu reakciju i domaćih i međunarodnih aktera koji su zahtevali da se ona pusti što pre. Ana Lalić je puštena odmah nakon saslušanja sledećeg dana, a sve optužbe protiv nje odbačene su krajem aprila. Ovaj incident ne samo da je izazvao mogući efekat zastrašivanja među građanima i onima koji su govorili o određenim pitanjima od javnog interesa, već se nakon toga povela kampanja mržnje protiv Ane Lalić, koju su uglavnom vodili provladini mediji. Organizacija Civil Rights Defenders je tada apelovala na Vladu Srbije da novinarima obezbedi prostor da dobiju informacije i informišu građane o dešavanjima u vezi sa pandemijom COVID-19. „Verujemo da ne postoji opravdanje za ukidanje prava novinara da postave pitanje na otvorenom i javnom forumu, uzimajući u obzir sve mogućnosti za tu vrstu interakcije koje nudi moderna tehnologija bez fizičkog prisustva", navodi se.[23]

Uopšteno gledano, novinari i aktivisti su često tokom pandemije bili mete uvreda na internetu. Uvrede su dolazile od drugih medija, javnih zvaničnika, nekada i anonimnih aktera, čime se ostvarivanje prava na slobodu izražavanja u Srbiji spustilo na nizak nivo, mada je od sve četiri države koje su analizirane u ovom izveštaju, Srbija već bila na najnižem mestu prema rangiranju Reportera bez granica (93. mestu) i procenjena je kao nebezbedna za novinare.[24] U drugom incidentu, albanska novinarka Sonila Meco je doživela maltretiranje na internetu nakon što je na Fejsbuku kritikovala komentare jednog doktora u vezi sa albanskim državljanima koji su zaustavljeni na granici sa susednom Grčkom i nije im dozvoljeno da uđu u zemlju.[25] Sredinom marta, građani Albanije su preko operatora Vodafone dobili neočekivanu glasovnu poruku u kojoj ih Premijer Edi Rama savetuje kako da u borbi protiv korona virusa peru ruke i „da se zaštite od medija".[26]

Nisu samo aktivisti, novinari i građani u Srbiji i Albaniji trpeli kada je reč o njihovom pravu na izražavanje u onlajn sferi. U Bosni i Hercegovini, bilo je slučajeva u kojima su građani novčano kažnjeni u skladu sa osporenom Odlukom, najviše zbog svojih objava na društvenim mrežama.[27] Na primer, lekar je novčano kažnjen kada je rekao da bolnica nema dovoljno opreme, a osoba iz Gradiške je novčano kažnjena jer se navodno „ponašala tako da izaziva nered i paniku tokom vanredne situacije" i uvredila je javna tela entiteta u Republici Srpskoj, itd.

21 T. Ćurčić, J. Tomić, D. Đorđević, Vlada pokušava da ograniči izveštavanje o koroni, Centar za istraživačko novinarstvo Srbije, 1. april 2020. godine
22 M. Milojević, Sprečavanje širenja panike ili 'disciplinovanje' doktora i novinara, Radio Slobodna Evropa/Radio Liberty, 12. april 2020. godine
23 Srpske vlasti moraju poštovati medijske slobode i pravo građana na informisanost, Civil Rights Defenders, 11. april 2020. godine
24 Reporteri bez granica, Srbija
25 Albanija: novinarka Sonila Meco nakon Fejsbuk objave dobila lavinu pretnji, Mapiranje medijskih sloboda, 7. april 2020. godine
26 G. Erebara, Rama svoj rat protiv medija vodi preko albanskih telefona, Balkan Insight, 13. mart 2020
27 Digitalna prava za vreme pandemije COVID-19, BIRD

NADZOR

Kako se konstatuje u najnovijem izveštaju organizacije Fridom haus (Freedom House), među zabrinjavajućim trendovima u vezi sa merama preduzetim tokom krize zbog pandemije COVID-19 je i opsežno prikupljanje veoma osetljivih podataka o ličnosti i uvođenje intruzivnih tehnologija za monitoring građana kao što su prediktivna policijska analitika, prepoznavanje lica i skeniranje termalnim kamerama.[28] Još gore je što su ove mere najčešće uvedene bez adekvatnih zaštitnih mehanizama kojima se sprečava zloupotreba ljudskih prava.

Zbog pandemije COVID-19 države Zapadnog Balkana su pribegle povećanim merama nadzora, jer je stvorena atmosfera da se širenje bolesti može sprečiti i držati pod kontrolom samo ako se uvede strog nadzor nad ponašanjem građana. Ograničenjima i zabranama kretanja, koja su ponekada trajala i po nekoliko dana, trebalo je isto tako iskontrolisati velika okupljanja i mase.

Na primer, građani Albanije su preko portala E-Albanija morali da zatraže dozvolu da bi mogli da izađu iz kuće da kupe namirnice ili prošetaju svoje ljubimce.[29] Dnevno je samo jedan član domaćinstva mogao da dobije dozvolu i bilo mu je dozvoljeno dva sata kretanja. Policija je u Tirani, glavnom gradu Albanije, koristila i dronove kako bi pratila poštovanje mera tokom zabrane kretanja.[30]

28 A. Šabaz, A. Fank, Lažni lek: Zloupotreba nadzora u ime javnog zdravlja, Freedom House, 2020
29 M. Brendl, T. Branković, A. Dirmiši, Demokratija i vanredno stanje, Friedrich Ebert Stiftung, 18. maj 2020.
30 Albanska policija koristi dronove kako bi sprovela zabranu kretanja, Glas Amerike, 16. april 2020.

U Srbiji je vanredno stanje na nivou države proglašeno sredinom marta i trajalo je do početka maja. Predsednik Srbije je na konferenciji za novinare koja je održana neposredno posle uvođenja vanrednog stanja upozorio građane da se „prate italijanski brojevi telefona“, misleći na praćenje lokacije mobilnih telefona, jer su se mnogo građani Srbije vraćali u državu iz inostranstva i dobili su naređenja da ostanu u obaveznoj samoizolaciji.[31] Pomenuo je da postoji i „drugi način“ da se prati kretanje onih koji ostave svoje telefone kako bi pokušali da „prevare svoju vladu“, ali nije objasnio koji je to način.

Mere povećanog nadzora, najviše praćenje kretanja građana, onemogućile su rad novinara, aktivista i branitelja ljudskih prava, naročito u javnom prostoru, koji sve više postaje prostor distopijske kontrole.[32] Niko sa sigurnošću ne može reći da se kada pandemija prestane napredni tehnološki alati koji su uvedeni da bi se zauzdao korona virus neće iskoristiti u druge svrhe – između ostalog da bi se ugušilo drugačije mišljenje i kritika vlasti?[33]

U Beogradu, glavnom gradu Srbije, postavlja se ogromni sistem za video nadzor, koji čini hiljade kamera koje imaju mogućnost prepoznavanja lica što je ozbiljno upozorenje za društveni aktivizam i rad na javnom interesu, jer se samo tkivo društva menja ako se ulice čitavog grada pokriju sistemom za pametni video nadzor.[34]

Uz nesrazmerno i nasumično ograničavanje prava i sloboda, sistem pametnog video nadzora u Beogradu postavljen je u suprotnosti sa nacionalnim i međunarodnim zakonskim standardima i propisima. Nije jasno definisana svrha toga, niti je ustanovljen jasan i strog zakonski okvir za korišćenje sistema pametnog nadzora od strane policije na javnim mestima pre nego što je sistem postavljen. Zajednički projekat srpskih državnih vlasti i kineske kompanije Huawei „Pametni grad“ razvija se na netransparentan način, bez objavljivanja informacija o uslovima ovog partnerstva i troškovima čitavog sistema. Nije bilo javne rasprave o mogućem društvenom i političkom uticaju ovih veoma intruzivnih tehnologija.[35]U Republici Srpskoj, jednom od entiteta u Bosni i Hercegovini, takođe je prijavljeno postavljanje intruzivnog video nadzora. Na osnovu izveštavanja medija, Ministarstvo unutrašnjih poslova Republike Srpske kupilo je više od 300 kamera, od kojih ukupno 66 kamera ima mogućnosti prepoznavanja lica.[36]

31 Reagovanja vlasti na COVID-19 negativno utiču na digitalna prava na Balkanu, International Freedom of Expression Exchange, 4. april 2020.
32 Zabraniti masovni biometrijski nadzor!, European Digital Rights, 13. maj 2020.
33 Dan posle pandemije: idemo li ka distopiji nadzora, SHARE Fondacija, 2. april 2020.
34 Sajt hiljade kamera: https://hiljade.kamera.rs/en/home/
35 Protivzakonito je i štetno za društvo da se uvede sistem pametnog nadzora u Beogradu, Hiljade kamera
36 MUP RS postavio kamere za prepoznavanje lica: gde nas sve snimaju?, Istok, 28. jul 2020.

RAD NA DALJINU

Kako su se društva više nego ikada ranije prebacile u onlajn sferu, branitelji digitalnih prava iskusili su različite prepreke u svom radu. U nekoliko prilika, novinari su imali ozbiljne probleme u obavljanju svoje uloge javnog čuvara, jer se ova uloga ne može u potpunosti ostvariti na internetu – neophodno je i izveštavanje sa terena. Stoga su novinarska udruženja insistirala na tome da se novinari izuzmu iz policijskog časa. U Srbiji je Nezavisno društvo novinara Vojvodine zahtevalo od vlasti da jasno definišu uslove pod kojima se novinari mogu kretati tokom perioda zabrane kretanja na samom početku vanrednog stanja.[37] Na kraju je profesionalnim novinarima dozvoljeno da, ako su zatražili dozvole, mogu da izveštavaju sa terena. Međutim, ovaj uslov nije važio za građane novinare, blogere i ostale koji nisu imali novinarske akreditacije, te se rad na daljinu za njih ispostavio veoma ograničavajućim.

U Albaniji je od početka godine bilo nekoliko protesta, kao što je razbijeni komemorativni skup za Dan Evrope koji je organizovalo civilno društvo 9. maja, i protesti protiv rušenja Narodnog pozorišta, veliki antirežimski protest koji je nasilno razbijen, kada je 37 ljudi uhapšeno uključujući i jednog novinara. Međutim, najveću zabrinutost izazvao je protest sredinom decembra zbog smrti mladića kog je ubio policajac, zbog čega je došlo do nasilja na ulicama i više od 300 građana je krivično gonjeno a troje novinara je nasilno uhapšeno.[38] Ovi slučajevi nasilja jasno guše pravo na slobodno udruživanje u Albaniji i imaju efekat zastrašivanja tokom ove krize.

Osim toga, jedna urednica sa Kosova je uhapšena zato što je kršila policijski čas iako je u stvari radila svoj posao.[39] Tatjana Lazarević, glavna urednica informativnog portala KoSSev bila je na poslu kada je uhapšena i iako je ubrzo puštena, takva vrsta incidenta dovodi do stvaranja efekta zastrašivanja ne samo za druge novinare, nego i za bilo koga čiji rad podrazumeva posmatranje situacije na terenu. Na kraju je Ministarstvo unutrašnjih poslova Kosova pojasnilo da se policijski čas ne odnosi na novinare i medijske radnike, ali ostaje nejasno da li su i branitelji ljudskih prava isto tako bili izuzeti iz policijskog časa.

U Bosni i Hercegovini, morala je da reaguje Institucija ombudsmena za ljudska prava BiH zbog ometanja rada branitelja ljudskih prava tokom krize.[40] Naime, u Federaciji Bosne i Hercegovine konferencije za novinare Kriznog štaba su se održavale ili za samo ograničeni broj novinara ili bez fizičkog prisustva novinara, ili su se davali odgovori samo na ona pitanja koja su prethodno bila poslata mejlom. Stoga je Institucija ombudsmena za ljudska prava BiH izdala zvanično obaveštenje pozivajući vlasti da u najvećoj mogućoj meri obezbede prisustvo novinara na konferencijama za novinare.

Slična situacija desila se i u Srbiji.[41] U jednom trenutku, predstavnicima medija je bilo dozvoljeno isključivo da unapred šalju pitanja na redovne konferencije za novinare u 15 časova koje su držali članovi Kriznog štaba. Ovo nije bila otvorena zabrana novinarima da dolaze na konferencije za novinare, iako su samo Javni medijski servis RTS i novinska agencija Tanjug tamo imali svoje kamere, a pitanja pojedinih novinara su u potpunosti bila preskočena. To je novinare sprečilo da ispune svoju ulogu javnih čuvara, a delovalo je da su ne samo pandemija, nego i vlasti nametnule tako njihov rad na daljinu.[42]

37 NDNV: omogućiti rad novinarima i za vreme policijskog časa, Danas, 18. mart 2020.
38 Albanske vlasti moraju da spreče policijsko nasilje i omoguće poštovanje prava na slobodu mirnog okupljanje, Savet Evrope, 15. decembar 2020.
39 Digitalna prava u doba pandemije COVID-19, BIRD
40 M. Brendl, T. Branković, A. Dirmiši, Demokratija i vanredno stanje, Friedrich Ebert Stiftung, 18. maj 2020.
41 Bez novinara na redovnim konferencijama u 15 časova, kaže Vlada Srbije, N1, 10. april 2020.
42 Mere protiv dezinformacija u vezi sa pandemijom COVID-19 ne smeju da podrivaju slobodu medija, Savet Evrope, 3. april 2020.

PITANJE KAPACITETA

Kao i u drugim oblastima, tokom pandemije su se branitelji ljudskih prava, aktivisti i ostali čuvari javnog interesa našli u situaciji koju nikada ranije nisu iskusili, naročito oni koji rade u manjim zajednicama. Uzimajući u obzir njihove kapacitete, kratkoročno i dugoročno gledano, „nova normalnost“ deluje kao težak izazov za civilni sektor u pogledu održivosti. Izgradnja kapaciteta jedne organizacije i inspirisanje ljudi da se bave društvenim aktivizmom isto tako postaju teže u doba krize, naročito usled ekonomskog pritiska.

Finansijski, tehnički i organizacioni kapaciteti civilnog društva dosta zavise od bespovratnih sredstava i projekata. Na Zapadnom Balkanu još uvek treba da se razvije kultura „kraudfandinga“, jer u regionu sigurno nema organizacija civilnog društva računati na to da veći deo njihovih prihoda dolazi od mikro donacija i članarina. Međutim, usled negativnog uticaja pandemije na svetsku ekonomiju, može se očekivati da iznosi donacija od predstavnika drugih država, kao što su ambasade i državne razvojne agencije budu smanjeni. U takvim okolnostima, biće teško omogućiti rast građanskog sektora i aktivizma kroz ograničena novčana sredstva i resurse.

Na primer, CIVICUS je međunarodna mreža organizacija civilnog društva, koja je u martu 2020. godine objavila otvoreno pismo donatorima i pokroviteljima zamolivši ih za što je moguće veću fleksibilnost, izvesnost i stabilnost kada su u pitanju njihovi partneri i dobitnici bespovratnih sredstava u doba krize usled pandemije COVID-19.[43] U pismu se navodi nekoliko načina kako se to može uraditi:

- Saslušati partnere dobitnike bespovratnih sredstava i zajedno istražiti kako im se na najbolji način može pomoći da se suoče sa ovom krizom, verujući da oni najbolje znaju šta im je potrebno iz svog konteksta;

- Podstaknuti redizajniranje i pomeranje planiranih aktivnosti i rezultata i obezbediti jasna uputstva kako da zahtevaju odobrenje za ove promene;

- Podržati nove i kreativne načine za kreiranje kulture solidarnosti i interakcije uz poštovanje fizičke distance i ostalih preventivnih mera;

- Ponuditi veću fleksibilnosti u isplaćivanju sredstava na osnovnu stvarnih potreba, pretvaranjem postojećih projektnih sredstava u sredstva koja nisu striktno vezana za određenu svrhu ili dodavanjem dodatnih sredstava kako bi se povećale rezerve ili pokrili neočekivani troškovi;

- Pojednostaviti procedure i vremenske okvire za izveštavanje i slanje prijava kako bi grupe civilnog društva bolje mogle da usmere svoje vreme, energiju i resurse na pružanje podrške najugroženijima umesto da pokušavaju da ispune velike zahteve u pogledu izveštavanja i dubinske analize.

Jedan od najvećih izvora zabrinutosti organizacija za ljudska prava i građanskog sektora jeste upravo tehnička infrastruktura, kao što su njihovi sajtovi, serveri, imejlovi, radni uređaji i ostalo. Naime, prema iskustvu SHARE Fondacije koja je pružala besplatnu tehničku pomoć i obuku pokazalo se da mnoge organizacije imaju oskudne resurse kada je reč o IT aspektu njihovog rada, što znači da često nemaju svoje IT zaposlene i da se oslanjaju na spoljne saradnike da upravljaju njihovom infrastrukturom. U okolnostima pandemije, zbog koje je došlo do radikalnog preokreta u funkcionisanju društva i organizacija, neki sajber napadi velikih razmera mogli bi imati nesagledive posledice za branitelje ljudskih prava usled nedostatka adekvatnih tehničkih i ljudskih kapaciteta da se ublaži napad i sanira šteta izazvana njime. Može doći do gubitaka dragocenih podataka koji su prikupljeni tokom godina rada ili recimo do gubljenja pristupa nalozima na društvenim mrežama ili imejl nalozima u organizaciji. Rad od kuće isto tako predstavlja rizik za digitalnu bezbednost, jer sigurnosne mere koje zaposleni preduzimaju na svojim domovima i privatnim uređajima možda nisu na istom nivou kao standardi organizacije.

43 Otvoreno pismo: Donatori moraju da deluju kako bi se osigurala otpornost civilnog društva tokom pandemije COVID-19, CIVICUS, 19. mart 2020. godine

DIGITALNI SAVETI

Suočivši se sa globalnom pandemijom, aktivisti i organizacije širom sveta prinuđeni su da većinu svoje komunikacija i saradnje presele u digitalni prostor. Iako je poslednjih 20 godina obeleženo ubrzanom digitalizacijom mnogih procesa u svakodnevnom životu, izgleda kao da je sve to do sada predstavljalo pripremu za iznenadnu tranziciju koja se desila za samo nekoliko nedelja na početku obaveznog karantina koji je uveden u svim delovima sveta.

Takva iznenadna promena dovela je do onoga što se isprva činilo logičnim, ali kasnije se ispostavilo da su to ishitrene odluke kada je reč o izboru tehnologija, usluga i softvera koji je trebalo da nadoknade pojavu tih nova ograničenja i fizičku udaljenost. Razumno je prihvatiti rešenja koja su popularna i laka za korišćenje, ali postavlja se pitanje u kojoj meri ona ispunjavaju uslove koji su neophodni za bezbedan rad aktivista i organizacija civilnog društva. Osim toga, ono što mi sada biramo će u velikoj meri uticati na tehnologije koje će dugoročno gledano prihvatiti organizacije i društvo u celini, tako da je ovo drugo pitanje više etičko: da li želimo da usvojimo vlasničke (komercijalne) servise čiji cilj je sticanje profita, ili hoćemo rešenja otvorenog koda koja se kreiraju u zajednicama, jer vidimo kako to utiče na diversifikaciju i decentralizaciju digitalnih ekosistema.

Odabir i razumevanja tehnologija koje koriste aktivisti u svom radu imaju ključni uticaj na njihov integritet i bezbednost, na otpornost njihovih organizacija i održivost društva koje gradimo.

Usled prirode njihovog posla, aktivisti za ljudska prava su češće izloženi provalama u sisteme informacione bezbednosti, oni se više nadziru i presreće im se komunikacija, izloženi su pokušajima cenzure usled tehničkih napada, neovlašćenom pristupu i ugrožavanju podataka o ličnosti, pretnjama, pritiscima i ostalim metodama čiji je cilj gušenje slobode govora i onemogućavanje njihovog rada. Otpornost na sve ove pretnje u digitalnom prostoru zavisi od tehnologija koje koristimo.

Nažalost, većinu alata na koje se danas oslanjamo stvorile su kompanije čiji poslovni modeli su zasnovani na ekstrakciji i monetizaciji podataka o ličnosti i navika korisnika ovih alata. Sada svi već dobro znamo da smo deo jedne „privrede nadzora“, ali nastavljamo da koristimo ove alate jer ih svi ostali koriste i vrlo je lako osloniti se na njih.

Međutim, sa tehničke tačke gledišta, glavni nedostatak većine komercijalnih i popularnih servisa i aplikacija jeste to da imaju zatvoreni kod. Zatvoreni (vlasnički) kod može se uporediti sa crnom kutijom, mi ne znamo šta se u njoj dešava i gde idu naši podaci, te se korišćenje ovih alata postavlja kao pitanje poverenja, ali mi korporacijama ili verujemo vrlo malo ili im ne verujemo uopšte. Ovakva vrsta kompromisa na koju smo spremni da bismo bez ikakvog napora mogli da koristimo tehnologiju može

biti veoma opasna. Pored toga što se korisničkim podacima trguje u komercijalne svrhe, dokazano je da bezbednosne službe mogu veoma lako presresti komunikaciju i da imaju direktan uvid u naše meta podatke. Korišćenjem modernih alata za sajber špijunažu, vlade širom sveta sprovode ciljane napade na političke disidente a često i angažuju zlonamerne hakere koji uz korišćenje sofisticiranih tehničkih metoda i socijalnog inženjeringa, uspevaju da upadnu u dobro zaštićene sisteme a da ih niko ni ne primeti. Na kraju, dobro poznata neprijatnost koju iskusimo svaki put kada neki od popularnih servisa na koje se oslanjamo na kratko postane nedostupan poziva nas da se zapitamo šta će se desiti kada prestanu da rade na duže, jer nije više pitanje da li će se to dogoditi nego samo kada će se to dogoditi.

S druge strane, primena i korišćenje u potpunosti odgovornih i bezbednih rešenja otvorenog koda često zahteva mnogo više truda i resursa. Za neke servise je neophodno angažovati sistemske inženjere da ih instaliraju, da iznajme ili kupe servere, da održavaju čitav sistem, da sprovode dodatnu obuku a mnoge organizacije nemaju takve kapacitete. Međutim, ovakva vrsta investicija omogućava veću kontrolu nad protokom podataka, kao i dugoročnu održivost informacionih sistema. U današnje vreme u okviru jedne organizacije treba razmišljati o tehnologiji isto koliko i o upravljanju, finansijama i ljudskim resursima.

Kada se uzmu u obzir ova pitanja, u odnosu na raspoložive resurse, pojedinci i organizacije mogu odlučiti na kom nivou će unaprediti svoj pristup tehnologiji i odabrati alate koje žele da koriste u radu. Na taj način se mogu ublažiti, tj. smanjiti rizici, uz male korake ka poboljšanju tehnološkog okruženja: korišćenje već dokazanih alternativnih rešenja umesto određenih alata, što zahteva minimalne napore u ovoj vrsti promene. Ovaj pristup neće rešiti probleme, ali će ih smanjiti, olakšavajući shvatanje tehnologije i povećavajući sigurnost u budućnosti, koja će biti potrebna zbog većih izbora i odluka. Ako posmatramo malo ambicioznije to posmatramo, to može biti potpuna promena u pristupu i paradigmi kada je reč o tehnologiji. Zahteva ozbiljnije ulaganje resursa, vremena i energije, ali dugoročno gledano donosi mnogo veću nezavisnost u kontroli podataka, kao i veliki sistemski i tehnološko-politički zaokret.

U naredna dva poglavlja dat je pregled i opis nekih od najsveobuhvatnijih alata i rešenja koje zajednica trenutno nudi, kojima se može garantovati bezbedna komunikacija i timski rad, ne samo u vremenima krize, već i u vremenima koje dolaze.

BEZBEDNA KOMUNIKACIJA

Aplikacije za razmenu trenutnih poruka (alternativna rešenja za WhatsApp, Facebook Messenger, Viber i druge)

Signal – Ova aplikacija za komunikaciju radi na većini platformi i operativinih sistema i jedan je od pionirskih poduhvata komuniciranja putem enkriptovanih trenutnih poruka. Korišćenjem ove aplikacije možete slati tekstualne poruke, što podrazumeva i komunikaciju grupe korisnika, slanje glasovnih poruka, deljenje foto i video sadržaja. Od skoro su dodali i podršku za razgovor i video pozive. Ova aplikacija služi i kao zamena za aplikacije za slanje SMS/MMS, ali je potrebno da sve strane u komunikaciji koriste ovu aplikaciju da bi mogla da koristi sopstveni protokol. Ovo je projekat otvorenog koda, koji vodi neprofitna organizacija i u potpunosti se finansira putem donacija, zato i ne monetizuje podatke svojih korisnika. Tokom razvoja ove aplikacije, aktivisti širom sveta su je koristili za bezbednu komunikaciju u represivnim režimima i situacijama povećanog policijskog nadzora, kao što su protesti u demokratskim društvima.

Wire – Jedna od najpopularnijih aplikacija sličnih Signalu, iako su se paralelno razvijale, Wire je imao neke prednosti koje ostali servisi nisu imali u to vreme, kao što je enkriptivani grupni čet, ili mogućnost registrovanja na servis i njegovo korišćenje bez unošenja broja mobilnog telefona. Ponudivši specifične mogućnosti koje se u poređenju sa konkurencijom više odnose na dodatnu zaštitu privatnosti pokazalo se kao veoma važno za napredak tehnologije i raznolikost čitavog ekosistema. S obzirom na to da se Wire aplikacija isto tako zasniva na otvorenom kodu i ne prodaje podatke o svojim korisnicima, finansira se tako što nudi napredne usluge za poslovne korisnike.

Telegram – Iako ova platforma nije u potpunosti zasnovana na otvorenom kodu (na aplikaciji je otvoren kod, ali ono što se dešava na serverima kompanije nije), do sada nije bilo incidenata koji su mogli ugroziti podatke o aktivistima koji koriste Telegram, i ovo je jedan od najpopularnijih servisa za bezbednu komunikaciju, naročito za razmenu informacija između velikih grupa ljudi putem grupa i kanala. I baš zato što omogućuje laku komunikaciju za veliki broj korisnika, uz intuitivni interfejs i ogromnu popularnost u opštoj populaciji, branitelji ljudskih prava često biraju Telegram. Iako je ova platforma izgradila odnos poverenja sa svojim korisnicima, savetuje se oprez jer sistem nije u potpunosti zasnovan na otvorenom kodu, poslovni model nije u potpunosti jasan i ne garantuje dugoročnu održivost.

Internet/video konferencijski sistemi (alternativna rešenja za Zoom, Skype, Google Meet, Microsoft Teams, i druge)

Jitsi Meet

U poslednjih nekoliko godina, mnoge organizacije i aktivisti počeli su da koriste Jitsi Meet kao primarnu platformu za video pozive zbog nekoliko ključnih osobina. Ova platforma je među prvima uvela enkripciju za usluge ovog tipa u otvorenom kodu, dok istovremeno ne traži instaliranje posebne aplikacije, već može da radi direktno na svim najpoznatijim internet pretraživačima samo klikom na jedan link. Za one organizacije koje imaju veće resurse, ova platforma se može preuzeti i instalirati na Linux serverima, što im nudi dodatni nivo sigurnosti.

BigBlueButton

Konkurentski Zoom u svetu vlasničkih i komercijalnih alata za video konferencije ima dostojnog protivnika u softverskom paketu BigBlueButton u svetu otvorenih i odgovornih tehnologija. Platforma ima mnoge karakteristike kojima se mogu pokriti potrebe velikih javnih događaja na internetu kao što je administracija korisnika, deljenje multimedijalnog sadržaja, prikazivanje prezentacija, alati za zajednički rad na beloj tabli/flipčartu, privatni i javni čet, manje sobe sa sastanke i drugo. Jedini zahtev je da vašu instancu instalirate na Linux servere, ili da koristite instancu drugih organizacija koje će vam je dati na korišćenje, što je sve češće slučaj u civilnom sektoru.

BEZBEDAN GROUPWARE SOFTVER

Timska komunikacija (alternativna rešenja za Slack, Microsoft Teams, Discord i druge)

Mattermost

Organizacije koje imaju dosta opsežnu internu komunikaciju i materijale često se uguše i izgube usled velikog obima imejl korespondencije. Mattermost svakako ima alate kojima je moguće umanjiti težinu vašeg inboksa i poboljšati komunikaciju kroz tematske čet kanale, intuitivnu pretragu, indeksiranje, i bezbedno deljenje dokumenata i fajlova. Nakon prvog instaliranja na server koji poseduje organizacija ili iznajmljeni server, nije potrebno veliko održavanje i administracija, pa je ovo zgodno za organizacije sa manjim tehnološkim kapacitetima. Svi podaci su enkriptovani i projekat se finansira tako što se pružaju podrška i dodatne usluge poslovnim korisnicima.

Element

Do skoro je bio poznat kao „Riot.im”, Element je čet klijent koji koristi moderan Matrix protokol – spoljni protokol za komunikaciju koji je razvijen kao standard otvorenog koda i cilj mu je da omogući interoperabilnost između različitih servisa za ćaskanje i video konferencije. To praktično znači da se mogu razmenjivati poruke sa korisnicima najpopularnijih platformi, uključujući i vlasničke servise kao što su Apple iMessage, Facebook Messenger, WhatsApp, Discord, Slack, i naravno, sa korisnicima aplikacija koje rade na otvorenom kodu kao što su Signal, Mattermost, IRC, Telegram i druge.

Ostali alati

U zavisnosti od potreba organizacije, treba pomenuti i još nekoliko alata koji se mogu koristiti kao alternativna rešenja za servise velikih kompanije koje prikupljaju podatke.

Etherpad je onlajn/internet servis za rad sa tekstom i izmenu teksta kroz saradnju u realnom vremenu (alterantivno rešenje za Google Docs) koji možete instalirati i na vaš server, ali postoje i besplatne instance na internetu kao što je **„Riseup Pad“** koji nudi ovu uslugu besplatno, a ne prikuplja IP adrese i poštuje vašu privatnost. Aplikaciji se može pristupiti i putem VPN-a ili **Tor pretraživača**, koje svakako morate koristiti ako želite da sakrijete svoju aktivnost na internetu.

Istu tehnologiju koju koristi Tor za onion usmeravanje koristi i **OnionShare,** servis za bezbedno deljenje fajlova. Ukratko rečeno i možda potpuno banalno, on radi tako što generiše enkriptovanu fajl adresu na kompjuteru kojoj sa druge strane može pristupiti samo korisnik koji koristi Tor protokol.

I na kraju, kada je reč o bezbednom skladištenju podataka i alternativnom rešenju za servise na „oblaku“ (zamena za Dropbox ili Google Drive), Nextcloud je jedan od najboljih. Zahteva instalaciju i održavanje na sopstvenom serveru, te svakako traži dodatne resurse u organizaciji, ali isto tako nudi i najviši nivo kontrole podataka.

Ipak, korišćenje ovih alata u svakodnevnom radu vam neće obezbediti totalni imunitet u odnosu na bezbednosne rizike, ali će vam omogućiti veću nezavisnost i bolje razumevanje tehnologije. Otpornost pojedinaca i organizacija nadalje zavisi od shvatanja ekosistema digitalnog prostora i odnosa između tehnologije i društva. Zato je važno da pored toga što ćemo usvojiti odgovorne alate, razumemo i šta je protok podataka, arhitektura nadzora i poslovni modeli tehnoloških korporacija koje sve više centralizuju internet kroz moderno kolonizovanje digitalnog prostora. Razumevanjem i prihvatanjem modernih tehnologija ohrabruje se razvoj alternativnih rešenja, dok se uz povećavanje pismenosti zajednice i društva u celini ohrabruje sloboda, otvorenost i decentralizacija interneta, što je postao preduslov za otpornost demokratije.

Zaključak

U odnosu na trenutnu situaciju, potrebno je da branitelji ljudskih prava, uz povećanje svoje budnosti, pomno posmatraju sve napore država u uvođenju restriktivnih zakonskih propisa i intruzivnih tehnologija pod izgovorom borbe protiv pandemije. Mogu biti uvedene mere u budućnosti koje mogu negativno uticati na slobodu izražavanja, pravo na privatnost i ostala povezana prava i slobode, kao što je pravo na protest ili slobodu okupljanja, i koje mogu biti tako „upakovane“, da neće biti ni vidljive na prvi pogled. Stoga, civilni sektor mora naročito biti na oprezu i preispitivati sve mere koje se navodno uvode da bi se sprečilo širenje korona virusa, jer mogu predstavljati uvođenje stalnog nadzora ili neki drugi vid nesrazmernog ograničenja ljudskih prava.

Trenutne okolnosti, veoma izazovne za branitelje ljudskih prava, aktiviste i uopšteno gledano civilni sektor, mogu se posmatrati i kao mogućnost za uvođenje alternativnih i bezbedniji tehničkih alata, kao što su slobodan softver i softver otvorenog koda. Iako može biti poteškoća prilikom prelaska na rad od kuće i primenu novih alata u tehničkoj infrastrukturi organizacije, na taj način se može obezbediti dugoročna fleksibilnost i otpornost u vremenima krize, naročito u manjim kolektivima i organizacijama koje ne mogu da ulože velike resurse. Na primer, projekat Galilejo nudi braniteljima ljudskih prava i ostalim akterima koji brane javni interes resurse za ublažavanje tehničkih napada, sprečavanje korišćenja njihove ranjivosti i zaštitu integriteta podataka.[44]

Međutim, kada je reč o radu na daljinu, organizacije moraju da se osiguraju da njihovi zaposleni kod kuće sprovode iste standarde digitalne bezbednosti kao i u poslovnim prostorijama. Osim toga, uz otvoreniji pristup u usvajanju i korišćenju slobodnog softver i softvera otvorenog koda zajednici se omogućuje da bude spremnija da se zalaže za to da internet bude slobodan, otvoren i decentralizovan.

44 Više informacija o Galilejo projektu potražite na: https://www.cloudflare.com/en-gb/galileo/

CIVIL RIGHTS DEFENDERS

LJUDSKA PRAVA U PANDEMIJI

Шведска
Sverige