
LJUDSKA PRAVA

U USLOVIMA PANDEMIJE



Švedska
Sverige

IMPRESSUM

Izdavač
Civil Rights Defenders

Za izdavača
Goran Miletic

Autori
SHARE Foundation

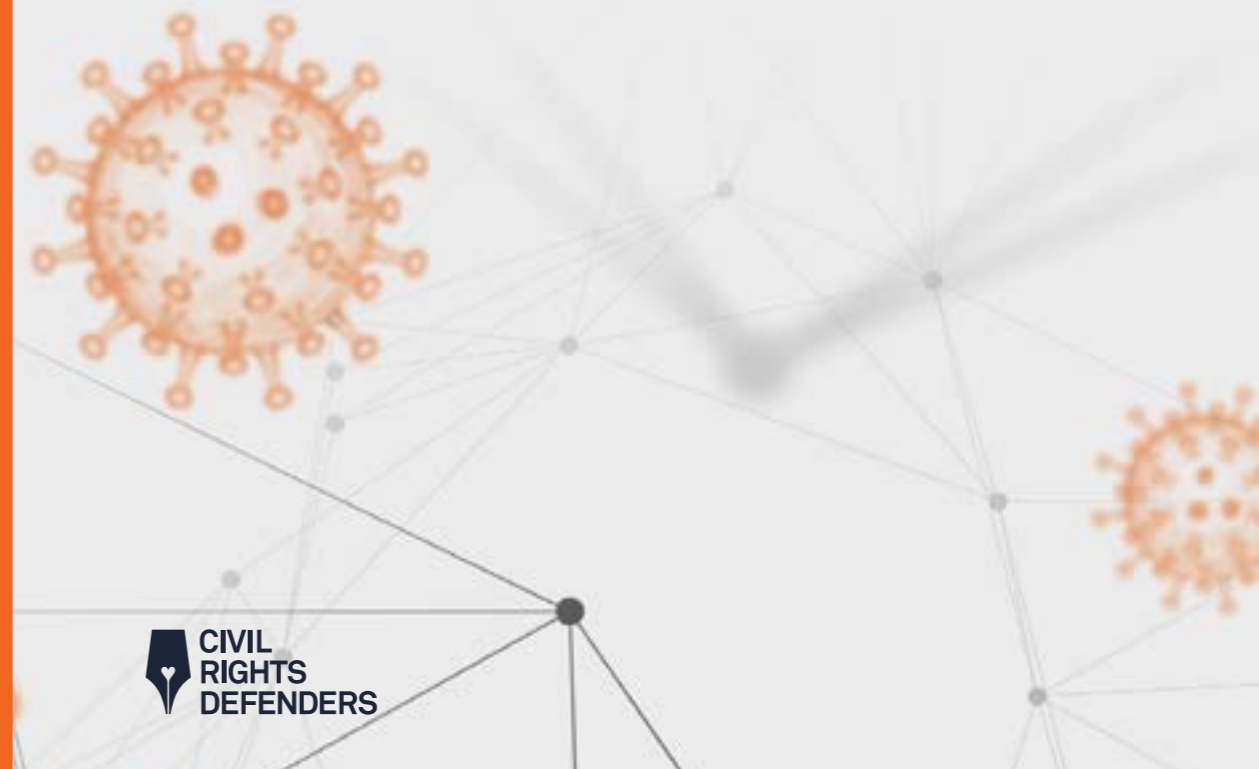
Bojan Perkov
Kristina Čendić
Filip Milošević
Andrej Petrovski
Milica Jovanović

Urednica
Neda Mirković

Dizajn
Marko Kovačevski

LJUDSKA PRAVA

U USLOVIMA PANDEMIJE



 CIVIL
RIGHTS
DEFENDERS

Ljudska prava u uslovima pandemije uzrokovane virusom COVID-19
7

Pregled stanja u regiji
8

Odgovori država na situaciju uzrokovanu virusom COVID-19
10

Utjecaj mjera za borbu protiv COVID-a
12

Sloboda izražavanja
12

Nadzor
14

Rad na daljinu
16

Pitanje kapaciteta
17

Digitalni savjeti
18

Sigurna komunikacija
20

Sigurni Groupware softver
21

Zaključak
21

LJUDSKA PRAVA U USLOVIMA PANDEMIJE

Pandemija uzrokovana virusom COVID-19, pojačavajući već postojeće pritiske na ljudska prava i njihove branitelje u cijelom svijetu, je zajednicama koje u državama svog prebivališta već trpe nejednakosti i nepravde donijela velike izazove u, jer su mnoge od tih država pribjegle izvanrednim mjerama za suzbijanje izbijanja epidemije. „Informirajte, osnažite i slušajte zajednice”, poručio je generalni direktor Svjetske zdravstvene organizacije u augustu ove godine, osvrćući se i propitujući odgovore država na “štetu koja je u socijalnom, ekonomskom i političkom smislu uzrokovana COVID-om 19”.¹

Izvršni direktor *Branitelja ljudskih prava* je u maju 2020. god. izjavio: „Neke mjere mogu se smatrati nužnima, no neke to zasigurno nisu – i iste se moraju ukinuti čim se ova situacija okonča. Nadalje, koristiti se pandemijom kako bi se maltretirali branitelji ljudskih prava ili zloupotrebila vladavina prava za ostavrenje političkih poena, čemu smo već svjedoci, je jednostavno rečeno – nedopustivo.“ Takođe je u obraćanju naglasio i ulogu organizacija koje se bave zaštitom ljudskih prava u procesu monitoringa i zahtijevao pozivanje na odgovornost nadležnih vlasti po pitanju prekoračenja granice između onoga što je zbilja nužno u jednom demokratskom društvu i onoga što je već zloupotreba moći i ovlasti.²

Iskustva iz regije Zapadnog Balkana su slična. Obzirom da su vlade u mnogim zemljama Balkana odgovore na pandemiju oblikovale militantno, pitanja javnog zdravstva ustupila su mjesto diskursu državne bezbjednosti gdje se različita mišljenja i pitanja smatraju znakovima pobune.

Kako je u nekim zemljama tradicionalni medijski prostor za izražavanje neslaganja već bio vrlo ograničen, nametnutim potpunim ili djelomičnim zatvaranjima i uvođenjem mjere policijskog sata većina društvenih i političkih aktivnosti premještena je u internetsku sferu. Pritisak na branitelje ljudskih prava, slijedom primjera, se takođe preselio u istu.

Zvanične mjere sprovedene u svrhu borbe protiv pandemije često su podrazumijevale povišen nivo nadzora i korištenja tehnologija za praćenje kretanja. Ovakvi uslovi su ozbiljno narušili privatnost rada u svakoj sferi u kojoj ga branitelji ljudskih prava obavljaju. Novinari, advokati i aktivisti koji se bave pitanjima ljudskih prava su se takođe suočili sa poteškoćama u smislu relociranja aktivnosti poput radionica, protesta i konferencija koje obavljaju u svojim zajednicama, takođe seleći ih u internetsku sferu a istovremeno održavajući svoje komunikacije sigurnima.

Uz prikupljanje primjera kršenja digitalnih prava i opisivanje vidljivih trendova u ograničavanju rada branitelja ljudskih prava u nekoliko zemalja jugoistočne Europe, ova publikacija nudi priliku za preispitivanje internetskih usluga i alata koji se koriste u svakodnevnom životu. Postoje etični i sigurni digitalni alati koji mogu zamijeniti velike komplekse poput Facebooka, Googlea, Amazona i ostalih globalnih IT divova koji gomilaju podatke. Oni su nam i dostupni a mogu pomoći da izbjegnemo cenzure koje nameću vlade, nadzor obavještajnih agencija te tehnološke napade kibernetičkih kriminalaca i zlonamjernih hakera.

¹ WHO Director-General's opening remarks at the media briefing on COVID-19 - 3 August 2020, World Health Organization, 3 August 2020 / Uvodno obraćanje generalnog direktora SZO-a /WHO na brifingu za predstavnike medija povodom situacije sa COVID-19 – održane 3 augusta 2020. God., World Health Organization, 3 august 2020.

² COVID-19 is no excuse for governments to abuse human rights, Anders L. Pettersson, The Globe Post, 1 May 2020. / COVID-19 nije opravdanje na osnovu kojeg bi vlade kršile ljudskih prava, Anders L. Pettersson, The Globe Post, 1 maj 2020.

PREGLED STANJA U REGIJI

Fundacija SHARE još od septembra 2014. god. vrši monitoring kršenja digitalnih prava, a od prošle godine, u partnerstvu sa BIRN-om (Balkan Investigative Reporting Network (BIRN), širi polje djelovanja kako bi bilježili incidente ovakve vrste i u Bosni i Hercegovini, Hrvatskoj, Mađarskoj, Sjevernoj Makedoniji i Rumuniji.³ Prvi zajednički poduhvat, nehotice se poklopio sa globalnom pandemijom, otkrivajući zabrinjavajuće događaje i trendove u regiji.

Proces monitoringa temeljise na praćenju različitih oblika prekršaja ili kršenja prava a sukladno definiranoj metodologiji,⁴ te sortiranju slučajeva u specificirane kategorije. Metodologijom je uspostavljeno sedam različitih kategorija prekršaja i kršenja digitalnih prava i sloboda:

A. Narušavanje i kršenje sigurnosti informacija: slučajevi upada/proboja u informacione sisteme, na primjer neovlašten pristup, DoS napadi (Distributed Denial-of-Service/Napad uskraćivanjem resursa) u svrhu onemogućavanja pristupa određenim sadržajima, krađa i uništavanje podataka i drugo.

B. Narušavanje i kršenje privatnosti informacija i ličnih podataka: slučajevi *curenja* informacija, protuzakonita obrada podataka ili presretanje komunikacija.

C. Pritisci zbog izražavanja i aktivnosti na internetu: ova narušavanja i kršenja i se odnose na čast i reputaciju, ugrožavanje sigurnosti, diskriminaciju i mržnju, slobodu izražavanja na radnom mjestu te pritiske na pojedince zbog objavljivanja informacija na internetu..

D. Manipulacija i propaganda u digitalnom okruženju: ova narušavanja i kršenja obuhvataju različite oblike dijeljenja sadržaja i manipulacije putem interneta a u svrhu ostvarivanja određenih ciljeva – za koje se kasnije uglavnom utvrdi da su ekonomske prirode.

E. Držanje posrednika odgovornim: ova narušavanja i kršenja odnose se na pritiske na pružaoce internetskih usluga, poput pružalaca usluga hostinga i zahtjeva za uklanjanje sadržaja i odbijanja usluga, prijetnjama zakonskim mjerama, kaznama ili blokiranjem.

F. Blokiranje i filterisanje sadržaja: u ovim slučajevima određene se sadržaje blokira tehnički na nivou države ili organizacije, ili kada algoritmi platforme blokiraju ili suspenduju zakonit sadržaj (npr. – videoprikaz parodije).

G. Drugo: druga narušavanja i kršenja digitalnih prava isloboda koja nisu obuhvaćena navedenim definiranim kategorijama.

Pored gore spomenutih kategorija, postupak monitoringa također pruža informacije o napadačima i oštećenima. Oštećeni mogu pripadnici sljedećih grupa: novinari, javne osobe, državni dužnosnici, građani, aktivisti i drugi. Ako je identifikacija slučaja moguća, opisi slučajeva sadrže i sredstva kojim je napad počinjen. Sredstva napada mogu biti tehničke prirode (napadi malvera/zlonamjernog softvera, ubrizgavanje koda, napadi aktivnostima izviđanja, napadi aktivnostima presretanja, napadi na mogućnost pristupanja sadržajima te napadi pretrpavanjem i/ili uskraćivanjem usluge) ili pravne prirode (privatne tužbe, krivične prijave, hapšenje i zatvaranje, važne presude, mjere konfiskacije i premetačie, prekršajne prijave) . Takođe, vrši se monitoring i ishoda predmeta, tj. monitoringom se pominju sve pravne i druge mjere poduzete u vezi sa slučajem i je li donesena pravomoćna sudska presuda ili nije.

Ovaj izvještaj predstavlja nalaze prikupljene za četiri zemlje: Albaniju, Bosnu i Hercegovinu, Kosovo i Srbiju a temelji se na podacima prikupljenim u periodu od 31 januara do 30 novembra 2020.⁵

³ SHARE Foundation and BIRN digital rights monitoring database: <https://monitoring.bird.tools/> / Baza podataka fondacije SHARE i BIRN-a o monitoringu digitalnih prava : <https://monitoring.bird.tools/>

⁴ More details about the SHARE Foundation and BIRN digital rights monitoring methodology can be found at: <https://monitoring.bird.tools/methodology/> / Više informacija o metodologiji monitoringa digitalnih prava koju koriste fondacija SHARE i BIRN dostupno je na: <https://monitoring.bird.tools/methodology/>

⁵ Please note: data for Kosovo was provided by Balkan Investigative Reporting Network (BIRN), while data for Albania was based on information provided by CRD Albania staff and "The Right to Information during Natural Disasters in Albania 2020" publication, authored by Dorian Matlija with the support of Res Publica center staff. / Napomena: podatke za Kosovo je dao BIRN (Balkan Investigative Reporting Network), dok se podaci za Albaniju temelje na informacijama koje je pružilo osoblje CRD Albanija i publikacija "The Right to Information during Natural Disasters in Albania 2020" (Pravo na informacije tokom prirodnih nepogoda u Albaniji u 2020.godini), čiji je autor Dorian Matlija, uz podršku osoblja centra Res Publica center staff.

KATEGORIJA PRIJESTUPA	Srbija	Bosna i Hercegovina	Albanija	Kosovo
A. Narušavanje i kršenje sigurnosti informacija	4	1	1	0
B. Narušavanje i kršenje privatnosti informacija i ličnih podataka	8	5	2	4
C. Pritisci zbog izražavanja i aktivnosti na internetu	30	9	2	3
D. Manipulacija i propaganda u digitalnom okruženju	15	6	2	4
E. Držanje posrednika odgovornim	0	1	0	0
F. Blokiranje i filterisanje sadržaja	0	0	1	0
G. Drugo	0	0	0	0
UKUPNO	57	22	8	11

Tokom pomenutog perioda, u Srbiji, Bosni i Hercegovini, Albaniji i Kosovu zabilježeno je 98 slučajeva kršenja digitalnih prava povezanih sa situacijom pandemije a što su slučajevi od hapšenja novinara i građana zbog informacija koje su plasirali putem interneta i konfiskovanja uređaja do *curenja* ličnih informacija. Osim ciljanih incidenata, sve je veći broj slučajeva koji uključuju nepropisno postupanje sa osjetljivim zdravstvenim podacima građana i namjerno nezakonito objavljivanje takvih podataka u javnosti.

Najprisutniji oblik narušavanja i kršenja prava u pomenutom periodu – otprilike polovica svih zabilježenih slučajeva, odnosi se na vršenje pritiska zbog izražavanja i aktivnosti na internetu, a manifestovan je kroz uvrede, prijetnje i zastrašivanje, objavljivanje neistina u svrhu klevetanja i sl.

Prema analizi o Zapadnom Balkanu,⁶ u nekim je zemljama pandemija razotkrila dugoročne probleme i služila je „kao akcelerator već postojećih trendova, kao što su kriza demokratije i nacionalizam“. U drugim zemljama, su joj se ubrzo pridružile predizborne kampanje izazivajući „nevjericu i bijes usmjeren protiv vlasti i države, otkrivajući duboko ukorijenjeno nepovjerenje prema potonjima“. U svim promatranim zemljama slobodi izražavanja nanosena je šteta.

U uslovima zatvaranja i izolacije (lockdown) politički pritisci na medijske sektore u tim zemljama su rezultirali ozbiljnim posljedicama poput centralizacije informacija, širenja lažnih vijesti i progona onih sa suprotnim stavovima, bilo da se radi o profesionalnim novinarima ili građanima. Istovremeno, mediji bliski vladama nisu se suzdržali da sami ne šire lažne vijesti. U nekim slučajevima vlada je imala tako snažnu kontrolu nad informacijama da su pokušali donijeti zakone kojima bi se sve osim zvaničnih informacija smatralo protuzakonitim. Ovime je demonstrirana moć na način da su u ovim zemljama još više oštećene i ometane demokratske procedure, a ljudska prava ograničavana pod izgovorom borbe protiv pandemije.

⁶ Policy Brief: The Western Balkans in Times of the Global Pandemic, Balkans in Europe Policy Advisory Group (BiEPAG), April 2020 / Analiza: „Zapadni Balkan u doba globalne pandemije“, Savjetodavna grupa za Balkan, april 2020.godine

U martu 2020. godine vlade nekih zemalja pomenutih u ovom izvještaju pribjegle su proglašavanju vanrednog stanja. U Srbiji je proglašeno 15. marta i trajalo je do 6. maja; u Bosni i Hercegovini vanredno stanje bilo je na snazi od 17. do 29. maja u Federaciji Bosne i Hercegovine i od 28. marta do 21. maja u Republici Srpskoj; a u Albaniji od 25. marta do 23. juna. Na Kosovu je 16. marta, pod nadzorom Ministarstva zdravlja, na snagu stupilo vanredno stanje u sektoru javnog zdravstva. Građani četiri zemlje suočili su se sa sličnim zabranama i izazovima tokom pandemije i iako su sva ograničenja izazvala glasnjiva negodovanja javnosti, aktivizam ljudskih prava morao se osloniti na internet više nego ikad do sad.

Vanredno stanje u Albaniji bilo je na snazi duže nego u drugim zemljama koje su obuhvaćene ovim izvještajem. Vlasti su insistirale na nužnosti zaštite zdravlja, no poštivanje ljudskih prava postalo je upitno, pogotovo kada govorimo o prvu uživanja slobode izražavanja na internetu. Tokom krize, vlada je pojačala kontrolu nad informacijama naročito u vezi sa temom širenja virusa, što je zauzvrat izazvalo brojna pitanja. U javnom diskursu su se opetovano ponavljale fraze nalik onima kod ratnog stanja, a oklopljena vozila na ulicama su u građanima pobuđivala strah.⁷ Kao i u drugi zemljama, građanstvo Albanije bilo je zbunjeno uvedenim mjerama. Uspostavljen je Tehnički komitet eksperata kako bi se donosile odluke o mjerama borbe protiv pandemije, no „rad Komiteta obilježen je ograničenim javnim informacijama o nadležnostima istog te gdje je granica između preporuka Komiteta i njihovog pretvaranja u političke odluke. Do početka maja čak ni ime predsjedavajućeg Komiteta nije bilo objavljeno”. Jednom prilikom, albanska policija za antiterorizam podnijela je krivične prijave protiv desetak ljudi navodeći da su koristile Facebook za širenje lažnih vijesti.⁸

Policija je očigledno pratila objave i komentare na Facebooku i na ovaj način saznala za dotične izjave. Ispostavlja se da je monopolizacija informacija jedan od najvećih problema sa kojima se Albanija suočila tokom krize. Premijer je bio vrlo aktivan i na društvenim mrežama, pored dominantnog prisustva u javnoj radioteleviziji. Zapravo, postoji podatak da je „samo u prvom mjesecu zatvaranja i izolacije premijer objavio 407 postova na Facebooku (13 dnevno) i 47 sati videozapisa, stvarajući tako prvo iskustvo Albanije sa upravljanjem putem društvenih mreža.”⁹ Prilično problematična činjenica je bila svjedočenje situaciji „da se većina odluka prvo pojavljivala i objavljivala na premijerovom Facebook profilu a tek zatim u službenom glasilu, dok su pri tom *pres-konferencije* bile zatvorene za novinare.” Ovime je bio ometan pristup tačnim javnim informacijama a „nacionalni mediji su imali ograničenu mogućnost pružanja dodatnih informacija javnosti i informacija suprostavljenih onima koje je davala vlada.”¹⁰

U Bosni i Hercegovini nije bilo konzistentne zvanične strategije za borbu protiv pandemije a zbog upravnih nadležnosti u zemlji. Svaki od dva entiteta, naime Federacija Bosne i Hercegovine i Republika Srpska, Brčko Distrikt BiH, i deset kantona u okviru Federacije Bosne i Hercegovine uveli su različite mjere u svrhu obuzdavanja pandemije. Ovakva situacija pokazala se kao veoma zbunjujuća za stanovnike Sarajeva obzirom da na to da se međuentitetske linije nalaze u i gradu pa su se mjere i ograničenja ponekad razlikovale na dvije strane ulice.¹¹ Tokom krize, javnost u Bosni i Hercegovini, uključujući i branitelje ljudskih prava, bila je suočena sa dezinformacijama o lokalnoj proizvodnji lijeka, nedostatku testova, da se gradovi iz aviona zasipaju virusom i tome slično. Nanesena je šteta i u oblasti zaštite ličnih podataka: vlasti su objavljivale imena ljudi koji su se oglušili o naredbe o samoizolaciji a čak se razmatrala opcija objavljivanja imena oboljelih u javnosti. Vlasti u Konjici i vlada Kantona 10 objavile su lične podatke osoba u samoizolaciji, a povukli su ih iz javnosti tek nakon što je Agencija za zaštitu podataka ovaj korak proglasila kršenjem zakona.¹² Najveći udarac na ljudska prava u Bosni i Hercegovini zadobiven je kada je entitet Republika Srpska usvojio uredbu o zabrani širenja panike i

nereda putem navodnih lažnih vijesti.¹³ Lokalni branitelji ljudskih prava i međunarodni akteri kritizirali su ovaj korak kao štetan po slobodu izražavanja, a od uredbe se ubrzo odustalo, ali tek nakon što je nekoliko građana već uhapšeno ili kažnjeno novčanom kaznom.

Kao da pandemija nije bila dovoljna, **Kosovo** se suočilo i sa političkom krizom jer je izglasano nepovjerenje vladi a što je samo doprinijelo sveukupnoj nesigurnosti i nepovjerenju građana. Kao i u drugim zemljama, vlasti su insistirale na tome da ljudi nose maske, da se drži fizička distanca, te su uvedene mjere ograničenja kretanja. Povodom mjera ograničenja, BIRN Kosovo i lokalna kompanija za razvoj softvera pod nazivom KUTIA, izradili su platformu „90 Minutëshi yt” („Your 90 Minutes“/„Vaših 90 minuta“) koja je građanstvu omogućavala da provjere u kojim terminima im je dopušteno napustiti dom, tako što bi u aplikaciju ukucali brojke koje čine njihov JMBG -od drugog do posljednjeg, ili unosom broja pasoša.¹⁴ Međutim, tokom krize građanstvo je bilo mnogo više prestravljeno hapšenjima lica koja su pričala o temama i pitanjima od javnog značaja i interesa. Hapšenje urednika iz Mitrovice bio je čin velikog pritiska na slobodu izražavanja.¹⁵ Jeza na Kosovu se dodatno pojačala kada je policija Kosova odlučila krivično goniti osobu koja je navodno podijelila tekstovnu poruku kojom poziva građanstvo da se testiraju na korona virus na Univerzitetkom Kliničkom Centru Kosovo (UCCK), tvrdeći da su određene krvne grupe podložnije zarazi.¹⁶ Na sve ovo, portal Sinjali objavljuje imena, adrese i datume rođenja za 210 građana u karantinu u Sjevernoj Mitrovici i drugim gradovima, što je procijenjeno kao narušavanje privatnosti.¹⁷ Nakon žestoke reakcije Udruženja srpskih novinara na Kosovu i misije OSCE-a na Kosovu, predmetni lični podaci su učinjeni nečitkima.

U Srbiji je izbijanje Covid-19 i uvođenje vanrednog stanja rezultiralo problematičnim mjerama koje su vlasti poduzele u borbi protiv pandemije. Navedeno je vidljivo kroz pokušaje kontrole protoka informacija, favoriziranju provladinih medija, netrpeljivosti prema nezavisnim medijima i braniteljima ljudskih prava te kršenju zaštite ličnih podataka. Zbog situacije izazvane pandemijom, različiti akteri prebacili su svoje aktivnosti na globalnu mrežu više nego ikada ranije što ih je učinilo još podložnijim digitalnim prijetnjama i napadima. Jedan od najozbiljnijih incidenata povezan je sa curenjem podataka koje se dogodilo kada su se pristupni podaci za ulazak u informativni sistem COVID-19 pojavile na internetu.¹⁸ Pristupni podaci za sistem koji obrađuje osjetljive podatke građana u svezi sa pandemijom bili su osam dana javno dostupni na sajtu jedne zdravstvene institucije. Iako su korisničko ime i lozinka za pristup uklonjeni nakon što je civilno društvo upozorilo nadležne vlasti, osam dana je bilo dovoljno da Google indeksira informacije i učini ih dostupnima kao rezultate pretraživanja. Pored ovoga, srbijanska vlada pokušala je centralizovati informacije vezane za pandemiju kroz uvođenje uredbe kojom se proglašava da su jedine pouzdane informacije one koje dolaze od vlasti, čime su svi drugi izvori informacija svrstani u izvore navodnih lažnih informacija. Novinari, aktivisti civilnog društva te čak i građani koji su govorili o pitanjima i problemima poput manjka medicinske opreme, nestašice goriva i slično optuživani su za širenje panike a neki su čak i uhapšeni.

7 G. Madhi, Albania: public information becomes a casualty of COVID-19/ Albanija: javne informacije postaju žrtvom virusa COVID-19, OBC Transeuropa, 11 juni 2020. godine

8 G. Emiri, Albania's War on 'Fear Mongers' Leaves Rights Activists Uneasy/ Albanski rat protiv „Sijača straha” kod aktiviste za ljudska prava stvara nelagodu BIRN, 29 juli, 2020. godine

9 G. Madhi, Albania: public information becomes a casualty of COVID-19/ Albanija: javne informacije postaju žrtvom virusa COVID-19, OBC Transeuropa, 11 juni 2020

10 Ibid.

11 G. Sandić-Hadžihanović, Entities and pandemic: On one side of the street one rule, on the other another/, Entiteti i pandemija: Na jednoj strani ulice jedna pravila, na drugoj druga, Radio Free Europe/Radio Liberty / Radio Slobodna Evropa/Radio Liberti, 14 maj 2020. godine

12 Bosnia and Herzegovina and Montenegro to Respect Right to Privacy of Citizens in Self-Isolation/ Bosna i Hercegovina i Crna Gora moraju poštivati privatnost građana u samoizolaciji, CRD, 25 mart 2020. godine

13 M. Milojević, Preventing the spread of panic or 'disciplining' doctors and journalists/ Prevencija širenja panike ili disciplinovanje ljekara i novinara, Radio Free Europe/Radio Liberty, / Radio Slobodna Evropa/Radio Liberti, 12 april 2020. godine

14 S. Todorović, BIRN Platform to Help Kosovars Follow COVID-19 Restrictions/ BIRN Platforma kao pomoć Kosovarima da se pridržavaju ograničenja u vezi sa virusom COVID-19, BIRD, 16 april 2020. godine

15 OSCE Media Freedom Representative concerned about pressure on KoSSev online portal and its editor-in-chief in Kosovo/ Predstavnik OSCE-a za slobodu medija zabrinut je zbog pritiska na internet portal KoSSev i njegovog glavnog urednika na Kosovu, Organization for Security and Co-operation in Europe, 12 april 2020. godine

16 Calling for coronavirus testing by false messages/Poziv na testiranje na koronu putem lažnih poruka, Kosovo online, 31 mart 2020. godine

17 COVID-19: political interference in the media in Kosovo/ COVID-19: uplitanje politike u medije na Kosovu, European Federation of Journalist./Evropska federacija novinara 4 april 2020. godine

18 A Password Pandemic. How did a COVID-19 password end up online?/ Lozinka za Pandemiju. Kako je lozinka za COVID-19 dospjela na internet, SHARE Foundation, 24 april 2020

Učinak mjera za borbu protiv Covid-19

SLOBODA IZRAŽAVANJA

Pandemija je imala značajni utjecaj na slobodu izražavanja širom svijeta. Kada je javno zdravlje ugroženo i kada države uvode vanredno stanje, građanima se mogu nametnuti određena ograničenja, međutim ona ne smiju biti pretjerana. Prema članu 19., čini se da su mnoge države iskoristile pandemiju da bi dodatno ojačale svoje represivne mjere i ograničile slobodu izražavanja i informiranja.¹⁹ Zemlje Zapadnog Balkana uvele su ograničenja koja su ugrozila slobodu izražavanja i u velikoj mjeri utjecala na rad aktivista i novinara.



Digitalne tehnologije su promijenile način na koji ostvarujemo svoje pravo na slobodno izražavanje, a omogućile su i brojnim akterima da preuzmu ulogu novinara. Stoga, sve češće koristimo pojmove kao što su medijski akteri i građani novinari, jer svi oni učestvuju u raspravama o pitanjima od javnog interesa. Pandemija je, više nego ikada ranije, izmjestila ove rasprave u internetsko okruženje, ali uz jedan takav preokret, povećao se i pritisak na one koji ostvaruju slobodu izražavanja ili izvještavaju o pitanjima od javnog interesa na internetu. Profesionalni novinari i drugi tradicionalni medijski akteri nisu jedina meta. Prema Akcionom planu Ujedinjenih nacija za bezbjednost novinara i pitanje nekažnjivosti i na temelju Općeg komentara br. 34 Komiteta UN-a za ljudska prava, „definicija medijskih aktera proširena je kao rezultat novih oblika medija u digitalnom dobu. Stoga, ona obuhvaća i druge koji doprinose javnoj raspravi i koji obavljaju novinarsku djelatnost ili imaju ulogu čuvara javnog interesa²⁰. Međutim, na Zapadnom Balkanu bili smo svjedoci prijetnji i uvreda upućenih onima koji su iznijeli drugačije informacije od onih koje su nam dali zvaničnici ili koji su izrazili svoje stavove o pandemiji, a u nekim smo slučajevima bili svjedoci i hapšenja i izricanja novčanih kazni.

¹⁹ Coronavirus: Impacts on freedom of expression/ Koronavirus: Utjecaj na slobodu izražavanja, Article 19/članak 19
²⁰ Recommendation CM/Rec(2016) of the Committee of Ministers to member States on the protection of journalism and safety of journalists and other media actors, Council of Europe, 13 April 2016 / Preporuka CM/Rec(2016)4 Komitet ministara Savjeta Evrope državama članicama o zaštiti novinarstva i sigurnost novinara i ostalih medijskih aktera, Savjet Evrope, 13. april 2016.

Među prvim koracima koje su neke zemlje poduzele nakon proglašenja vanrednog stanja bio je pokušaj kontrole protoka informacija. Javnost ima pravo ne samo ostvarivati svoju slobodu izražavanja, već i da prima informacije. Međutim, 28. marta Vlada Srbije zabranila je bilo kome izvan Kriznog štaba da daje informacije o pandemiji, proglašavajući da će se bilo koja informacija iz drugih izvora smatrati netačnom i neprovjerenom. Preciznije, ako bi neko dijelio takve informacije, ta bi osoba bila odgovorna i snosila bi pravne posljedice zbog širenja dezinformacija za vrijeme vanrednog stanja²¹. Svjedoci smo sličnih događaja u Bosni i Hercegovini, kada je u entitetu Republika Srpska donesena Odluka o zabrani izazivanja panike i nereda, koja se, između ostaloga, odnosila i na društvene mreže i medije²². Takva odluka nanijela je štetu ostvarivanju prava na slobodu izražavanja, a lokalni branitelji ljudskih prava i međunarodni akteri pozvali su da se ista što prije ukine. Ubrzo se odustalo od ove odluke, ali je već nekoliko građana bilo novčano kažnjeno ili uhapšeno. Kršenje ove odluke kažnjavalo se novčanom kaznom u iznosu od 500 do 1.500 eura za fizička lica i od 1.500 do 4.500 eura za pravna lica.

Jedan od najozbiljnijih slučajeva koji je imao zastrašujući učinak bio je slučaj Ane Lalić, novinarka koja je uhapšena zbog pisanja o stanju u bolnici u Novom Sadu. Ana je uhapšena 1. aprila, samo nekoliko sati nakon objavljivanja njenog članka „Klinički Centar Vojvodine pred pucanjem: bez zaštite za medicinske sestre“. U ovom članku govorila je o pitanjima od javnog interesa - nedostatku zaštitne opreme kao što su maske i rukavice u Kliničkom centru Vojvodine. Bolnica je protiv nje podnijela prijavu navodeći da je članak narušio njihov ugled i uznemirio javnost neprovjerenim informacijama. Nakon hapšenja, oduzeti su Anin laptop i telefoni, a ona je privedena. Njeno hapšenje izazvalo je vrlo burnu reakciju, kako domaćih, tako i međunarodnih aktera, koji su tražili njezino što brže puštanje na slobodu. Ana Lalić puštena je sutradan odmah nakon saslušanja, a sve optužbe protiv nje povučene su krajem aprila. Ovaj incident nije samo prouzrokovao mogući efekt zastrašivanja među građanima i onima koji su govorili o određenim pitanjima od javnog interesa, već se nakon toga povela medijska hajka protiv Ane Lalić, koju su uglavnom vodili provladini mediji. Organizacija Civil Rights Defenders tada je pozvala Vladu Srbije da novinarima obezbedi prostor za prikupljanje informacija i informiranje građana o događajima vezanim za pandemiju COVID-19. „Smatramo da nema opravdanja za ukidanje prava novinara da postavljaju pitanja na otvorenom i javnom forumu, uzimajući u obzir sve mogućnosti koje moderna tehnologija nudi za takvu interakciju bez nužnog fizičkog prisustva“, naveli su²³.

Općenito, novinari i aktivisti su često tokom pandeije bili mete uvreda na internetu. Uvreda su stizale iz drugih medija, javnih zvaničnika, a ponekad i od anonimnih aktera, čime se ostvarivanje prava na slobodu izražavanja u Srbiji spustilo na nizak nivo, iako od četiri zemlje koje pokriva ovaj izveštaj, Srbija je već bila na nanajnižem mjestu prema rangiranju Reportera bez granica (93. mjesto) te je ocijenjena kao nesigurna zemlja za novinare²⁴. U drugom incidentu, albanska novinarka Sonila Meço doživjela je maltretiranje na internetu nakon što je na Facebooku kritizirala komentar jednog liječnika u vezi sa albanskim državljanima koji su bili zaustavljeni na granici sa susjednom Grčkom i kojima nije bio dozvoljen ulazak u zemlju²⁵. Sredinom marta građani Albanije dobili su neočekivanu glasovnu poruku putem mobilnog operatera Vodafone u kojoj ih je premijer Edi Rama savjetovao da peru ruke i “da se zaštite se od medija²⁶” u borbi protiv koronavirusa.

Ali nisu samo u Srbiji i Albaniji patili aktivisti, novinari i građani kada je riječ o njihovom pravu na izražavanje na internetu. U Bosni i Hercegovini bilo je slučajeva u kojima su građani novčano kažnjavani u skladu sa osporenom odlukom, uglavnom zbog njihovih objava na društvenim mrežama.²⁷ Na primjer, liječnik je novčano kažnjen kada je rekao da bolnica nema dovoljno opreme, a osoba iz Gradiške je kažnjena jer se navodno “ponašala tako da izaziva nered i paniku tokom vanredne situacije” i vrijeđala javna tijela u Republici Srpskoj, itd.

²¹ T. Curcic, J. Tomic, D. Djordjevic, Government Attempts to Restrict Reporting on Coronavirus, Center for Investigative Journalism of Serbia, 1 April 2020/ T.

²² Curčić, J. Tomić, D. Đorđević, Vlada pokušava da ograniči izveštavanje o koroni, Centar za istraživačko novinarstvo Srbije, 1. april 2020. godine

²³ M. Milojević, Preventing the spread of panic or 'disciplining' doctors and journalists, Radio Free Europe/Radio Liberty, 12 April 2020 / M. Milojević,

Sprečavanje širenja panike ili 'disciplinovanje' doktora i novinara, Radio Slobodna Evropa/Radio Liberty, 12. april 2020. godine

²⁴ Serbia's Authorities Must Respect Media Freedoms and Citizens' Rights to be Informed, Civil Rights Defenders, 11 April 2020 / Srpske vlasti moraju poštovati

medijske slobode i pravo građana na informisanost, Civil Rights Defenders, 11. april 2020. godine

²⁵ 24 Reporters without borders, Serbia/ Reporteri bez granica, Srbija

²⁶ Albania: journalist Sonila Meço receives torrent of abuse after Facebook post, Mapping Media Freedom, 7 April 2020 / Albanija: novinarka Sonila Meço nakon

objave na Facebooku dobila lavinu pretnji, Mapiranje medijskih sloboda, 7. april 2020. godine

²⁷ G. Erebara, Rama Takes his War on Media to Albanians' Phones, Balkan Insight, 13 March 2020 / G. Erebara, Rama svoj rat protiv medija vodi preko albanskih

telefona, Balkan Insight, 13. mart 2020

²⁸ Digital Rights in the Time of COVID-19, BIRD / Digitalna prava za vreme pandemije COVID-19, BIRD

NADZOR

Prema najnovijem izvještaju Freedom Housea, među zabrinjavajućim trendovima u vezi sa merama poduzetim tokom pandemijske krize COVID-19 je i opsežno prikupljanje vrlo osjetljivih ličnih podataka i uvođenje nametljivih (intruzivnih) tehnologija za nadzor građana, kao što su prediktivna policijska analitika, prepoznavanje lica i skeniranje termalnim kamerama²⁸. Da bi stvari bile još gore, ove mjere su se često uvodile bez adekvatnih zaštitnih mehanizama kojima bi se spriječila kršenja ljudskih prava.

Zbog pandemije Covid-19, zemlje Zapadnog Balkana pribjegle su pojačanim mjerama nadzora jer se stvorila atmosfera da se širenje bolesti može spriječiti i držati pod kontrolom samo ako se uvede strog nadzor nad ponašanjem građana. Ograničenja i zabrane kretanja (*eng.lockdown*), koja su se ponekad protezala i na nekoliko dana, također su trebala zadržati kontrolu nad velikim okupljanjima i gužvom. Na primjer, građani Albanije morali su preko portala E-Albanija dobiti dozvolu za izlazak iz



svojih domova kako bi mogli kupiti namirnice ili prošetati svoje kućne ljubimce. Dnevno je samo jedan član domaćinstva mogao dobiti dozvolu koja mu je omogućavala dva sata kretanja. Policija u glavnom gradu Albanije, Tirani, je također koristila i dronove kako bi pratila poštivanje mjera tokom zabrane kretanja.

Na primjer, građani Albanije morali su preko portala E-Albanija dobiti dozvolu za izlazak iz svojih

28 A. Shahbaz, A. Funk, False Panacea: Abusive Surveillance in the Name of Public Health, Freedom House, 2020 / A. Šabaz, A. Funk, Lažni lek: Zloupotreba nadzora u ime javnog zdravlja, Freedom House, 2020

domova kako bi mogli kupiti namirnice ili prošetati svoje kućne ljubimce²⁹. Dnevno je samo jedan član domaćinstva mogao dobiti dozvolu koja mu je omogućavala dva sata kretanja. Policija u glavnom gradu Albanije, Tirani, je također koristila i dronove kako bi pratila poštivanje mjera tokom zabrane kretanja.³⁰

U Srbiji, u kojoj je nacionalno vanredno stanje proglašeno sredinom marta i trajalo je do početka maja, Predsjednik države je na konferenciji za novinare održanoj ubrzo nakon uvođenja vanrednog stanja upozorio građane da se „prate italijanski telefonski brojevi“, pritom misleći na praćenje lokacija mobilnih telefona, zbog velikog broja građana Srbije koji su se tada vraćali u zemlju iz inostranstva i kojima su bile izdate obavezne naredbe za samoizolaciju³¹. Također je spomenuo i da postoji „druga metoda“ praćenja kretanja onih koji se riješavaju svojih telefona u pokušaju „da prevare vladu“, ali nije objasnio koja je to metoda.



Mjere pojačanog nadzora, uglavnom praćenje kretanja građana, onemogućile su rad novinara, aktivista i branitelja ljudskih prava, posebno u javnom prostoru, koji sve više postaje prostor distopijske kontrole³². Niko ne može sa sigurnošću reći da se nakon zaustavljanja pandemije napredni tehnološki alati, koji su uvedeni za suzbijanje koronavirusa, neće koristiti u druge svrhe - između ostaloga, da bi se ugušilo drugačije mišljenje i kritika vlasti?³³

U Beogradu, glavnom gradu Srbije, postavlja se ogroman sistem video nadzora koji se sastoji od hiljada kamera sa mogućnostima prepoznavanja lica, što je ozbiljno upozorenje za društveni aktivizam i rad u javnom interesu, jer se samo tkivo društva menja ako se ulice čitavog grada pokriju sistemom za pametni video nadzor³⁴.

Ograničavajući prava i slobode nesrazmjerno i neselektivno, sistem pametnog video nadzora u Beogradu postavljen je u suprotnosti sa nacionalnim i međunarodnim pravnim standardima i propisima. Njegova svrha nije jasno definirana, niti je, prije samog postavljanja, ustanovljen jasan i strog zakonski okvir za upotrebu sistema pametnog nadzora od strane policije na javnim mjestima. Zajednički projekt srpskih državnih vlasti i kineske kompanije Huawei, „Pametni grad“, razvija se na netransparentan način, bez objavljivanja informacija o uslovima ovog partnerstva i cijeni cjelokupnog sistema. Nije bilo javne rasprave o mogućem društvenom i političkom utjecaju ovih izuzetno nametljivih (intruzivnih) tehnologija³⁵. U Republici Srpskoj, jednom od entiteta u Bosni i Hercegovini, također je prijavljeno postavljanje intruzivnog video nadzora. Prema medijskom izvještavanju, Ministarstvo unutrašnjih poslova Republike Srpske nabavilo je više od 300 kamera, od kojih 66 kamera ima mogućnosti prepoznavanja lica.³⁶

29 M. Brändle, T. Brankovic, A. Dyrnishi, Democracy and the State of Emergency, Friedrich Ebert Stiftung, 18 May 2020 / M. Brendl, T. Branković, A. Dirmiši, Demokracija i vanredno stanje, Friedrich Ebert Stiftung, 18. maj 2020

30 Albanian Police Use Drones to Enforce Lockdown, Voice of America, 16 April 2020 / Albanska policija koristi dronove kako bi sprovela zabranu kretanja, Glas Amerike, 16. april 2020.

31 Government responses to COVID-19 adversely affect digital rights in the Balkans, International Freedom of Expression Exchange, 4 April 2020 / Reagovanja vlasti na COVID-19 negativno utiču na digitalna prava na Balkanu, International Freedom of Expression Exchange, 4. april 2020.

32 Ban biometric mass surveillance!, European Digital Rights, 13 May 2020 / Zabraniti masovni biometrijski nadzor!, European Digital Rights, 13. maj 2020.

33 The day after the pandemic: are we moving towards a dystopia of surveillance, SHARE Foundation, 2 April 2020 / Dan posle pandemije: idemo li ka distopiji nadzora, SHARE Fondacija, 2. april 2020.

34 Thousands of Cameras website: <https://hiljade.kamera.rs/en/home/> / Sajt hiljade kamera: <https://hiljade.kamera.rs/en/home/>

35 It is against the law and harmful for society to introduce the system of smart surveillance in Belgrade, Thousands of Cameras/ Protivzakonito je i štetno za društvo da se uvede sistem pametnog nadzora u Beogradu, Hiljade kamera

36 The Ministry of Interior set up facial recognition cameras: Where all we are being surveilled?, Istok, 28 July 2020 / Ministarstvo unutrašnjih poslova postavilo je kamere za prepoznavanje lica: gde nas sve snimaju? Istok, 28. jul 2020.

Kako su društva više nego ikad prije preusmjerila svoje funkcioniranje na internet, branitelji digitalnih prava naišli su na razne prepreke u svom radu. U nekoliko navrata su se novinari suočili sa ozbiljnim problemima u izvršavanju svoje uloge čuvara javnog interesa jer se ta uloga ne može u potpunosti izvršavati na internetu - potrebno je i izvještavanje sa terena. Stoga su novinarska udruženja insistirala da se novinari izuzmu iz policijskog sata. U Srbiji, na samom početku vanrednog stanja, Nezavisno društvo novinara Vojvodine zatražilo je od vlasti da razjasne uslove pod kojima se novinari mogu kretati tokom perioda zabrane kretanja³⁷. Konačno, profesionalnim novinarima je bilo dozvoljeno da izvještavaju sa terena ako su se prijavili za dozvole. Međutim, ovo se nije odnosilo na građane - novinare, blogere i druge koji nisu imali novinarske akreditacije, pa se pokazalo da je rad na daljinu za njih predstavljao prilično ograničenje.

U Albaniji je od početka godine bilo nekoliko rastjeranih protesta, poput komemorativnog skupa na Dan Evrope, organiziran od predstavnika civilnog društva 9. maja, kao i protesta protiv rušenja Narodnog pozorišta, veliki antirežimski protest koji je bio nasilno prekinut kada je uhapšeno 37 ljudi, uključujući i jednog novinara. Ipak, najveću zabrinutost izazvao je protest koji se održao sredinom decembra zbog smrti mladića kojeg je ubio policajac. Ovaj je događaj rezultirao uličnim nasiljem, a kao rezultat toga više od 300 građana je krivično gonjeno, a tri novinara su nasilno uhapšena³⁸. Jasno je da ovi slučajevi nasilja ometaju pravo na slobodno udruživanje u Albaniji i imaju zastrašujući učinak tokom ove krize.

Pored toga, urednica sa Kosova uhapšena je zbog kršenja policijskog sata iako je zapravo radila svoju posao³⁹. Tatjana Lazarević, glavna urednica informativnog portala Kossev, bila je na poslu kada je uhapšena, a iako je ubrzo puštena, jedan takav incident mogao je biti zastrašujući ne samo za druge novinare, nego i za bilo koga čiji rad podrazumijeva praćenje stanja na terenu. Na kraju, Ministarstvo unutrašnjih poslova Kosova pojasnilo je da se policijski sat ne odnosi na novinare i medijske radnike, ali ostaje nejasno jesu li i aktivisti koji štite ljudska prava također bili izuzeti iz policijskog sata.

U Bosni i Hercegovini, morala je da reaguje Institucija ombudsmana za ljudska prava BiH zbog ometanja rada branitelja ljudskih prava tokom krize⁴⁰. Naime, u Federaciji Bosne i Hercegovine konferencije za novinare Kriznog štaba su se održavale ili samo za ograničeni broj novinara ili bez fizičkog prisustva novinara, ili su dati odgovori samo na ona pitanja koja su prethodno bila poslana e-poštom. Stoga je Institucija ombudsmana za ljudska prava Bosne i Hercegovine izdala zvaničnu preporuku pozivajući vlasti da u najvećoj mogućoj meri osiguraju prisustvo novinara na konferencijama za novinare.

Slična situacija dogodila se i u Srbiji⁴¹. U jednom trenutku, na redovnim konferencijama za novinare u 15 sati, koje su održavali članovi Kriznog štaba, većini medija bilo je dozvoljeno isključivo slati unaprijed pitanja e-poštom. Ovo nije bila otvorena zabrana novinarima da dolaze na konferencije za novinare, iako su tamo svoje kamere imali samo Javni medijski servis RTS i državna novinska agencija Tanjug, a pitanja pojedinih novinara su u potpunosti bila preskočena. To je spriječilo novinare da ispune svoju ulogu čuvara javnog interesa, a činilo se da je njihov rad na daljinu nametnula ne samo pandemija, već i vlasti⁴².

37 NDNV: Enable journalists to work during curfew as well, Danas, 18 March 2020/ NDNV: Omogućite novinarima rad i za vreme policijskog časa, Danas, 18. marta 2020

38 Albanian authorities must prevent further police violence and uphold the right to freedom of peaceful assembly, Council of Europe, 15 December 2020/ Albanske vlasti moraju spriječiti dalje policijsko nasilje i podržati pravo na slobodu mirnog okupljanja, Savjet Evrope, 15. decembra 2020.

39 Digital Rights in the Time of COVID-19, BIRD/Digitalna prava u doba COVID-19, BIRD

40 M. Brändle, T. Branković, A. Dyrnishi, Democracy and the State of Emergency, Friedrich Ebert Stiftung, 18 May 2020/ M. Brändle, T. Branković, A. Dyrnishi, Demokratija i vanredno stanje, Friedrich Ebert Stiftung, 18. maja 2020.

41 No journalists at daily pandemic briefings, Serbian government says, N1, 10 April 2020/ Nema novinara na redovnim konferencijama o pandemiji, kaže Vlada Srbije, N1, 10. aprila 2020

42 Press freedom must not be undermined by measures to counter disinformation about COVID-19, Council of Europe, 3 April 2020 / Sloboda medija ne smije se podriivati mjerama za suzbijanje dezinformacija o COVID-19, Savjet Evrope, 3. aprila 2020.

Kao i na drugim područjima, tijekom pandemije branitelji ljudskih prava, aktivisti i drugi čuvari javnog interesa našli su se u situaciji koju nikada prije nisu doživjeli, posebno oni koji rade u manjim zajednicama. S obzirom na njihove kapacitete, kratkoročno i dugoročno gledano, čini se da je „nova normalnost“ težak izazov za građanski sektor u smislu održivosti. Izgradnja organizacije i nadahnuće ljudi za društveni aktivizam također postaje teže u kriznim vremenima, posebno uslijed ekonomskih pritisaka.

Finansijski, tehnički i organizacijski kapaciteti civilnog društva u velikoj mjeri zavise od grantova (bespovratnih sredstava) i projekata. Kulturu „crowdfundinga“ još treba razvijati na Zapadnom Balkanu, a u regiji vjerojatno ne postoje organizacije civilnog društva koje se mogu osloniti na mikro-donacije i članarine kao veći dio svoga prihoda. Međutim, zbog negativnog utjecaja pandemije na svjetsku ekonomiju, može se očekivati smanjenje donacija predstavnika drugih zemalja, poput ambasada i razvojnih agencija. U takvim okolnostima organičenih novčanih sredstava i resursa bit će teško omogućiti civilnog sektora i aktivizma.

Na primjer, CIVICUS je međunarodna mreža organizacija civilnog društva, koja je u martu 2020. godine objavila otvoreno pismo donatorima i pokroviteljima tražeći od njih što veću fleksibilnost, izvjesnost i stabilnost kada su u pitanju njihovi partneri i korisnici bespovratnih sredstava u ovim kriznim vremenima uslijed pandemije COVID-19⁴³. U pismu se navodi nekoliko načina na koje se to može učiniti:

- Saslušati partnere - korisnike bespovratnih sredstava i zajedno istražiti kako im se najbolje može pomoći u suočavanju sa ovom krizom, vjerujući da oni najbolje znaju šta im treba u njihovom vlastitom kontekstu;
- Potaknuti redizajniranje i premještanje planiranih aktivnosti i rezultata te dati jasna uputstva kako zatražiti odobrenje za ove promjene;
- Podržati nove i kreativne načine stvaranja kulture solidarnosti i interakcije uz poštovanje fizičke distance i drugih preventivnih mjera;
- Ponuditi veću fleksibilnost u isplati sredstava na temelju stvarnih potreba, pretvaranjem postojećih projektnih grantova u sredstva koja nisu striktno vezana za određenu svrhu ili isplatom dodatnih sredstava kako bi se povećale rezerve ili pokrili neočekivani troškovi, i
- Pojednostaviti procedure i vremenske okvire za izvještavanje i apliciranje kako bi grupe civilnog društva mogle bolje usmjeriti svoje vrijeme, energiju i resurse na pružanje podrške najugroženijima umjesto da pokušavaju zadovoljiti striktno zahtjeve izvještavanja i dubinske analize.

Jedan od glavnih razloga za zabrinutost organizacija za zaštitu ljudskih prava i građanskog sektora je upravo tehnička infrastruktura, odnosno njihovi sajtovi, serveri, e-mejllovi, radni uređaji itd. Naime, iskustvo fondacije SHARE u pružanju besplatne tehničke podrške i obuke pokazalo je da mnoge organizacije imaju oskudne resurse kada je riječ o IT aspektu njihovog rada, što znači da često nemaju svoje IT zaposlenike i da se u upravljanju svojom infrastrukturom oslanjaju na vanjske saradnike. U okolnostima pandemije, koja je dovela do radikalnih promjena u funkcioniranju društva i organizacija, cyber napadi velikih razmjera mogli bi imati pogubne posljedice za branitelje ljudskih prava zbog nedostatka odgovarajućih tehničkih i kadrovskih kapaciteta za ublažavanje napada i saniranje štete uzrokovane njime. To može značiti gubitak dragocjenih podataka prikupljenih godinama ili, na primjer, gubitak pristupa računima na društvenim mrežama ili e-mail porukama organizacije. Rad od kuće, također, može predstavljati rizik za digitalnu sigurnost jer mjere sigurnosti koje zaposlenici poduzimaju u svojim domovima i privatnim uređajima možda nisu na istom nivou kao i standardi organizacije.

43 Open letter: Donors and supporters must act to ensure civil society resilience against COVID-19 pandemic, CIVICUS, 19 March 2020 / Otvoreno pismo: Donatori i pokrovitelji moraju djelovati kako bi osigurali otpornost civilnog društva tokom pandemije COVID-19, CIVICUS, 19. marta 2020.

Suočeni sa globalnom pandemijom, aktivisti i organizacije širom svijeta prisiljeni su preseliti najveći dio komunikacije i saradnje u digitalni prostor. Iako je posljednjih 20 godina obilježeno ubrzanom digitalizacijom mnogih procesa u svakodnevnom životu, čini se da je sve do sada bilo priprema za iznenadnu tranziciju koja se dogodila u samo nekoliko nedelja na početku obaveznog karantina koji je bio uveden diljem svijeta.

Takva iznenadna promjena donijela je neke naizgled logične, ali ishitrene odluke o izboru tehnologija, usluga i softvera koje bi trebale nadomjestiti nova ograničenja i fizičku udaljenost. Razumno je prihvatiti rješenja koja su popularna i jednostavna za upotrebu, ali postavlja se pitanje u kojoj mjeri ona ispunjavaju uslove koji su neophodni za siguran rad aktivista i organizacija civilnog društva. Uz to, odabiri koje sada donosimo uvelike će utjecati na to koje će tehnologije organizacije i društvo u cjelini dugoročno prihvatiti, pa je drugo pitanje više etičke prirode: želimo li usvojiti vlasničke (komercijalne) usluge koje donose profit, ili rješenja otvorenog koda koja se kreiraju u zajednici i kako to utječe na diverzifikaciju i decentralizaciju digitalnog ekosistema.

Odabir i razumijevanje tehnologija koje aktivisti koriste u svom radu imaju ključni utjecaj na njihov integritet i sigurnost, na otpornost njihovih organizacija i održivost društva koje gradimo.



Zbog prirode njihovog posla, aktivisti za ljudska prava češće su izloženi provalama u informaciono-sigurnosne sisteme, pojačanom nadzoru i presretanju komunikacija, pokušajima cenzure tehničkim napadima, neovlašćenom pristupu i ugrožavanju ličnih podataka, prijetnjama, pritiscima i drugim metodama čiji je cilj gušenje slobode govora i onemogućavanje njihovog rada. Otpornost na sve te prijetnje u digitalnom prostoru zavisi od tehnologija koje koristimo.

Nažalost, većinu alata na koje se danas oslanjamo stvorile su kompanije čiji se poslovni modeli temelje na izvlačenju i monetizaciji (unovčavanju) ličnih podataka i navika korisnika ovih alata. Sada svi jako dobro znamo da smo dio jedne "ekonomije nadzora", ali i dalje koristimo ove alate jer ih svi drugi koriste i vrlo je lako osloniti se na njih.

Međutim, sa tehničkog gledišta, glavni nedostatak većine komercijalnih i popularnih usluga i aplikacija je taj što imaju zatvoreni kod. Zatvoreni (vlasnički) kod možemo usporediti sa crnom kutijom - ne znamo što se u njoj događa i kamo idu naši podaci, tako da je korištenje ovih alata pitanje povjerenja, a kad je riječ o korporacijama, vjerujemo im vrlo malo ili im uopće ne vjerujemo. Ovaj kompromis koji smo spremni prihvatiti kako bismo bez ikakvog napora koristili tehnologiju može biti vrlo opasan.

Pored toga što se korisničkim podacima trguje u komercijalne svrhe, dokazano je da sigurnosne službe mogu vrlo lako presretati komunikaciju i imati direktan uvid u naše metapodatke. Koristeći savremene alate za cyber špijunažu, vlade širom svijeta izvode ciljane napade na političke neistomišljenike i često angažiraju zlonamjerne hakere koji sofisticiranim tehničkim metodama i socijalnim inženjeringom uspijevaju neprimjetno prodrijeti u dobro zaštićene sisteme. Konačno, dobro poznata nelagoda koju osjećamo svaki put kad neki od popularnih servisa na koje se oslanjamo na kratko postane nedostupan poziva nas da se zapitamo što će se dogoditi kada ovi servisi prestanu raditi na duže vrijeme, jer nije pitanje hoće li se to dogoditi, već samo kada će se to dogoditi.

S druge strane, primjena i korištenje potpuno odgovornih i sigurnih rješenja otvorenog koda često zahtijevaju mnogo više truda i više resursa. Za određene usluge ili servise potrebno je angažirati sistemske inženjere koji će ih instalirati, posjedovati ili zakupiti servere, održavati čitav sistem, provesti dodatnu obuku, a mnoge organizacije nemaju takve kapacitete. Međutim, ova vrsta ulaganja omogućava veću kontrolu nad protokom podataka, kao i dugoročnu održivost informacionih sistema. Danas je vrijeme kada o tehnologiji unutar organizacije treba razmišljati jednako kao i o upravljanju, finansijama ili ljudskim resursima.

Kada se ova pitanja uzmu u obzir, u odnosu na raspoložive resurse, pojedinci i organizacije mogu odlučiti na kojem će nivou unaprijediti svoj pristup tehnologiji i izbor alata za rad. To može biti ublažavanje - smanjenje rizika, postignuto malim koracima ka poboljšanju tehnološkog okruženja: recimo, zamjenom određenih alata za koje već postoje dokazane alternative, što zahtijeva minimalni napor kako bi se postigle ova promjena. Ovaj pristup neće riješiti probleme, ali će ih smanjiti, olakšavajući razumijevanje tehnologije i povećavajući vjeru u buduće veće izbore i odluke. Ako na ovu temu gledamo malo ambicioznije, to može biti potpuna promjena u pristupu i paradigmi kada je tehnologija u pitanju. Zahtijeva ozbiljnije ulaganje resursa, vremena i energije, ali dugoročno donosi mnogo veću nezavisnost u kontroli podataka, kao i veliki sistemski i tehnološko-politički zaokret.

Ispod je pregled i opis nekih od najsveobuhvatnijih alata i rješenja koje zajednica trenutno može ponuditi, a koji bi mogli obezbijediti sigurnu komunikaciju i timski rad, ne samo tokom krize, već i u vremenima koja dolaze.

SIGURNA KOMUNIKACIJA

Aplikacije za razmjenu instant poruka (alternativna rješenja za WhatsApp, Facebook Messenger, Viber i druge)

Signal - Ova aplikacija za komunikaciju radi na većini platformi i operativnih sistema i jedan je od pionirskih napora komuniciranja putem šifriranih (enkriptiranih) poruka. Pomoću ove aplikacije možete slati tekstualne poruke, što uključuje i komunikaciju grupe korisnika, slanje glasovnih poruka, dijeljenje fotografija i video sadržaja. Također su nedavno dodali podršku za chat (razgovor) i video pozive. Ova aplikacija služi i kao zamjena za aplikacije za slanje SMS-a / MMS-a, ali je potrebno da ju sve strane u komunikaciji koriste kako bi se mogao koristiti njen vlastiti protokol. Ovo je projekt otvorenog koda, koji vodi neprofitna organizacija i u potpunosti se financira donacijama, što mu omogućava rad bez unovčavanja podataka svojih korisnika. Dok se još ova aplikacija razvijala, aktivisti širom svijeta koristili su je za sigurnu komunikaciju u represivnim režimima i situacijama pojačanog policijskog nadzora, poput protesta u demokratskim društvima.

Wire - Jedna od najpopularnijih aplikacija sličnih Signalu. Iako su se paralelno razvijale, aplikacija Wire je imala neke prednosti koje ostale u to vrijeme nisu imale, poput šifriranog (enkriptovanog) grupnog chata ili mogućnosti registracije i korištenja usluge bez unošenja broja mobilnog telefona. Ponuda takvih specifičnih mogućnosti koje su orijentirane na dodatnu privatnost u odnosu na konkurenciju pokazala se vrlo važnom za napredak tehnologije i raznolikost cjelokupnog ekosistema. Budući da je aplikacija Wire također aplikacija otvorenog koda i ne prodaje podatke o svojim korisnicima, financira se pružanjem naprednih usluga za poslovne korisnike.

Telegram - Iako ova platforma nije u potpunosti zasnovana na otvorenom kodu (aplikacija je otvorenog koda, ali ono što se događa na serverima kompanije nije), do sada nije bilo poznatih slučajeva kompromitiranja podataka aktivistakoji koriste Telegram, a ovo je definitivno jedna od najpopularnijih usluga za sigurnu komunikaciju, posebno za razmjenu informacija između velikih grupa ljudi putem grupa i kanala. I upravo zbog ove jednostavnosti komunikacije u većem obimu (odnosno za veliki broj korisnika), intuitivnog sučelja i velike popularnosti u široj javnosti, Telegram je često opcija za aktiviste za ljudska prava. Iako je platforma izgradila odnos povjerenja sa svojim korisnicima, savjetuje se oprez jer sistem nije u potpunosti utemeljen na otvorenom izvoru, poslovni model nije potpuno jasan i ne garantira dugoročnu održivost.

Internet/video konferencijski sistemi (alternativna rješenja za Zoom, Skype, Google Meet, Microsoft Teams, itd.)

Jitsi Meet

U posljednjih nekoliko godina, mnoge organizacije i aktivisti počeli su koristiti Jitsi Meet kao primarnu platformu za video pozive zbog nekoliko ključnih karakteristika. Ova platforma je među prvima u otvorenom izvoru uvela šifriranje (enkripciju) za usluge ove vrste, dok istovremeno ne zahtijeva instaliranje posebne aplikacije, već može raditi izravno na svim najpoznatijim internetskim preglednicima samo klikom na jedan link. Za organizacije sa većim resursima, platforma se može preuzeti i instalirati na vlastitim Linux serverima, što nudi dodatni nivo sigurnosti.

BigBlueButton

Konkurentski Zoom u svijetu vlasničkih i komercijalnih alata za video konferencije ima dostojnog protivnika u softverskom paketu BigBlueButton koji je predstavnik otvorenih i odgovornih tehnologija. Platforma ima brojne značajke koje zadovoljavaju potrebe velikih javnih događaja na netu, poput administracije korisnika, dijeljenja multimedijskog sadržaja, prikazivanja prezentacija, alata za zajednički rad na ploči/flipchartu, privatnog i javnog chata, manjih soba za sastanke i još mnogo toga. Jedini zahtjev je instalacija vlastite instance na Linux serverima ili korištenje instance drugih organizacija koje ga mogu učiniti dostupnim za upotrebu, što je sve češći slučaj u civilnom sektoru.

SIGURNI GROUPWARE SOFTVER

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

Mattermost

Organizacije koje imaju prilično opsežnu internu komunikaciju i materijale često su pretrpane i izgubljene zbog velikog obima e-mail korespondencije. Platforme poput Mattermosta definitivno su alati koji mogu smanjiti teret na poštanske sandučice (*eng.inbox*) i poboljšati komunikaciju kroz tematske kanale za chat, intuitivnu pretragu, indeksiranje i sigurno dijeljenje dokumenata i datoteka. Nakon početnog instaliranja na vlastitom ili unajmljenom serveru organizacije, nije potrebno puno održavanja i administracije, pa je pogodno za organizacije sa manjim tehnološkim kapacitetima. Svi podaci su šifrirani (enkriptirani), a projekt se financira pružanjem podrške i dodatnih usluga poslovnim korisnicima.

Element

Donedavno poznat pod nazivom «Riot.im», Element je chat klijent koji koristi moderni Matrix protokol - vanjski komunikacijski protokol koji je razvijen kao standard otvorenog koda i čiji je cilj omogućiti interoperabilnost između različitih chat usluga i video konferencija. To praktično znači da se poruke mogu razmjenjivati sa korisnicima najpopularnijih platformi, uključujući i vlasničke servise kao što su Apple iMessage, Facebook Messenger, WhatsApp, Discord, Slack, i naravno sa korisnicima aplikacija otvorenog koda kao što su Signal, Mattermost, IRC, Telegram i druge.

Ostali alati

U zavisnosti od potreba organizacije, treba pomenuti nekoliko drugih alata koji se mogu koristiti kao alternativna rješenja za servise velikih kompanija koje prikupljaju podatke.

Etherpad je web uređivač teksta koji omogućuje saradnju u realnom vremenu (alternativno rješenje za Google Docs) koji također možete instalirati na svoj server, ali postoje i besplatne instance na internetu poput **“Riseup Pad”** koji nudi ovu uslugu besplatno, ne prikuplja IP adrese i poštuje privatnost korisnika. Aplikaciji se može pristupiti i putem VPN-a ili **Tor pretraživača**, koje svakako morate koristiti ako želite sakriti svoju aktivnost na internetu.

Istu tehnologiju koju koristi Tor za *onion* usmjeravanje koristi i **OnionShare**, usluga sigurnog dijeljenja datoteka. Ukratko, i možda potpuno banalno, OnionShare radi tako da generira šifriranu (enkriptiranu) adresu datoteke na kompjuteru kojoj sa druge strane može pristupiti samo korisnik koji koristi Tor protokol.

I na kraju, kada je u pitanju sigurno skladištenje podataka i alternativne usluge u „oblaku“ (zamjene za Dropbox ili Google Drive), **Nextcloud** je u prvom planu. Zahtijeva instalaciju i održavanje na vlastitim serverima, što definitivno zahtijeva dodatne resurse u organizaciji, ali nudi i najviši nivo kontrole podataka.

Konačno, ovi alati i njihovo usvajanje u svakodnevnom radu ne pružaju potpuni imunitet protiv sigurnosnih rizika, ali nam daju veću nezavisnost i podstiču na daljnje razumijevanje tehnologije. Otpornost pojedinaca i njihovih organizacija dalje zavisi od razumijevanja ekosistema digitalnog prostora i odnosa tehnologije sa društvom. Zbog toga je važno da uz prihvaćanje odgovornih alata razumijemo i tokove podataka, arhitekturu nadzora i poslovne modele tehnoloških korporacija koje sve više centraliziraju internet modernom kolonizacijom digitalnog prostora. Razumijevanje i prihvaćanje odgovornih tehnologija podstiču razvoj alternativa, dok povećana pismenost zajednica i društva u cjelini podstiče slobodu, otvorenost i decentralizaciju interneta, što je postalo preduslov za otpornost demokratije.

Zaključak

U trenutnoj situaciji, napori vlada da uvedu restriktivne propise i nametljive (intruzivne) tehnologije pod izgovorom borbe protiv pandemije, trebali bi biti pod većim nadzorom branitelja ljudskih prava, koji također trebaju biti oprezniji. Mjere uvedene u budućnosti mogu sadržavati odredbe koje mogu negativno utjecati na slobodu izražavanja, pravo na privatnost i druga srodna prava i slobode, poput prava na protest ili slobode okupljanja, i koje mogu biti tako „upakovane“, da neće biti ni vidljive na prvi pogled. Stoga civilni sektor posebno treba biti oprezan i propitivati mjere koje se naizgled uvode radi suzbijanja širenja koronavirusa, ali mogu biti uvod u stalni nadzor ili druga nesrazmjerna ograničenja ljudskih prava.

Trenutne okolnosti, iako su vrlo izazovne za branitelje ljudskih prava, aktiviste i civilni sektor generalno, također mogu biti prilika za uvođenje alternativnih i sigurnijih tehničkih alata, kao što su slobodan softver i softver otvorenog koda. Iako prelazak na rad od kuće i primjena novih alata u tehničkoj infrastrukturi organizacije može rezultirati određenim poteškoćama, na taj način se može osigurati dugoročnu fleksibilnost i otpornost u kriznim vremenima, posebno za manje kolektive i organizacije koji nemaju puno resursa za ulaganje. Na primjer, projekt Galileo nudi braniteljima ljudskih prava i drugim akterima od javnog interesa resurse za ublažavanje tehničkih napada, spriječavanje eksploatacije njihove ranjivosti i zaštitu integriteta podataka⁴⁴.

Međutim, kada je riječ o radu na daljinu, organizacije moraju osigurati da njihovi zaposlenici kod kuće provode iste digitalne sigurnosne standarde kao i u poslovnim prostorijama. Pored toga, otvoreniji pristup usvajanju i upotrebi besplatnog softvera i softvera otvorenog koda omogućuje zajednici da se spremnije zalaže za to da Internet bude slobodan, otvoren i decentraliziran.



⁴⁴ More information about Project Galileo is available at: <https://www.cloudflare.com/en-gb/galileo/> Više informacija o projektu Galileo dostupno je na: <https://www.cloudflare.com/en-gb/galileo/>



LJUDSKA PRAVA

U USLOVIMA PANDEMIJE

