DIGITALNE HRONIKE

–

DECENIJA SLOBODE I REPRESIJE NA INTERNETU U SRBIJI

PREDGOVOR

Svest o internetu kao mogućem političkom prostoru u Srbiji začeta je tokom masovnih studentskih i građanskih protesta 1996/97. godine. U vreme kada su tradicionalni mediji bili pod čvrstom kontrolom režima, mali broj nezavisnih pionira našao je alternativni kanal za razmenu informacija. Taj prostor, tada tek u povoju, delovao je kao autentična i neukrotiva margina javne sfere – mesto izvan domašaja države, još nestrukturisano po uzusima moći, regulisano samo neposrednim potrebama onih koji ga naseljavaju. Ali ne zadugo.

Danas, tri decenije kasnije, internet opslužuje centralni teren političkog, ekonomskog i društvenog sukobljavanja. Nekadašnje utočište za one koji su lišeni glasa, izraslo je u složen ekosistem medijskih kanala i infrastruktura podložnih nadzoru, manipulaciji i komercijalizaciji. Pretnje su sve sofisticiranije – od zakonskih ograničenja i regulatornih pritisaka, do algoritamskog utišavanja, targetiranih napada i sistemske nevidljivosti.

U tom promenjenom pejzažu, povrede digitalnih prava nisu izuzeci, već pokazatelji dubljih društvenih i političkih trendova. U početku su se javljale kao izolovani incidenti, praćeni fragmentarnim informacijama i glasinama koje je bilo teško potvrditi: pritisci zbog objava na mrežama, napadi na sajtove nezavisnih medija, selektivno uklanjanje sadržaja. I naša reakcija isprva je bila sporadična, bez strategije i kontinuiteta. Prekretnicu su označile velike poplave 2014. godine, kada su pokušaji da se kritički glasovi na internetu utišaju postali vidljivi, koordinisani i politički artikulisani. U trenutku krize, internet je služio kao ključno sredstvo informisanja i građanske mobilizacije; upravo tada se javljaju i prve sistemske intervencije u digitalne slobode. Internet postaje novi front tenzija između moći i autonomije građana.

Iz te spoznaje proistekla je potreba da se formuliše trajniji odgovor. Ne samo zbog pojedinačnih slučajeva, već zbog rastuće težnje da razumemo obrasce – da beležimo, analiziramo i prepoznajemo mehanizme moći u digitalnom okruženju. Tako je nastao SHARE Monitoring, program kontinuiranog praćenja digitalnih prava u Srbiji i okosnica naše misije.

Publikacija koja je pred vama obuhvata prvih deset godina monitoringa. Ona nije puka hronologija incidenata, već i mapa promena: tehničkih, političkih, pravnih i kulturnih. Svaki slučaj koji smo zabeležili nosi u sebi trag šire dinamike – odnosa moći, otpora i neizvesnosti. Naš cilj nije samo da dokumentujemo, već i da razumemo kako se digitalna prava oblikuju, šta ih ugrožava i kako se ona brane. Iznad svega, ovo je i poziv na budnost jer se prava – i u digitalnom i u fizičkom prostoru – grade, gube i osvajaju iznova, svakog dana.

Na pragu druge decenije monitoringa, suočeni smo sa brojnim globalnim izazovima: tehnološke inovacije su dobile novu, zapanjujuću brzinu; učvršćuje se komercijalna kontrola nad infrastrukturom; državni nadzor je normalizovan, a javna sfera fragmentisana. Za to vreme, na ulicama i trgovima širom Srbije ponovo vri pobuna.

Priču o pravima i slobodama na internetu u Srbiji uveli smo u pisanu istoriju. Kršenja digitalnih prava sada su dokumentovana i služe kao osnov da se o tim pravima misli strateški, solidarno i dugoročno.

Andrej Petrovski i Danilo Krivokapić
Beograd, maj 2025.

IMPRESUM

IZVRŠNI UREDNICI: Andrej Petrovski i Danilo Krivokapić

UREDNICE: Mila Bajić i Snežana Bajčeta

AUTORI:

Javno informisanje: od poplava do paralelnog informisanja | Mila Bajić

Kratka istorija nadzora: od metapodataka, preko kamera do špijunskih softvera | Bojan Perkov

Kritična infrastruktura: nespretna digitalizacija, neodgovornost države i posledice | Bojan Perkov i Snežana Bajčeta

Ranjive grupe i digitalno isključivanje: diskriminacija kao stub digitalne nejednakosti | Mila Bajić

Tehnologija: od internet neutralnosti do platformizacije | Snežana Bajčeta

Jedna decenija i sedam izbornih godina | Milica Jovanović

LEKTURA: Milica Jovanović

DIZAJN I PRELOM: Olivia Solis Villaverde

ILUSTRACIJE: Ruben Cruces-Perez

POJMOVNIK

algoritamsko odlučivanje
Primena kompjuterskih sistema prilikom obrade velikih količina podataka (ponekad i ličnih) u cilju izvođenja zaključaka potrebnih za donošenje odluka. Na primer, algoritamsko odlučivanje može da se koristi da bi se odredilo koje vrste reklama kompanije plasiraju korisnicima u zavisnosti od njihovih digitalnih navika. Ovi podaci se prikupljaju netransparentno i tačnost zaključaka koje izvode ovi algoritmi može biti veoma upitna.

astroturfing
Veštačko preuveličavanje podrške i angažmana (*engagement*) na društvenim mrežama, uglavnom kroz korišćenje armija botova za objavljivanje određenih ideja i komentara. Ovakva vrsta podrške deluje kao organska, čime se manipuliše javnost da lakše prihvata određene ideje zbog navodno široke podrške koju uživaju. Takvim taktikama mogu da pribegavaju političke partije, kompanije, pa i državne institucije.

biometrija
Krovni termin koji obuhvata proces merenja bioloških karakteristika kako bi se one pretvorile u biometrijske podatke, i/ili naknadnu obradu biometrijskih podataka ili podataka zasnovanih na biometriji, kao i čitavu oblast izrade i primene ovih tehnologija

biometrijska identifikacija
Proces mašinskog predviđanja identiteta osobe, putem poređenja njenih biometrijskih podataka sa podacima iz određene baze ili više baza (npr. nacionalna baza podataka ličnih karata, baza podataka traženih lica), iznad određenog praga verovatnoće.

biometrijski nadzor
Sistem koji osmatra biometrijske karakteristike ljudi na bilo koji način koji nije pod punom kontrolom i sa pristankom osobe na koju se podaci odnose.

botovanje
Kolokvijalno se odnosi na osobe koje preko svojih naloga najčešće na društvenim mrežama i vestima na onlajn portalima ostavljaju komentare podrške ili kritike, u zavisnosti od zadatih instrukcija. Iako se izvorno reč bot odnosi na automatizovane programe namenjene da replikuju ljudsko ponašanje, u široj javnosti se tako nazivaju i ljudi koji po komandi ostavljaju poruke i pružaju podršku na internetu.

curenje vs probijanje (*leak vs breach*)
Curenje (*leak*) se odnosi na nenamerno otkrivanje, objavljivanje ili gubljenje podataka iz informacionih sistema. Do curenja može doći kada osobe koje su za sistem nadležne ne preduzmu dovoljne ili odgovarajuće mere za njegovu zaštitu.

Probijanje (*breach*) odnosi se na neautorizovan pristup podacima unutar informacionih sistema kako bi se ukrali, prikupili i/ili objavili podaci. Probijanje mogu da izvrše uzbunjivači ali i zlonamerni akteri, najčešće sa ciljem iznude pod pretnjom da će prikupljeni podaci biti objavljeni.

velike tehnološke kompanije (*big tech*)
Tehnološki giganti, najčešće se odnosi na pet najvećih američkih kompanija – Alfabet, Epl, Meta, Amazon i Majkrosoft, kojima se poslednjih godina pridružuju i kineske – grupa Baidu, Alibaba, Tencent i Šaomi. Ove kompanije zajedno drže monopol nad najvažnijim digitalnim tržištima usluga kao što su pretraživanje interneta, oglašavanje, komunikacija i umrežavanje.

veštačka inteligencija
Kapacitet mašina da opaze, analiziraju i razumeju informacije, koji se može primeniti u autonomnom obavljanju zadataka u različitim oblastima kao što su prepoznavanje govora, kompjuterski vid ili obrada prirodnog jezika.

gongo
„Nevladine" organizacije koje sponzoriše vlada u cilju širenja svojih političkih stavova i interesa u društvu. Veza između takvih organizacija i vlasti često nije jasno obelodanjena, pa može doći do konfuzije u javnosti, budući da oponašaju autentične građanske organizacije od kojih se razlikuju po ciljevima, aktivnostima i porukama koje plasiraju.

digitalno nasilje
Prenošenje ustaljenih nasilničkih praksi u digitalni prostor. Proganjanje, zlostavljanje, napadi, uvrede i zloupotrebe koje se odigravaju u digitalnom prostoru uz pomoć digitalnih alata. Perpetuiraju klimu nasilja u društvu i najčešće targetiraju već ranjive i marginalizovane grupe.

efekat zebnje (*chilling effect*)
Obeshrabrivanje učešća u javno-političkom životu, najčešće kroz ograničavajuće i preteće prakse vlasti i njenih saradnika. Širenje zebnje u društvu vodi u autocenzuru i ućutkavanje kritike.

isključivanje
Prakse isključivanja iz javnog života u digitalnom prostoru najčešće se postižu napadima kao što su pretnje i uvrede preko društvenih mreža i organizovanim prijavljivanjem targetiranih naloga sa ciljem njihovog gašenja ili odustajanja. Na ovaj način se targetiranim osobama šalje poruka da je bolje da se suzdrže od pokretanja određenih tema i iznošenja svojih stavova. Isključivanje je čest cilj napada na žene i druge marginalizovane grupe na internetu, posebno kada osporavaju ustaljene prakse i stereotipe.

moderacija
Uređivanje sadržaja na društvenim mrežama, medijskim portalima i drugim delovima interneta. Moderacija sadržaja može biti srazmerna i neophodna, ali bez adekvatnih pravila može da prevazilazi te okvire i pređe u cenzuru. Neke od najvećih platformi za deljenje sadržaja danas koriste automatizovanu moderaciju koja retko uzima u obzir sve potrebne nijanse, kao što su rasne, etničke, nacionalne, rodne i druge predrasude i stereotipi, kao i dati kulturni kontekst pojedinačnih zemalja u kojima operišu.

državni nadzor
Često se odnosi na vlast koja na prodorne i netransparentne načine nadgleda građane i sve koji stupaju na njenu teritoriju. Cilj je uspostavljanje kontrole u društvu i pojačano prisustvo vlasti u svim oblastima života. U ovakvim državama, vlast nadgleda sve i uvek, uglavnom protivpravno i u suprotnosti sa ljudskim pravima i slobodama.

operacije uticaja (*influence operations*)
Organizovani napori prikupljanja informacija i širenja propagande protiv neistomišljenika i neprijatelja. Cilj ovih operacija je diskreditacija i uticaj na javno mnjenje kroz predstavljanje informacija na način koji favorizuje određenu stranu. Operacije uticaja uglavnom upošljavaju individue, zajednice, nekada i poznate ličnosti, pa i medije, kako bi učvrstili narativ koji zastupa određena strana. Mogu biti orkestrirani iznutra, od strane domaćih aktera (vlasti ili privatnih organizacija) ili spolja, preko inostranih činilaca.

platformizacija
Institucionalna transformacija digitalnog ekosistema prema infrastrukturnim, ekonomskim i normativnim principima digitalnih platformi. Ova promena zahvata sve sfere društvenog života, profesije i kulturne prakse i vođena je platformskim vrednostima.

paralelno informisanje
Uspostavljanje informativnog ekosistema u kojem postoji strukturno defavorizovanje pravovremenog, sveobuhvatnog i tačnog informisanja. Takvu vrstu ograničenja uglavnom uspostavljaju vlasti putem kontrolisanih medija i aktera koji nastoje da usmeravaju javno mnjenje u pravcu bespogovorne podrške vladajućih stranaka.

ekonomija pažnje (*attention economy*)
Poslovne strategije fokusirane na osvajanje pažnje korisnika kao osnovne vrednosti u daljim transakcijama. Primera radi, društvene mreže često upošljavaju netransparentne algoritme kako bi što duže zadržale korisnike na svojim servisima, gde im se u isto vreme plasiraju reklame za robu i usluge.

podaci o ličnosti
Podaci koji se odnose na konkretnu osobu koju ti podaci identifikuju ili je, uz neke dodatne alate ili dopunske podatke, mogu identifikovati. Ime i prezime, adresa, otisak prsta, zdravstveni karton, istorija aktivnosti na internetu (metapodaci, šerovi, lajkovi, klikovi), istorija pretrage interneta, IP adresa kompjutera ili smartfona i slično predstavljaju primere podataka o ličnosti. Podaci o ličnosti mogu biti zloupotrebljeni na razne načine, stoga je pravilno rukovanje njima uređeno Zakonom o zaštiti podataka o ličnosti.

sajber incident
Svaki događaj koji negativno utiče na poverljivost, integritet ili dostupnost informacionog sistema ili informacija koje se u njemu obrađuju, a koji može dovesti do gubitka kontrole nad sistemom, ometanja ili prekida rada sistema, ili kompromitovanja informacija.

spajver (*spyware*)
Špijunski softver je vrsta zlonamernog softvera (malware) koja prikuplja podatke iz inficiranog sistema i prosleđuje ga dalje, obično onome ko ga je napravio (službe bezbednosti ili drugi zlonamerni akteri). S takvim malverom, neovlašćeno se mogu preuzeti lozinke, lični podaci, prepiske itd.

ružni blizanci (*ugly twins*)
Sajtovi koji svojim vizuelnim identitetom oponašaju izgled autentičnih sajtova čime dovode korisnike u zabludu, bilo da im je cilj finansijska prevara ili širenje lažnih vesti. Najčešće koriste vrlo slična imena i veb adrese kao sajtovi koje plagiraju. Ovaj trend u medijskoj sferi posebno je aktuelan u cilju kompromitacije nezavisnih medija i dezinformisanja javnosti.

PRE UVODA: STUDENTI SU USTALI

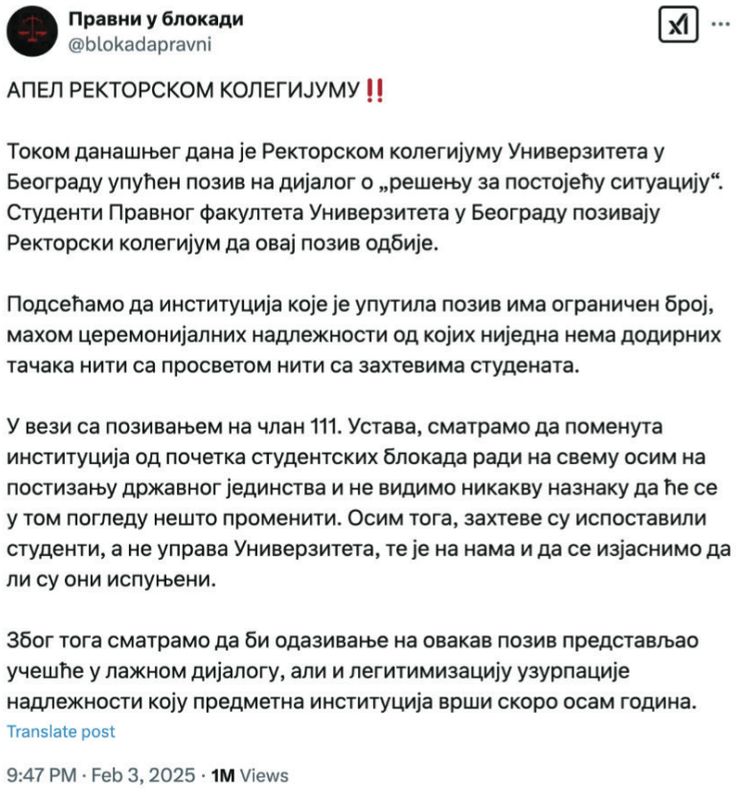
05. mart 2025. godine

U samoj završnici prve decenije praćenja povreda digitalnih prava, počeli su najveći studentski protesti u istoriji Srbije - a prema nekim tvrdnjama i najveći studentski protesti u Evropi posle 1968.[1] Ovi protesti započeli su blokadama fakulteta širom zemlje nakon pada nadstrešnice na novosadskoj Železničkoj stanici 1. novembra 2024. godine, kada je poginulo 15 ljudi. Građani su ključne uzročnike ovog tragičnog događaja prepoznali u dugogodišnjoj korupciji i neodgovornosti institucija kao servisa apsolutne vlasti u zemlji. To ih je motivisalo da izađu na ulice i iskažu svoje nezadovoljstvo odavanjem počasti stradalima.

Nakon što su se i studenti Fakulteta dramskih umetnosti pridružili građanima na ulici, fizički su napadnuti od strane nekoliko osoba među kojima su bili i funkcioneri SNS-a.[2] Studenti FDU su na ovaj napad odgovorili potpunom blokadom svog fakulteta i upućivanjem liste zahteva vlastima, među kojima je iznošenje kompletne dokumentacije radova na nadstrešnici i procesuiranje onih koji su napali studente. Do danas nije ispunjen nijedan studentski zahtev.

Plenumski princip donošenja odluka bez pojedinačnih vođa, jasno artikulisani zahtevi i smisleni javni nastupi postepeno su izgradili čvrst studentski front kojem su se priključili gotovo svi fakulteti u zemlji, čime je zaustavljen povratak u ustaljenu svakodnevicu i smeštanje slučaja nadstrešnice u red tragedija iz prošlosti. Jasna determinisanost i organizovanost ohrabrila je građane i prilično uzdrmala vlast koja se prvi put nakon 12 godina našla pred zahtevom da omogući da nadležne institucije efikasno, odgovorno i u skladu sa zakonima rade svoj posao. To bi podrazumevalo napuštanje ključnih principa vladavine SNS, prema kojima je odlučivanje o svim pitanjima u zemlji skoncentrisano u rukama jednog čoveka.

Studenske blokade su rezultirale i važnom promenom u društvenom diskursu koji je tokom prethodne decenije bio centriran na Aleksandra



Правни у блокади
@blokadapravni

АПЕЛ РЕКТОРСКОМ КОЛЕГИЈУМУ ‼️

Током данашњег дана је Ректорском колегијуму Универзитета у Београду упућен позив на дијалог о „решењу за постојећу ситуацију“. Студенти Правног факултета Универзитета у Београду позивају Ректорски колегијум да овај позив одбије.

Подсећамо да институција које је упутила позив има ограничен број, махом церемонијалних надлежности од којих ниједна нема додирних тачака нити са просветом нити са захтевима студената.

У вези са позивањем на члан 111. Устава, сматрамо да поменута институција од почетка студентских блокада ради на свему осим на постизању државног јединства и не видимо никакву назнаку да ће се у том погледу нешто променити. Осим тога, захтеве су испоставили студенти, а не управа Универзитета, те је на нама и да се изјаснимо да ли су они испуњени.

Због тога сматрамо да би одазивање на овакав позив представљао учешће у лажном дијалогу, али и легитимизацију узурпације надлежности коју предметна институција врши скоро осам година.

Translate post

9:47 PM · Feb 3, 2025 · **1M** Views

Izvor: @blokadapravni, https://x.com/blokadapravni/status/1886516840945287601

Vučića kao glavnog aktera. Nalazi iz praćenja izbora 2023. godine još jednom su potvrdili da su gotovo svi najčitaniji mediji u zemlji apsolutno podređeni pružanju beskompromisne podrške vladajućoj stranci i predsedniku.[3] Takođe, ukupna javna agenda u Srbiji u potpunosti je definisana prema temama i pitanjima koja daju prostor za neograničeno favorizovanje ličnosti i vlasti Aleksandra Vučića. Uz to, način na koji se definišu i uokviruju teme od javnog značaja u potpunosti je usklađen sa političkim, partijskim i ličnim interesima vrha strukture vladajuće partije. Studentski protest prvi put nakon više od decenije ustaljene javne dinamike, uspeo je da redefiniše tok i okvire javnih tema i diskusija u zemlji.

Umesto direktne komunikacije sa predsednikom, koji se prethodnih godina pozicionirao kao ključna adresa za rešavanje svih problema u državi i društvu, studenti su jasno istakli da u instituciji Predsednika ne vide nadležnost koja bi mu omogućila da se bavi njihovim zahtevima, u skladu sa ovlašćenjima propisanim Ustavom. Povratak na pojmove ustavnosti, nadležnosti, granica ovlašćenja i slično, i dosledno javno komuniciranje u tim okvirima, rezultiralo je konačnim razbijanjem čvrste uzurpatorske matrice u kojoj je moć locirana isključivo u rukama jedne osobe.

Uprkos ovoj tektonskoj promeni, Vučić je u svom paralelnom informativnom i javnom prostoru nastavio i čak intenzivirao svoje prisustvo. Tako je od 2. novembra u proseku imao više od tri objave na Instagramu dnevno, i to bez storija, dok je njegov nalog na TikToku, gde je i dalje relativno nov korisnik, emitovao video objave svaki drugi dan. Na televiziji se od početka godine pojavljivao u proseku dva puta dnevno, što bi značilo da ako se ovaj trend nastavi, njegovo prisustvo na televiziji ove godine biće udvostručeno u odnosu na prethodnu kada nam se sa malih ekrana obraćao u proseku jednom dnevno.[4] Mada su ti sadržaji delimično nastali kao direktan odgovor na tekuće događaje u društvu, oni dobrim delom izgledaju kao

simulacija normalnosti uprkos trenutnoj situaciji, što predstavlja uobičajenu strategiju vlasti za borbu protiv neistomišljenika.

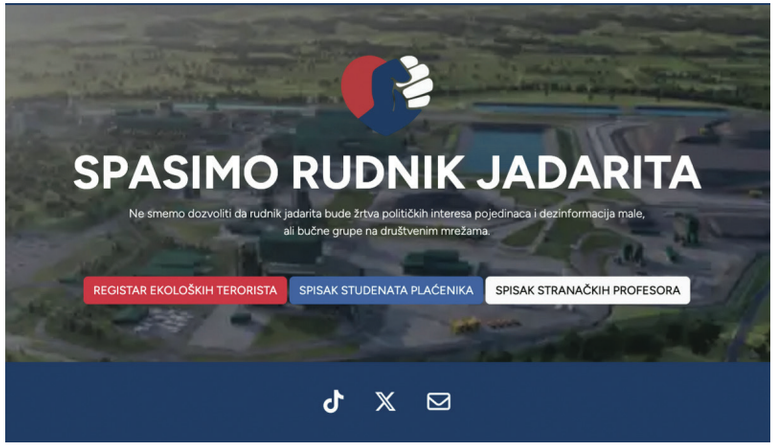
Okupirani javni prostor koji zauzimaju tradicionalni mediji, vladajuća koalicija koristi gotovo isključivo za obračun sa neistomišljenicima - studentima i građanima koji traže istinu, odgovornost i pravdu. Na prorežimskim onlajn medijima trendovi su još gori, pa se bez ikakvih granica širi mržnja i dezinformacije i izazivaju tenzije u društvu. Početkom januara, na portalu Novosti osvanuo je tekst u kojem se za dvojicu studenata, koji su lažno okarakterisani kao „vođe" protesta, navodi da su strani državljani koji su došli u Srbiju kako bi destabilizovali zemlju. Kao dokaz za svoje tvrdnje, medij je priložio slike njihovih pasoša,[5] što predstavlja flagrantno kršenje prava na privatnost i sa sobom povlači pitanje - odakle Novostima uvid u lična dokumenta dvojice studenata?

novosti.rs

HRVATI VOĐE BLOKADA NA FON-U U BEOGRADU: Još jedna potvrda snažno...

Ipak, hajka na studente preko onlajn medija ovde nije stala. Ubrzo su počele da kruže priče o mentalnom stanju studentkinje koja je ujedno i aktivistkinja Inicijative mladih za ljudska prava i koja je već mesecima targetirana u tabloidima i prorežimskim medijima. Kao i do sada, nijedan od tih tekstova ne sadrži bilo kakve informacije ili činjenice, pa se čini da pre svega imaju zadatak da oponašaju kredibilan medijski izvor, koji se zatim širi kao talas dezinformacija putem društvenih mreža, ili kao referenca u javnim nastupima predstavnika vlasti.

Sredinom januara, kopacemo.com objavio je spisak prosvetara koji su politički aktivni. Na spisku se nalaze isključivo profesorke, profesori, učiteljice i učitelji afilisani sa opozicionim strankama uz dodatak još nekih, uglavnom netačnih informacija sa ciljem diskreditovanja. Nekoliko meseci ranije, sajt je objavio i spiskove studenata „plaćenika" i ekoloških „terorista", sa istim ciljem usmerenih napada i širenja dezinformacija. Ovakvi spiskovi i sajtovi najčešće se kriju iza pokreta koje niko ne potpisuje imenom i prezimenom i koji očigledno rade u službi režimske politike.



Digitalni prostor se pokazao kao jedno od najdinamičnijih bojnih polja tokom ovih demonstracija. U januaru se na sajtu sns.rs našla poruka podrške studentskim i građanskim protestima nakon čega je sajt ekspresno ugašen. Uprkos činjenici da se na adresi sns.rs ne nalazi zvanična prezentacija vladajuće stranke, već je taj domen godinama u vlasništvu privatnog lica, jedina razlika je bila u tome što je od januara ugašeno direktno preusmeravanje sa ove adrese na zvaničnu adresu sns.org.rs. Još zanimljivije od brzine uklanjanja stranice jeste činjenica da je BIA prijavila sajt zbog zloupotrebe, iako sajt ni na koji način ne ugrožava nacionalnu bezbednost, što bi bio jedini razlog zbog čega bi ova bezbednosna agencija mogla da se bavi sadržajima sajtova na internetu, a svakako ne stranačkim.[6] Nakon reagovanja SHARE Fondacije, sajt je ubrzo vraćen.

To su samo neke od taktika iz arsenala vlasti koja se služi digitalnom represijom u želji da konsoliduje i održi poluge moći. S obzirom na transnacionalnu prirodu digitalne represije, lako je uočiti ovakve obrasce i u drugim zemljama u kojima postupke vlasti osporavaju borkinje i borci za ljudska prava i slobode. Zbog toga je od velike važnosti osvajanje slobode na svim dostupnim frontovima, a to uključuje i digitalni. Studentski pokret pokazao je

da je moguće probiti barijeru ćutanja i cenzure i oživeti nadu u svim slojevima društva. Mada je isprva bilo dilema i pitanja o političkim ubeđenjima generacije Z, kao i njihove motivacije da se uključe u društvenopolitičke borbe, ispostavilo se da je ta generacija znatno više liberalna i anti-autoritarno nastrojena od prethodnih. [7]

Sa svojim gotovo urođenim poznavanjem društvenih mreža, studenti su lako uspeli da privuku pažnju i iznesu svoje zahteve i stavove na jasan i razumljiv način. Efikasno digitalno komuniciranje mnogo je doprinelo širenju poruka ovog pokreta, mobilisanju šire javnosti i izgradnji nove vrste zajedništva koja se ne deli po generacijskim, ideološkim, teritorijalnim niti drugim granicama. U skladu sa time, svaki fakultet ubrzo nakon stupanja u blokadu otvorio je svoj nalog na X i Instagramu, neki su se proširili i na TikTok. Svi ovi nalozi zajedno uspeli su da stvore novu mrežu za širenje i plasiranje informacija, čime su okupili široku zajednicu kojoj su oni postali važan informativni izvor. Ovakvi „neformalni" kanali komunikacije koji nisu posredovani medijima uskoro su se proširili i na lokalne zajednice, komšiluke i

druge aktivne građanske grupe koji su na ovaj način počele da razmenjuju informacije o protestima, aktivnostima i akcijama. Signal, Telegram, pa čak i Vajber koji je najzastupljeniji među starijom populacijom, postali su glavni alati za pružanje otpora i samoorganizovanje građanki i građana. Zanimljivo je da su ove grupe, stranice i nalozi doprineli otkrivanju i identifikovanju onih koji su tokom blokada raskrsnica studente i građane verbalno i fizički napadali, kao i popisivanje svih preduzeća i lokala koji su eksplicitno odbijali da pruže podršku protestima i podržavali vladajuću stranku.

Izvor: @studentblokade, https://x.com/studentblokade/status/1863739523143790932

Primer Srbije pokazuje kako kontinuirana derogacija ljudskih prava u digitalnom okruženju efikasno briše prostor za slobodno izražavanje, informisanje, organizovanje i aktivizam, čineći digitalni svet produženom rukom analogne svakodnevice. Poslednji trend vlasti da veštačkoj inteligenciji pripisuje procurele snimljene instrukcije za izazivanje nasilja nad studentima pokazuje slabo poznavanje najnovijih tehnologija, ali i odlučnost da ih podredi svojim propagandnim tokovima. S druge strane, situacija kojoj svedočimo ukazuje da svako iskustvo digitalne slobode može da se prelije u Novi Sad, Despotovac, na Slaviju i bilo koju ulicu i trg. Trenutno takvoj slobodi gledamo u susret.

Sa svojim gotovo urođenim poznavanjem društvenih mreža, studenti su lako uspeli da privuku pažnju i iznesu svoje zahteve i stavove na jasan i razumljiv način. Efikasno digitalno komuniciranje mnogo je doprinelo širenju poruka ovog pokreta, mobilisanju šire javnosti i izgradnji nove vrste zajedništva koja se ne deli po generacijskim, ideološkim, teritorijalnim niti drugim granicama. U skladu sa time, svaki fakultet ubrzo nakon stupanja u blokadu otvorio je svoj nalog na X i Instagramu, neki su se proširili i na TikTok. Svi ovi nalozi zajedno uspeli su da stvore novu mrežu za širenje i plasiranje informacija, čime su okupili široku zajednicu kojoj su oni postali važan informativni izvor. Ovakvi „neformalni" kanali komunikacije koji nisu posredovani medijima uskoro su se proširili i na lokalne zajednice, komšiluke i druge aktivne građanske grupe koji su na ovaj način počele da razmenjuju informacije o protestima, aktivnostima i akcijama. Signal, Telegram, pa čak i Vajber koji je najzastupljeniji među starijom populacijom, postali su glavni alati za pružanje otpora i samoorganizovanje građanki i građana. Zanimljivo je da su ove grupe, stranice i nalozi doprineli otkrivanju i identifikovanju onih koji su tokom blokada raskrsnica studente i građane verbalno i fizički napadali, kao i popisivanje svih preduzeća i lokala koji su eksplicitno odbijali da pruže podršku protestima i podržavali vladajuću stranku.

Primer Srbije pokazuje kako kontinuirana derogacija ljudskih prava u digitalnom okruženju efikasno briše prostor za slobodno izražavanje, informisanje, organizovanje i aktivizam, čineći digitalni svet produženom rukom analogne svakodnevice. Poslednji trend vlasti da veštačkoj inteligenciji pripisuje procurele snimljene instrukcije za izazivanje nasilja nad studentima[8] pokazuje slabo poznavanje najnovijih tehnologija, ali i odlučnost da ih podredi svojim propagandnim tokovima. S druge strane, situacija kojoj svedočimo ukazuje da svako iskustvo digitalne slobode može da se prelije u Novi Sad, Despotovac, na Slaviju i bilo koju ulicu i trg. Trenutno takvoj slobodi gledamo u susret.

UVOD

Digitalni prostor danas predstavlja ključno okruženje za društveno-političku borbu, diskusiju i debatu, sponu sa međunarodnim događajima, mesto gde su se gotovo sve industrije delimično ili potpuno preselile, koristeći najbolje i najgore što ima da ponudi. Mediji koriste internet kako bi došli do što šire publike, a u toj potrazi služe se raznim alatima za osvajanje pažnje i angažmana. Ipak, posebno u slučaju informativnih medija, postoji ozbiljna opasnost da se u toj trci počnu oslanjati na netransparentne i neetičke prakse. U tom smislu, može se tvrditi **da su sami mediji postali medijum,** odnosno da je samo njihovo postojanje kao vesnika informacija u digitalnoj eri važnije od poruke koju šalju. Bilo da su u pitanju mediji koji se mogu okarakterisati kao glasnogovornici vlasti ili oni koji se određuju kao glas potlačenih i neprivilegovanih, ili pak mediji svih građana i građanki, njihova uloga u informativnom ekosistemu određena je interesima koje zastupaju. Ova uloga određuje o kojim događajima će izveštavati i na koji način, ali i kako će tretirati prava svoje publike.

Razvoj tehnologija promenio je, u prvom redu, ulogu medija, spajajući nekada jasno diferenciran svet proizvođača i publike vesti. Na udaru je najpre bio informativni integritet tradicionalnih proizvođača vesti. Interaktivnost društvenih mreža omogućila jene samo široku proliferaciju informacija, već i platformu za diseminaciju dezinformacija, lažnih vesti i propagande. Najzad, mogućnosti veštačke inteligencije tek pokazuju obrise svog delovanja na svet informisanja, kuratorstva vesti, uređivanja i donošenja ključnih odluka u novinarskoj profesiji.

Arhitektura interneta u ranim fazama dosta je dosledno oslikavala digitalnu transformaciju i umrežavanje društva kao globalne procese. Međutim, kako je rastao značaj digitalnog prostora, potreba za fragmentacijom postajala je sve veća i uglavnom je pratila nacionalne okvire. Ovo je u jednu ruku bio rezultat rastućeg digitalnog tržišta gde se profit nametnuo kao primarni cilj, a velike tehnološke kompanije su se pozicionirale kao ključni akteri u oblikovanju ali i kontroli novog digitalnog prostora. Kako su društvene mreže i druge platforme koje pružaju usluge sve više naseljavale internet, **rasparčavanje digitalnog okruženja** je postalo neminovno.

Uz to, nacionalni interesi država su se takođe pojačali. Rastuća fragmentacija regulacije digitalnog prostora se u pojedinim slučajevima, kao što su Kina i Rusija, pokazuje zabrinjavajuće tendencije, vodeći u centralizaciju informacija, cenzuru i kršenja ljudskih prava.[9] Nedostatak globalnog konsenzusa o pravima i slobodama u digitalnom prostoru u zavisnosti od geolokacije pristupa, otvara čitavo polje potencijalnih opasnosti i neizvesnosti. U Srbiji, ali i mnogim drugim zemljama, država u digitalnom prostoru nastoji **da se postavi kao kontrolor radije nego regulator,** odnosno da pravila u digitalnom prostoru upodobi sopstvenim interesima, a na štetu građanki i građana, javnosti, ljudskih prava. Nebrojeno je slučajeva u kojima država pokazuje isključivo reaktivni umesto proaktivnog pristupa povredama prava u digitalnom okruženju. Relevantno zakonodavstvo ili kasni ili se ne primenjuje efikasno ili potpuno izostaje u oblastima u kojima su neophodni pažljivo razvijeni mehanizmi koji bi suzbili različite oblike urušavanja prava i sloboda i omogućili značajnu rekompoziciju digitalnog okruženja.

Nasilje počinjeno u oflajn prostoru i dalje se posmatra kao primarna vrsta nasilja sa kojom se ljudi susreću u svakodnevnom životu. Međutim, nasilje koje se dešava u digitalnom prostoru je sveprisutno, u nekim slučajevima podjednako, a u nekima čak i kompleksnije i drastičnije od onog u fizičkom okruženju. Mnoga istraživanja pokazuju da je onlajn nasilje u kontinuiranom porastu, pogotovo u vremenima političke i društvene nestabilnosti kao što su pandemija koronavirusa, izbori, krize i slično. Ipak, i dalje postoji zabluda da je

nasilje doživljeno u digitalnom prostoru manje štetno nego ono počinjeno u neposrednom fizičkom okruženju. Ovakav pristup nasilju počinjenom u digitalnom svetu lako vodi u relativizaciju pojedinih oblika nasilja koje su svojstvene tom okruženju, kao što su sajber proganjanje, širenje štetnih i neistinitih sadržaja u cilju diskreditacije i ućutkivanja, ali i onih vrsta nasilja koje su u digitalnom prostoru samo pojačane, kao što su otkrivanje ličnih podataka (doksovanje), manipulacija sadržaja, govor mržnje, diskriminacija, vređanje i pretnje.

S tim u vezi, jasno je da je **digitalno okruženje samo proširilo prostor za već utvrđene matrice štetnog ponašanja.** Patrijarhalne strukture koje su generacijama prisutne, vrlo brzo i lako su se transponovale u digitalno okruženje, služeći se tehnologijom za adaptaciju mrežama. Automatizovani sistemi zasnivaju se na zastarelim, pristrasnim nalazima i podacima i iz njih izvode zaključke koji mogu biti opasni pogotovo po marginalizovane i ugrožene društvene grupe. Nepotpune informacije koje za cilj imaju širenje panike i dezinformisanje javnosti pospešene su brzinom i dalekosežnošću društvenih mreža, kao i padom poverenja u tradicionalne izvore informisanja, i ujedno su uspele da se transformišu u uspešne strategije za ostvarivanje zarade.

Digitalni prostor u Srbiji svakako jeste globalno određen, ali je i posebno oblikovan u okolnostima specifičnog društveno-političkog konteksta, slabosti digitalnog tržišta, nerazvijenih institucija i predominantne uloge koju država nastoji da uspostavi u ovom okruženju. Dok se velikim tehnološkim kompanijama pripisuje važna uloga u svetskoj politici, tržišnim kretanjima i globalnoj preraspodeli moći, građanke i građani Srbije stoje **između platformski organizovanog digitalnog sveta i države koja je mnogo više zainteresovana da politički trijumfuje** u novim okolnostima, nego da uspostavi sistem zaštite prava, sloboda i demokratije.

KONCEPTUALNA SKICA

Tokom analize desetogodišnje baze slučajeva povreda ljudskih prava u digitalnom okruženju zabeleženo je pet koncepata koji bliže opisuju stanje u Srbiji. Ovi koncepti zajedno predstavljaju svojevrsnu mapu uma srpskog interneta, kao i pet ključnih oblasti koje nude uvid u (ne)promenjive stubove koji opisuju i oblikuju povrede digitalnih prava korisnica i korisnika.

PRIVATNOST

U doba hiperumreženosti, privatnost se pozicionirala kao jedna od najvažnijih vrednosti. Privatnost kao lično pravo trenutno se nalazi na meti raznih aktera – od države i privatnih kompanija, do zlonamernih pojedinaca. Ugrožavanje privatnosti može imati različite oblike; u digitalnom okruženju najveće pretnje predstavljaju neovlašćeno i netransparentno prikupljanje i čuvanje podataka, kao i njihovo naknadno korišćenje u druge svrhe, često bez saglasnosti.

PRAVO NA INFORMISANJE

Prema Univerzalnoj deklaraciji o ljudskim pravima, „svako ima pravo na slobodu mišljenja i izražavanja, što obuhvata i pravo da ne bude uznemiravan zbog svog mišljenja, kao i pravo da traži, prima i širi informacije i ideje bilo kojim sredstvima i bez obzira na granice".[10] Pravo na pravovremeno, tačno i sveobuhvatno informisanje je ključno za pravilno funkcionisanje demokratskog poretka i počiva na poverenju u izvore informisanja, u ovom slučaju medije i one koji kreiraju vesti.

DIGITALNA INFRASTRUKTURA

Ovaj koncept odnosi se na digitalne sisteme, tehnologiju i kompanije od vitalne važnosti za funkcionisanje društva i privrede. Iako su počele uglavnom kao digitalni pružaoci usluga, ove infrastrukture su zbog svog dometa i neraskidivosti sa savremenim

životom postale krucijalne za funkcionisanje, čime su postale deo kritične infrastrukture društva. Neadekvatna zaštita te infrastrukture poslednjih godina sve češće dovodi do ugrožavanja prava građanki i građana kao korisnika javnih usluga. Ova infrastruktura danas uključuje i velike tehnološke platforme koje su postale sveprisutne u eri tehnološkog razvoja i digitalne ekspanzije širom sveta. Njihov primarni cilj je profit, zbog čega mogu značajno doprineti podrivanju ljudskih prava i sloboda. Takođe, digitalnoj infrastrukturi pripadaju i segmenti tradicionalnih infrastruktura koje su vitalne za funkcionisanje države (energetika, zaštita životne sredine, saobraćaj, IKT itd.), a koji se tokom sopstvenog razvoja digitalizuju.

DRŽAVNA KONTROLA

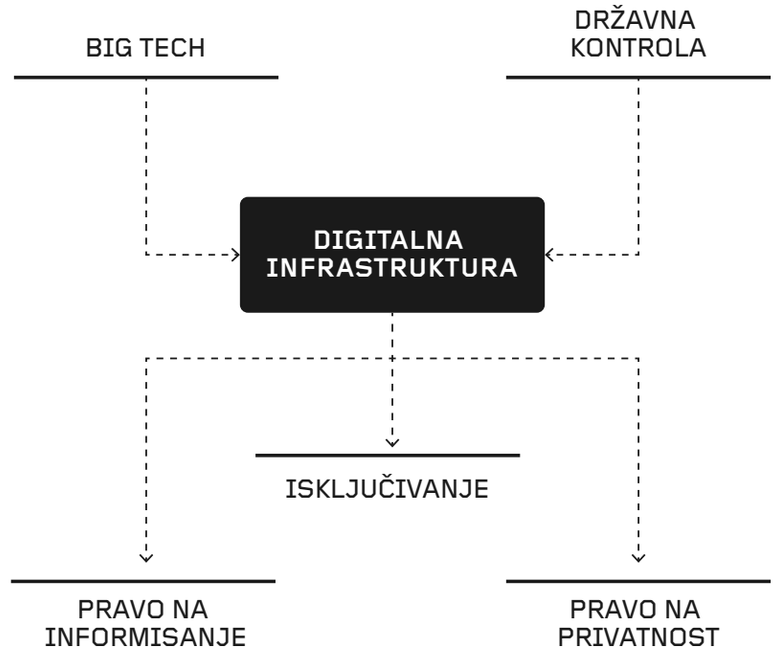
Država kroz razne strategije i mahinacije teži da zadrži kontrolu nad svojim stanovništvom, da nadzire i diktira svoju agendu, dok sa druge strane vodi računa o onima koji je kritikuju i u skladu sa time reaguje. Neke od najzastupljenijih zabeleženih taktika su kontrola medijskog okruženja, uticaj na popularne narative na društvenim mrežama kroz simulaciju spontane i apsolutne podrške.

ISKLJUČIVANJE

Strategije društvenog isključivanja odnose se na različite vidove ograničavanja pristupa javnom prostoru i informacijama određenim grupama i pojedincima i pojedinkama. Cilj je izolacija i ostrakizovanje, najčešće kao odgovor na iznete stavove i uverenja, svojevrsno kažnjavanje. Društveno inspirisano isključivanje najvidljivije je na društvenim mrežama. Međutim, isključivanje može dolaziti i od različitih struktura moći, najčešće onih koje su u sprezi sa državom. Medijske radnice i radnici, aktivistkinje i aktivisti, članice i članovi civilnog društva i marginalizovane grupe posebno su na meti ovakvih taktika.

VELIKE TEHNOLOŠKE KOMPANIJE

Velike tehnološke kompanije imaju centralnu poziciju na globalnom tržištu digitalnih usluga. Njihova monopolistička pozicija i nesrazmerno velika moć u odnosu na druge čini ih ključnim akterima digitalnog ekosistema. Ove kompanije uspostavljaju pravila, principe i strukturu ukupnog digitalnog okruženja, a u skladu sa profitno definisanim vrednostima i ciljevima i zahvaljujući platformskom mehanizmu koji je u centru njihovog poslovanja. Zbog ovakvog profitno orijentisanog pristupa, usluge koje ove kompanije nude, najčešće društvene mreže, mogu biti pogodne za autoritarne i represivne vlade koje teže da koncentrišu svoju moć i priguše ljudska prava i slobode.

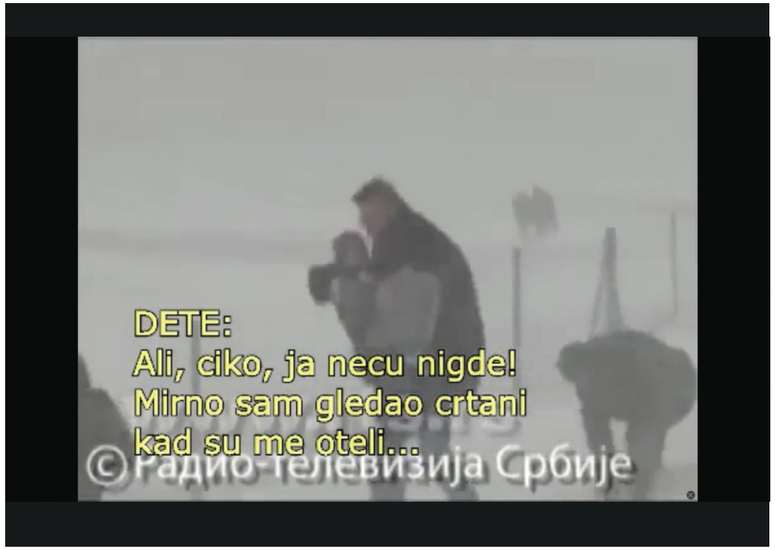


JAVNO INFORMISANJE: OD POPLAVA DO PARALELNOG INFORMISANJA

KAKO JE SVE POČELO

Pre deset godina, u martu 2014. godine, održani su vanredni parlamentarni izbori u kojima Srpska napredna stranka odnosi ubedljivu pobedu. Iako postoji mnogo faktora koji su omogućili da SNS tada ostvari ubedljivu pobedu sa više od milion glasova razlike, posebno je značajna uloga koju je digitalni prostor imao u ovoj predizbornoj kampanji. Naime, tadašnja digitalna događanja predstavljala su odskočnu dasku za većinu zloupotreba i manipulacija koje su obeležile prethodnu deceniju. Takođe, ovi izbori predstavljali su prekretnicu u načinu na koji se pristupa istraživanju digitalnih prava i sloboda, kao i razumevanju njihovog značaja u oblikovanju javnog mnjenja.

Na početku 2014. godine, ogromna snežna oluja pogodila je zemlju i stvorila priliku da tadašnji prvi potpredsednik Vlade Aleksandar Vučić krene u akciju spašavanja. Tako se i desilo – ubrzo su osvanuli snimci Vučića koji kroz smetove nosi i spašava dete u sada dobro poznatom Feketiću. Neki su ovo videli kao herojski čin, drugi kao manje više tipično skupljanje političkih poena u kampanji, dok su treći odlučili da je snimak odličan materijal za šalu. Ubrzo je na internetu osvanuo isti taj video kome su dodati titlovi koji su aludirali na to da je cela akcija nameštena predstava za televizijske kamere. Vučić je satirično prikazan kao Supermen, Isus i druge dobro poznate ličnosti. Ipak, nakon nekoliko dana, video je uklonjen sa interneta bez mnogo objašnjenja i niko nije bio siguran šta se sa njim dogodilo. Video je više puta ponovo kačen na Jutjub ali je svaki put ekspresno uklonjen, a kada je tadašnji šef internet tima SNS Mario Maletić na Tviteru upitan kako uspevaju tako brzo svaki put da uklone sadržaj, odgovor je bio – *um caruje, a i masa ljudi dobro dođe*.[11] U kontekstu naše priče, ovo se može posmatrati kao prvi dobro zabeležen i popularizovan slučaj uklanjanja sadržaja usled organizovanog prijavljivanja.



Nikola Momčilović, „prisluškivanje ppv-a“, https://www.dailymotion.com/video/x1at500

Samo nekoliko meseci kasnije, poplave koje su pogodile Srbiju i nanele velike štete potvrdile su da smo se između ostalog, nalazili na početku bujice povreda digitalnih prava u Srbiji. U želji za pravovremenim i tačnim vestima, građanke i građani pokušavali su da se informišu o prirodnoj katastrofi koja je pogodila razne delove zemlje ali i o nemogućnosti države da pruži adekvatnu pomoć. Umesto toga, razne vesti i portali polako su postajali nedostupni, i to upravo oni koji su bili kritični prema odgovoru vlasti na poplave. Onlajn portal Teleprompter koji je objavio nekoliko tekstova, uključujući i snimke sa mesta poplava, brzo se našao na meti napada koji su se lako mogli protumačiti kao cenzura.[12] Napadani su i mali portali kao što je „Kolumnista“ koji je 19. maja objavio tekst „Kratak uvod u diktaturu“.[13] U ovom tekstu nalazili su se snimci iz Svilajnca, Krupnja i drugih mesta koja su takođe bila pogođena poplavama a o kojima se malo pričalo u kojem je autor zauzeo veoma kritički ton prema vlasti. Ubrzo nakon objavljivanja, sadržaj portala postao je nedostupan. Napadi su prvo dolazili u vidu direktnih pretnji redakciji portala, a zatim su usledili i tehnički napadi, i vrlo je brzo postalo jasno da je u pitanju cenzura sadržaja koji se kritički odnosio prema reakciji države na poplave i evakuaciju stanovništva.

U to vreme, slučajevi digitalne cenzure i dalje su bili sporadični i samim tim nisu u široj javnosti predstavljali razlog za brigu. Ipak, nakon afere „Feketić“, polako je postajalo jasno da je upravljanje digitalnim sadržajima predstavljalo novo informaciono bojno polje u političkom životu Srbije. Važno je napomenuti da je inicijalna reakcija medija ali i šire zajednice bila veoma proaktivna – svi uklonjeni tekstovi i sadržaji brzo su objavljivani na drugim portalima i na taj način su uspeli da odole potpunoj cenzuri u digitalnom prostoru. Iako u ovom slučaju uspešan, ovakav tip otpora pokazao je da je vreme za reviziju i usavršavanje taktika ućutkivanja.

Prvih pet godina monitoringa digitalnih prava i sloboda u Srbiji obeležili su tehnički napadi, najčešće na nezavisne i lokalne medijske portale. Ovo je predstavljalo svojevrsni pritisak na medije koji su već uveliko tvorci i distributeri informacija i u digitalnom prostoru. Monitoring u prvim godinama uglavnom mapira i razvoj sistema tehničkih napada usmerenih na onlajn informacioni ekosistem.[14] Onesposobljavanje usluge, i naknadno činjenje sadržaja nedostupnim, je početkom 2014. godine bio jedan od najčešće zabeleženih oblika tehničkih napada na medije. Godinama su se taktike ometanja rada onlajn medija razvijale, a neki od najviše zabeleženih oblika podrazumevali su činjenje sadržaja nedostupnim putem tehničkih metoda (DDoS napadi), neovlašćen pristup sistemima i računarske prevare. Napadi na dostupnost sadržaja, poput DDoS napada, preovladavali su u gotovo svim godinama praćenja, posebno tokom društvenih događaja od većeg značaja. Ovi napadi su uglavnom bili usmereni na preopterećivanje servera kako bi se onlajn sadržaj učinio nedostupnim korisnicima.

Jedan od prvih slučajeva koji je najavio izazove po informisanje u digitalnom prostoru desio se u decembru 2013. godine, kada je tekst o odobravanju korišćenja službenog vozila ćerki guvernerke Narodne banke Srbije Jorgovanke Tabaković uklonjen sa sajta Radija 021, što je objašnjeno kao odluka uredničkog kolegijuma. Centar za istraživačko novinarstvo Srbije (CINS) preneo je tekst, a nedugo zatim njihov portal našao se pod tehničkim napadom usled koga je tekst obrisan. Slična stvar desila se na portalu Autonomija, odakle je tekst takođe uklonjen pod nejasnim okolnostima nakon tehničkih poteškoća sa sajtom.[15]

I dalje među najzastupljenijima stoji slučaj Peščanika, koji se više puta nalazio na meti tehničkih napada, od onesposobljavanja pravilnog funkcionisanja sajta što je čitaocima onemogućavalo pristup portalu, do neovlašćenog ubacivanja tekstova. Nakon što je u maju 2014. godine objavljen tekst o plagiranom doktoratu tadašnjeg ministra policije Nebojše Stefanovića,[16] sajt je oboren usled velikog broja organizovanih i targetiranih napada.[17] Kako je navedeno iz odeljenja za visokotehnološki kriminal, botovska mreža od oko 550 servera je istovremeno slala veliki broj zahteva prema severu medija i na taj način onesposobila njegovo delovanje. Jasno je bilo odmah da je napad direktna osveta za objavljeni tekst ali to ni na koji način nije obeshrabrilo Peščanik da prestane da se bavi ovom i drugim društveno korisnim temama, što je sa sobom donelo još mnoštvo napada, kako u 2014. tako i u 2015. godini. Od 2015. do 2020. godine zabeleženo je skoro 80 tehničkih napada na medije, od kojih je samo pet dobilo sudski epilog i presudu.[18]

Napadi na tehničku strukturu medija i danas predstavljaju ozbiljan problem i alat za ućutkivanje nepodobnih medija. Razlog zbog kojeg ovakvi napadi i dalje opstaju je zato što su jeftini i jednostavni za izvesti, i dok je teško otkriti počinioce, mogu da stvore ozbiljne komplikacije za medije koji se nađu na meti.[19]

U junu 2017. godine, SHARE Labs je objavio prvi deo svog istraživačkog serijala priča o metodama političko-informacionog ratovanja u Srbiji.[20] Ova analiza težila je da razume na koje načine su politički akteri u Srbiji koristili različite digitalne kanale i taktike kako bi oblikovali javno mnjenje i manipulisali informacijama. Ona je takođe predstavljala i genealogiju monitoringa digitalnih prava i internet sloboda u Srbiji, koji je SHARE Fondacija pokrenula 2014. godine nakon majskih poplava, sa primarnim ciljem beleženja, ali i razumevanja raznolikih fenomena zarobljavanja onlajn prostora u svojstvu kontrole, kako informacija, tako i javnosti.[21] SHARE Fondacija je odlučila da zabeleži ove slučajeve, prvenstveno kako bi pokazala primere nove vrste digitalne represije koji mogu postojati u onlajn prostorima. Nažalost, ovakvi slučajevi nastavili su da se dešavaju i ubrzo je monitoring povreda digitalnih prava i internet sloboda zaživeo kao jedan od ključnih stubova rada SHARE-a. Deset godina kasnije, monitoring predstavlja jedinstvenu bazu podataka sa više od devetsto slučajeva, koja može da doprinese razumevanju urušavanja ljudskih prava i sloboda u digitalnom prostoru iz nekoliko uglova. Prevare, pretnje i manipulacije poprimale su razne oblike u digitalnom prostoru, i samim tim dovele do nekoliko glavnih zaključaka.

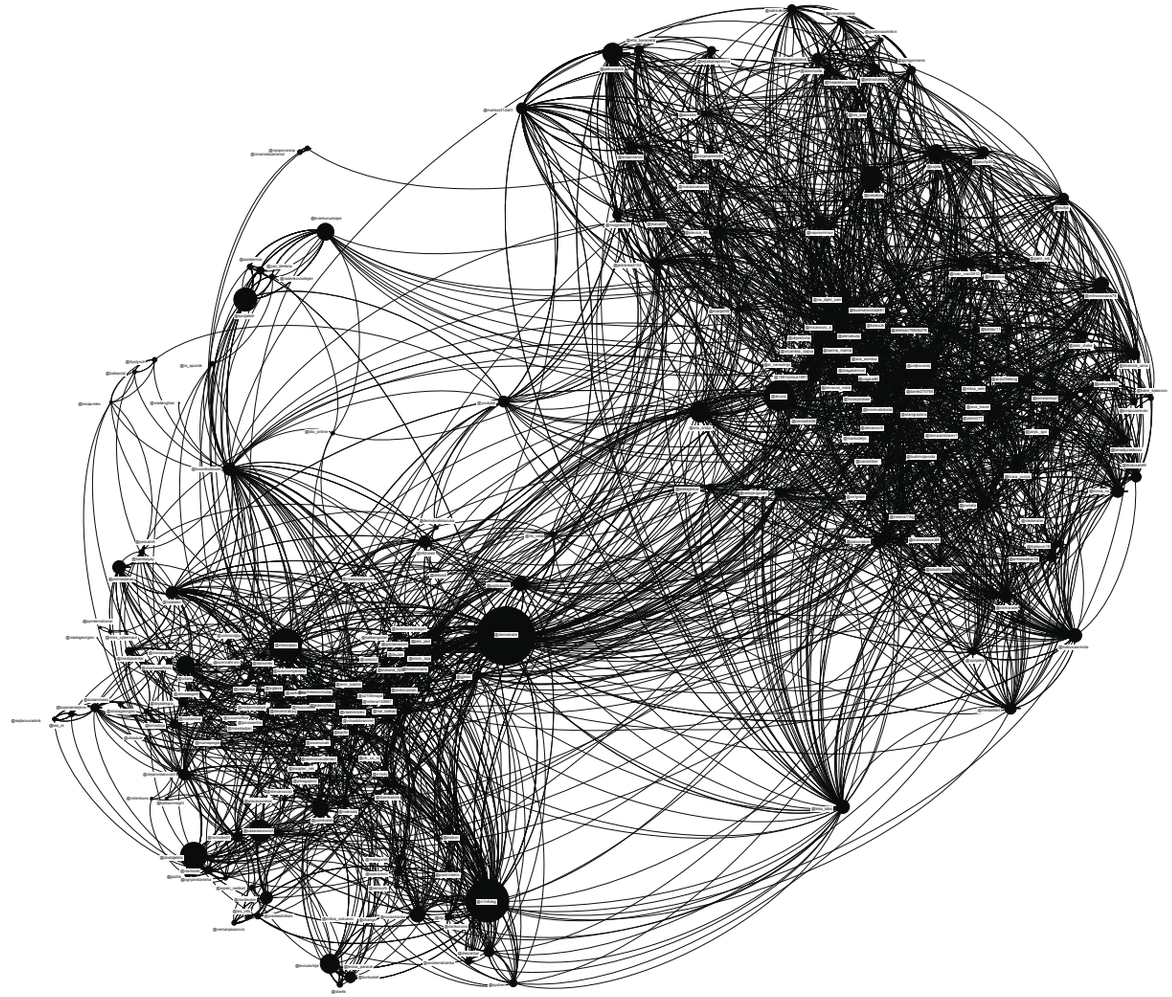
FABRIKOVANI ANGAŽMAN

Akteri povezani sa vlašću često veštački preuveličavaju svoju podršku i angažman na društvenim mrežama kreiranjem lažnih profila i organizovanjem armija botova, praksa poznata pod imenom *astroturfing*.[22] Iako je izvorno, bot najčešće naziv za automatizovani proces u kojem mašina oponaša ljudsko ponašanje na mrežama, na primer komentarisanje, lajkovanje ili promovisanje određenog sadržaja. U Srbiji je bot takođe postao pandan za armije aktivista ili članova vladajuće stranke koji po direktivi sprovode kampanje

uticaja, najčešće u političke svrhe.[23] Ova fabrikovana podrška koristi se kako bi se provladini stavovi, najčešće plasirani do same vlasti, činili popularnijim i dominantnijim nego što jesu kroz široku rasprostranjenost, dok se usput guše autentični glasovi kritičara, drugačija mišljenja i politički stavovi.

U Metinom izveštaju o zabeleženim pretnjama za 2023. godinu, kompanija je kao studiju slučaja analizirala mrežu koja je 2022. godine otkrivena u Srbiji. Mreža se sastojala od više od 5,000 naloga na Fejsbuku, 12 grupa kao i broja naloga na Instagramu (u izveštaju nije jasno koji je tačan broj naloga koji je uklonjen sa Instagrama obzirom da u jednom delu izveštaja piše 100 a u drugom 1,060).[24] Naknadno je otkriveno da je ova mreža zapravo kontrolisana od strane Internet tima Srpske napredne stranke.[25] Prema Metinoj definiciji, koordinisano neautentično ponašanje (*coordinated inauthentic behaviour*) podrazumeva mrežu naloga i grupa koje za cilj imaju uticaj na javnu debatu i oblikovanje javnog mnjenja. Najčešće ove mreže počinju sa nekoliko lažnih naloga koji umreženo deluju kako bi širili svoje poruke i stavove u vidu raznih sadržaja, kao što su vesti, mimovi ili tradicionalne objave, preko što više kanala, grupa i platformi.[26] Ono što ove mreže razlikuje od tradicionalnih botovskih operacija je strukturna sofisticiranost – ove kampanje upošljavaju ljude koji decentralizovano deluju iz većeg broja tačaka, za razliku od tradicionalnijih botovskih farmi koje su uglavnom lokalizovane. Glavni cilj ovih mreža je da na prividno „organski" način predstave ogromnu popularnost vladajuće stranke ali i da diskredituju kritičare i opozicione aktere. Takođe je utvrđeno da su nalozi u okviru ove mreže u nekim slučajevima i direktno ostavljali komentare ispod medijskih vesti na portalima.

Ova saznanja naslanjaju se na istraživanja iz 2019. godine o sistemu Tvrđava (Castle), za koji je otkriveno da je Srpska napredna stranka koristila kako bi instruirala botovske komentare na sajtovima medija.[27] Priče o armijama botova koji su plaćeni za komentarisanje vesti na

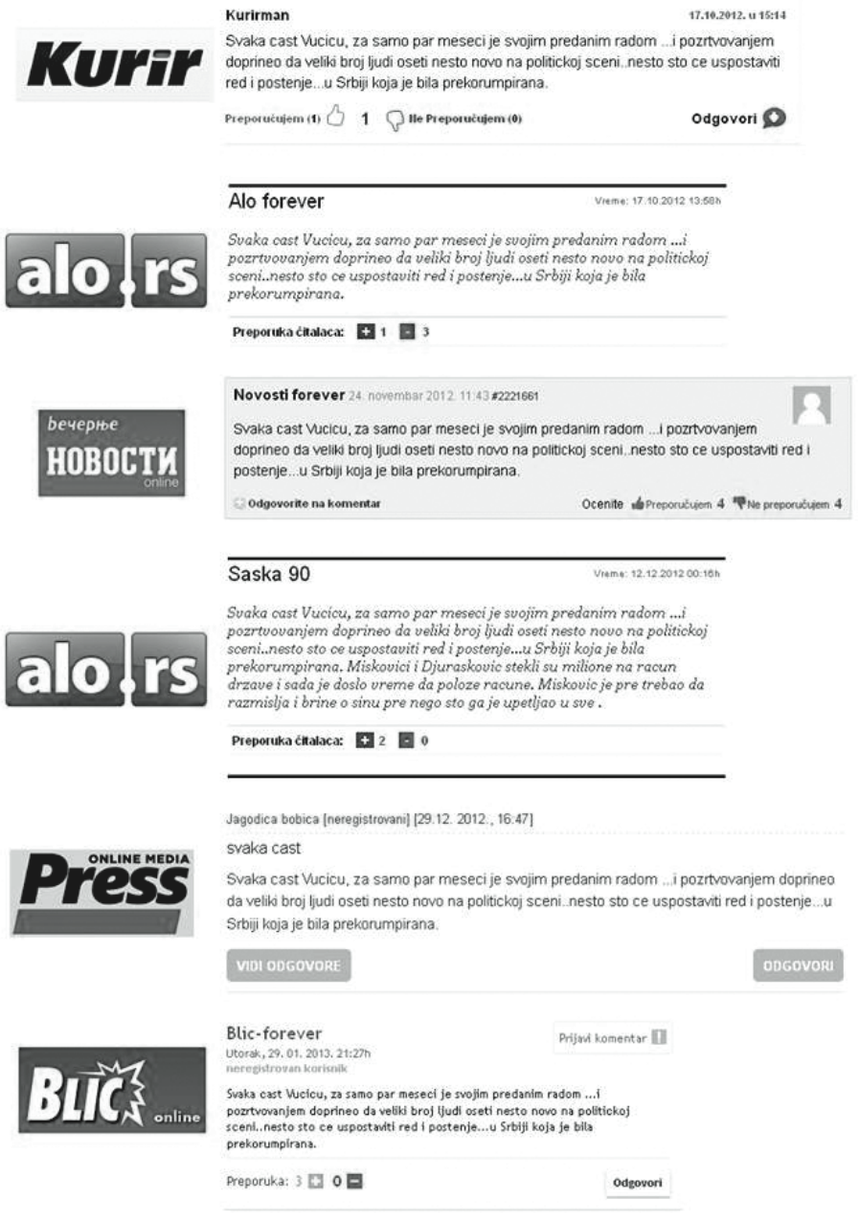


Analiza onlajn medija i društvenih mreža: Izbori u Srbiji - 2016, labs.rs

portalima pojavljivale su se i pre toga, ali su uspešnije zataškavane i nisu izazvale veće reakcije u javnosti. U prilog ovim nalazima išla je i činjenica da su krajem godine procurile informacije direktno iz godišnjeg izveštaja Internet tima u kojima je SNS tvrdio da su za godinu dana njihovi botovi ostavili oko 10 miliona komentara na vestima onlajn medijskih portala.[28] Iste godine, Tviter je sa svoje platforme uklonio oko 8,500 naloga koji su sistemski radili na promociji Aleksandra Vučića i SNS-a, kao i napadali opoziciju i civilni sektor u zemlji.[29] U analizi je otkriveno da je predsednikov nalog retvitovan preko milion puta a sadržaj vezan za predsednika, kao što su vesti na onlajn medijima i objave podrške još više od toga. Ubrzo nakon toga, Fejsbuk je takođe identifikovao i uklonio klaster lažnih naloga koji su koordinisano promovisali vladajuću stranku i predsednika.

Tokom 2019. godine tako je otkriveno da internet tim SNS-a koristio aplikaciju preko koje im je bilo omogućeno automatizovano ostavljanje pluseva i minusa na komentarima vesti postavljenih na portalima onlajn medija.[30] CINS je kroz analizu zaključio je da je aplikacija VotR2 centralizovala proces odabira vesti na čijim komentarima se ostavljaju plusevi i minusi, kao i koja ocena se ostavlja u odnosu na sadržaj komentara. Aplikacija je takođe pružala direktan pristup sajtovima Kurira i Espresa, neki od najčitanijih i posećenijih medija u zemlji. Na ovaj način, SNS je težio da utiče na javno mnjenje kroz nametanje i favorizovanje određenih stavova u komentarima na najčitanije vesti, najčešće kako bi se nametnula lažna slika zadovoljstva vlašću i fabrikovala spirala podrške predsedniku.

Pre ovih saznanja, još krajem 2014. godine otkriven je Valter, softver koji je od uređaja SNS simpatizera pravio automatizovane botove koji su kontrolisani preko eksternih servera.[31] To je značilo da je program korišćen za ostavljanje pozitivnih ili negativnih glasova na komentarima na vestima objavljenih od strane sajtova medija kao što su Blic, B92, Kurir i Večernje novosti. Valter je funkcionisao tako



Pristupljeno sa: https://www.pogledi.rs/forum/thread-1342-page-4.html

što je Internet tim vladajuće stranke podešavao server koji je slao identifikacioni broj komentara, zajedno sa atributom koji pokazuje da li glasanje treba da bude pozitivno ili negativno. Nakon toga bi softver lokalno rešavao komandu, odlazio onlajn i glasao na određeni način. Ovi procesi odvijali su se bez znanja korisnika uređaja. Kako je softver mogao samostalno da izvršava komande kao što je poseta sajtovima, vrlo je lako mogao biti iskorišćen za izvođenje DDoS ili drugih napada velikom količinom zahteva, opet bez znanja osobe koja je na svom uređaju instalirala program.[32]

U analizi predizborne kampanje na društvenim mrežama 2022. godine, SHARE Fondacija jasno je identifikovala strategiju vladajuće stranke za pridobijanje političke podrške na platformama, pre svega na Tviteru.[33] Otkriveno je da je mala količina naloga, uglavnom pripadajući istaknutim članovima Srpske napredne stranke, diktirala na koje objave se i kako reaguje. Ovi nalozi bi u najčešćem broju slučajeva, podelili objavu u kojoj ili hvale predsednika i uspehe vladajuće stranke i na taj način signalizirali pratiocima i korisnicima da dalje promovišu te sadržaje. U većini slučajeva je u pitanju bilo mehaničko retvitovanje, bez ikakvog dodatnog komentara ili sadržaja od strane naloga korisnika koji vrše retvitovanje. U drugim slučajevima targetirani su nalozi opozicionih kandidatkinja i kandidata, stranaka pa čak i medijskih radnica i radnika ili članica i članova civilnog društva koji su diskreditovani i vređani od strane ovih „nalogodavaca" i koji su dovodili do slične vrste masovne reprodukcije ovog sadržaja. Jedina razlika bila je u tome što su ovi sadržaji koji su bili napadi, mnogo češće zavređivali dodatne komentare od korisnica i korisnika koji su ih delili, uglavnom u vidu uvreda i širenja neistinitih informacija.

Priloženi slučajevi koordinisane manipulacije jasno ukazuju na spregu zvaničnih kanala informisanja, kao što su onlajn mediji i nezvaničnih pošiljalaca informacija, kao što su komentari na vestima u onlajn medijima, ali i nalozi na društvenim mrežama. Veza između ovih činilaca dostigla je stadijum u kojem je više nemoguće sa sigurnošću tvrditi čija je šteta po javno mnjenje veća, jer je uigranost ovog sistema (kontra)informisanja toliko sofisticirana i proteže se, zabeleženo, makar deceniju unazad.

Tokom 2023. godine na Tviteru je objavljen spisak SNS botova na kome se nalazilo oko tri hiljade ljudi, sa imenima i prezimenima, okrugom, mestom i linkom ka profilima.[34] Spisak je brzo pokrenuo debate u društvu o zatrovanosti javnog prostora u zemlji, kao i činjenici da je većina ljudi sa ovog spiska, ako je verovati podacima, zaposlena u javnim preduzećima, što bi značilo da su za sve komentare koje ostavljaju tokom radnog vremena, plaćeni parama iz budžeta države.[35] Usledile su razne analize koje su pokušale da ponude jasniju sliku o botovskoj strukturi Srbije, gde su žarišta,[36] šta ove strukture čini posebnim,[37] ali najviše od svega – kako je ova mreža tako sofisticirana da uspeva da odoli svakom njenom razotkrivanju? I sam predsednik se oglasio na Instagramu nekoliko dana nakon objavljivanja spiska, ali ne da ponudi odgovor na neka od ovih pitanja ili pokrene konstruktivnu društvenu diskusiju, već da ponosno poruči „da, i ja sam SNS bot".[38]

Razna istraživanja su pokazala da delovanje botova direktno utiče na prirodno uključivanje građana u javne debate i predstavlja veliku opasnost po demokratsko uređenje u digitalnim prostorima, dok u isto vreme dovodi po povećane polarizacije u društvu.[39] U nekim slučajevima, ovo se radi direktnim i svesnim deljenjem dezinformacija i lažnih vesti, učestvovanjem u teorijama zavera i demonizovanjem neistomišljenika. Sa druge strane, kampanje koje su više proračunate ne moraju eksplicitno da nameću mišljenja i stavove, već svojom frekventnošću mogu da stvore lažni utisak veće podrške za određene aktere i njihove poteze. Uprkos upornom otkrivanju ovih informativnih mahinacija, jasno je da internet mašinerija vladajuće stranke ne jenjava, a čak se i čini da se sve manje trudi da sakrije svoje delovanje. Ovakve kampanje uticaja predstavljaju kamen

temeljac za kontrolu javnog prostora i debate u Srbiji i direktno su povezane sa vlašću kroz sve organizacione strukture, ali i sa drugim akterima kao što su mediji.

KONTROLA MEDIJA I JAVNOG INFORMISANJA

Sa druge strane, dok botovi omogućavaju amplifikaciju određenih informativnih sadržaja, važno je obratiti pažnju i na medije kao ključne kreatore ovog sadržaja. Širom sveta, pokazalo se da mediji i drugi tvorci sadržaja bliski državnim strukturama strateški objavljuju sadržaje koji su isključivo u skladu sa interesima vlasti. Algoritamski mehanizam omogućava da provladin sadržaj na štetu kritičkog dopre do veće publike, dakle, kontrolom medijske produkcije i cirkulacije sadržaja na digitalnim platformama, država uspeva da efikasno usmerava pažnju javnosti, promovišući narative koji služe njihovim političkim ciljevima.

Koncentracija informative u svega nekoliko medija omogućila je državi da uz pomoć nekoliko zakona koje je usvojila lako preuzme nezvaničnu ulogu glavne i odgovorne urednice iz senke. U avgustu 2014. godine donet je set medijskih zakona – o javnom informisanju, javnim medijskim servisima i elektronskim medijima. Ovim zakonima predviđen je konačni izlazak države iz vlasničke strukture medija i prelazak sa direktnog budžetskog finansiranja pojedinih medija na sistem projektnog, konkursnog sufinansiranja. Iako su ovi zakoni delovali kao dobra polazna osnova za obezbeđivanje pluralizma i održivosti medija, ispostavilo se da je vlast paralelno uspostavila sistem rasturanja slobodnog, fer i nezavisnog medijskog okruženja.

Srbija je u svojoj želji za kontrolom informativnog prostora počela da se služi sličnim (ako ne identičnim) strategijama kao i Mađarska. Naime, na čelu sa premijerom Viktorom Orbanom, Mađarska je od 2010. godine krenula u kampanju urušavanja medijskih sloboda kroz favorizovanje provladinih medija, kao i kažnjavanje nezavisnih i kritičkih medija kroz birokratski maltretman u vidu ograničavanja državnih sredstava, tužbe i kontrolu oglašivača.[40] Još jedna zabeležena taktika je devaluacija tradicionalnih (*legacy*) medija, sa ciljem njihovog uništavanja i kupovine od strane onih koji su bliski vlasti, čime se omogućava potpuna kontrola nad njihovom novom uređivačkom politikom. Takođe, uspostavljena je jasna podela između provladinih i nezavisnih medija i na taj način su sve novinarke i novinari i mediji koji ne rade u interesu agende vlasti prozvani špijunima, izdajnicima, stranim plaćenicima i opozicionim aktivistima. Ovakve iliberalne strategije takođe su obeležile prethodnu deceniju medijske deterioracije u Srbiji, sa jasno prepoznatljivim šablonima iz mađarskog, ali i drugih primera iz sveta. Iako su privođenja i hapšenja novinarki i novinara zbog njihovog izveštavanja u prvom mahu izostali iz režimskog plana, jasno je da je u poslednjih deset godina i to u nekim slučajevima postalo validno oruđe za vlast.

Iako je i u Medijskoj strategiji Srbije za period od 2020. do 2025. godine jasno ustanovljeno da država mora da izađe iz vlasničkih struktura medija, novi medijski zakoni koji su na snagu stupili 2024. godine propisuju da Telekom Srbija, državni telekomunikacioni operater, ima pravo da osniva svoje medije.[41] Donošenje ovakvih zakona na jasan način legalizuje koncentraciju informative, ne samo u jednoj tački, već u celoj mreži koja se direktno nalazi pod pokroviteljstvom države. Na osnovu RATEL-ovog Izveštaja o tržištu elektronskih komunikacija za drugi kvartal 2024. godine, Telekom Srbija je obuhvatala 44 odsto od procenjenih 8,5 miliona pretplatnika mobilne telefonije, dok Yettel i A1 Srbija pojedinačno pokrivaju 32, odnosno 24 odsto tržišta. Telekom Srbija ubedljivo dominira tržištem fiksnog širokopojasnog pristupa – od 2,18 miliona pretplatnika fiksne širokopojasne veze, Telekom Srbija drži skoro 56,8 odsto, SBB opslužuje 26,9 odsto tržišta, dok ostatak pokriva manje od 20 odsto ukupnog tržišta.[42]

U januaru 2021. godine, Telekom Srbija potvrdila je potpisivanje sporazuma o izdavanju optičkih kablova iz svoje infrastrukture Yettelu.[43] U julu 2022. godine, nakon zatvaranja perioda izveštavanja za ovu godinu, Telekom Srbija kupila je telekomunikacionu kompaniju Globaltel od vlasnika Pink media grupe Željka Mitrovića po nepoznatoj ceni.[44] U aprilu 2021. godine, Junajted Media i SBB, koji su obe deo holandske Junajted grupe, podneli su krivičnu prijavu protiv Telekoma i Telenora zbog navodnog zaključivanja restriktivnog sporazuma, za koji se verovalo da bi mogao da stvori presedan koji otežava konkurentima da uđu na tržište.[45] Dve godine od početka slučaja, tužiteljka beogradskog Višeg javnog tužilaštva Bojana Savović, kojoj je prvobitno bio dodeljen predmet smenjena je sa funkcije, potez za koji se spekulisalo da je povezan sa njenom istragom o državnoj elektroprivredi, a predmet je ustupljen drugom tužiocu koji je prijavu brzo odbacio.[46] Kao odgovor na tužbu, Telekom je podneo tužbu za odštetu od skoro 80 miliona evra navodeći da mediji N1 i Nova.rs, koji su u vlasništvu Junajted grupe, kritički izveštavaju o državnom operateru na način koji bi mogao da predstavlja čin nelojalne konkurencije. Privredni sud je tužbu odbacio u maju 2022. godine.[47]

Pretpostavka da će razvoj novih tehnologija omogućiti sveobuhvatnije i kvalitetnije informisanje građana i građanki u vreme kada je ovaj monitoring bio u početnim fazama nije bila sasvim odbačena. Deset godina kasnije, međutim, nema dileme da tehnodeterminizam u bojama društvenog optimizma nije imao utemeljenje. Sudeći prema informativnoj praksi u Srbiji, društveno-politički tas je ne samo prevladao tehnološke mogućnosti, nego je i učvrstio strukturu u kojoj se glavni informativni tok odvija kao paralelna stvarnost – stvarnost koja je potisnuta na marginu javne sfere, u privatne okvire digitalne svakodnevice.

Uspostavljanje paralelnog sistema informisanja podrazumevalo je nekoliko ključnih poteza – od osnivanja i uspostavljanja paralelnih medija koji su ne samo kreatori informativnog poretka, već i destabilizatori ukupnog medijskog sistema Srbije, preko kreiranja sveobuhvatnog mehanizma diseminacije pogodnih „vesti", do centralizacije i uspostavljanja pune kontrole nad informativnim ekosistemom kojim se diriguje iz jednog centra, a u kojem mediji i javni (digitalni) akteri imaju jasno definisane uloge. Takav informativni perpetuum temelji se na čvrstoj infrastrukturi – vlasničkoj, uredničkoj, klijentelističkoj – koja obezbeđuje nesmetani protok u kojem su nezavisni mediji, relevantne informacije i kritičko rezonovanje defavorizovani u korist glasova pristalica koji doprinose održanju društveno-političkog statusa kvo.

Prvi nivo paralelnog informisanja uspostavlja se već u oflajn svetu i taj mehanizam ima nekoliko elemenata. Jedan podrazumeva uspostavljanje i/ili održanje kontrole nad medijima iz postojećeg medijskog pejzaža. Među njima svakako najistaknutije mesto imaju tabloidi, javni medijski servis, ali i mediji koji su u talasima autoritarizacije u Srbiji stajali kao ključni tradicionalistički, konzervativni stubovi režima, poput Večernjih novosti i Politike. Takođe, indikativan primer ovakvog vida zarobljavanja medija je promena vlasničke strukture NIN-a, zbog koje je redakcija najstarijeg nedeljnika na ovim prostorima napustila ovu medijsku kuću i osnovala novi nedeljnik Radar.[48] Jedan od glavnih ciljeva ovakvog delovanja je predupređivanje nepogodnih vesti i iznošenja informacija koje su kritički nastrojene prema vlasti.

Drugi aspekt odnosi se na osnivanje medija koji treba da posluže kao „paralela" postojećim nezavisnim medijima. S obzirom na to da je medijsko tržište u Srbiji već decenijama prezasićeno, osnivanje novih medija koji bi doprineli održanju vlasti nije bez jasne svrhe. Tako je ova dekada obeležena „ružnim blizancima", odnosno medijskim portalima koji su u svom nazivu pa i vizuelnom identitetu kopirali postojeće nezavisne medije, dok su uređivački kompas usmeravali ka potvrđivanju glavnog informativnog toka. Onlajn portali Južne

vesti, Ozonpress i Kolubarske imali su svoje lažnjake (www.juznevesti.info, www.ozonpress.rs, www.kolubarski.info), a gotovo svaki uvid u poslovanje, vlasničke i organizacione veze novoformiranih portala prema pravilu su vodili ka Srpskoj naprednoj stranci.

Najzad, ni istraživački medijski segment nije prošao bez svoje kopije u vidu portala, kao što je Antidot, kao sredstva dezinformisanja javnosti u vezi sa vrlo osetljivim temama, kao što su sudski procesi, rad slobodnih medija i slično. Treći stub ovog mehanizma odnosi se na finansijsku održivost pogodnih medija. Tako je sistemska zloupotreba zakonski predviđenog javnog sufinansiranja medijskog sadržaja u Srbiji vremenom omogućila da proliferacija informacija bude preselektovana još u fazi dodele namenjenih sredstava. Ovaj pristup zahtevao je nešto kompleksniji pristup budući da je uzurpiranje procedure dodele sredstava medijima uključivalo i osnivanje organizacija i tela koja bi obezbedila željeni ishod takvih konkursa. U tu svrhu je bilo potrebno kreirati čitav paralelni civilni sektor, čija je svrha da potisne postojeći i preuzme njegovu društvenu ulogu. Kao i u prethodnim godinama najskuplji projekti dodeljeni su TV stanicama, i to onim čija je uređivačka politika naklonjena vlasti.[49]

Iako istraživanja i dalje pokazuju da na mrežama kao što su X (nekada Tviter) i Fejsbuk, novinarke i novinari i mediji i dalje prednjače u uticaju kada je u pitanju kreiranje i vođenje razgovora, taj uticaj se brzo izjednačava sa uticajnim ličnostima, drugim korisnicima i alternativnim izvorima informacija.[50] Ovo ukazuje na promenu paradigme u informativnom ekosistemu – informacije, stavovi i vesti se više cene od istomišljenika nego od objektivnih i tačnih činjenica i izvora. Pitanje poverenja u izvore informisanja temelji se na nekoliko važnih kriterijuma, među kojima su vlasnička struktura medija, politička afilijacija, percepcije o cenzuri i drugi. U društvima kao što je Srbija, u kojoj je na prvi pogled medijski pluralizam na veoma visokom nivou, lako se može steći utisak da je na snazi informativno izobilje koje podstiče i podržava nesmetano širenje velikog broja informacija.

Istraživanja konzistentno pokazuju porast zastupljenosti onlajn medija (portala) kao relevantnog izvora informisanja – 2021. godine našli su se na trećem mestu (64%) glavnih izvora informisanja za javnost.[51] Istraživanje iz 2020. godine pokazalo je da se sajtovi tradicionalnih medija nalaze se među tri glavna izvora informisanja, a čak 92% korisnica i korisnika interneta vestima pristupa preko mobilnog telefona.[52] Jasno je da je rastući uticaj digitalnog prostora neosporan i nezanemarljiv u društvu, ali ono što ipak ovdašnji slučaj čini posebnim je i dalje visok stepen oslanjanja na tradicionalne medije, čak i u digitalnom prostoru. Poznata je činjenica da je medijski ekosistem u Srbiji duboko polarizovan, neravnopravan i netransparentan.

Uoči decembarskih izbora 2023. godine, SHARE Fondacija je odlučila da se posveti analizi najposećenijih medijskih portala u političkom informativnom sistemu kako bi bolje razumela njihovu ulogu kao i na koji način se građanke i građani informišu tokom predizborne kampanje.[53] Analizom je utvrđeno da, pored činjenice da su izbori tematski zauzeli potpuno marginalnu poziciju, odnosno nepotpunih 20% ukupnog sadržaja za vreme predizborne kampanje, gotovo tri četvrtine centralnog informativnog sadržaja u medijima uopšte nije ni pominjalo vlast. Ovo jasno ukazuje na to da medijsko okruženje po svojim ustaljenim šablonima funkcioniše nezavisno od predizbornog perioda, kao i da je kontrola informacija na tako visokom nivou da je nepotrebno uopšte vršiti koncentrisanu, izbornu promociju vlasti, dok se opozicija ili ne pominje ili demonizuje. Većina medija čija uređivačka politika se temelji na favorizovanju vlasti ispunjavaju formalnu ulogu medijuma i služe više kao digitalni pamflet za prenošenje promotivnog materijala i takozvanih *bezsadržinskih vesti* kao što je na primer, objava predsednika Vučića na Instagramu ili TikToku, umesto nuđenja čitaocima informacija ili činjenica. Sve u

svemu, analiza onlajn medijskog ekosistema u predizbornoj kampanji pokazala je da 80% najčitanijih portala u zemlji koordinisano nudi sliku državnog blagostanja i prosperiteta, izbegava argumentovano debatovanje suprotstavljenih stavova i potiskuje iznošenje važnih informacija i činjenica zarad promocije.

Ovakvo informativno polje je rezultat dugogodišnjeg sistemskog podrivanja poverenja u medijski sadržaj, najčešće kroz kršenje etičkih principa i diseminacije neistinitih i obmanjujućih informacija. Najčitaniji onlajn mediji uglavnom su produžeci svojih tradicionalnih pandana (televizija i štampanih novina). Stoga nije neočekivano da će svoju tradicionalnu uređivačku politiku preneti i u digitalni prostor. Prema analizi, utvrđeno je da je kontrola informativnog onlajn prostora kroz definisanje ključnih tema za rezultat imala koncentrisanje medijske agende koja vlast pozicionira u prvi plan, dok je takođe postojao jasno marginalizovan spektar društveno-političkih pitanja i problema koji predstavljaju tematsku paralelu dominantnom narativu. Interesantna je bila činjenica da tri četvrtine centralnog informativnog sadržaja onlajn medija uopšte nije pominjala vlast, što ukazuje na to da je medijsko okruženje neometano poslovalo po svojim ustaljenim šablonima nezavisno od predizbornog perioda. Ovi podaci pokazali su da iako su onlajn mediji među primarnim izvorima informisanja za javnost, ne postoje visoki kriterijumi kada je u pitanju kvalitet i relevantnost informacija koje se plasiraju. Takođe se pokazalo da većina medija koji su poznati po svom eksplicitnom favorizovanju vlasti, više služe kao distributeri i promoteri narativa koji dolaze od vlasti, nego tvorci i generatori novosti.

CENZURA I ODMAZDA ZA IZNETE STAVOVE

Mehanizmi cenzure koriste se za ograničavanje prostora za debatu i diskusiju, pogotovo na platformama koje su ponekad pod pritiskom da uklone ili ograniče kritične objave. Podrazumeva se i taktika nadzora, jer oni koji se suprotstavljaju vlasti često prijavljuju zastrašivanje ili uznemiravanje, što dovodi do efekta zebnje kada je u pitanju otvoreno političko izražavanje.

Tranzicija informacionog ekosistema u digitalno okruženje sa sobom je donela obećanja kao što su šira rasprostranjenost informacija, lakši pristup izvorima i demokratičnije mogućnosti informisanja. Ipak, ispostavilo se da se u prethodnih deset godina medijsko prisustvo u digitalnom prostoru susrelo sa mnoštvom izazova i među prvima na meti su se našli pružaoci vesti. Bilo da je zbog izveštavanja koje se smatra politički nepodobnim, kao što je otvaranje tema od društvenog značaja koje ukazuju na propuste vlasti i nadležnih organa, ili izveštavanje o događajima koji se bi mogli da poremete aktuelno javno mnjenje, uloga medija kao branitelja prava na informisanost na prvoj liniji često je stavljena na test.

Digitalni napadi na tehničku infrastrukturu medija su u stalnom porastu, što pokazuju podaci međunarodnih organizacija za zaštitu novinarki i novinara i medijskih radnica i radnika.[54] Sa druge strane, sposobnosti medija da se odbrane od ovakvih napada često su nedovoljne, uglavnom zbog nedostatka kapaciteta, i ljudskog i finansijskog. Za deset godina praćenja napada na medije u digitalnom okruženju, jasno se može istaći veza između medija koji su se nalazili na meti ovakvih napada i sadržaja zbog kojih su bili targetirani.

Nezavisni mediji koji su najčešći glasnogovornici protiv korupcije, klijentelizma i drugih mahinacija vlasti, redovno se nalaze na meti napada sponzorisanih od strane državnog aparata. Prema poslednjim podacima Reportera bez granica, u 2024. godini zabeležen je povećan pritisak na slobodu medija, kao i zabrinjavajući pad u podršci i poštovanju autonomije medija.[55] U Srbiji pogotovo se skreće pažnja na učestalost diseminacije lažnih vesti, pretnji i napada na novinarke i novinare i širenje i uticaj propagande kroz medije bliske

vlasti. Nezavisni istraživački mediji, novinarke i novinari iz godine u godinu nalaze se u sve neprijateljskijim uslovima rada u Srbiji. Tužbe za klevetu i uvredu takođe su korišćene u cilju zastrašivanja novinarki i novinara. Istraživački mediji koji se bave spregama kriminala i vlasti najčešće se nalaze na meti ovih tužbi poznatih kao strateške tužbe protiv učešća javnosti (SLAPP suits). Ovakve tužbe za jasan cilj imaju zastrašivanje, najčešće medija, koji svojim izveštavanjem ukazuju uglavnom na problematične poslovne prakse ili nelegalno poslovanje. Tužiteljke i tužioci u ovim predmetima često ni ne očekuju da ovi slučajevi budu usvojeni, već samo teže da pošalju poruku kritičarima.[56] Ovakve tužbe teže da stvore efekat zebnje za dalje izveštavanje, primarno kroz duge sudske procese koji mogu imati teže psihičke i finansijske posledice.

Od maja 2021. godine, protiv KRIK-a je podneto 16 tužbi, najčešće od strane onih koji su bliski vrhu vlasti.[57] Analiza SLAPP slučajeva iz marta 2024. godine pokazuje da domaći pravni okvir nije dovoljno osposobljen da na adekvatan način pristupi ovakvim slučajevima.[58] Utvrđeno je da ovakve tužbe skoro nikada nisu izolovani incidenti, odnosno da su često praćeni i drugim postupcima koji se mogu odnositi na druge tekstove, objave na društvenim mrežama ili čak i fizičkim akcijama. Takođe je zaključeno da u okviru domaćeg sudstva postoji suštinsko nerazumevanje osnovnih principa zaštite za optužene u ovakvim slučajevima, kao što su međunarodni standardi, stepen kritike koje javne ličnosti moraju da trpe zbog svog statusa kao i krajnjeg cilja zbog kojeg ova lica podnose ovakve tužbe, što je uglavnom zastrašivanje, cenzura i odmazda za iznete stavove.

Ovakvo ophođenje prema novinarkama, novinarima i medijima, kao i članicama i članovima civilnog društva i aktivistkinjama i aktivistima, relativizuju napade i doprinose kulturi nasilja u društvu. Kao rezultat, ove grupe se suočavaju sa povećanim brojem direktnih i indirektnih pretnji i uvreda na društvenim mrežama od strane pojedinaca ali i organizovanih grupa. Novinarke i novinari iz medija koji su kritični prema vlasti često su na meti verbalnih i fizičkih pretnji, čak i pretnji smrću, dok novinarke najčešće uz to dobijaju i pretnje koje su rodne i seksualne prirode. Onlajn napadi postali su toliko česti da se dobar deo njih više ni ne prijavljuje, a epilozi su skoro nepostojeći. Za razliku od slučajeva same kritike vlasti na mrežama, koje se, ako je u pitanju kritika predsednika ponekada završe privođenjem, a ako je u pitanju kritika vlasti uopšteno, nekada i otkazom. Upravo to se dogodilo nuklearnoj inženjerki koja je, nakon što je na X-u komentarisala ophođenje vlasti u danima nakon masakra u Ribnikaru i Mladenovcu, otpuštena iz Direktorata za radijacionu i nuklearnu sigurnost i bezbednost. Iako se na X-u predstavlja po pseudonimom i tvrdi da nikada nije tvitovala u toku radnog vremena, objašnjeno joj je da su joj društvene mreže već dve godine bile pod praćenjem i kao usmeni odgovor na to zašto je dobila otkaz rečeno joj je „Tako zahtevaju službe!“, dok se u rešenju o otkazu nalaze citati njenih tvitova.[59]

Sa druge strane, šest godina nakon poplava, kada se vrhunac cenzure ogledao u tehničkim napadima i obaranju sajtova medija koji su izveštavali o stanju u pogođenim područjima, 2020. godina predstavila je uvod u represivnije taktike. U aprilu 2020. godine, kada je pandemija koronavirusa već uveliko uzurpirala svakodnevni život i broj preminulih od bolesti je eksponencijalno rastao, država je pokušala da preuzme kontrolu nad informacionim tokovima na još jedan način. Samo dan nakon što je objavila tekst o lošim uslovima rada u kovid sistemu, kao i nedostatku opreme u Kliničkom centru Vojvodine,[60] novinarka Ana Lalić uhapšena je i određeno joj je zadržavanje od 48 sati.[61] Nekoliko dana ranije, Vlada Srbije je tiho objavila odluku o centralizovanju informacija u vezi sa pandemijom, što je značilo da sve vesti koje se tiču širenja virusa, broja obolelih i umrlih i opšteg stanja, javnost dobija isključivo od predsednice Vlade Ane Brnabić ili članova Kriznog štaba.[62] Ova vest protumačena je između ostalog kao pokušaj dodatne cenzure i oštro kritikovana, u trenutku kada je vanredno stanje i dalje na snazi, a građanke

i građani se između straha i tuge bore sa ogromnim količinama teorija zavera i dezinformacija po mrežama.[63] Dan nakon što je Lalić privedena, Vlada je povukla odluku. Iako je u ovom slučaju pokušaj državne cenzure izbegnut, činjenica da je do nje uopšte došlo ostala je kao podsetnik ne samo mogućnosti, već i pravca u kojem država smatra da bi se trebalo kretati u trenucima kada su pravovremene i tačne informacije od presudnog značaja.

Novinari i aktivisti takođe su privođeni zbog učestvovanja i podrške protestima, između ostalog i tokom protesta protiv državnih napora da u Srbiju dovede kompaniju Rio Tinto. Dvoje novinara i aktivista iz Sombora obeleženi su kao organizatori protesta u Somboru i kao dokaz, priložene su njihove objave sa društvenih mreža kao i njihovi tekstovi objavljeni na portalu SO Info.[64] Takođe, tokom 2021. godine, ponovo u jeku protesta protiv Rio Tinta, aktivistima iz Niša je policija dolazila na vrata zbog pozivanja na protest u tom gradu preko Fejsbuka.[65] Tokom protesta povodom izbornih krađa u decembru 2023. godine, studentima i studentkinjama Univerziteta u Beogradu su, uz pomoć medijske aparature vlasti, objavljivani lični podaci i slike iz ličnih karata odnosno iz baza policije.[66] U isto vreme, po društvenim mrežama počeli su da cirkulišu snimci sa protesta na kojima se jasno vidi kako neidentifikovane osobe listaju upravo ove slike iz policijskih baza na svojim telefonima.

Početkom novembra 2024. godine srušila se nadstrešnica Železničke stanice u Novom Sadu pri čemu je 15 ljudi izgubilo život. Ova tragedija brzo je mobilisala građane u potrebi da neko odgovara za ovaj zločin, ali činilo se da su prioriteti vlasti ipak bili usmereni na sanaciju štete negde drugde. Ubrzo po objavljivanju vesti i dok su spasilačke ekipe i dalje izvlačile ljude iz ruševina, Srbija danas, Informer, B92, RTV Pančevo, Pink, Alo, Happy, Telegraf, K1 i drugi mediji počeli da objavljuju da se obrušio stari deo stanice.[67] Železnička stanica u Novom Sadu svečano je otvorena prošle godine i to u dva navrata i uz posete visokih zvaničnika SNS-a, a za projekat rekonstrukcije stanice izdvojeno je 65 miliona evra.[68] Prema slikama i snimcima korisnica i korisnika društvenih mreža jasno je da je i urušena nadstrešnica podlegla rekonstrukciji, što su potvrđivali i medijski tekstovi iz jula prošle godine.[69,70] Ipak, na dan tragedije, na društvenim mrežama počele su da cirkulišu fotografije koje su jasno ukazivale na činjenicu da su neki od ovih medija takođe izmenili svoje tekstove iz jula, u kojima su sklonili svako pominjanje renoviranja nadstrešnice.[71] Uprkos brojnim dokazima koji su priloženi na društvenim mrežama, vlast se držala svoje zvanične priče da nadstrešnica nije bila uključena u projekat renoviranja, što je uporno ponavljano i u medijima. Pronalaženje sličnih primera u svetu je skoro nemoguće i razmere ovakve vrste kontrolisane cenzure u trenucima tragedije samo dovode do povećanog besa i tuge kod građanki i građana. Iako je posle nekoliko nedelja narativ o „staroj nadstrešnici" menjan drugim taktikama manipulacije javnom debatom, snažan društveni revolt ovog puta je svoju artikulaciju našao u blokadama fakulteta širom zemlje, svakodnevnom odavanju počasti preminulima petnaestominutnom ćutnjom i blokadama gradskih ulica, i velikim protestima.[72]

Zarobljavanje medijskog prostora je jedan od prvih koraka u efektivnom porobljavanju institucija i demokratskih društava, i prelaska u hibridne autokratske režime.[73] Iako se može činiti da eksplicitna represija kao što su hapšenje i osuđivanje medija, civilnog društva i aktivista ukazuju da zemlja i dalje nije zastranila sa demokratskog puta i da umesto toga država bira da ignoriše one koji su kritički orijentisani, istina je da su strategije za izlaženje na kraj sa neistomišljenicima mnogo kompleksnije i teže izbegavaju osudu međunarodne zajednice. Prisluškivanje i nadzor, dugi sudski sporovi koji za cilj imaju finansijsko uništenje malih i nezavisnih medija, cenzura i nametnuta autocenzura, informativni razgovori zbog objava na mrežama, armije botova instruisane da daju privid podrške vlasti, kontrola medijskog sektora i demonizovanje neistomišljenika nose

skupu cenu zatvaranja demokratskih prostora za debatu i slobodno mišljenje, stvaraju efekat zebnje i učvršćuju kontrolu nad društvom.

Trg Slavija, Beograd, 22. decembar 2024., izvor: @javniskupovi

KRATKA ISTORIJA NADZORA: OD METAPODATAKA, PREKO KAMERA DO ŠPIJUNSKIH SOFTVERA

Razvoj tehnologije otvorio je značajne mogućnosti državnog nadzora. Može se reći da Srbija u tom smislu prati trendove, ali i da pokazuje tendencije proširivanja tehnoloških kapaciteta nadzora. Nakon masovnog pristupanja zadržanim podacima o telefonskih komunikacijama građana, a usled sve češćih protesta u Srbiji, na red su došli javni prostori, odnosno upotreba biometrijskog video nadzora kao potencijalne metode za kontrolu nezadovoljstva građana i disciplinovanje neistomišljenika.

Dok su sa jedne strane ulozi vremenom postajali sve veći, implikacije biometrijskog video nadzora po ljudska prava postajale su sve kompleksnije. Dok se kod zadržanih podataka o komunikacijama išlo na zaobilaženje redovnog postupka preko direktnog pristupa podacima čija je legalnost upitna, nadležni organi su prvo nabavili i instalirali sistem biometrijskog video nadzora, a onda ušli u proces „legalizovanja" takve tehnologije inoviranjem pravnog okvira. Najzad, spajver i targetiranje pripadnika civilnog društva podstaklo je sumnju da se granica intruzivnosti nadzora ponovo pomera, što je potvrđeno istraživanjem organizacije *Amnesty International* krajem 2024. godine. Sada su na meti našli mobilni telefoni koji omogućavaju direktan uvid u život bilo koga od nas. A da na našem telefonu postoji spajver, ne mora da ukazuje baš ništa.

Paralelno sa smanjenjem demokratskih kapaciteta u Srbiji tehnologije su napredovale, uključujući metode i razmere nadzora nad komunikacijama građana, javnim prostorima i potencijalno svim sadržajima koje imamo na svojim mobilnim uređajima. Uz javne obračune i kampanje blaćenja novinara, medija, javnih ličnosti, pripadnika civilnog društva i političkih oponenata nadzor postaje čvrsta poluga statusa kvo i represije nad građanima koji ne podržavaju vladajuće strukture.

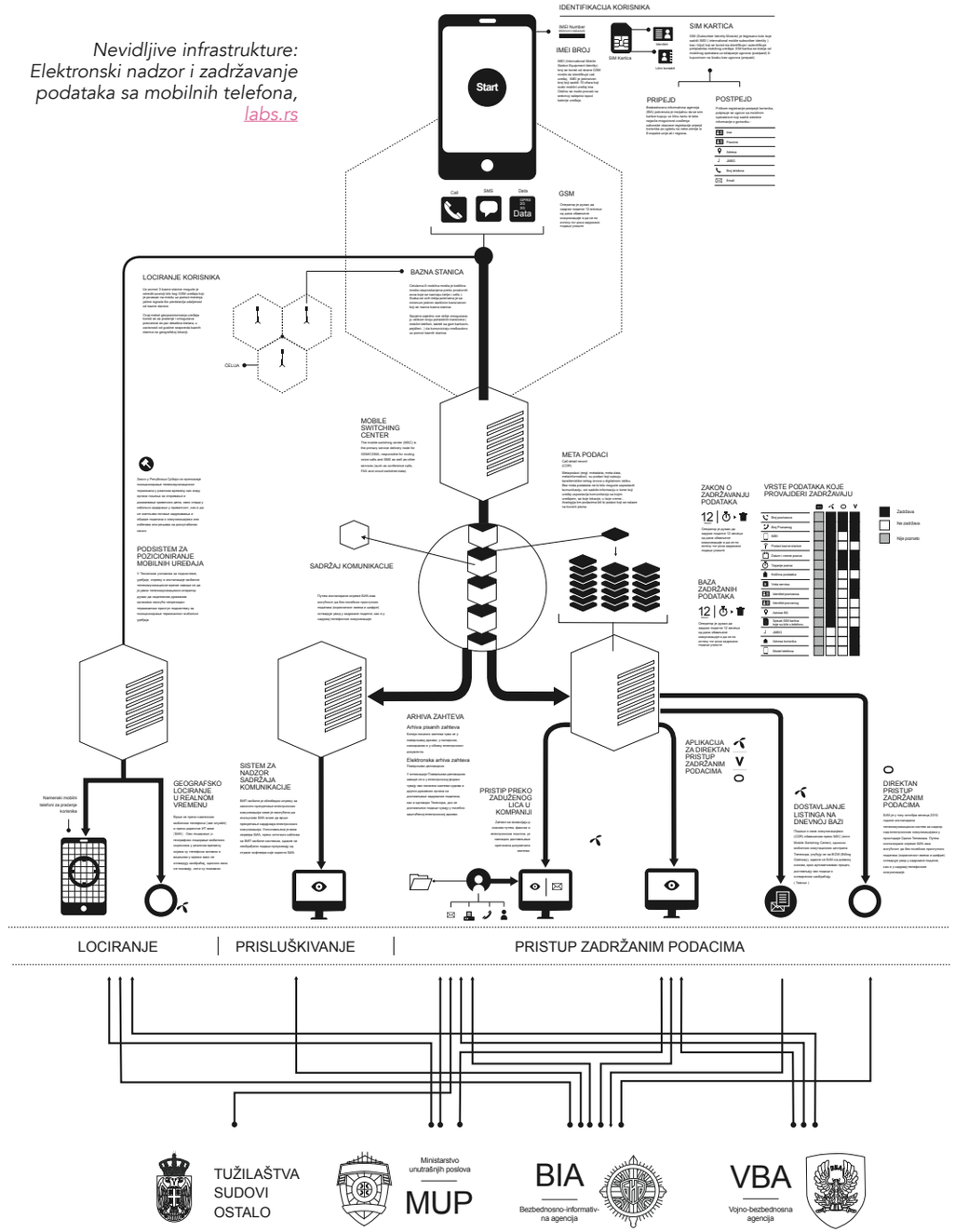
KAKO JE POČELO: IZABERI BROJ, BILO KOJI BROJ TELEFONA

Operatori elektronskih komunikacija – provajderi telefonije i usluga pristupa internetu – prikupljaju podatke o nama u mnogo većoj razmeri nego što smo možda svesni. Njihove baze sadrže ogromne količine tzv. metapodataka,[74] pojma koji je posle Snoudenovih otkrića 2013. godine postao deo mejnstrim narativa.[75] „Podaci o podacima" predstavljaju sve ono što opisuje komunikaciju a nije deo sadržaja komunikacije. Na primeru telefonskog poziva, to su recimo broj koji poziva, broj koji se poziva, datum, vreme i trajanje poziva, serijski broj sim kartice pozivaoca, serijski broj sim kartice pozvanog (IMSI), serijski broj uređaja pozivaoca, serijski broj uređaja pozvanog (IMEI), bazna stanica sa kojom je bio povezan pozivalac i bazna stanica sa kojom je bio povezan pozvani (ergo njihove lokacije).

Potencijal baza operatora i metapodataka za vršenje policijsko-bezbednosnih poslova, dodatno podstaknut EU Direktivom o zadržavanju podataka, doveo je do toga da praksa pristupa zadržanim podacima o svim ostvarenim komunikacijama bude zakonom propisana.[76] To znači da svi operatori telefonije i interneta imaju obavezu da godinu dana čuvaju sve metapodatke o našim komunikacijama, uključujući i lokaciju sa koje je komunikacija ostvarena, kao i da nadležnim državnim organima odnosno policiji i službama bezbednosti, omoguće pristup tim podacima.[77] Međutim, iako je Direktiva o zadržavanju podataka preokrenuta u pravnom sistemu EU još 2014. godine zbog košenja sa pravom na privatnost propisanog Univerzalnom deklaracijom o ljudskim pravima,[78] domaći Zakon o elektronskim komunikacijama (ZEK)[79] nije pratio ovaj razvoj događaja. Čak i kada je 2023. godine usvojen novi ZEK, ostale su da važe odredbe stare verzije zakona koje se odnose na zadržavanje i pristup metapodacima o komunikacijama.[80]

Jedno od brojnih pitanja u vezi sa ovom problematičnom praksom jeste pristup, odnosno zaštita ovih podataka. Zaštitni mehanizam koji

Nevidljive infrastrukture: Elektronski nadzor i zadržavanje podataka sa mobilnih telefona, labs.rs



propisuje ZEK je takav da svi organi koji ostvaruju pristup podacima, ali i sami operatori, jednom godišnje Povereniku za informacije od javnog značaja i zaštitu podataka o ličnosti dostavljaju evidencije o pristupima metapodacima. Upravo je putem ovog mehanizma tim SHARE Fondacije pristupio infrastrukturi nadzora posredstvom zadržanih podatka. Poverenik je 2014. godine u odgovoru na zahtev za pristup informacijama od javnog značaja dostavio oko 2000 strana u vezi sa izveštajem o izvršenom nadzoru nad sprovođenjem i izvršavanjem Zakona o zaštiti podataka o ličnosti od strane operatora mobilne i fiksne telefonije u Srbiji.[81] Pregledom dokumentacije utvrđeno je da pored „redovnog" kanala pristupanja podacima (podnošenje zahteva uz nalog suda – odgovor operatora) nadležni organi direktno, takoreći samostalno, pristupaju bazama zadržanih podataka kroz posebne aplikacije razvijene za tu namenu. Tako se otvorilo pitanje ustavne zaštite tajnosti sredstava komuniciranja, koja zahteva sudsku odluku u slučajevima kada se odstupa od ustavnih garancija. Budući da su metapodaci sastavni deo komunikacije, imaju isti stepen zaštite kao i sam sadržaj, što je Ustavni sud i potvrdio odlukom iz 2013. godine.[82] Direktnim pristupom podacima o svakoj komunikaciji dramatično se krši privatnost komunikacije, bez obzira što se ne ostvaruje uvid u sam sadržaj telefonskih poziva ili SMS poruka. Takođe, pomoću dovoljne količine metapodataka mogu se utvrditi dnevno kretanje, navike, krugovi bliskih osoba i saradnika i drugi detalji života svake osobe koja koristi mobilni telefon.[83]

Kasnija istraživanja (2014-16 i 2017)[84] nadzora putem zadržanih podataka ukazala su da je direktan pristup metapodacima rasprostranjena praksa, odnosno da su tokom samo jedne godine pripadnici MUP-a ostvarili približno 200.000 pristupa kod jedinog operatora koji je takve pristupe beležio – tadašnjeg Telenora. Od 2018. godine, Telenor je prestao da Povereniku dostavlja informacije o samostalnim pristupima podacima,[85] a proces izveštavanja sveden je na formalno ispunjavanje zakonskih obaveza umesto stvarnog sprovođenja mehanizma kontrole.[86] Imajući u vidu da su evidencije koje Poverenik dobija raznolike po sadržaju i strukturi, kao i da suštinski ne daju pravu sliku celokupnog stanja, može se zaključiti da ovakav proces zapravo ne služi svrsi kontrole nadzora kroz pristupanje zadržanim podacima.

Paralelno sa zadržavanjem podataka inicirana je i obavezna registracija pripejd SIM kartica, koja je predložena još krajem 2013. godine,[87] ali predlog tada nije prošao, a nova prilika ukazala se 2016. godine kada su razmatrane izmene ZEK.[88] Skoro deceniju nakon prvog predloga, obavezna registracija pripejd kartica utvrđena je usvajanjem novog Zakona o elektronskim komunikacijama, kada je Ministarstvo informisanja i telekomunikacija početkom 2024. godine donelo Pravilnik o tehničkim uslovima za registraciju pripejd korisnika,[89] koje stupa na snagu 10. februara 2025. godine. Obaveznom registracijom korisnika pripejd kartica se sistem kontrole u neku ruku kompletira, imajući u vidu da je to bio jedini procep kada je reč o sveobuhvatnom nadzoru nad elektronskim komunikacijama.

Ključni argument za uvođenje ovakvih mera nadzor uglavnom je borba protiv kriminala. Međutim, efikasnost ozakonjenih mera nadzora za takvu svrhu je više nego upitna. Organizovane kriminalne grupe su sve veštije u planiranju i skrivanju aktivnosti i umesto tradicionalnih mobilnih mreža koriste specijalizovane aplikacije i uređaje poput Sky ECC, Ghost ili EncroChat.[90] Međutim, policijske službe širom sveta i sa takvim tehnologijama ne uspevaju da izađu na kraj i uspešno presretnu informacije o vršenju krivičnih dela.

POD BUDNIM OKOM

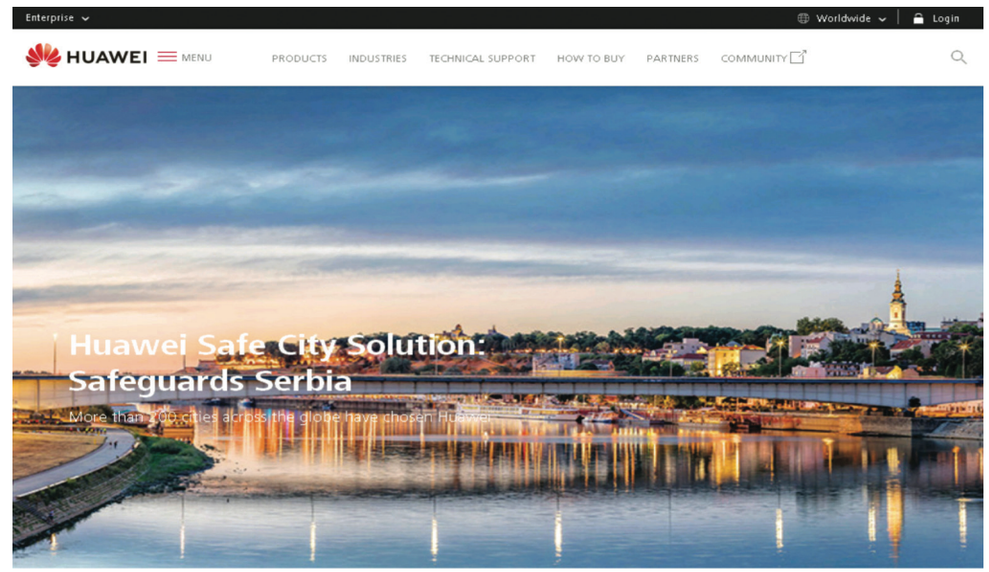
U Srbiji ne postoje posebne odredbe Zakona o zaštiti podataka o ličnosti kojima se reguliše video nadzor, već se primenjuju opšta pravila. U poslednjih deset godina, slučajevi kao što su „Beogradska arena", sudar kod Vlade Srbije i tabloidno praćenje aktiviste na

javnog značaja, tražeći dokumentaciju o lokacijama stacionarnih kamera, uključujući i analizu na osnovu koje su baš te lokacije odabrane, kao i detalje o javnoj nabavci i relevantnim procedurama. MUP je odgovorio da su svi dokumenti u vezi sa javnom nabavkom video nadzora zaštićeni stepenom tajnosti „poverljivo", dok tražene informacije o lokacijama i analizi nisu sadržane ni u jednom dokumentu, što je bilo u direktnoj suprotnosti sa izjavama zvaničnika.

Naročito interesantno je bilo pronalaženje informacija o studiji slučaja na sajtu kineskog IT giganta Huavej, koji je bio implementacioni partner MUP-a za projekat nove mreže video-nadzora. Huavej je na sajtu objavio mnoštvo detalja o mogućnostima video-nadzora i opremi koje ministarstvo nije stavilo na uvid javnosti. Nedugo nakon što je SHARE Fondacija objavila tekst o studiji slučaja,[93] ona više nije bila dostupna na sajtu Huavej, ali je njen sadržaj arhiviran na vreme.[94] Dakle, strana privatna kompanija je pružila više informacija o mogućnostima sistema nego sam državni organ koji treba da implementira projekat i rukovodi video-nadzorom.

Bio je to početak nove bitke za očuvanje privatnosti u javnom prostoru, imajući u vidu da intruzivne tehnologije poput prepoznavanja lica samo pojačavaju negativne efekte duboko ukorenjenih odnosa moći i kontrole. Zajednica eksperata, entuzijasta i boraca za ljudska prava oformila je inicijativu #hiljadekamera kako bi kroz postojeće pravne mehanizme i podizanje svesti u javnosti ukazala na nespojivost masovnog biometrijskog nadzora sa principima demokratskog društva.[95] U skladu sa Zakonom o zaštiti podataka o ličnosti za implementaciju takve obrade podataka neophodno je da se prethodno izvrši procena uticaja na ljudska prava i slobode i traži mišljenje Poverenika.[96] MUP je u septembru 2019. godine pripremio Procenu uticaja o najavljenom sistemu video nadzora, za koju je Poverenik izdao mišljenje da nije urađena u skladu sa relevantnim odredbama ZZPL.[97]

Aerodromu „Nikola Tesla", između ostalih, pokazuju dinamičnu istoriju zloupotrebe snimaka sa video nadzora.[91] Ipak, deluje da ne postoji adekvatna odgovornost niti svest da je video nadzor pre svega sredstvo koje bi trebalo da zadovolji određeni društveno značajni cilj, kao na primer zaštitu imovine ili javne bezbednosti, umesto da bude sredstvo za ostvarivanje bilo čijeg političkog, ličnog ili nekog drugog interesa.



Izvor: arhivirana stranica „Huawei Safe City Solution: Safeguards Serbia", mart 2019.

Početkom 2019. godine su ministar Nebojša Stefanović i direktor policije Vladimir Rebić, tada dva najviša funkcionera u oblasti unutrašnjih poslova, najavili da se priprema uvođenje sistema pametnog video nadzora sa 1000 kamera na 800 lokacija u Beogradu, koji će imati mogućnosti prepoznavanja lica i registarskih tablica.[92] U nedostatku javno dostupnih informacija o ovom poduhvatu, SHARE Fondacija poslala je MUP-u zahteve za pristup informacijama od

Na leto 2020. godine, u jeku pandemije, usledila je sledeća faza. Druga Procena uticaja MUP-a dostavljena Povereniku na mišljenje sadržala je mnogo više informacija, a pre svega u pogledu same infrastrukture.[98] Došli smo do ukupnog broja od 8.100 kamera različite vrste i namene – pored stacionarnih kamera na stubovima, saznali smo za kamere na vozilima policije i uniformama, kao i za mobilne uređaje (eLTE terminali) koji bi bili deo sistema. Poverenik je u novom mišljenju istakao da trenutno ne postoji pravni osnov za upotrebu takvog video nadzora i upozorio MUP da bi nameravanim radnjama direktno kršili zakon.

SHARE Fondacija i druge organizacije civilnog društva, zajedno sa ekspertima iz akademije učestvovali su na više sastanaka koje je MUP organizovao tokom 2021. i 2022. godine, kako bi se razgovaralo o potencijalnim zakonskim rešenjima za sistem pametnog video nadzora. Međutim, kako bi se obezbedio pravni osnov za primenu sistema, objavljena su dva Nacrta zakona o unutrašnjim poslovima. Prva verzija nacrta iz 2021. godine izazvala je brojne reakcije domaće i međunarodne javnosti i ubrzo je povučena iz procedure.[99] Prema rečima tadašnjeg ministra unutrašnjih poslova Aleksandra Vulina, nacrt je povučen na molbu predsednika Srbije Aleksandra Vučića.[100]

S obzirom da su se bližili parlamentarni, predsednički i lokalni izbori u aprilu 2022. godine, bilo je možda i očekivano da se tako značajan i sveobuhvatan propis ostavi za novu Vladu. Kraj 2021. godine su obeležili ekološki protesti i blokade, a u javnosti se pojavila bojazan da policija koristi sistem prepoznavanja lica kako bi putem video nadzora identifikovala učesnike i kažnjavala ih. Međutim, prema Poverenikovom nadzoru u sedištu MUP-a i Policijskoj upravi za grad Beograd, utvrđeno je da tehnologija prepoznavanja lica nije korišćena tokom protesta.[101]

Drugi nacrt zakona objavljen je pred kraj 2022. godine, u susret novogodišnjim praznicima i u paketu sa Nacrtom zakona o obradi podataka i evidencijama u oblasti unutrašnjih poslova.[102] Bile su predviđene opcije automatizovane i poluautomatizovane pretrage biometrijskih podataka kako bi se po potrebi utvrđivali identitet lica, njihova lokacija ili kretanje u realnom vremenu. Uzimajući u obzir iskustvo sa curenjem podataka i zloupotrebama ovlašćenja, delovalo je da distopijski scenario biometrijskog praćenja i identifikacije nezadovoljnih građana, aktivista, novinara ili političkih protivnika nije daleko. Ipak, opet pod pritiskom stručne javnosti, predsednica Vlade Ana Brnabić najavila je u poslednjim danima 2022. godine da se Nacrt zakona o unutrašnjim poslovima povlači iz procedure i da će biti sprovedene „široke konsultacije" o budućoj legislativi.[103] Od tada nije bilo novih predloga za legalizaciju upotrebe biometrijskog video nadzora u Srbiji.

Treba imati u vidu da bi usvajanje zakona koji bi regulisao upotrebu tehnologije za masovni biometrijski nadzor otvorilo veliko pitanje proporcionalnosti i opravdanosti odstupanja od prava na privatnost, ali i neophodnosti uvođenja takve mere u demokratskom društvu. Tokom 2023. godine Srbiju su zadesili brojni potresi, od masovnih ubistava u osnovnoj školi „Vladislav Ribnikar" i prigradskim naseljima Dubona i Malo Orašje, do protesta „Srbija protiv nasilja" posle kojih su raspisani vanredni izbori. Usledio je period prolongirane društvene i političke nestabilnosti, dok policija početkom novembra 2024. još uvek čeka novog direktora.[104]

NAVOĐENI PROJEKTILI

Špijunski softver koristi se od kada se koriste i računari i spada među najčešće korišćene vidove malicioznih programa (malware). Spajveri su moćno oružje jer mogu daljinski da pruže detaljne uvide u praktično sve informacije na uređaju koji zaraze, od prepiski, kontakata, fotografija, lokacije, kredencijala za pristup i tako dalje.

Sve ono što svakodnevno imamo na mobilnim telefonima glavna je meta napada spajverom.

Iako od spajver industrije i predstavnika država čujemo da se ovi alati koriste za borbu protiv kriminala i očuvanje nacionalne bezbednosti, mete spajvera su najčešće novinari, aktivisti, disidenti ili opozicionari. Informacije o masovnim zloupotrebama spajvera postale su predmet većeg interesovanja javnosti nakon što je kolektiv „Zabranjene priče" u saradnji sa forenzičkom laboratorijom organizacije *Amnesty International* i grupom medija objavio „Projekat Pegasus".[105] Objavljena je kolekcija priča[106] koje su na osnovu procurelih informacija ukazale na masovnu zloupotrebu Pegasus spajvera[107] u brojnim državama širom sveta, među kojima je bila Mađarska kao članica Evropske unije, ali i autoritarni režimi poput Saudijske Arabije.

U drugim EU članicama, Španiji,[108] Grčkoj[109] i Poljskoj,[110] kasnije su otkriveni spajver skandali koji su ostavili značajne društvene i političke posledice. U Grčkoj je zbog Predator spajvera koji je korišćen za targetiranje novinara i opozicije, skandal nazvan aferom „Predatorgejt".[111]

Ono što je naročito problematično kod naprednih spajvera kao što je Pegasus jeste infekcija uređaja koja ne zahteva reakciju mete (*zero-click*)[112] već je dovoljno da samo dobije malicioznu poruku. Takođe, infekciju uređaja spajverom često nije jednostavno otkriti, već je potrebno izvršiti detaljnu forenzičku analizu[113] koja ne garantuje da će biti otkriveno više informacija o samom targetiranju – ko stoji iza napada i sa kojim ciljem.

Kada je reč o Srbiji, upotreba spajvera ima već neku vrstu tradicije, imajući u vidu da su se još 2013. godine pojavile indicije u dokumentima Vikiliksa o nabavci softvera FinFisher/FinSpy[114] i Trovicor.[115] Posle curenja korporativnih podataka kompanije „Hacking Team",[116] otkriveni su mejlovi koji ukazuju da su bar dve domaće službe bezbednosti, BIA i VBA, bile u kontaktu sa predstavnicima HackingTeama i posrednicima.

Citizen Lab, istraživačka grupa sa Univerziteta u Torontu koja dugi niz godina prati upotrebu spajvera i drugih alata za nadzor, objavila je 2020. godine istraživanje o proizvodima kompanije *Circles*,[117] koja je povezana sa NSO grupom poznatom po tome što razvija Pegasus spajver. Nalazi Citizen Laba ukazali su na to da je Srbija jedna od država u kojoj je primećena tehnička infrastruktura povezana sa Circles proizvodima i da je njen potencijalni rukovalac BIA.

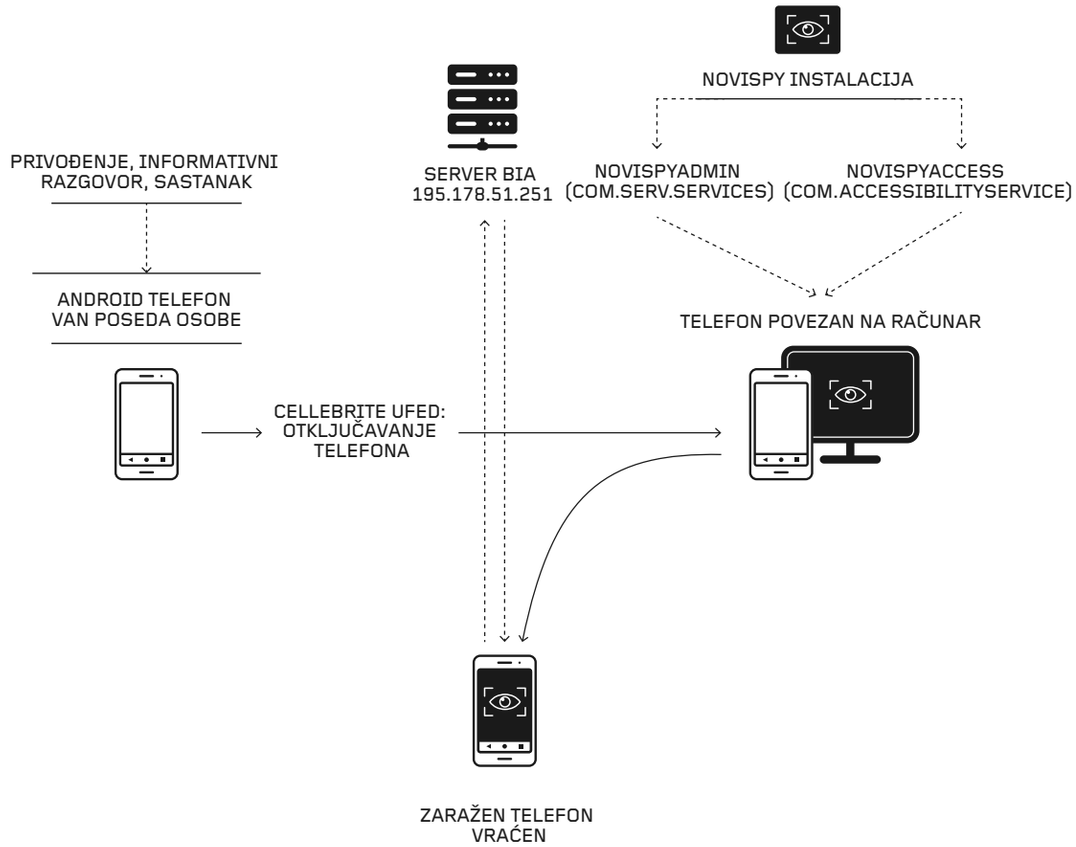
Pejzaž spajver pretnji je dosta širok i mada je moguće pretpostaviti da se koristi određena infrastruktura ili ranjivost, bez jasnih indikacija o targetiranju veoma je teško donositi zaključke o upotrebi spajvera. Guglova grupa za analizu pretnji (TAG) je u maju 2022. godine objavila nalaze o ranjivostima u Android operativnom sistemu i Chrome pretraživaču koje se mogu iskoristiti za targetiranje mobilnih telefona Predator spajverom.[118] Nalazi Gugla su se poklopili sa istraživanjem Citizen Laba da je Srbija jedna od država za koju se pretpostavlja da je korisnik Predator spajvera.[119]

Prelomni trenutak dogodio se krajem oktobra 2023. godine, kada je Apple korisnicima širom sveta poslao sistemske notifikacije[120] da su njihovi uređaji potencijalne mete spajvera. Dvoje predstavnika civilnog sektora iz Srbije zatražili su pomoć od SHARE Fondacije pošto su dobili takve notifikacije.[121] Uz pomoć organizacija Amnesty International,[122] Access Now[123] i Citizen Lab,[124] potvrdili smo da je spajverom bila targetirana ranjivost u HomeKit funkcionalnosti iPhone uređaja i da su napadi pokušani u avgustu 2023. godine. Pegasus spajver je ranije dovođen u vezu sa napadima na HomeKit i brojnim drugim ranjivostima.[125] O slučaju targetiranih predstavnika civilnog sektora iz Srbije izvestili su brojni svetski mediji, uključujući i britanski Gardijan.[126]

A onda je *Amnesty International* u decembru 2024. godine objavila izveštaj o dramatičnim razmerama upotrebe intruzivnih tehnologija protiv aktivista i novinara širom Srbije. Naime, tehničkom analizom je utvrđeno da su policija i BIA koristili forenzički alat kompanije *Cellebrite* da otključaju zaštićene telefone, a zatim direktno instaliraju spajver koji su istraživači nazvali *NoviSpy*. Pored mogućnosti da pravi skrinšotove sa telefona ih šalje na server BIA, *NoviSpy* može da ostvari intruzivne dozvole za pristup lokaciji, mikrofonu i kameri.[127]

Aktivistička zajednica predvođena organizacijama poput Amnesty International, Citizen Lab i Access Now pružila je ključni doprinos otkrivanju spajvera u raznim delovima sveta razvojem metodologija[128] i otvorenih alata kao što je Mobile Verification Toolkit (MVT).[129] Njihove aktivnosti su takođe podstakle kompanije Epl i Gugl da obaveštavaju korisnike koji su potencijalno targetirani spajverom. Još jedan značajan razvoj događaja je pojava opcije „Lockdown Mode"[130] u podešavanjima na Apple uređajima, za onemogućavanje funkcija koje se mogu zloupotrebiti kao ulazne tačke za spajver. Međutim, tehničke mere ne bi trebalo da budu jedina brana od špijunaže, već bi upotreba spajvera trebalo da se tretira kao što je već slučaj sa svakim drugim malicioznim softverom, odnosno da bude kažnjiva.

Prema Krivičnom zakoniku, posedovanje, distribucija i upotreba špijunskih softvera, kao vrste računarskih virusa, predstavlja krivično delo.[131] Takođe, svaki neovlašćeni pristup zaštićenim uređajima i podacima je kriminalizovan. Konačno, iako je primena posebnih dokaznih radnji i posebnih mera nadzora i obrade podataka u izuzetnim slučajevima zakonita, špijunski softveri svojom intruzivnom i neselektivnom prirodom prevazilaze granice zakonskih principa neophodnosti, srazmernosti, zaštite podataka o ličnosti i zaštite privatnosti. Dakle, neselektivna priroda upotrebe špijunskih softvera podrazumeva ne samo obradu podataka targetiranog lica, već i podataka svih ostalih lica koji se nalaze na uređaju. Takođe, kada se uzmu u obzir odredbe Zakona o zaštiti podataka o ličnosti,[132] Zakonika o krivičnom postupku[133] i drugih propisa koji uređuju uslove za odstupanje od prava na tajnost sredstava komunikacije, upotreba špijunskih softvera predstavlja neselektivno i obimom neograničeno prikupljanje podataka, tj. duboko zadiranje u privatnost građana.



KRITIČNA INFRASTRUKTURA: NESPRETNA DIGITALIZACIJA, NEODGOVORNOST DRŽAVE I POSLEDICE

Internet mapa Srbije, labs.rs

Život u savremenom društvu nezamisliv je bez složenih infrastruktura koje omogućavaju usluge poput zdravstvene zaštite, komunikacija, snabdevanja strujom ili vodom, transporta, finansija. Prekid funkcionisanja ili isporuke roba i usluga ovih sistema, mreža i objekata može ugroziti nacionalnu bezbednost, zdravlje i živote ljudi, imovinu, životnu sredinu, bezbednost građana, ekonomsku stabilnost, pa i funkcionisanje cele države. Stoga se ova specifično značajna infrastruktura naziva *kritičnom* i uređuje posebnim zakonom, koji propisuje nadležnost i odgovornost organa i organizacija u ovoj oblasti.[134]

Istorija kritičnih infrastruktura koja datira još od antike, predstavlja odgovor na povećanje potreba ljudi da u sve složenijim društvenim okolnostima jednostavnije funkcionišu i imaju kvalitetniji život. Posle industrijske revolucije, najveću transformaciju kritičnoj infrastrukturi su donele digitalne tehnologije, prvenstveno zahvaljujući mogućnostima boljeg povezivanja, efikasnijeg rukovođenja, praćenja i kontrole ovih sistema. Međutim, tehnološke mogućnosti prate i jednako značajne ranjivosti kritične infrastrukture pred različitim sajber napadima, isprva možda više iz radoznalosti nego iz loše namere pojedinaca, do vrlo sofisticiranih targetiranih napada koje izazivaju kolapse ogromnih razmera, a u kojima su neretko glavni akteri države.

Kritična infrastruktura, a posebno digitalna, može biti opasan instrument u rukama države, budući da svaka vrsta zloupotrebe može imati ogromne posledice, bilo da je meta druga država i njena infrastruktura, bilo da je reč o sopstvenoj kritičnoj infrastrukturi putem koje se može vršiti snažan pritisak i kontrola nad građanima. Stoga bilo kakva vrsta zloupotrebe ove vrste predstavlja jedan od važnih pokazatelja stanja ljudskih prava i demokratičnosti vlasti u jednoj zemlji.

ISTORIJA SAJBER NAPADA NA KRITIČNU INFRASTRUKTURU U SVETU[135]

RANI SAJBER INCIDENTI ('80-TE I '90-TE)

NAPAD: Napadi usmereni na akademske i državne institucije. Morisov crv (1988) bio je jedan od prvih značajnih sajber napada. Zaražavanjem hiljada računara, izazvao je poremećaje velikog obima.

KONTRAMERE: Bazične mere sajber bezbednosti fokusirane na tradicionalne antivirus softvere i odbranu mreže od spoljnih pretnji. Uviđa se potreba za robusnijim strategijama i merama zaštite.

STUXNET (2010)

NAPAD: Sajber oružje koje je targetiralo iranski nuklearni program i pokazalo da napadi na kritičku infrastrukturu imaju posledice na fizičke objekte.

KONTRAMERE: Države i organizacije počinju da razmatraju naprednije sisteme zaštite industrijskih kontrolnih sistema (ICS) i kritične infrastrukture od ovakvih napada.

PORAST DRŽAVNO SPONZORISANIH NAPADA (2010-TE)

NAPAD: Sve veća uloga država u sajber napadima: 22 dana dug sajber napad na Estoniju (2007), iranski napad na naftnu kompaniju Saudi Aramco (2012), napad Severne Koreje na Sony Pictures (2014). Ovim napadima identifikovane su kritične ranjivosti u različitim sektorima..

KONTRAMERE: Sveobuhvatne strategije za zaštitu protiv sajber napada, uključujući deljenje informacija, saradnju javnog i privatnog sektora i uspostavljanje institucija specijalizovanih za sajber bezbednost.

SAJBER NAPADI NA ELEKTROMREŽU U UKRAJINI (2015-2016)

NAPAD: Sajber napadi na ukrajinski elektroprenosni sistem (2015. i 2016) koji su izazvali nestanak struje širom zemlje. Napadi su pripisani hakerima podržanim od Rusije.

KONTRAMERE: Prepoznat značaj saradnje države i operatora kritične infrastrukture. Formiranje javno-privatnih partnerstava unapredilo je razmenu informacija o pretnjama i smanjilo jaz u znanjima i ekspertizi, što je dovelo do razvoja robusnijih odbrambenih mera.

WANNACRY RANSOMVER (2017)

NAPAD: Globalni ransomver napad iz 2017. godine. Targetirao je računare koji koriste Microsoft Windows da bi na njima enkriptovao podatke, nakon čega je tražen otkup u bitkoinima u zamenu za dekripciju. Značajno je uticao na sektore poput zdravstvene zaštite, transporta i finansijskih usluga.

KONTRAMERE: Svest o značaju čuvanja rezervnih kopija podataka, redovnom ažuriranju softvera, upravljanju ranjivostima i planovima za oporavak od sajber napada. Organizacije počinju da ulažu u obuke o sajber bezbednosti, podizanje svesti o fišingu i mogućnostima zaražavanja malverom.

TRITON/TRISIS NAPAD (2017)

NAPAD: Napad na petrohemijsku fabriku u Saudijskoj Arabiji 2017. Bio je to prvi poznati sajber napad koji je eksplicitno dizajniran da manipuliše industrijskim kontrolnim sistemima i sistemima bezbednosnih instrumenata. Ovaj slučaj je ukazao na mogućnosti da sajber napadi ugroze bezbednost ljudi u objektima kritičke infrastrukture.

KONTRAMERE: Organizacije i stručnjaci počeli da rade na specijalizovanim rešenjima kao što su obezbeđivanje segmentacije mreže i integracija mera sajber bezbednosti u dizajn industrijskih sistema.

SOLARWINDS (2019)

NAPAD: Jedan od najsofisticiranijih sajber napada u istoriji. Inficirano je preko 18.000 organizacija, uključujući i državne službe, biznise i univerzitete.

KONTRAMERE: Incident je otkrio ranjivosti u lancima snabdevanja softverom, što je podstaklo detaljnu reviziju bezbednosnih praksi dobavljača. Kompanije su počele da uvode strože procedure za proveru trećih strana i redovno procenjuju njihove bezbednosne kontrole. „Zero trust" arhitektura stekla je popularnost kao pristup za sprečavanje lateralnog kretanja unutar mreža, osiguravajući da uređaji ili korisnici nemaju podrazumevano poverenje za pristup informacijama.

COLONIAL PIPELINE RANSOMVER NAPAD (2021)

NAPAD: U maju 2021. godine, Colonial Pipeline naftovod pretrpeo je jedan od najvećih napada na ključnu nacionalnu infrastrukturu u istoriji SAD. Napad je izazvao nedostatke goriva i paničnu kupovinu.

KONTRAMERE: Povećan fokus na mere kao što su jačanje mrežne bezbednosti, usvajanje naprednih alata za detekciju pretnji i sprovođenje rigoroznih bezbednosnih procena. Pojačana saradnja javnog i privatnog sektora u koordinaciji odgovora na incidente.

Razvoj kritične infrastrukture u Srbiji obeležavaju ne samo ranjivosti koje prate globalne trendove, već i specifični problemi lokalnog konteksta. Pokazuje se da je insistiranje na tehnosolucionizmu uz nedostatak ekspertize i adekvatne prevencije ovakvih incidenta otvorilo široko polje problema sa ozbiljnim posledicama za pojedince, društvo i državu. Tome svakako doprinosi nemar ili pak odsustvo svesti prvenstveno o značaju zaštite podataka o ličnosti, privatnosti, osetljivih podataka, bezbednosti informacija i slično, koji su za sada najviše bili ugroženi usled nedovoljno zaštićenih kritičnih infrastruktura. Sve ovo deluje dodatno problematično ukoliko se uzme u obzir rast nivoa sofisticiranosti ovakvih napada koji u Srbiji ne nalazi odgovarajući zakonski i institucionalni odgovor, budući da su postojeći zakoni više usmereni na saniranje posledica nego na prevenciju.

Srbija je prvi Zakon o informacionoj bezbednosti dobila 2016. godine, a skoro deceniju kasnije kaska se u nadzoru nad poštovanjem njegovih odredbi.[136] Kao organ nadležan za nadzor imenovano je Ministarstvo za poslove informacione bezbednosti, što je uglavnom u dosadašnjim vladama spadalo u resor telekomunikacija. Međutim, imajući u vidu složenost izazova i ograničene kapacitete ministarstva, nisu ostvarena očekivanja u pogledu nadzora nad sprovođenjem Zakona o informacionoj bezbednosti. Poverenik je delimično nadležan za sajber incidente, odnosno samo u situacijama kada postoje indicije da su ugroženi podaci o ličnosti građana. Međutim, uloga Kancelarije Poverenika uglavnom je ograničena na „post mortem" delovanje, tj. sprovođenje nadzora nakon što se incident već dogodio.

U Srbiji, primera radi u periodu kada je Ana Brnabić bila premijerka, digitalizacija je bila jedan od strateških prioriteta Vlade. Iako građani jesu dobili značajne mogućnosti da putem servisa kao što je eUprava ili drugi e-portali obave različite poslove, utisak je da su bezbednost informacija i zaštita podataka o ličnosti na ovim servisima imali sasvim sporedni značaj. Tako je 2018. godine na eUpravi evidentiran propust u administraciji servera, koji je omogućio da građani pristupaju delu sajta gde ostavljaju svoje lične podatke i kroz vezu koja nije adekvatno zaštićena.[137]

JEDAN FAJL ZA SVE

Decembar 2014. godine obeležio je slučaj Agencije za privatizaciju, incident koji predstavlja prekretnicu koja je uspostavila neku vrstu modela za to kako će se slični slučajevi u budućnosti odvijati.[138] Internetom je kružio link ka fajlu koji je sadržao podatke o ličnosti više od 5 miliona građana koji su se 2008. godine prijavili za besplatne akcije, dakle gotovo celokupnog punoletnog stanovništva Srbije. Imena i prezimena, imena roditelja, matični brojevi, status u evidenciji agencije – svako ko se prijavio za besplatne akcije i na Gugl pretrazi upisao svoj JMBG mogao je da dobije link ka ovom fajlu kao rezultat. Nakon što je tim SHARE Fondacije obavestio Poverenika za informacije od javnog značaja i zaštitu podataka o ličnosti o ovom alarmantnom saznanju, brzom reakcijom onemogućen je dalji pristup podacima.

Međutim, u nadzoru koji je sprovela Kancelarija Poverenika, utvrđeno je da je fajl bio javno dostupan od februara 2014. godine, dakle približno 10 meseci, i da je za to vreme preuzet „više puta".[139] Dakle, baza podataka o ličnosti gotovo svih punoletnih građana završila je izvesno u nepoznatim rukama nepoznato puta. Tadašnja v.d. direktorka Agencije obavestila je Poverenika da je u pitanju pomoćni fajl namenjen pretrazi na sajtu Agencije i napomenula da se do interne adrese fajla moglo doći samo neovlašćenim pristupom veb serveru Agencije. Agencija je podnela krivičnu prijavu protiv NN lica povodom incidenta koja, koliko je poznato, do danas nije dobila pravni epilog. Sa druge strane, Poverenik je već početkom 2015. godine upozorio Agenciju da nije preduzela odgovarajuće tehničke,

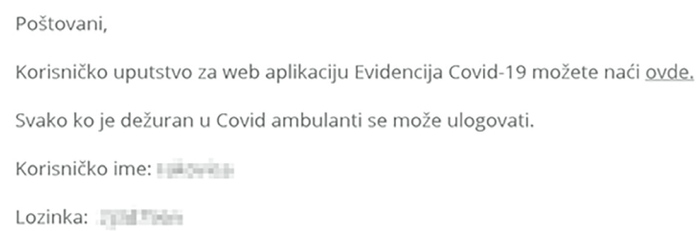
kadrovske i organizacione mere zaštite podataka o ličnosti. Pošto nema ovlašćenje za direktno sankcionisanje, Poverenik je takođe podneo zahtev za pokretanje prekršajnog postupka protiv Agencije i odgovornih lica pred nadležnim sudom.

Postupak je prolongiran i međuvremenu je Agencija ugašena u januaru 2016. godine, a prekršajna odgovornost zastarela je početkom 2017. godine.[140] Za najveći proboj u privatnost građana Srbije i kompromitaciju JMBG kao jedinstvenog i nepromenjivog identifikatora niko nije odgovarao. Nisu ni preduzete bilo kakve mere ublažavanja posledica kompromitacije JMBG, odnosno zamene službene upotrebe ovog identifikatora nekim drugim koji ne bi otkrivao podatke o osobi poput datuma rođenja. Recimo, u Hrvatskoj je 2009. godine uveden osobni identifikacijski broj (OIB) koji je nasumično generisan i ne sadrži druge podatke o ličnosti, a dodeljuje ga Poreska uprava.[141] U Srbiji takođe postoje jedinstveni brojevi koji ne otkrivaju podatke o ličnosti, poput Ličnog broja osiguranika (LBO) ili broja lične karte, koji bi mogli biti adekvatnije rešenje od matičnog broja.

U međuvremenu usvojeni su novi Zakon o zaštiti podataka o ličnosti (ZZPL), koji je uskladio domaći okvir pravni okvir sa Opštom uredbom EU o zaštiti podataka – GDPR, kao i Zakon o informacionoj bezbednosti (ZIB)[142] koji je, između ostalog, propisao mere zaštite informacionih sistema od posebnog značaja u javnom i privatnom sektoru. Sa regulatornog aspekta, išlo se ka standardima EU, ali digitalizacija javnih usluga je i dalje nespretno kaskala za utvrđenim standardima, uz naknadno razmišljanje o zaštiti podataka o ličnosti i informacionoj bezbednosti.

Bezbednosna kultura u društvima poput Srbije ne može da se izgradi brzo, a samo usvajanje zakona nije dovoljno. Potrebno je da postoji sistemsko-strateški pristup informacionoj bezbednosti i zaštiti podataka o ličnosti koji će na odgovarajući način usmeriti javni sektor da štiti IKT sisteme, u skladu sa njihovim nadležnostima i mogućnostima. Prema podacima istraživanja o sajber kulturi u Srbiji za 2020. godinu[143] koje je objavio Nacionalni CERT, tek svaki četvrti građanin veruje da država obezbeđuje bezbednost njihovih podataka, što ukazuje na nisku stopu poverenja u državne organe po pitanju informacione bezbednosti.

PANDEMIJA JEDNE LOZINKE


Poštovani,

Korisničko uputstvo za web aplikaciju Evidencija Covid-19 možete naći ovde.

Svako ko je dežuran u Covid ambulanti se može ulogovati.

Korisničko ime:

Lozinka:

Pandemija jedne lozinke. Kako je šifra za Covid-19 završila na internetu?, SHARE Fondacija

Početak 2020. godine zatekao je svet u haosu izazvanom pandemijom virusa kovid-19, najvećom globalnom krizom u dosadašnjem toku 21. veka. Praćenje kontakata, zabrane kretanja i slične mere su tokom pandemije otvarale prostor ka distopiji nadzora.[144]

U Srbiji je vanredno stanje proglašeno ubrzo nakon prvog potvrđenog slučaja infekcije kovidom i razvijen je *Informacioni sistem COVID-19*, centralizovani informacioni sistem za prikupljanje i obradu svih podataka o pandemiji.[145] U IS COVID-19 podatke su unosile sve zdravstvene ustanove u kojima se leče oboleli, svi instituti i zavodi za javno zdravlje, sve laboratorije u kojima se sprovodilo testiranje, kao i „drugi nadležni organi i organizacije" bez jasnijeg određenja. Polovinom aprila 2020. godine, tim SHARE Fondacije je otkrio da

su pristupni kredencijali za IS COVID-19 bili indeksirani na Guglu, samim tim javno dostupni na sajtu jedne zdravstvene institucije.[146] Odmah po saznanju za incident obavestili smo Poverenika za informacije od javnog značaja i zaštitu podataka o ličnosti, Nacionalni CERT i Ministarstvo trgovine, turizma i telekomunikacija. Svesni rizika, informacije smo podelili javno tek pošto smo se uverili da je onemogućen neovlašćen pristup sistemu. Korisničko ime i lozinka bili su osam dana javno dostupni na sajtu što je dovoljno da se ova stranica indeksira na Guglu i bude pretraživa.

Po već ustaljenom obrascu, Poverenik je posle incidenta sproveo nadzor nad Institutom za javno zdravlje „Dr Milan Jovanović Batut", koji je bio rukovalac sistema, odnosno odgovorni entitet za sve u vezi sa obradom podataka o ličnosti. Zbog niza propusta u rukovođenju sistemom, Poverenik je Institutu izrekao samo opomenu.[147] Između ostalog, ispostavilo se da Institut kao rukovalac u trenutku incidenta nije imao zaključene ugovore sa obrađivačima podataka, a pre svega sa Republičkim fondom za zdravstveno osiguranje (RFZO) koji je pružao tehničku podršku korisnicima. Nadzorom je utvrđeno da nisu bile preduzete odgovarajuće mere zaštite sistema, niti je bila urađena procena uticaja na zaštitu podataka, koja je prema ZZPL u ovom slučaju bila obavezna pre nego što se sistem pusti u rad. Naročito je bilo interesantno da je Institut tvrdio da nije došlo do „pokušaja logovanja na sistem" pre promene pristupnih kredencijala, a RFZO da „podaci nisu kompromitovani", iako je predstavnik službe Poverenika istakao da je uspeo da se uloguje u IS COVID-19 sa javno objavljenim kredencijalima. Na osnovu ovoga moglo se zaključiti da sistem nije beležio pristupe, što je jedna od glavnih mera kontrole pristupa i mera propisana ZIB. Tokom trajanja nadzora, Institut je ispunio neke od obaveza, bar formalno. Ipak, suštinski je ponovo izbegnuta odgovornost za veliki sajber incident, ovog puta u naročito osetljivom trenutku za celo društvo i nad najosetljivijim podacima o zdravlju građana.

JAVNA PREDUZEĆA POD KLJUČEM

Ransomver je jedan od najozbiljnijih izazova po informacionu bezbednost na globalnog nivou, s obzirom na to da može da se koristi za više ciljeva, bilo da su oni ekonomski (sajber kriminal) ili politički (sajber ratovanje). Napad ransomverom funkcioniše tako što se pristup podacima u informacionom sistemu prvo onemogućava enkripcijom, a onda napadač zahteva naknadu u kriptovalutama da bi meti obezbedio dekripcioni ključ sa kojim mogu da povrate pristup podacima.

Pored korporativnog sektora, napada ransomverom nisu pošteđene ni obrazovne ustanove, bolnice i druge institucije od kritičnog značaja za društvo. Uspešno izvedeni ransomver napadi mogu da naprave ogromnu materijalnu štetu i onesposobe redovno funkcionisanje usluga. Kada je Kolonijal pajplajn naftovod napadnut 2021. godine, snabdevanje gorivom na istočnoj obali SAD bilo je otežano i nastala je panika među građanima koji su masovno kupovali benzin.[148]

Ransomver u Srbiji nije bio tema koja je privlačila veću pažnju van stručnih krugova sve do marta 2020. godine, kada se na meti našla Informatika, novosadsko javno komunalno preduzeće, čija je celokupna infrastruktura bila zaražena malicioznim softverom koji zaključava računare i servere.[149] Bio je to prvi javno poznati slučaj ransomver napada na domaći javni sektor, i to u jeku kriza u vezi sa koronavirusom. Iako je Informatika imala antimalver softver, upravo kada se napad desio saznalo se da njihova licenca nije uključivala ransomver zaštitu. Forenzička analiza otkrila je da je ransomver verovatno ušao kroz mejl, te da se kroz ceo sistem širio kada je neko od zaposlenih otvorio poruku sa zaraženim prilogom. Kada se izvrši napad ransomverom, napadači koji su ekonomski motivisani po pravilu ostave poruku o zahtevima i uputstvo za uplatu u kriptovalutama. Informatici su najpre tražili 50 bitkoina koji je u to vreme vredeo oko 10.000 dolara, da bi nakon kratke prepiske spustili

otkup na 20 bitkoina. Gradska uprava Novog Sada je odbila da plati otkup, pa su podaci i bekap ostali zaključani.

Tokom nadzora, Poverenik je ustanovio da je pored podataka zaposlenih oko 2000 računara bilo kompromitovano napadom, te da zaposleni nisu mogli da pristupe mejl nalozima. Nisu bili ugroženi podaci o ličnosti građana koji se obrađuju u svrhu izdavanja računa u okviru objedinjene naplate zato što su podaci obrađivani na Linuksu, a ransomver je napadao samo Windows operativne sisteme. Ipak, napadom su bile zahvaćene rezervne kopije što je onemogućilo povraćaj zaključanih podataka, gradske kamere nisu funkcionisale, a posledica je bila i nemogućnost obračuna zarada, evidencije bolovanja i svih drugih vrsta kadrovske evidencije. Naposletku, Informatika je pristupila izradi nove hardversko-softverske arhitekture informacionog sistema preduzeća.

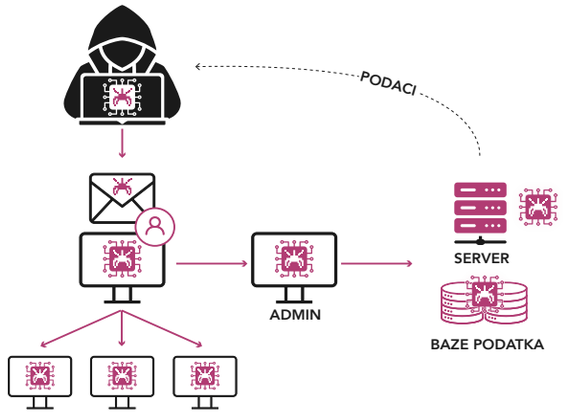
Kriza informacione bezbednosti koja je zahvatila Novi Sad nije dugo trajala, a po stanju stvari nije značajno uticala na svest o rizicima poput ransomvera. Incident u jednom lokalnom javnom preduzeću se možda nije činio kao presedan, ali sledeći veliki ransomver napad izazvao je mnogo više pažnje. U junu 2022. godine dogodio se incident u infrastrukturi Republičkog geodetskog zavoda (RGZ) usled koga je otpočeo niz problema jer su servisi postali nedostupni spoljnim korisnicima.[150]

Imajući u vidu da je u okviru RGZ Katastar nepokretnosti, izazvan je zastoj na tržištu nekretnina jer javni beležnici nisu imali pristup informacionom sistemu, a RGZ je tvrdio da su u napadu oštećeni delovi sistema koji ne sadrže podatke o ličnosti i nepokretnostima.[151] Iz saopštenja RGZ mogli smo da saznamo da se radilo o Phobos ransomveru, ali da nije identifikovana poruka za zahtevom za otkup.[152] Servisi RGZ su postepeno puštani u rad u nedeljama nakon incidenta, pa su tako i službe katastra širom Srbije otpočinjale rad sa građanima,[153] da bi od 11. jula sve službe bile ponovo funkcionalne.[154]

Poverenik je u drugoj polovini jula objavio saopštenje o sprovedenom nadzoru nad RGZ i zaključio da nema povrede podataka o ličnosti prema ZZPL, jer predmet napada „nisu bili serveri na kojima se čuvaju baze podataka sa podacima o ličnosti i nepokretnostima kao ni E-katastar".[155] Zapisnik Poverenika iz sprovedenog nadzora pokazao je da je napad došao sa IP adresa sa teritorija Bugarske, Holandije, Litvanije i Sejšela, te da su zloupotrebljeni pristupni kredencijali naloga zaposlene koji se dugo vremena nije koristio jer je bila na bolovanju.[156] U napadu je prema nalazima Poverenika od ukupno 460 servera RGZ bilo kompromitovano 20 aplikativnih servera, kao i 6 radnih stanica od nešto više od 3000. Nalaz službe Poverenika da nije nastupila povreda podataka o ličnosti bio je u najmanju ruku neočekivan, pošto se i gubitak pristupačnosti svakako kategoriše kao povreda podataka.[157]

Kraj 2023. godine obeležio je incident sa Elektroprivredom Srbije (EPS), jednim od najvećih i najvažnijih preduzeća u Srbiji. Na sajtu EPS je 19. decembra objavljeno saopštenje sa vrlo šturim informacijama, u kome se navodi da se kompanija oporavlja od nezapamćenog hakerskog napada, ali da proizvodnja i snabdevanje električnom energijom nisu ni na koji način ugroženi.[158] Istovremeno su zamolili korisnike portala „Uvid u račun" za strpljenje i podsetili da je nedavno i slovenačka elektroprivreda doživela sličan napad, kao da je to olakšavajuća okolnost. Izdavanje novembarskih računa za struju je kasnilo[159] i građanima je bilo onemogućeno da račune plaćaju na šalterima EPS praktično dva meseca – tek je u drugoj polovini februara 2024. godine v.d. generalnog direktora izašao u javnost sa informacijom da su šalteri proradili.[160] Odgovornost za napad je preuzela hakerska grupa Qilin, koja je na dark veb sajtu objavila slike dokumentacije EPS i zapretila objavljivanjem svih poverljivih informacija do kojih su došli ukoliko ne dobiju otkup u roku od 10 dana.[161] Grupa Qilin je zatim u januaru 2024. godine omogućila za preuzimanje oko 34 gigabajta podataka.[162] Međutim, ove podatke je bilo veoma teško preuzeti radi potvrđivanja autentičnosti pošto se

linku za preuzimanje moglo pristupiti samo preko Tor mreže,[163] koja je veoma spora.



Iz EPS su u obaveštenju Povereniku naveli da u momentu slanja nije došlo do kompromitacije podataka o ličnosti, kao i da su izolovane „baze koje koriste sistemi za naplatu, izdavanje računa, u kojima se nalaze podaci građana, zatim sistemi koji sadrže podatke o poslovanju i partnerima, ali i baza ljudskih resursa u kojima su podaci zaposlenih".[164] Poverenik jeste sprovodio nadzor u EPS tokom januara 2024. godine,[165] ali se nije naknadno oglašavao u vezi sa eventualnim povredama podataka o ličnosti.

Nakon niza velikih kompromitujućih ransomver napada u Sjedinjenim Američkim Državama, tamošnje ministarstvo pravde odlučilo je da ovakve slučajeve tretira sa sličnom ozbiljnošću kao i terorističke napade, i na taj način jasno pokazalo da ove napade smatra ogromnom pretnjom po svoju državu.[166] Iako je Srbija znatno manje tržište, i samim tim od manjeg interesa za svetske ucenjivače, slučaj Informatike, i kasnije RGZ-a i EPS-a jasno pokazuju da su ovakvi napadi ne samo mogući i ovde, već mogu imati ozbiljne posledice po funkcionalnost kritične infrastrukture.

RANJIVE GRUPE I DIGITALNO ISKLJUČIVANJE: DISKRIMINACIJA KAO STUB DIGITALNE NEJEDNAKOSTI

Višegodišnji monitoring pokazao je da se specifična forma nasilja posebno uobličila prema ženama i devojčicama, ali i mnogim drugim ranjivim pojedincima i zajednicama kao što su LGBTQAI+, etničke manjine, izbeglice i migranti i socio-ekonomski ugrožene grupe. Isključivanje iz digitalnih prostora predstavlja ozbiljnu strategiju za ućutkivanje glasova marginalizovanih grupa kojima su ovi kanali ponekada najvažnija glasila. Načini na koje se ovo isključivanje postiže variraju i neretko se služe dodatnim spornim praksama kao što je širenje govora mržnje, uvreda i diskriminatornih komentara i organizovanog napadanja i prijavljivanja na mrežama. Mehanizmi zaštite na mrežama su svakako niski, tako da su dodatno ugrožene grupe izložene velikom broju napada koje je često jako teško dokazati i sankcionisati. U isto vreme, institucionalne zaštite za ove grupe često su sporne i u analognom prostoru, što dodatno otežava situaciju i dovodi do relativizacije ovakvih napada u digitalnom prostoru. Kroz nekoliko ključnih grupa koje se nalaze na udaru ovakvih opasnih praksi – žene, izbeglice i migranti, nacionalne i etničke manjine, deca i mladi i socio-ekonomski ugroženi – lako se ispisuje priča posrnulog sistema države koji umesto da pruža zaštitu, zanemaruje, ignoriše i u nekim slučajevima čak i podstiče nejednakost unutar svoje zemlje.

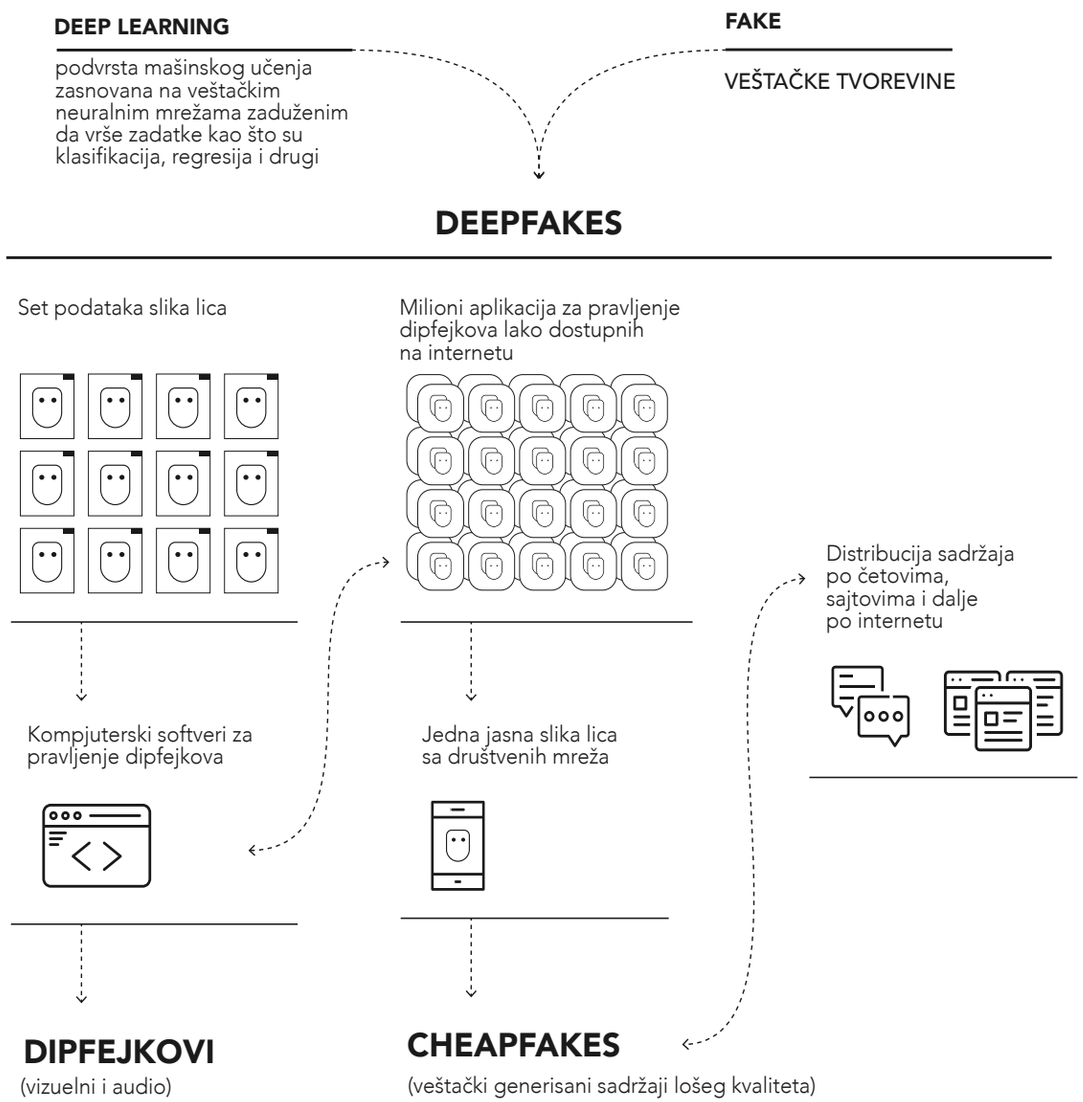
RZDN KAO KONSTANTA

Rodno zasnovano nasilje posredstvom tehnologije, ili rodno zasnovano digitalno nasilje karakteriše napade koji se zasnivaju na mizoginim, homofobnim i/ili seksističkim stereotipima, a pomognuti su korišćenjem digitalnih tehnologija. Neretko se obrasci ‘tradicionalnog’ rodno zasnovanog nasilja prenose u digitalni prostor, što potvrđuje njihovu štetnost i destruktivni potencijal. Ovakvi napadi često za cilj imaju ućutkivanje i zastrašivanje žena i drugih marginalizovanih grupa, sa namerom da ih isključe iz debate i javnog prostora.[167] Prethodna decenija jeste doprinela umrežavanju

i na taj način pomogla ženama, devojkama i devojčicama koje su se suočile sa rodno zasnovanim nasiljem da svoja iskustva podele na mrežama, kao što je to bilo sa kampanjama #metoo i #nisamprijavila, koje su obe zaživele u Srbiji nakon užasnih saznanja o rodno zasnovanom seksualnom uznemiravanju i napadima. Ipak, kako se monitoring izoštravao u beleženju ovakvih slučajeva, postalo je jasno da obim ovakvih napada ne jenjava, ali se itekako razvija i poprima nove oblike.

Tehnološki izvršeno rodno zasnovano nasilje ne podleže ni socio-ekonomskom statusu, godinama niti političkom opredeljenju, i samim tim je skoro nemoguće obuhvatiti sve incidente. Po uzoru na svetske trendove, slučajevi koji zavređuju najviše pažnje su napadi na novinarke, javne ličnosti i političarke, često zbog njihovih stavova i aktivističkog angažmana. Ipak, u poslednjih nekoliko godina, rasprostranjenost napada koji se temelje na rodnim karakteristikama je eksponencijalno porasla i ovakvi slučajevi se sve češće beleže i kod „običnih" građana. Česta anonimnost izvršitelja, a time i osećaj nekažnjivosti, neretko pruža dodatan vetar u leđa za dalje napade i maltretiranje, a nedovoljna zakonska regulisanost ovakvih incidenata može biti obeshrabrujuća za one koje se nađu na oštećenoj strani. Drugi problem predstavlja (ne)poverenje da će na ovakve slučajeve adekvatno reagovati policija i tužilaštvo, kao i same kompanije koje su vlasnice društvenih platformi. Neretko se događa da od Fejsbuka, Instagrama, TikToka ili Telegrama ili nema odgovora ili su u pitanju opšti odgovori na prijave u kojima se navodi da su njihovi kapaciteti preopterećeni brojem prijava koje dobijaju i da nemaju procenu kada će pristupiti slučaju. Čak i kada do reakcije dođe i u najvećem broju slučajeva ovi nalozi budu ugašeni, ne postoji nikakav sistem zaštite koji sprečava kreiranje novih naloga i ponovnog upadanja u ciklus zlostavljanja od strane izvršilaca.

Seksistički i mizogini komentari i uvrede predstavljaju konstantu od samog početka monitoringa pre deset godina, samo se njihova



rasprostranjenost još više proširila. U većini slučajeva zabeleženih u monitoringu, svaki napad na političarke, novinarke, javne ličnosti i druge žene praćen je pogrdnim komentarima o njihovom izgledu i drugim rodno obojenim uvredama i komentarima. Sa druge strane, ubrzani napreci u digitalnim tehnologijama otvaraju nove prostore za zloupotrebe i nasilje, pogotovo kada su u pitanju alati za manipulaciju ili potpuno fabrikovanje sadržaja. Prema podacima iz 2023. godine, za manje od 25 minuta može besplatno da se napravi dipfejk pornografski video u trajanju od minut uz pomoć samo jedne jasne fotografije lica. Isto istraživanje takođe je pokazalo da je 98% svih dipfejk videa koji postoje na internetu pornografski sadržaj koji je sintetizovan putem veštačke inteligencije i da u 99% odsto slučajeva ovi sadržaji targetiraju žene.[168] U svojoj osnovi, pretnja veštački generisanog sadržaja intimne prirode ide mnogo dublje od samog sadržaja – ovaj sadržaj poručuje ženama i devojkama da njihova tela ne pripadaju njima, već samo njihov lik je dovoljan da se od njega reproducira novo telo, koje nije stvarno ali je vidljivo. Osećaj otuđenja izazvan posredstvom ovih sadržaja kod žena prebroditeljki ovakvog nasilja može izazvati ogromne psihološke probleme i uticati na njihovu percepciju sebe.

Uz rast popularnosti generativne veštačke inteligencije, rastu i zloupotrebe u polju rodno zasnovanog onlajn nasilja. Na raskrsnici tehnologija koje omogućavaju generisanje veštačkih sadržaja uz pomoć autentičnih slika i snimaka, poznatih kao dipfejk (deepfake) tehnologija, i osvetničke pornografije, postavljaju se mnoga pitanja na koja je i dalje teško pronaći odgovore. Ni državni organi, ni tehnološke platforme nisu još pronašli adekvatan način da se suoče sa ovim rastućim trendom, i sve dok se to ne dogodi veliki broj žena i devojaka naći će se u nemogućim situacijama. Ovo je svakako potvrđeno kada je prošle godine nepoznata osoba otvorila naloge na različitim društvenim mrežama radi targetiranja devojaka iz beogradskog naselja Batajnica. Na ovim nalozima objavljene su slike i snimci devojaka, uključujući seksualno eksplicitne, koji su najvećem broju slučajeva bili praćeni uvredljivim i zlostavljačkim komentarima. Sa tih naloga su objavljivani i eksplicitni snimci devojaka napravljeni posredstvom generativne veštačke inteligencije. Mnoge objave pratili su i lični podaci devojaka, njihova imena, adrese na kojima rade, pa čak i kućne adrese. U sličnom scenariju, nalozi su prijavljivani više puta ali su ili ostajali aktivni ili, u slučaju da jesu deaktivirani, pojavljivali su se novi koji su samo nastavljali tamo gde su prethodni stali. Iz policije je izostala hitna reakcija, a ni Tužilaštvo za visokotehnološki kriminal nije bilo preterano ažurno u obaveštavanju devojaka o razvoju slučaja.[169] Doduše, ovaj slučaj je delimično dobio zaključak pozitivan za oštećene devojke, ali je malo verovatno da će se incident poslužiti kao motiv institucijama da razmotre odgovarajuće sistemske promene.

Dok je 2020. godine koronavirus predstavljao ozbiljnu pretnju po javno zdravlje i paralisao ne samo Srbiju već i ceo svet, žene su ujedno morale da se obračunavaju i sa još jednom epidemijom. Istraživanja su pokazala jasnu vezu između pandemije koronavirusa i porasta rodno zasnovanog nasilja širom celog sveta, sa posebnim akcentom na rodno zasnovano digitalno nasilje koje je bilo u eksponencijalnom porastu.[170] Pored nasilja koje žene u ovakvim situacijama trpe kod kuće, dešava se da se nađu i na nasumičnoj meti, na mestima gde bi trebalo da budu zaštićene i sigurne. Naime, krajem 2020. godine, iz privremene kovid bolnici koja je bila smeštena u Areni, na Tviteru su osvanule fotografije devojke koja se skidala u sobi za preglede uz komentar „Lepša strana kovida".[171] Iako je na mrežama osoba koja je okačila sliku naišla na salve kritika i objava je brzo uklonjena, to ne znači da fotografija već nije sačuvana zauvek u dubinama interneta. Da stvar bude još gora, gotovo svi mediji preneli su „vest" i usput koristili izvornu fotografiju, neki cenzurisanu ali ne i svi. Ovakav potez medija donekle ilustruje duboke korene ovog rodnog problema, gde uprkos osudi poteza i dalje biraju da fotografiju dalje cirkulišu i na taj način privuku čitaoce.

Tokom 2021. godine, otkrivene su broje Telegram grupe u kojima su se razmenjivale intimne fotografije i snimci žena, devojaka i devojčica bez njihovog znanja i saglasnosti. Uz ove sadržaje takođe su objavljivana imena i prezimena žena, iz kojeg su mesta kao i njihovi profili na društvenim mrežama. Ubrzo je ustanovljeno da su ove grupe aktivne u celom regionu kao i da broje desetine hiljada članova.[172] Nakon što je u javnost dospela informacija o postojanju ovih grupa kao i o vrstama sadržaja koji se u njima razmenjuje, veliki broj grupa je ubrzo ugašen, ali su se mnoge opet pojavljivale. Otkrivanje ovih grupa pomoglo je da se u javnosti podigne svest o takozvanoj „osvetničkoj pornografiji", njenim oblicima i pretnjama po žene i devojke.[173] „Osvetnička pornografija" predstavlja jedan od prvih oblika rodno zasnovanog digitalnog nasilja koji je uspeo da globalno skrene pažnju na neravnopravnost digitalnog nasilja između muškaraca i žena, kao i da pokrene neke države da preuzmu aktivniju ulogu u zaštiti žena, devojaka i devojčica na internetu. Ipak, proces podizanja svesti o ovom vidu nasilja je sam po sebi predstavljao veliki izazov za borkinje za ženska prava, jer su se od samog početka susretale sa neslaganjem, napadima, kritikama i opstrukcijama. Sam termin „osvetnička pornografija" dokaz je toga koliko je ova borba delikatna i višeslojna – obe reči mogu imati negativnu konotaciju, od sugestije da su intimni sadržaji podeljeni bez saglasnosti na neki način 'pornografski', do ideje da su ovakvi sadržaji objavljeni u cilju 'osvete'.

Ipak, tokom 2023. godine, otkriveno je 16 novih aktivnih Telegram grupa u kojima su se ovakvi sadržaji i dalje razmenjivali.[174] U nekim od ovih grupa, po saznanjima organizacije „Osnažene", koja je tokom 2024. godine sprovela istraživanje ovih grupa kroz direktnu analizu sadržaja koji su se našli u njima, je čak bilo i kupovine i prodaje ovih sadržaja.[175] Najveća grupa imala je skoro 55 hiljada članova, a neke od grupa napravljene su još pre dve godine. Nakon objave istraživanja, kompanija Telegram odmah je ugasila 13 grupa, a kasnije i ostale. Ipak, uprkos velikom odzivu javnosti i interesovanja za temu, niko i dalje nije krivično osuđen ni u jednom od ovih slučajeva. Administrator grupe „Nišlijke" Nemanja Stojiljković uhapšen je 2021. godine, zbog distribucije dečije pornografije, ali je u oktobru 2023. godine Posebno javno tužilaštvo za visokotehnološki kriminal utvrdilo da nema osnova za krivično gonjenje. Prema odgovoru VTK: „U predmetu formiranom po krivičnoj prijavi MUP-a Republike Srbije SBPOK Odeljenja za suzbijanje visokotehnološkog kriminala podnetoj 6. februara 2023. godine, doneto je rešenje o odbačaju krivične prijave obzirom da nisu postojali osnovi sumnje da je prijavljeni izvršio krivično delo za koje se krivično gonjenje preduzima po službenoj dužnosti."[176] Između ostalog, jedan od razloga zbog čega je procesuiranje ovakvih slučajeva i dalje nemoguće u Srbiji je taj što ne postoji posebno krivično delo koje se odnosi na pravljenje i distribuciju intimnog sadržaja bez saglasnosti, iako se organizacije za ženska prava za to bore već godinama.

Tokom rasprave o izmenama i dopunama Krivičnog zakonika u oktobru 2024. godine, grupa organizacija za ženska i ljudska prava ponovo su istakle važnost kriminalizacije ovog krivičnog dela, uz obrazloženje da trenutno postoji zakonski i društveni jaz koji ne dozvoljava da ovakva društvena ponašanja budu adekvatno procesuirana.[177] Nakon završetka rasprave, Ministarstvo pravde je u saopštenju od 1. novembra navelo: „U toku javne rasprave pažnju je privukla inicijativa da se Krivični zakonik dopuni novim krivičnim delom Neovlašćeno deljenje i zloupotreba snimka intimne sadržine koju je podržao veći broj organizacija civilnog društva i pojedinaca. Ministarstvo pravde je stanovišta da je ova inicijativa opravdana i da će da iznađe i predloži najbolje zakonsko rešenje kojim će se zaštititi intimni sadržaj od zloupotrebe i širenja putem društvenih mreža."[178]

Iako mali, koraci neke vrste postoje kada je u pitanju kriminalizacija zloupotrebe intimnih sadržaja u Srbiji. Slovenija, Hrvatska i Crna gora već su ovo krivično delo uvele u svoje pravne sisteme. Ostaje nada da posle pritiska iz javnosti i donekle prepoznavanja problema od

strane države, postoji prostor da se u Srbiji makar uspostavi neka vrsta pravnog mehanizma koja bi ovakve slučajeve mogla da adresira i možda pomogne u njihovoj budućoj prevenciji.

	Krivična odgovornost	Gonjenje po službenoj dužnosti	Gonjenje po predlogu
Slovenija	✓ DA	✓ DA	× NE
Hrvatska	✓ DA	× NE	✓ DA
Crna gora	✓ DA	✓ DA	× NE
Srbija	× NE		

Kriminalizacija zloupotrebe slike i snimka intimne sadržine u regionu (kraj 2024.)

IZBEGLICE I MIGRANTI

Od početka migrantske krize uslovljene ratovima na Bliskom Istoku i u Africi 2015. godine, skoro milion ljudi iz Sirije, Avganistana, Eritreje, Iraka i Libije prošlo je, često smrtonosnom rutom, preko Mediterana da dođe do Evrope.[179] Kao odgovor na veliki broj izbeglica, Evropska unija počela je da pristupa ovoj krizi kao prvenstveno bezbednosnom riziku, često zanemarujući njene ljudske aspekte. FRONTEX, agencija zadužena za kontrolu eksternih granica unije, preuzela je ključnu ulogu u ovom procesu, i brzo počela da razvija i pušta u promet nadzorne sisteme. Ovi sistemi za nadzor često su arbitrarni i netransparentni i nejasno je na kakvim algoritmima su zasnovani, što pokazuju temeljne i dugogodišnje analize.[180]

Dokazano je da su sistemi za nadzor koji se koriste kako bi dokumentovali izbeglice i migrante, koji na teritoriju Evropske unije dolaze preko mora i prolaze Balkanskom rutom preko Hrvatske, često pušteni u rad sa ciljem neovlašćenog prikupljanja njihovih ličnih podataka, kao i da se služe alatima za profilisanje kako bi targetirali ljude.[181] Srbija, kao zemlja koja se graniči sa dve zemlje članice i efektivno se nalazi na granici Evropske unije, često predstavlja prolaznu destinaciju za populacije koje preko njene teritorije pokušavaju da nastave svoj put. Mađarka i Hrvatska su već više puta bile na meti kritika zbog korišćenja ovakvih invazivnih i dehumanizujućih sistema, kao i povećane upotrebe policijske brutalnosti.[182] Imajući to u vidu, tehnologije koje se u Srbiji koriste za nadzor ovih populacija i dalje su nedovoljno istražene, sa jedne strane zbog nedostatka dostupnih informacija, što kod organizacija za ljudska prava stvara sumnje da bi ovakvi sistemi mogu biti u upotrebi i u Srbiji.

Izveštaj organizacije Border Violence Monitoring Network ustanovio je da, i pored ograničenih informacijama o korišćenju ovakvih sistema, Srbija ima razvijenu saradnju i sa FRONTEX-om i sa Višegrad grupom koja uključuje i dobavljanje i korišćenje ovih tehnologija. Ipak, primeri korišćenja od strane srpske policije najčešće su opisani kao eksperimentalni, tako da izostaje podataka o redovnim praksama i korišćenju. Takođe je napomenuto da je prema zvaničnim podacima, EU u periodu od 2015-2022 godine Srbiji pomogla da podigne tehničke kapacitete na granicama kroz donacije nadzornih sistema u vrednosti od preko 1.85 miliona evra.[183] Digitalni nadzor na granicama predstavlja podjednako veliku opasnost kao ograde i žice, u nekim slučajevima možda i veću jer je teško uvek ga uočiti i znati sve njegove sposobnosti. Istraživanja pokazuju da je digitalizacija granične bezbednosti jedan od ključnih noviteta poslednjih godina i da na taj način države teže da unaprede svoje bezbednosne kapacitete na granicama, često bez uzimanja u obzir ograničenja i opasnosti po ljudska prava.[184]

Tokom pandemije koronavirusa 2020. godine, informativnim prostorom se brzo proširila pandemija dezinformacija i teorija zavera. Između ostalih, na društvenim mrežama se brzo proširila teorija da je

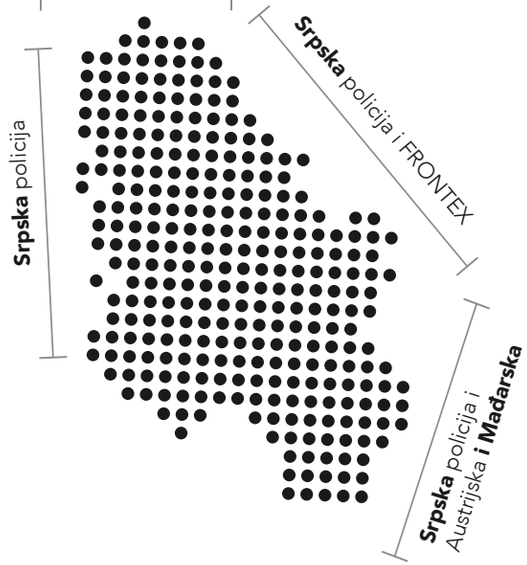
policijski čas u Srbiji zapravo bio paravan za naseljavanje migranata i izbeglica u zemlji. Grupa „STOP Naseljavanju Migranata" na Fejsbuku je u jednom trenutku imala preko 300,000 članova.[185] U grupi su se svakodnevno delile fotografije i snimci koji su navodno potvrđivali činjenicu da država koristi svoje resurse kako bi naseljavala ove ljude na teritoriji Srbije. Instrumentalizacija lažnih vesti u svrhu zastrašivanja i širenja panike često dovodi do konsolidacije teorija zavere, što je bilo očigledno kada se pogledaju glavni izvori preko kojih su se vesti delile u ovoj Fejsbuk grupi. Newspanel.rs je bio jedan od ključnih medijskih kanala sa kojeg su se unutar grupe delile vesti vezane za migrante i izbeglice. Ovaj sajt ne nudi nikakve izvore za vesti i informacije koje deli, nema podatka o autorima članaka, već se oslanja na zapaljivu retoriku i često nudi linkove do poruka sa Tviter naloga koje uglavnom impliciraju neku od pomenutih teorija zavere.

Činjenica da je Fejsbuk platforma na kojoj se takve grupe najviše prate je veoma zabrinjavajuća, pogotovo što smo već veoma svesni da je regulacija takvih grupa veoma spora, a u nekim slučajevima i nemoguća, posebno kada su u pitanju prekršaji kao što je govor mržnje.[186] Iako se već godinama nalazi na meti kritika i osuda, Fejsbuk je retko usvajao i proveravao izveštaje o govoru mržnje iz zemalja u kojima nisu imenovani predstavnici. Iako je Fejsbuk, posebno za slučaj Srbije, bio pozvan da obrati pažnju, bilo kakva reakcija tehnološkog giganta je izostala, a Srbija još uvek nije dobila predstavnika zemlje za ovu društvenu mrežu.[187] To svakako potkrepljuje i lista pravila na stranici gorepomenute Fejsbuk grupe, u kojoj je jasno navedeno da je zabranjeno 'širenje lažnih informacija, govor mržnje i uznemiravanje i nepoštovanje tuđe privatnosti'.

Iako ne može tačno da se tvrdi koliki su uticaj ovakve grupe imale na oflajn delovanje, jasno je da je samo njihovo postojanje već dovoljni pokazatelj da ovakve ideje cirkulišu društvom, pogotovo ako se uzme u obzir brojnost samo jedne od njih. Ipak, u maju 2020. godine,

SISTEMI NADZORA NA GRANICAMA SRBIJE

Od 2014-2024. godine više od €220 miliona pomoći u oblasti migracija i upravljanja granicama je dato Srbiji od strane EU



DONATORI:

FRONTEX
EUROPOL
EU COMISSION
IOM
EU DEVELOPMENT FUND

DOBAVLJAČI:

Damiba Group
DJI
Nutech
Yuneec
Hirrus
Smart Building Technologies

- Senzori za otkucaje srca
- Skeneri vozila
- Long range acoustic devices (LRAD)
- Nadzorne kamere
- Tornjevi (praćenje telefona)
- IMSI hvatači
- Mobile surveillance system (MSS)
- Radari
- Laseri
- Dronovi
- Senzori
- Termalne kamere

član ekstremističke desničarske grupe Levijatan je kolima uleteo u migrantski prihvatni centar u Obrenovcu. Ceo događaj je prenosio uživo na svom Fejsbuk profilu i ubrzo nakon upada je uhapšen.[188] Neke od poruka koje je mladić ponavljao dok se snimao ličile su na jezik koji je korišćen u objavama u ovim i sličnim grupama. Iz vlasti se ni u jednom trenutku nije čulo eksplicitno demantovanje ovakvih bespredmetnih teorija zavera i širenja panike.

Rasistički komentari nisu retkost na srpskim društvenim mrežama, pa je tako početkom ove godine na Instagramu osvanuo nalog koji je bez znanja objavljivao fotografije i lokacije građana i turista Srbije koji su afričkog porekla.[189] Ovakve „uočen si" (spotted) stranice, anonimno objavljuju fotografije i informacije koje im korisnici šalju i često su tematske, ali uvek krše privatnost onih koji se na njima nađu. Ovakve stranice već godinama objavljuju fotografije žena i devojaka u javnim prostorima i pozivaju korisnike da komentarišu njihov izgled i često mogu sadržati i uznemirujuće komentare.[190]

DECA I MLADI

Nakon tragičnog masakra u Osnovnoj školi Vladislav Ribnikar u Beogradu 3. maja 2023. godine, povela se ozbiljna diskusija u društvu oko nasilja kojim su deca i mladi svakodnevno okruženi i izloženi. Neki od nadležnih, uključujući predsednika i tadašnju ministarku zdravlja Danicu Grujičić, odmah su okrivili internet i sve njegove domete, zagovarajući uvođenje ograničavanja sadržaja za mlade, ili privremeno gašenje svih društvenih mreža u zemlji „makar na mesec dana".[191] Drugi su svoje kritike zadržali prevashodno za kulturu nasilja koja je široko rasprostranjena u društvu i koja se plasira sa televizija sa nacionalnom frekvencijom, a vidljiva u svim porama društva, od skupštine do rijalitija. Važno je napomenuti da „ukidanje" društvenih mreža ili sveobuhvatno ograničavanje sadržaja bez adekvatnih bezbednosnih provera i sistema može lako dovesti do filtriranja i ograničavanja delova interneta, što samo u sebi sadrži još brojne neispitane probleme.[192] Davanje takvih mogućnosti državi može izazvati zloupotrebe i čak stvoriti kontraefekat.

Samo nekoliko dana nakon tragedije, na društvenoj mreži TikTok počeli su da kruže navodni snimci tragedije.[193] Iako je ubrzo utvrđeno da je u pitanju drugi incident koji se dogodio pre nekoliko godina u Sjedinjenim američkim državama, indikativno je da je dosta mlađih korisnika imalo kontakt sa ovakvim sadržajem. Takođe su ubrzo po mrežama počeli da se pojavljuju razni nalozi i sadržaji koji su veličali dečaka koji je ubistva počinio, koji su pretili sličnim scenarijima i koji su relativizovali ove događaje, svi većinski postavljani od strane dece i mladih.[194] Mentalno zdravlje dece i mladih i uticaj koji na njih mogu imati sadržaji koje svakodnevno gledaju na društvenim mrežama i pretražuju na internetu već je podrobno zabeležen, ali čini se da svaki put ovi razgovori ostanu bez epiloga. Studija SHARE Fondacije sprovedena 2023. godine ukazala je na neke od glavnih izazova i opasnosti sa kojima se deca i mladi sreću u digitalnom prostoru, uključujući i štetan ili sadržaj neprilagođen uzrastu kao što su sadržaji koji promovišu samopovređivanje i nezdravu mršavost, štetni kontakti kao što su onlajn nasilništvo i agresija, pretnje i govor mržnje i neželjeni seksualni kontakt i zloupotreba ličnih podataka.[195]

Nove opasnosti takođe ne zaobilaze najranjivije i najmlađe populacije, što je bilo jasno kada je početkom 2024. godine u osnovnoj školi na Novom Beogradu, grupa đaka sedmog i osmog razreda su iskoristili fotografije svojih vršnjakinja i učiteljica kako bi napravili eksplicitne snimke koristeći aplikacije za kreiranje dipfejk sadržaja.[196] Iako je ovaj slučaj nekoliko dana u javnosti služio za otvaranje tema digitalne bezbednosti kod mladih, diskusije su se kretale u već dobro poznatom pravcu – ograničavanje pristupa internetu mladima. Ipak, rasprostranjenost ovakvih sadržaja među mladima jasan su pokazatelj normalizacije ovakvog ponašanja u društvu i zahtevaju mnogo dublja i sistemska rešenja, počevši

od obrazovnog sistema, pa sve do mnogo strože osude ovakvog ponašanja za sve počinitelje, čime bi se postavio pozitivan primer za mlade.

LGBTQAI+ POPULACIJA

Razvoj veštačke inteligencije i digitalnih tehnologija donosi brojne mogućnosti, ali i ozbiljne izazove za prava LGBTQAI+ zajednice. Ovi izazovi uključuju kršenje privatnosti, širenje mržnje, diskriminaciju i sužavanje prostora za slobodno izražavanje. Tehnološki alati, ukoliko nisu etički razvijeni i pažljivo regulisani, mogu postati oruđe za marginalizaciju i kršenje ljudskih prava ranjivih grupa. U svetu, jedan od ključnih problema je upravo pitanje privatnosti. Algoritmi veštačke inteligencije mogu koristiti ogromne količine podataka prikupljenih sa društvenih mreža za profilisanje korisnika, uključujući seksualnu orijentaciju ili rodni identitet, često bez njihovog znanja ili pristanka. Takve informacije mogu biti zloupotrebljene u zajednicama u kojima LGBTQAI+ osobe nemaju adekvatnu pravnu ili društvenu zaštitu, izlažući ih riziku od diskriminacije, ugnjetavanja ili čak nasilja.

Društvene mreže često postaju prostor za širenje govora mržnje i dezinformacija usmerenih protiv članica i članova LGBTQAI+ zajednice. Iako platforme sve učestalije koriste veštačku inteligenciju za moderaciju sadržaja, mnogi algoritmi su skloni pristrasnosti ili često ne prepoznaju kontekstualne nijanse. Ovo rezultira time da govor mržnje prema LGBTQAI+ osobama i zajednici ostaje neprimećen ili neadekvatno sankcionisan. Ovaj fenomen dodatno ograničava vidljivost LGBTQAI+ pitanja i smanjuje osećaj sigurnosti korisnika na tim platformama. U Srbiji, mnogo je manji stepen oslanjanja na automatizovanu moderaciju za uklanjanje sadržaja, pa se veći akcenat stavlja na korisnice i korisnike da budu odgovorni za stavove koje iznose na mrežama. Nažalost, činjenica je da su patrijarhalni obrasci ponašanja i dalje duboko ugravirani u svakodnevicu u Srbiji, kako u analognom tako i u digitalnom okruženju. Ovo je često vidljivo kroz interakcije koje pripadnici LGBTQAI+ zajednice mogu imati na društvenim mrežama, najčešće u toku rasprava. Kao prva linija napada, najčešće se koristi njihovo seksualno opredeljenje ili rodni identitet, nevezano od argumenata ili teme neslaganja.

Kao i u većini ranjivih grupa o kojima je u ovoj priči reč, posledice za izostanak reakcije na povećanu diskriminaciju na nasilje nad pripadnicama i pripadnicima LGBTQAI+ populacije u onlajn prostoru neretko rezultiraju jako realnim i vidljivim oflajn nasiljem. Prajd info centar u Beogradu bio je godinama česta meta napada na aktivistkinje i aktiviste, lomljenja prozora i druge vidove vandalizovanja.[197] Iako su svi incidenti prijavljeni, počinioci nikada nisu pronađeni ni procesuirani, uprkos svim dokazima i činjenici da se centar nalazio u centru grada okružen kamerama za nadzor, kako gradskim, tako i od samog centra. Ono što je dodatno zabrinjavajuće je da objavljivanje ovih napada na mrežama često privlači veliki broj komentara podrške, ali ne za centar i zajednicu, već za počinioce.[198]

Osim pojedinaca, organizacije koje pružaju pravnu i psihološku pomoć LGBTQAI+ zajednici, takođe su često targetirane. Nakon slučaja policijske brutalnosti početkom 2024. godine, u kojem je mladiću policija upala u stan tokom noći i verbalno i fizički ga maltretirala uz homofobne uvrede, organizacija *Da se zna,* koja je o ovom slučaju izveštavala javnost i podnela krivične prijave protiv policije, našla se na meti napada tabloida.[199] Njihova organizacija je diskreditovana, objavljivane su neistinite informacije i fabrikovani izvori i dokazi u medijima. Niko od nadležnih institucija nije reagovao na ove napade, kao ni u slučaju koji je bio okidač za ove napade.

Nakon masovnih ubistava u maju prošle godine organizovani su masovni protesti na ulicama. I dok su opozicioni političari i stranke napadani od strane vlasti na televiziji i u štampi, učesnici protesta napadani su i diskreditovani od strane pristalica vladajuće stranke

najčešće preko društvenih mreža. Tako je aktivista Gej strejt alijanse Lazar Pavlović postao jedna od glavnih meta zbog svog kreativnog iskazivanja građanskog nezadovoljstva. Dan nakon što je Pavlović bio na protestu u majici na kojoj je pisalo „lešinar tata", kao odgovor na argument vlasti da opozicija i građani „lešinare" i politizuju smrti dece i ljudi u Ribnikaru i Mladenovcu, po društvenim mrežama su počele da se šire laži o njegovom privatnom životu. Politika je u svom onlajn izdanju objavila tekst sa ciljem da Pavlovića diskredituje, objavljujući njegove privatne fotografije sa društvenih mreža i iznoseći insinuacije o njegovom seksualnom opredeljenju.

U Beogradu je prošle godine zakazano održavanje Evroprajda za septembar 2022. godine, što su mnoge javne ličnosti podržale, ali su brzo usledili rutinski napadi na mrežama uz homofobne uvrede. Nakon što je Srpska pravoslavna crkva veoma vokalno osudila održavanje događaja i čak pokrenula peticiju za zabranu Parade ponosa, jasno se oformila agenda odbrane „tradicionalnih vrednosti i porodice". Ovo su i bili najčešće korišćeni argumenti u napadima na pripadnike LGBTQAI+ zajednice i one koji su podržavali održavanje Evroprajda, u organizovanoj kampanji napada i uvreda koja je započela mesecima pre nego što je događaj održan, uz često zakazivanje litija i protestnih šetnji protiv prajda. Reditelj Stevan Filipović bio je jedna od javnih ličnosti koja se našla na meti velikih napada, sa jedne strane zbog svoje podrške Evroprajdu, a sa druge strane zbog svoje jave rasprave sa glumcem Viktorom Savićem, koji je poznat po svojim verskim stavovima i koji je takođe javno napadao održavanje ovog događaja. Filipović je na društvenim mrežama danima dobijao ogromne količine pretnji i uvreda.[200]

Kada je u Beogradu prošle godine u partnerskom nasilju ubijena trans devojka od strane svog dečka, tabloidi u Srbiji danima su izveštavali o ovom događaju. Nažalost, jedna od stvari koja je obeležila izveštavanje bilo je nesmotreno izveštavanje o devojčinom rodnom identitetu, uz često korišćenje njenog imena (*deadnaming*) i fotografije pre procesa tranzicije.[201] U izveštavanju su takođe navođeni brojni drugi detalji iz života devojke, kao i opisi samog ubistva i planirano mesto sahrane. Organizacije za zaštitu LGBTQAI+ prava ukazale su na štetnost ovakvog senzacionalističkog sadržaja, kao i na činjenicu da su i društvene mreže bile pune ovakvih komentara.[202]

Važno je da se ne zaboravi da je borba za digitalna prava deo šireg zalaganja za jednakost i prava svih, uključujući LGBTQAI+ zajednicu, u društvu koje teži inkluzivnosti, poštovanju i ravnopravnosti. Uloga svih u društvu je da ne dopuste ovakav govor i uvrede da prolaze nekažnjeno i da se ustale kao svakodnevni govor jer na taj način put ka jednakosti postaje sve dalji i ispunjen novim preprekama. Sa globalnim porastom desničarskih politika, sve je veći akcenat na takozvanom očuvanju „tradicionalnih vrednosti" i sistemima koji su represivni prema manjinama. Anti trans i LGBTQAI+ zakoni su u porastu širom sveta, i predstavljaju ozbiljnu opasnost za prava i slobode ovih zajednica.[203]

SOCIO-EKONOMSKI UGROŽENE GRUPE

Pristup internetu i digitalna inkluzija su ključni faktori za pojedince kako bi mogli u potpunosti da učestvuju u društveno-političkom životu. Tehnologija pored svih svojih benefita, istovremeno produbljuje socio-ekonomske nejednakosti i izlaže marginalizovane grupe dodatnim rizicima. Socio-ekonomski ugrožene grupe, uključujući siromašne, nezaposlene, radnike na nesigurnim poslovima i osobe bez pristupa formalnom obrazovanju, suočavaju se sa brojnim izazovima u digitalnom dobu. Bez pažljivog upravljanja i regulisanja, tehnologije koje obećavaju inkluzivnost mogu postati oruđe za diskriminaciju, marginalizaciju i dalje produbljivanje digitalnih podela.

Digitalni jaz, odnosno razlika u pristupu tehnologiji između socio-ekonomski privilegovanih i ugroženih grupa, predstavlja jedan od najvećih problema kada je u pitanju ravnopravno uključivanje svih zajednica u svakodnevne digitalne tokove života. Ljudi u socio-ekonomski nepodobnim situacijama, iako možda imaju pristup uređajima i brzom internetu, mogu biti nedovoljno tehnološki pismeni kako bi na adekvatan način navigirali digitalni svet. Ova isključenost dovodi do daljeg pogoršanja njihove marginalizacije, jer im se uskraćuje pristup obrazovanju, zapošljavanju, zdravstvenim uslugama i javnim informacijama koje su sve češće dostupne samo onlajn. Osim toga, algoritmi koji se koriste u procesima donošenja odluka, poput zapošljavanja, odobravanja kredita ili određivanja socijalnih beneficija, često mogu ponavljati društvene predrasude sadržane u podacima na kojima su trenirani.

Socio-ekonomski ugrožene grupe često mogu biti meta za prikupljanje podataka, od strane privatnih kompanija, ali i države. Zloupotrebljavanje nepodobne društvene pozicije može ove ljude dovesti u situaciju da njihovi lični podaci budu iskorišćeni protiv njih. U novembru ove godine, grupa Lokalni front iz Kraljeva objavila je na društvenim mrežama spisak SNS članova i glasača sa preko 10,000 imena i prezimena, uključujući i brojeve telefona i adrese. Iako ovakvi spiskovi nisu nikakav novitet u Srbiji, i tokom proteklih godina su spiskovi simpatizera i glasača koje je vladajuća stranka pravila nekoliko puta curili u javnost, na ovom spisku su se takođe nalazili i opisi socijalnih situacija članova.[204] Nije u potpunosti jasno zbog čega spisak sadrži ove podatke, ali može se pretpostaviti da je u pitanju poluga za potencijalno ucenjivanje ljudi. SNS je u nekoliko navrata tokom prethodnih godina građankama i građanima delila takozvani helikopterski novac, najčešće u trenucima percipirane društvene krize, tokom pandemije i uoči izbora, a glavni primaoci ove pomoći su penzioneri, socijalno ugroženi i mladi.[205] Naime, u prethodnih četiri godine, država je ukupno 15 puta delila novac iz državnog budžeta određenim grupama građana iz različitih razloga.[206] Na ovaj način, vlast stvara iluziju prosperiteta ali i dobre volje prema narodu, kroz akt koji suštinski deluje kao nesebično delo.

Ipak, stvarna situacija je mnogo komplikovanija i daleko od one koju bi država volela da projektuje. Oni koji u svakodnevnom životu zavise od socijalne pomoći države često se nalaze u situaciji da tu pomoć ne dobijaju redovno, da ta pomoć nije dovoljna za dostojanstven život, ili u najgorim slučajevima, da im ta pomoć bude uskraćena. U martu 2022. godine, Vlada Republike Srbije donela je Zakon o socijalnoj karti, prema kojem je trebalo da se reše neki od problema sa kojima se primaoci socijalne pomoći susreću. Po zakonu je predviđeno uspostavljanje sistema *Socijalne karte* koji je zamišljen da bude centralizovani digitalni registar svih primaoca socijalne pomoći. Ova evidencija je razvijena od strane Ministarstva za rad, zapošljavanje socijalna i boračka pitanja i trebalo je da koristi kako bi najugroženiji građani ostvarili svoje pravo na adekvatnu i pravovremenu socijalnu zaštitu.[207] Registar je uz pomoć automatizovanog procesa trebalo da dostavlja obaveštenja o promeni socio-ekonomskog statusa, omogući lakši pristup svim podacima registrovanih u sistemu i vrši analitičku obradu podataka. Ipak, u razgovorima sa primaocima socijalne pomoći, ubrzo je utvrđeno da je novi sistem imao mnogo više mana nego prednosti, i da je po neke bio i ekstremno štetan.

Među najvećim problemima izdvojila se automatizacija ovog sistema – procene socijalno-ekonomskog statusa pojedinaca socijalni radnici su vršili posredno kroz sistem, umesto kroz razgovore sa ljudima koji se nalaze u ovom sistemu.[208] Na ovaj način je potpuno eliminisan ljudski faktor u procesu donošenja odluka, što se potpuno kosi sa načelima socijalnog rada i sistemom socijalne zaštite. Takođe je navedeno da je algoritam koji registar koristi nedovoljno transparentan u načinu na koji prikuplja i obrađuje podatke jer nije dostupan javnosti na uvid, iako su te informacije tražene još 2022. godine kada je sistem uspostavljen. Utvrđeno je i da je ovaj sistem u svojoj osnovi diskriminatoran prema siromašnoj i romskoj populaciji,

što je dodatno pospešeno netransparentnošću ovih tehnologija, kao i da ljudi koji su zbog grešaka automatizovanog donošenja odluka neosnovano izbačeni iz sistema primanja socijalne pomoći nisu vraćeni nakon što je ukazano na grešku. Sudeći po tome, digitalizovanje sistema socijalne pomoći imalo je kontraefekat na najugroženije i umesto pružanja pomoći, doveo je do produbljene diskriminacije i isključivanja. Prema podacima *Inicijative A11,* trenutni broj korisnika koji je isključen iz sistema socijalne zaštite zbog problema sa registrom *Socijalne karte* je 44.106.[209]

U retrospektivi, jasno se može zaključiti da je pandemija bila prekretnica za veliki broj negativnih digitalnih praksi usmerenih prema marginalizovanim grupama. Zaštita digitalne fasade mnogima koji učestvuju u onlajn nasilju stvaraju osećaj nekažnjivosti, ali takođe i nedostatak odgovornosti za poruke koje ostavljaju. Teško je saosećati se sa nekim ko je sa druge strane ekrana i osobe koje učestvuju u napadima često u komentarima nailaze na podršku za uvrede i pretnje koje ostavljaju. Činjenica je da niko nije bezbedan i svako se može pronaći sa druge strane organizovanih napada i na meti sajber nasilja, što ovaj problem čini rasprostranjenijim nego što deluje na prvi pogled.

TEHNOLOGIJA: OD INTERNET NEUTRALNOSTI OD PLATFORMIZACIJE

MIT O NEUTRALNOM INTERNETU

Tehnologija je neutralna. To je prva pretpostavka optimistične slike interneta sa početka njegovog razvoja: nova otvorena mreža doprineće društvenom razvoju, većoj participaciji, uključivanju, boljoj informisanosti, povezaće ljude, olakšati komunikaciju, međukulturnu razmenu, osnažiti demokratiju. Samo bi eventualne pojedinačne zloupotrebe mogle delimično poremetiti ovu „funkcionalnu anarhiju" kao „neregulisani i neregulabilni prostor slobode bez cenzure". Tako su još tokom devedesetih godina pokrenuta pitanja o nelegalnom sadržaju na internetu, prvenstveno o problemu proliferacije pornografskog sadržaja, a zatim i piraterije i kršenja autorskih prava.[210] Međutim, incidentni karakter ovih problema, neusaglašenost o načinima njihovog prevazilaženja, kao i liberalno okruženje u kojem će, primera radi, Prvi amandman zaštititi Yahoo od odgovornosti u tužbi francuske vlade zbog aukcije nacističkih suvenira (2000), opredelile su višedecenijsku uzdržanost u pogledu regulisanja ili upravljanja onlajn sferom.[211]

Optimistična ideja o neutralnoj tehnologiji i benefitima koje omogućava iščitava se i iz situacija poput arapskog proleća i trijumfa građanskog novinarstva, različitih *grassroots* pokreta i mogućnosti za aktivizam u autoritarnim režimima visokog stepena kontrole, ali i doprinosa u osvetljavanju marginalizovanih tema i inicijativa. Dostupnost interneta vrlo lako je postala jedna od mera demokratičnosti, kao alternativni prostor koji oponira tradicionalnim, neretko zarobljenim i kontrolisanim institucijama i organizacijama, čiji su najbolji primer mediji. Pad poverenja u medijske institucije koincidirao je, pa čak i pospešio rast poverenja u njihove alternative, prvenstveno društvene mreže. Međutim, upravo medijski sektor pokazuje da nije mnogo vremena prošlo od kako se „informativno obilje" pretvorilo u „informativnu zatrpanost". „Građansko" novinarstvo neretko nije više od amaterskog deljenja neproverenih ili polu-informacija, a sporadične lažne vesti ekspandirale su u

sistemski informativno-propagandni poremećaj koji je u krizama poput pandemije kovida-19 imao nesagledive posledice.

Dolazak interneta u Srbiju vezuje se za 1996. godinu i dan Univerziteta u Beogradu, kada je Akademska mreža Srbije povezana na svetsku mrežu. Takođe je zanimljivo napomenuti da je sajt studentskih protesta '96. godine bio jedan od prvih koji je privukao veliku pažnju međunarodne umrežene zajednice i pružio uvid u situaciju u zemlji koja je do tada bila prilično odsečena od ostatka sveta, najviše u informativnom smislu.[212] Studenti Univerziteta u Beogradu videli su mobilizatorski potencijal interneta pre vise od dve decenije i na taj način uspeli da pomognu da internet dobije revolucionarnu ulogu u borbi protiv državne represije, i digitalni dokazi za to i dalje postoje.[213] Danas, internet u Srbiji predstavlja sastavni deo svakodnevnog života, podaci Republičkog zavoda za statistiku pokazuju da više od 90% građana i građanki Srbije koristi internet više puta u toku dana.[214] Međutim, tokom nekoliko decenija postojanja internet u Srbiji se značajno promenio i to u pravcu smanjenja otvorenosti i slobode koje su izazvane kako globalnim trendovima tako i lokalnim okolnostima. Naime, protekla decenija u Srbiji je obeležena različitim slučajevima kao i nastojanjima da se zakonski uobliči „filtriranje interneta", kao tehnološka mogućnost uskraćivanja pristupa određenim sadržajima. Uspostavljanje potencijalnih filtera dostupnih sajtova najuočljivije je bilo u oblasti igara na sreću, koja je trebalo da uspostavi praksu diskrecionih odluka o blokiranju pristupa sadržajima i servisima i to od strane pružalaca internet usluga, odnosno da posluži kao polje legalizacije filtriranja interneta.[215]

Između optimističke slike interneta kao neograničenog prostora slobode i bojazni da će globalna mreža postati instrument u rukama odabrane manjine, previđa se činjenica da ekspanzija novih tehnologija nije samo geografska, multisektorska i masovna, niti „samo tehnološka". U svega nekoliko decenija razvoja, tehnologije bez kojih je savremeni život sada nezamisliv postale su *novo društveno okruženje* u kojem kupujemo, pronalazimo smeštaj, družimo se, informišemo, lečimo, obrazujemo, i ne samo to. Granica između onlajn i oflajn sveta danas više ne postoji. Sada živimo u konvergiranom svetu analognog i digitalnog u kojem tehnologija predstavlja *vrednosno određenu strukturu* koja u potpunosti redefiniše uspostavljene institucije, profesije, organizacije, norme, društvene strukture, politički život, u prevodu – svakodnevicu svakog pojedinca.

Ova promena je višestruko određena. Prvo, tehnologija u interakciji sa društvom poprima i amplifikuje vrednosti onih koji je koriste, a posebno onih koji stoje na čvorištima mreže, kao što su tvorci digitalnih tehnologija i svetske vlade. Drugo, tržišna *winner-take-all* logika pokazuje se kao formula prema kojoj je digitalna infrastruktura brzo izgubila status otvorenosti i ravnopravne konkurentnosti, i na globalnom (slobodnom) tržištu uspostavila gigante koje prepoznajemo kao BigTech, odnosno velike tehnološke kompanije. Zahvaljujući normativno i vrednosno određenoj infrastrukturi, svega nekoliko tehnoloških giganata uspelo je da u kratkom roku prema sopstvenim *platformskim mehanizmima* oblikuje ukupan (ne samo digitalni) ekosistem u kojem živimo.

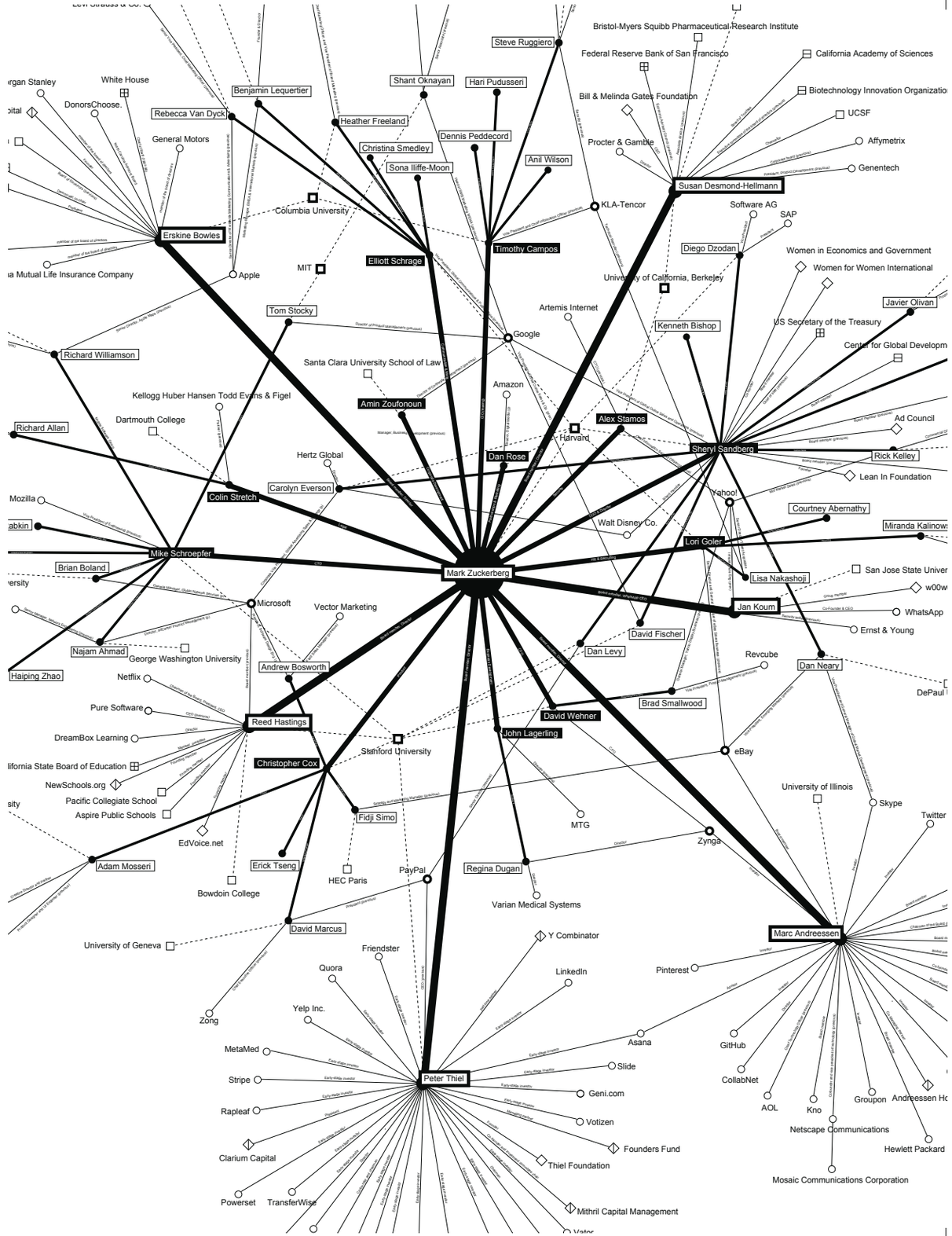
BIGTECH I PLATFORMIZACIJA

Ako bi se ilustrovao savremeni digitalni ekosistem, to bi bila hijerarhizovana i visoko centralizovana, netransparentna, profitno orijentisana, ideološki i vrednosno obojena struktura globalnog obuhvata. Vrhovi te strukture rezervisani su za najveće igrače, poput Gugla, Mete, Amazona, koji su u svega par decenija dostigli status čuvara kapija celokupne digitalne sfere. Ove kompanije su zahvaljujući sveprožimajućoj tehnologiji sopstvenih platformi čija je osnovna uloga da *posreduju* usluge na digitalnom tržištu monopolizovale čitave sektore (društvene mreže, internet pretraživanje, usluge smeštaja,

trgovine, transporta,...). Najzad, njihova infrastruktura, poslovna logika, pravila i uslovi korišćenja njihovih usluga u potpunosti su promenili značaj i ulogu podataka, tržišne modele, odnos prema digitalnom sadržaju i mogućnosti ostvarivanja prava i sloboda u digitalnom okruženju. Takva sveprožimajuća platformizacija otvorila je veliko pitanje: ima li demokratije u digitalnom svetu? I šta to znači za pojedince i društvo?

Prvi stub platformizacije je *datafikacija*, odnosno tehnološka mogućnost platformi poput Fejsbuka, Bukinga, Ep stora da najrazličitije aspekte našeg ličnog i društvenog života prevodi u podatke. Svaki vid bilo kakve interakcije na platformama (lajkovanje, skrolovanje, fokus pažnje, pretraživanje, kliktanje, deljenje sadržaja) pretvara se u podatak. Svaka aktivnost svakog korisnika može biti uhvaćena, algoritamski procesuirana i dodata u „profil" tog korisnika. Ovako prikupljeni podaci ključni su resurs za posrednike trećih strana, pre svega oglašivače koji od njih mogu da imaju najveću finansijsku korist. Cirkulacija podataka ka njima, međutim, otvara brojna pitanja, poput zaštite privatnosti podataka, politika platformi i sprovođenja sopstvenih pravila, do društvenih implikacija takvog mehanizma.

Kembridž analitika (*Cambridge Analytica*) skandal najbolje oslikava razmere ovog problema. Dve godine nakon Bregzit kampanje i pobede Donalda Trampa na američkim izborima 2016. godine, otkriveno je da su podaci preko 50 miliona korisnika Fejsbuka prikupljeni i zloupotrebljeni kroz aplikaciju koju je privatna kompanija Kembridž analitika razvila i povezala na ovu platformu. Utvrđeno je da su ovi podaci prikupljani kako bi se napravili sofisticirani modeli za sprovođenje političkih kampanja kroz sadržaje koji su mogli da utiču na formiranje stavova korisnika u ovim presudnim izborima.[216]



The Human Fabric of the Facebook Pyramid, labs.rs

Ovi modeli su sa ogromnom dozom sigurnosti mogli da plasiraju ciljane sadržaje korisnicima, upravo jer su bili zasnovani na podacima sa njihovih naloga, kao što su mesto stanovanja, godine, grupe koje prate i slično. Pošto su podaci povlačeni kroz ove aplikacije, to je značilo da su korisnici morali da popunjavaju određene kvizove kako bi aplikaciji dali pristup svojim podacima, ali ono što je posebno sporno je da su ove aplikacije onda povlačile podatke svih onih koje su korisnici koji su popunjavali ove kvizove imali u prijateljima. Na ovaj način, korisnici usluga ove kompanije, među kojima su se našli kampanja Leave.

EU i politička kampanja Donalda Trampa, imali su u svojim rukama ozbiljno oružje za manipulaciju izbornim procesom.[217] Ovakva zloupotreba podataka korisnika ukazala je na ozbiljne bezbednosne propuste Fejsbuka i cele Mete i pokrenula pitanja o transparentnosti njihovog postupanja, ali i dostupnosti korisničkih podataka lošim akterima. Nekoliko godina kasnije, otkriveno je da su ovi sistemi korišćeni i 2015. godine kako bi se uticalo na ishod predsedničkih izbora u Nigeriji, što ukazuje na to da razmere štete koje su ovi sistemi naneli globalno je i dalje nepoznata do kraja.[218]

Osam godina kasnije, bitka oko uticaja Kembridž analitike i Metinog udela u ovom skandalu još uvek traje, i dok tehnološki gigant uporno tvrdi da nema osnova da zbog ovog kršenja privatnosti svojih korisnika pravno odgovara, čini se da Ustavni sud SAD smatra da ipak postoji određena doza odgovornosti. Zbog toga je sud odbio Metinu žalbu, što znači da će kompanija morati na sudu da dokaže da je posredovanje trećih strana na njihovoj platformi direktno uticalo na bezbednost njihovih korisnika i štetno uticalo na poslovanje.[219]

Iako korišćenje podataka desetina miliona korisnika Fejsbuka bez pristanka, njihovo profilisanje i algoritamsko mikrotargetiranje nije prošlo u potpunosti nekažnjeno u Americi i Britaniji, nedostatak čvrstih zakonskih okvira i dalje izaziva opasnost da se ovakve zloupotrebe

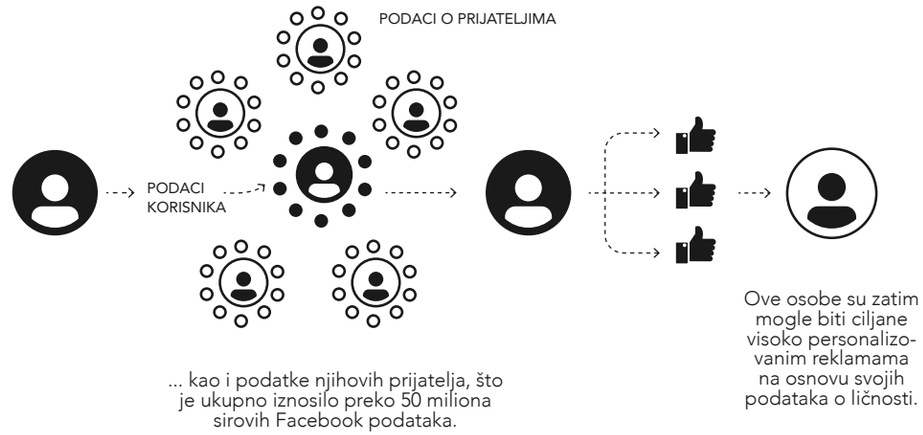
Cambridge Analytica: kako je ukradeno 50 miliona Facebook podataka

1
Približno 320.000 američkih birača („seeders“) je plaćeno $2-5 da urade detaljan test ličnosti/političkih stavova koji je zahtevao da se prijave putem svog Facebook naloga.

2
Aplikacija je takođe prikupljala podatke kao što su lajkovi i lične informacije sa Facebook naloga učesnika testa...

3
Rezultati testa ličnosti su povezani sa njihovim Facebook podacima — kao što su lajkovi — kako bi se otkrili psihološki obrasci.

4
Algoritmi su kombinovali te podatke sa drugim izvorima, kao što su birački spiskovi, da bi kreirali superiornu bazu podataka (u početku za 2 miliona ljudi u 11 ključnih država*), sa stotinama podataka po osobi.



Analyzing Medium posts to understand impact of Cambridge Analytica Scandal, Medium

ponove. Takođe je indikativno da se krivična odgovornost u ovakvim slučajevima najčešće ne odnosi direktno na povredu prava korisnika, već akcionara čija je zarada na neki način ugrožena ovim skandalima.

Najskoriji primer predložene regulative u Evropskoj uniji jasno pokazuje da platforme u slučajevima kada se od njih očekuje da svoju nadležnost povećaju i sprovode sa više odgovornosti biraju

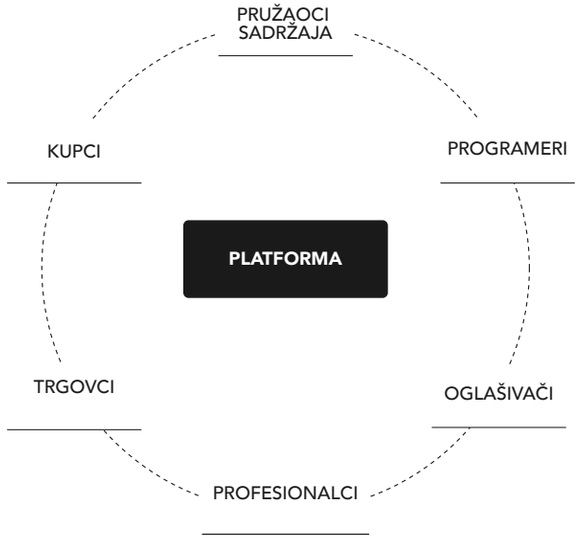
lakši put. Evropski parlament je u martu ove godine uveo nova pravila o transparentnosti i targetiranju političkog oglašavanja na mrežama, prema kojem su platforme na kojima se ove reklame plasiraju u većoj meri odgovorne za njihov sadržaj.[220] Prema novom zakonu, sve reklame koje su političkog karaktera moraće jasno da budu obeležene kao takve i da sadrže detaljne informacije o naručiocima ovih reklama, uključujući koliko su plaćene, kao i informacije za korisnike, uključujući da li su direktno targetirani određenim reklamama.

U cilju ograničavanja stranog uticaja, takođe će biti zabranjeno plasiranje političkih reklama koje dolaze izvan EU tri meseca pred izborne procese. U zakonu je takođe naglašeno da se ova pravila neće odnositi na neplaćene reklame, kao i da lični stavovi, politička mišljenja i nesponzorisani novinski sadržaji neće podlagati ovim pravilima. Ovaj zakon, koji je predviđen da stupi na snagu na jesen 2025. godine, samo je još jedan u nizu svetskih regulativa koje za cilj imaju pooštravanje pravila u digitalnom prostoru kako bi se obezbedila transparentnost i odgovornost u izbornim procesima.

Međutim, kao odgovor na predloženi zakon, Gugl je najavio potpunu zabranu političkih sadržaja na svojim servisima, koja je već na snazi u drugim jurisdikcijama kao što su Kanada i Brazil.[221] U svom saopštenju, kompanija je navela da pravila predložena od strane EU nisu dovoljno jasna kako bi omogućila kompaniji da ih sprovede na svojim servisima, i zbog toga je donesena odluka o potpunom ukidanju političkog sadržaja. Dalekosežne posledice ovakvog isključivanja najviše će osetiti organizacije civilnog društva koje svojim zagovaranjem ukazuju na društveno-političke probleme koji se nekada ne pronalaze u zvaničnim programima političkih stranaka, ili u gorem slučaju, su namerno zanemareni ili potisnuti. Iako je Gugl sam ovo naglasio tokom prošlogodišnje rasprave o novom zakonu, na kraju je ipak doneta odluka da se svaki vid političkog oglašavanja uklanja.[222]

Zatim, platformizacija potpuno rekomponuje tržišnu strukturu, tako što platforme postaju ključni tržišni posrednici u novim biznis modelima u kojima povezuju kupce, odnosno korisnike, sa prodavcem odnosno primarnim pružaocem usluge, tako što „servisiraju" sve tržišne strane. Tako u medijskoj industriji, na primer, Instagram ili Jutjub predstavljaju nove intermedijatore ili mečmejkere (*matchmakers*) koji povezuju oglašivače i publiku. Tu vezu su prethodno uspostavljali samo mediji. Zato je nova tržišna kompozicija višestrana, a ključna formula uspeha vezivanja za određene platforme zapravo je u besplatnom pristupu koji je omogućen krajnjim korisnicima, odnosno u jeftinim alatima za njihovo targetiranje koji su dati na raspolaganje zainteresovanim tržišnim stranama, bilo da je u pitanju korporacija, politička partija ili institucija.

Tržišna vrednost na platformama ne izražava se samo novcem. Njena valuta su i podaci, broj i osobenosti korisnika i, svakako najznačajnija, pažnja. Platformsko tržište zapravo povezuje „tražioce pažnje" sa onima kojima je pažnja potrebna bilo da bi nešto prodali, promovisali, informisali. Korisnička pažnja, sa druge strane, nije provocirana samo ponudom, već i samom korisničkom bazom kojoj pripadamo. Naime, svaki novi korisnik ne samo da proširuje bazu korisnika već i kvalitativno menja njenu vrednost – što se proizvod više kupuje ili usluga više koristi, u korisničkim očima je vrednost tog proizvoda ili usluge veća. Tako je rasla i vrednost platformi koje su prve uspostavile ove modele poslovanja. Naime, konačni ishod mrežnog efekta i petlje privlačnosti platformi je da „pobednik dobija sve". To je razlog zbog kojeg je nekoliko platformi uspelo ne samo da ostvari enorman rast i razvije ogromnu korisničku bazu, već da uspostavi strukturne uslove monopolizacije. Monopolska pozicija učinila ih je „čuvarima kapija" digitalnog tržišta.

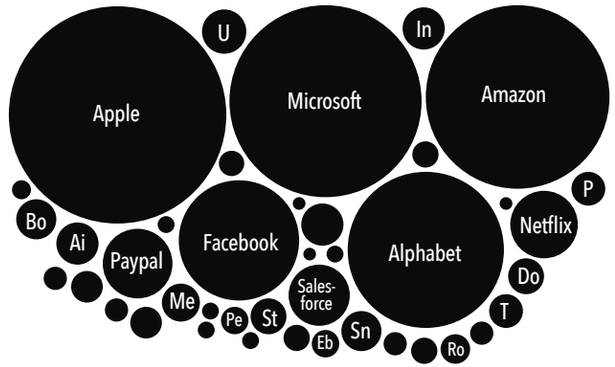


Generički sistem višestranih platformi, izvor: Øverby i Audestad (2018). Introduction to Digital Economics. Foundations, Business Models and Case Studies. Second Edition. Springer

Najzad, najveći platformski igrači intervenišu, ili makar imaju mogućnost da intervenišu u sadržaj i cirkulaciju sadržaja koji posreduju. Njihovo kuratorstvo nije vođeno bilo kakvim profesionalno određenim principima, već korisničkim podacima i netransparentnim tehno-komercijalnim strategijama. Dakle, ukupni sadržaj sa kojim se susrećemo posredstvom platformi za nas je selektovan kroz proces personalizacije, moderacije i na osnovu reputacionog statusa sadržaja. Između previše i premalo, ljudske ili algoritamske intervencije nalaze se pravila o tome kako se ovaj proces odvija. Ta pravila utemeljena su u specifičnim vrednostima, koje nisu javno već profitno orijentisane i usmerene su, pre svega, na očuvanje monopolskog statusa najvećih igrača. Stoga će nam umesto najkvalitetnije usluge ili sadržaja uglavnom biti ponuđen onaj sa najviše profitnog potencijala.

Geografska distribucija 100 vodećih globalnih digitalnih platformi prema tržišnoj kapitalizaciji za 2021. godinu

Amerika



Airbnb
Allcergy
Booking
Carvana
Chegg
Doordash
Dropbox
Ebay
Etsy
Expedia
Grainger
Grubhub
Instacart
Inbuit
Luft
Match
Mercadoline
Opendoor
Palancir
Peloton
Pinterest
Roblox
Roku
Slack
Snap
Splunk
Square
Stripe
Teladoc
Twilio
Twitter
Uber
Wish
Zillow

Evropa

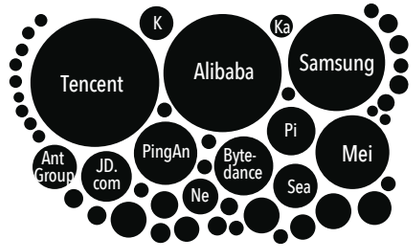
Adyen
Autol
Checkout
Delivery
Hero
Edenred
HelloFresh
Farfetch
Klarna
Spotify
Just Eat T.
Yandex

Afrika

Naspers
Prosus

Izvor: Holger Schmidt, dostupno na www.netzoe-konom.de (podaci od maja 2021).
Napomena: Kao referenca, tržišna kapitalizacija Apple-a iznosi 2,22 biliona dolara, dok je za Mercado Libre 88,7 milijardi dolara, za Baidu 80,2 milijarde dolara, a za Spotify 59,7 milijardi dolara.

Azija i Pacifik



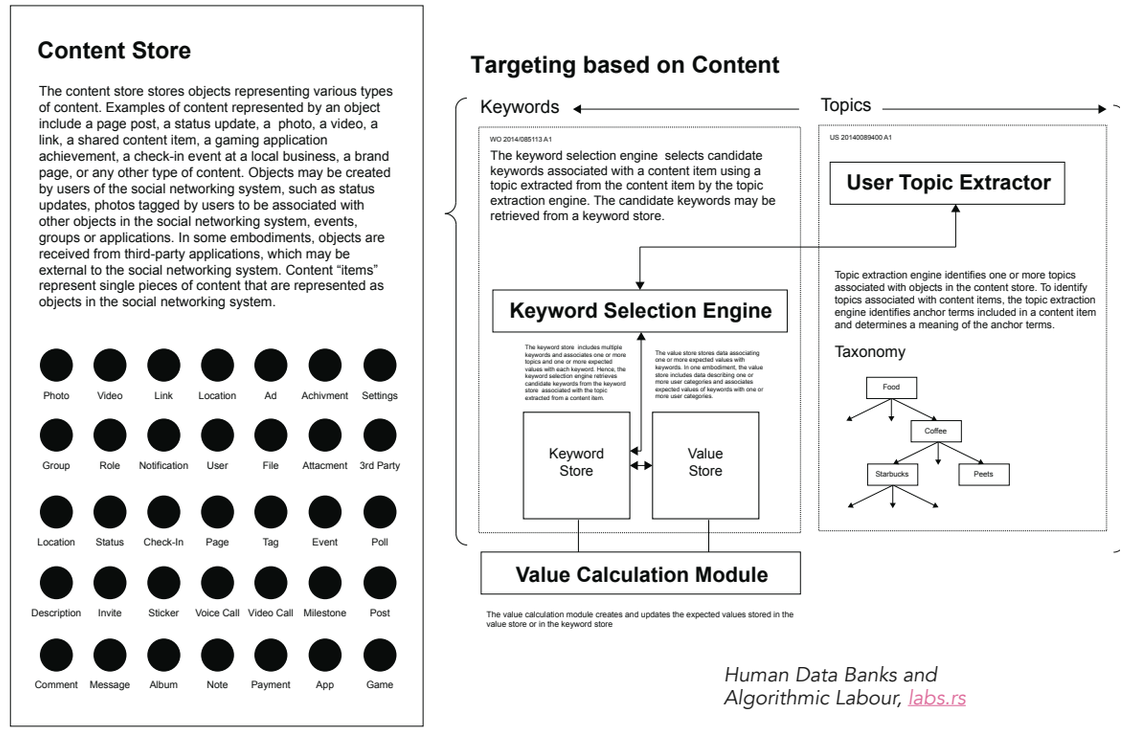
Baidu
Beike
Billbill
BYJU
Chehaoduo
Coupang
Dada Nexus
Didi Chuxing
Go-Jek
Grab
JD Digits
Kakao
Kuaishou
Lufax
Manbang
Meicai
Meituan
Mercari
Naver
Netease
Ola
Oyo
Paytm
Pinduoduo
PingAn Health
Rakuten
Rea
Sea Group
Seek
Sensetime
Tokopedia
Trip.com
VipShop
WeBank
Webockor
Weibo
YonYou
Yuanfudao

Platformska ekonomija 2021. godine, Fundacion Solon

Posledice logike platformskog mehanizma su takve da, primera radi, konačnu uređivačku odluku o sadržaju Gardijana ili Njujork Tajmsa ipak donosi Gugl, Meta ili X. Ova debata pokrenuta je još 2016. godine kada je Fejsbuk obrisao objavu norveškog novinara koji je, referišući na značaj fotografije u istoriji rata, objavio fotografiju Napalm devojčice, koja je 1972. godine dobila Pulicerovu nagradu.[223] Na razmere mogućeg uticaja na novinarski rad i medijske slobode ukazuje i primer iz Srbije. Naime, u septembru 2019. Tviter nalog dnevnog lista Danas bio je „privremeno zaključan" nedelju dana zbog tumačenja platforme da „datum rođenja" Danasa nije u skladu sa pravilima jer je u trenutku registracije naloga 2009. Danas imao manje od 13 godina. Još nekoliko dana bilo je potrebno da se baza pratilaca ovog medija u potpunosti obnovi.[224]

Nebrojeni su primeri nedoslednosti, netransparentnosti i nejasnih kriterijuma platformske moderacije. Dodatni sloj problema stvorile su regulatorne okolnosti: jurisdikcija u kojoj su platforme poput Fejsbuka nastale predstavlja sigurnu luku za tehnološke kompanije koje se prema američkim zakonima u tom trenutku tretiraju kao ništa više od telefonske linije. Platforme su, naime, obični provodnici. Nisu izdavači, te stoga nisu odgovorne za sadržaj koji posreduju, a i ako sporadično intervenišu na bilo koji način, ne postoje jasni kriterijumi o tome zbog čega se i kako takva moderacija sprovodi.

U Sjedinjenim državama, član 230 Zakona o pristojnosti u komunikacijama (*Communications Decency Act, Section 230*) jasno propisuje da posrednici kao što su velike tehnološke kompanije ne podlažu odgovornosti za sadržaje koji se dele putem njihovih servisa. Ovim pravilom, koje je ustanovljeno još devedesetih godina, platforme su uspele u raznim slučajevima da sa sebe sklone odgovornost, kao na primer u slučaju genocida nad Rohingama u Mjanmaru, u kojem je utvrđeno da je Fejsbuk direktno posredovao u širenju nasilja i govora mržnje nad ovom etničkom grupom, koje je za cilj imalo jačanje ultranacionalističkih sentimenata i



Human Data Banks and Algorithmic Labour, labs.rs

islamofobije i dovelo do genocida nad ovom etničkom grupom od strane mjanmarske vojske u oktobru 2016. godine.[225] Tokom 2022. godine, u javnost je izneto više od hiljadu poverljivih dokumenata koji su pokazali da je Fejsbuk direktno bio svestan količine govora mržnje koji se širio sa njihovih platformi, promovisanja teorija zavera koje osporavaju globalno zagrevanje, dezinformacija o vakcinama i pandemiji kovida, štetnog rada njihovih algoritama koji su devojčicama i mladim ženama preko Instagrama plasirali nezdrave standarde lepote, i mnoge druge štetne sadržaje.[226]

EVROPSKI ODGOVOR – DIGITAL X ACT

Globalni doseg najvećih digitalnih platformi učinio je platformizaciju geografski neograničenom. Međutim, liberalni društveno-politički okvir u kojem su one prvenstveno nastale ne važi u svim delovima sveta gde se one koriste. Na evropskom kontinentu godinama traje debata o tome kako uspostaviti osnovna pravila o tome šta i kako može da cirkuliše onlajn svetom, a šta bi ipak trebalo da bude ograničeno ili nedopustivo. Na tragu tradicije države blagostanja prvo su pojedinačne evropske zemlje nastojale da uspostave relevantno zakonodavstvo. Međutim, to nije imalo mnogo efekta. Prvo, brzo je postalo jasno da su najveće digitalne platforme izvesno moćnije od država, kako u pogledu efikasnosti zaobilaženja zakona, odnosno kaznenih politika. I drugo, pristup i adresat regulacije bio je pogrešan. U Nemačkoj i Francuskoj usvajani su zakoni čiji je cilj bio da uspostave pravila za uklanjanje nelegalnog sadržaja, lažnih vesti i govora mržnje sa interneta.[227] Međutim, pokazalo se da regulisanje sadržaja može ozbiljno da ugrozi slobodu izražavanja, pluralizam i raznovrsnost digitalne ponude, jer regulatorni princip zapravo ne izaziva platformski mehanizam, već se na njega nadovezuje novim slojem moderatorske intervencije. Analizom ovih zakona utvrđeno je da su, u nekim slučajevima, čak 99 odsto uklonjenih i ograničenih komentara na platformama predstavljali zakonski dozvoljeni govor. Ovakvi nalazi pokazuju da su platforme u strahu od sankcija od strane država odlučile da odgovore preteranom moderacijom.[228] Na ovaj način platforme ipak prioritizuju profit u odnosu na transparentan i otvoren prostor za javnu debatu i gde su pojedinačni sadržaji i korisnici ti koji snose najveće posledice.

Evropska unija je primenila drugačiji pristup, a efekti nove regulacije tek počinju da se primećuju. Brisel se opredelio za sistemski pristup u čijem fokusu su procedure a ne digitalni sadržaj, novi propisi imaju zakonsku snagu i uglavnom podrazumevaju obaveze dužne pažnje (*due dilligence obligations*) koje su skalirane prema broju korisnika odnosno ulozi i društvenom značaju pojedinačne platforme. Takav pristup trenutno predstavlja globalni standard i najsveobuhvatniju regulativu usmerenu prema velikim tehnološkim kompanijama. U prvom redu, to je sveobuhvatan model zasnovan na obaveznom i redovnom mapiranju i smanjenju sistemskih rizika koje izazivaju najveći digitalni akteri svojim dizajnom, radom i uslugama koje pružaju. Ovaj pristup podrazumeva kompleksan institucionalni dizajn u kojem ulogu ima niz institucija od Evropske komisije, nacionalnih institucija, nezavisnih tela, zatim akteri iz digitalne industrije, eksperti, pa i sami korisnici.

Nova evropska regulatorna generacija obuhvata niz *akata* i drugih dokumenata koji nisu sektorski usmereni, koliko nastoje da norme iz različitih resora učine sprovodivim i u digitalnom svetu. Najviše pažnje je svakako izazvao Digitalni paket akata, koji regulišu digitalne servise i tržišta, *Digital Services Act* i *Digital Markets Act*. Ova dva ambiciozna zakona obećavaju *odgovornije* digitalno okruženje i *demokratizaciju* digitalnog tržišta, prvo regulacijom velikih onlajn platformi i pretraživača kao centralnih provajdera digitalnih usluga i drugo, regulacijom „čuvara kapija" odnosno razbijanjem tržišnog monopola najmoćnijih igrača u digitalnoj industriji.[229]

U vreme pisanja ovog teksta Evropska komisija je samo na osnovu Akta o digitalnim uslugama protiv velikih onlajn platformi pokrenula više istraga, kako zbog diseminacije nelegalnog i manipulativnog sadržaja, netransparentnosti i obmanjujućeg interfejsa (X), obmanjujućeg oglašavanja, političkog sadržaja i uskraćivanja mogućnosti za praćenje sadržaja u vezi sa izborima (Fejsbuk i Instagram), rizika za maloletnike (TikTok), nelegalnih proizvoda i servisa „zavisničkog dizajna" (Temu).[230]

EKSPERIMENT: SRBIJA

Iako se mogućnost prelivanja *de facto* efekata evropske regulacije izvan granica Evropske unije već široko razmatra pod sintagmom „briselski efekat", aktuelna situacija ne daje mnogo prostora za optimizam. Naime, slučaj Srbije upravo ukazuje da su posredni regulatorni efekti vrlo ograničeni, a da neusklađenost sa aktuelnim evropskim zakonodavstvom sa sobom nosi niz problema. Čak i eventualno usklađivanje nacionalnih propisa sa evropskim bez adekvatne institucionalne baze za njihovo sprovođenje, posebno prema najvećim igračima u digitalnoj industriji (poput Gugla, Epla, Mete, TikToka), činilo bi normativnu usklađenost praznom formalnošću bez bilo kakvih efekata.

Iako postojeći zakonodavni okvir u Srbiji, uključujući Zakon o elektronskoj trgovini, Zakon o zaštiti konkurencije i Zakon o zaštiti podataka o ličnosti, predstavlja solidnu normativnu osnovu za dalje usklađivanje legislative sa novom generacijom propisa iz Digitalnog paketa, implementaciju postojećih zakona prate problemi primenjivosti pojedinih odredbi usled neprilagođenosti propisa, slabe kaznene politike i ograničene efikasnosti. Primera radi, Meta ni šest godina nakon usvajanja Zakona o zaštiti podataka o ličnosti nije imenovala predstavnika u Srbiji, iako je to zakonska obaveza. Još pre četiri godine SHARE Fondacija je podnela niz prekršajnih prijava protiv globalnih tehnoloških kompanija Povereniku za zaštitu podataka o ličnosti, ovlašćenom da pokrene inspekcijski postupak koji u slučaju kršenja zakona može da izrekne kaznu u visini od sto hiljada dinara za kompaniju i 20.000 dinara za njenog direktora.[231]

Ove simbolične kazne za kompanije čiji je profit nezamisliv, pokazale su se potpuno neefikasnim, toliko da su same kazne „isplativije" od angažovanja predstavnika, pogotovo kada se uzme u obzir da su prema evropskoj uredbi o zaštiti podataka, koji domaći ZZPL praktično kopira, kazne za kompanije do 10 miliona evra ili 2 odsto ukupnog godišnjeg profita.[232] Dodatno, ograničena odgovornost velikih platformi u Srbiji pripisuje se i malom i nekonkurentnom digitalnom tržištu, zbog čega kompanije nemaju dovoljno motiva da unajmljuju lokalne moderatore štetnog sadržaja ili određuju interne timove koji bi se bavili Srbijom ili regionom Zapadnog Balkana. Činjenica da Srbija ne raspolaže efikasnim mehanizmima zaštite prava korisnika već je više puta imala štetne posledice po prava; najskoriji primer je upotreba podataka Metinih korisnika iz Srbije u svrhe treninga modela veštačke inteligencije.[233]

To svakako nije prvi eksperiment Mete na teritoriji Srbije. Još 2017. godine ova platforma je testirala potencijalno uvođenje *Explore Feeda* pored postojećeg *News Feeda*, od kojeg je posle nekoliko meseci odustala.[234] Iako su posledice bile drugačije, jer su više pogodile medije nego korisnike, indikativna je činjenica da je pored Srbije ovaj eksperiment sproveden još samo u Slovačkoj, Boliviji, Gvatemali, Kambodži i Šri Lanki, iz čega se može zaključiti da Srbija spada u zemlje pogodne za lansiranje i testiranje eksperimentalnih tehnologija globalnih kompanija. Isto se pokazalo i kada je Tviter 2021. godine uveo novu oznaku za određene medije u Srbiji, obeležavajući ih kao saradnike vlasti.[235] Ovaj potez protumačen je kao pritisak i eksplicitno targetiranje medija, uz to što nije bilo potpuno jasno o kakvoj je kvalifikaciji tačno reč. Nije neutemeljeno zaključiti da Radio-televizija Srbije, odnosno javni servis koji je u vlasništvu države „sarađuje" sa državom. Nezavisno od činjenice da RTS ima reputaciju nepružanja pravovremenih, tačnih i objektivnih informacija građanima koji joj plaćaju pretplatu, nije se činilo da je ovo bila poenta Tviterovog poteza.[236]

U zemljama sa oslabljenim institucijama, nedovoljno razvijeni regulatori koji često ne poseduju dovoljno kapaciteta, teško ostvaruju kontrolnu ulogu nezavisnih tela, za šta nedostaje i politička podrška. Posledično, ljudska prava građana i građanki u Srbiji pred digitalnim

izazovima nalaze se u specifičnom vakuumu između korporativnih interesa, političke volje i skromnih institucionalnih kapaciteta.

Međutim, zaštita javnog interesa i prava građana svakako ne može biti prepuštena digitalnom korporativnom sektoru. Velika curenja podataka građana poslednjih godina upravo se i vezuju za najpopularnije digitalne platforme, koje su čak i promišljale strategiju „normalizacije" javnog narativa o takvim incidentima.[237] Tamo gde nema adekvatne regulatorne kontrateže za takve slučajeve i gde je sistem zaštite ličnih podataka inače slab, ljudska prava su najranjivija. Srbija je opet u redu takvih zemalja, što potvrđuje i primer curenja podataka gotovo celokupnog punoletnog stanovništva Srbije propustom Agencije za privatizaciju 2014. godine i objavljivanje medicinskih podataka građana tokom pandemije kovida-19 usled propusta u bezbednosti sistema.[238]

Princip zaštite podataka stoji u suprotnosti ili, pak, u ravnoteži sa principom otvorenosti i dostupnosti javno relevantnih podataka. U tenziji ova dva normativa, platforme imaju poseban značaj, posebno u zemljama u kojima princip tajnosti podataka uglavnom služi kao sredstvo za prikrivanje korupcije i drugih neregularnosti, kao što je na primer kršenje izbornih procedura. Svaki vid ukidanja dostupnosti podataka na digitalnim platformama koji omogućavaju praćenje, analizu i procenu regularnosti izbornih procesa, dodatno urušava uveliko oslabljene demokratske principe i onemogućava bilo kakvu transparentnost izbornih kampanja.[239]

Najzad, Maskov potez nakon kupovine Tvitera da najjeftiniji paket za pristup podacima sa preimenovane X platforme naplaćuje 42.000 dolara mesečno, tendenciozno je najavio zatvaranje platformskih podataka za javnost.[240] Još ranije, 2016. godine započeto je postepeno gašenje Metinog alata *CrowdTangle* koji je istraživačima otključavao svet podataka sa Fejsbuka i Instagrama.[241] To je zadalo ozbiljan udarac budućim istraživanjima zloupotreba na društvenim mrežama, jer je u pitanju bio jedan od najvažnijih i preciznijih alata za istraživačku zajednicu, a koji je razvila jedna velika tehnološka kompanija, što je po sebi predstavljalo gotovo presedan.

Prema novim evropskim pravilima, otvorene baze i dostupnost javno relevantnih podataka trenutno stoje kao centralne tačke oslonca za istraživače i javnost koja ima pravo na uvid u sve tehnološke, infrastrukturne, finansijske, reklamne i algoritamske mehanizme koji predstavljaju faktore od značaja za izborni proces. U tom smislu, svetska izborna 2024. godina bila je globalno eksperimentalna: od Sjedinjenih Država, gde se ključni postizborni transferi odvijaju upravo između digitalne industrije i države, preko EU koja tek aktivira novi mehanizam odgovornosti platformi, do zemalja poput Srbije koja je samo inovirala izborne neregularnosti, legitimisala netransparentnost i praktično ugasila svaki institucionalni kontrolni mehanizam. Umesto da nove tehnologije doprinesu demokratiji s početka priče, deluje da je sprega nekontrolisane političke moći i manipulativnim potencijalom platformi u stanju da u kratkom roku zbriše gotovo svaki obris demokratije jednog društva.`

REFERENCE

1 Nataša Anđelković, "Hrvoje Klasić: Studentski protesti u Srbiji veći od onih 1968.", BBC na srpskom, 03. februar 2025, https://www.bbc.com/serbian/articles/clynx1gvw8qo/lat

2 "Rekapitulacija događaja od 22.11. do 18.12.", Kolubarske, 19. decembar 2024, https://www.kolubarske.rs/sr/vesti/valjevo/14328/Rekapitulacija-doga%C4%91aja-od-2211-do-1812.htm

3 Mila Bajić i Snežana Bajčeta, „Izbori 2023 na informativnoj margini: Analiza predizborne kampanje u onlajn medijima", SHARE Fondacija, januar 2024, https://www.sharefoundation.info/wp-content/uploads/Izbori-na-informativnoj-margini-2023.pdf

4 "Vučić se od početka 2025. javnosti obratio čak 59 puta - nekad i više puta u danu", 021, 23. februar 2025, https://www.021.rs/story/Info/Srbija/402343/Vucic-se-od-pocetka-2025-javnosti-obratio-cak-59-puta-nekad-i-vise-puta-u-danu.html

5 "„Novosti" ugrožavaju bezbednost studenata", N1, 03. januar 2025, https://n1info.rs/vesti/novosti-ugrozavaju-bezbednost-studenata/

6 Danica Đokić, "BIA prijavila sajt SNS.rs odmah pošto je na njemu objavljena parola 'Ruke su vam krvave', iako za to nije nadležna", Cenzolovka, 21. februar 2025. https://www.cenzolovka.rs/mediologija/bia-prijavila-sajt-sns-rs-odmah-posto-je-na-njemu-objavljena-parola-ruke-su-vam-krvave-iako-za-to-nije-nadlezna/

7 Joe Caluori, "OK Zoomer: Gen Z's radical views on civil liberties and law and order", National Center for Social Research, 23. maj 2024. https://natcen.ac.uk/ok-zoomer-gen-zs-radical-views-civil-liberties-and-law-and-order

8 Beta, "Vučić o navodnom snimku Zobenice: Poslao mi je poruku da je to veštačka inteligencija", N1, 28. novembar. 2024. https://www.danas.rs/vesti/politika/vucic-o-navodnom-snimku-zobenice-poslao-mi-je-poruku-da-je-to-vestacka-inteligencija/

9 Charles Mok, „China and Russia Want to Rule the Global Internet", The Diplomat, 22. februar 2022, https://thediplomat.com/2022/02/china-and-russia-want-to-rule-the-global-internet/

10 Univerzalna deklaracija o ljudskim pravima, OHCHR, https://www.ohchr.org/sites/default/files/UDHR/Documents/UDHR_Translations/cnr.pdf

11 Iva Martinović, „Cenzura Supermena i uzdizanje vođe", Radio Slobodna Evropa, 3. februar 2014, https://www.slobodnaevropa.org/a/cenzura-supermena-i-uzdizanje-vodje/25251909.html

12 Danilo Redžepović, „Kako je hakovan Teleprompter", Peščanik, 19. april 2015, https://pescanik.net/kako-je-hakovan-teleprompter/

13 Aleksandar Bečić, „Kratak uvod u diktaturu", Kolumnista, 19. maj 2014, https://archive.li/d5dlE (portal u međuvremenu obrisan)

14 „Greška 404: Digitalna prava u Srbiji 2014-2019", SHARE Fondacija, 2019, https://resursi.sharefoundation.info/wp-content/uploads/2019/11/Greska_404.pdf

15 Milica Stojanović, „Hakovan tekst: Istina ima rok trajanja", CINS, 11. decembar 2013, https://www.cins.rs/hakovan-tekst-istina-ima-rok-trajanja/

16 „Kako do doktorata? Lako! Slučaj ministra Stefanovića", Peščanik, 1. jun 2014, https://pescanik.net/kako-do-doktorata-lako-slucaj-ministra-stefanovica/

17 Milica Jovanović, "Istraga je u toku", Peščanik, 7. jun 2014, https://pescanik.net/istraga-je-u-toku/

18 Vuk Jeremić, „Bezbedni hakerski obračuni sa medijima: Samo pet presuda posle 79 napada", Cenzolovka, 12. februar 2020, https://www.cenzolovka.rs/pritisci-i-napadi/bezbedni-hakerski-obracuni-sa-medijima-samo-pet-presuda-posle-79-napada/

19 „New surge of DDoS attacks threatens media freedom in Europe", International Press Institute, 19. februar 2024, https://ipi.media/new-surge-of-ddos-attacks-threatens-media-freedom-in-europe/

20 „Političko-informaciono ratovanje: kratko uputstvo: Deo 1: Propaganda, dominacija i napadi na onlajn medije", SHARE labs, 31. jul 2017, https://labs.rs/sr/politicko-informaciono-ratovanje-kratko-uputstvo/

21 SHARE Monitoring Baza, https://monitoring.labs.rs/

22 Jovy Chan, 2024, „Online astroturfing: A problem beyond disinformation", Philosophy & Social Criticism, 50(3), pp. 507-528, https://journals.sagepub.com/doi/10.1177/01914537221108467

23 „Šta su zapravo botovi i po čemu je Srbija specifična u odnosu na ostatak sveta?", N1, 12. jul 2023, https://n1info.rs/vesti/sta-su-zapravo-botovi-i-po-cemu-je-srbija-specificna-u-odnosu-na-ostatak-sveta/

24 Quarterly Adversarial Threat Report, Meta, februar 2023, https://about.fb.com/wp-content/uploads/2023/02/Meta-Quarterly-Adversarial-Threat-Report-Q4-2022.pdf

25 „Tepić: Koliko je državnih službenika u internet mreži botova SNS?", Stanka slobode i pravde, 25. februar 2023, https://ssp.rs/vesti-i-najave/aktivnosti/tepi%C4%87-koliko-je-dr%C5%BEavnih-slu%C5%BEbenika-u-internet-mre%C5%BEi-botova-sns/

26 Mila Bajić, „Od objave do obmane: Šta nam govori Metin poslednji izveštaj?", SHARE Fondacija, 9. mart 2023, https://www.sharefoundation.info/sr/od-objave-do-obmane-sta-nam-govori-metin-poslednji-izvestaj/

27 Anđela Milivojević, „Castle: Kako srpska vlast manipuliše razumom, a građani za to još i plaćaju", Balkan Insight, 18. jun 2020, https://balkaninsight.com/sr/2020/06/18/castle-kako-srpska-vlast-manipulise-razumom-a-gradani-za-to-jos-i-placaju/

28 Tomislav Marković, „Kako su SNS botovi napisali 10 miliona komentara", Al Jazeera, 22. decembar 2018, https://balkans.aljazeera.net/opinions/2018/12/22/kako-su-sns-botovi-napisali-10-miliona-komentara

29 Daniel Bush, „'Fighting Like a Lion for Serbia': An Analysis of Government-Linked Influence Operations in Serbia", Stanford Internet Observatory, 2. april 2020, https://fsi-live.s3.us-west-1.amazonaws.com/s3fs-public/serbia_march_twitter.pdf

30 Anđela Milivojević i Milica Šarić, „SNS botovi imali pristup Kuriru i Espresu", CINS, 4. septembar 2019, https://www.cins.rs/sns-botovi-imali-pristup-kuriru-i-espresu/

31 Danilo Redžepović, „OBJAVLJUJEMO: Sve tajne 'SNS botova' – fotografije, uputstva, programe, telefone …", Cenzolovka, 8. oktobar 2014, https://www.cenzolovka.rs/vesti/objavljujemo-sve-tajne-sns-botova-fotografije-uputstva-programe-telefone/

32 „Političko-informaciono ratovanje: kratko uputstvo: Deo 1: Propaganda, dominacija i napadi na onlajn medije", SHARE labs, 31. jul 2017, https://labs.rs/sr/politicko-informaciono-ratovanje-kratko-uputstvo/

33 Mila Bajić, „Nedovršena priča: Analiza predizborne onlajn kampanje 2022“, SHARE Fondacija, jun 2022, https://www.sharefoundation.info/wp-content/uploads/Izbori-2022.-izvestaj.pdf

34 Miloš Đošić, „Spisak botova osvanuo na internetu: Niko od naprednjaka se do sada nije oglasio“, N1, 9. jul 2023, https://n1info.rs/vesti/spisak-botova-osvanuo-na-internetu-niko-od-naprednjaka-se-do-sada-nije-oglasio/

35 „Službenici partijskog interesa: Za državne pare ‘botuju’ za SNS“, N1, 11. jul 2023, https://n1info.rs/vesti/za-sta-su-placeni-radnici-u-drzavnim-preduzecima-ako-za-vreme-posla-botuju/

36 Stefan Kosanović, Ivan Subotić i Stefan Janjić, „Bot-armija: najaktivniji su Kruševac i Šabac, a Mali Zvornik i Novi Kneževac prvi ‘po glavi stanovnika’“, Fake News Tragač, 8. jul 2023, https://fakenews.rs/2023/07/08/bot-armija-najaktivniji-su-krusevac-i-sabac-a-mali-zvornik-i-novi-knezevac-prvi-po-glavi-stanovnika/

37 „Šta su zapravo botovi i po čemu je Srbija specifična u odnosu na ostatak sveta?“, N1, 12. jul 2023, https://n1info.rs/vesti/sta-su-zapravo-botovi-i-po-cemu-je-srbija-specificna-u-odnosu-na-ostatak-sveta/

38 „Vučić podelio: Da, i ja sam SNS bot“, N1, 11. jul 2023, https://n1info.rs/vesti/vucic-podelio-da-i-ja-sam-sns-bot/

39 Loni Hagen, Stephen Neely, Thomas E. Keller, Ryan Scharf, and Fatima Espinoza Vasquez, „Rise of the Machines? Examining the Influence of Social Bots on a Political Discussion Network“, Social Science Computer Review, 40(2), (2020): 264-287, https://doi.org/10.1177/0894439320908190

40 „New report: Hungary dismantles media freedom and pluralism“, International Press Institute, 30. decembar 2019, https://ipi.media/new-report-hungary-dismantles-media-freedom-and-pluralism/

41 „’Zagađenje javnog prostora’: Šta konkretno znači za građane to što će Telekom moći da osniva medije?“, N1, 24. oktobar 2023, https://n1info.rs/vesti/zagadjenje-javnog-prostora-sta-konkretno-znaci-za-gradjane-to-sto-ce-telekom-moci-da-osniva-medije/

42 „Pregled tržišta elektronskih komunikacija u Republici Srbiji – drugi kvartal 2024. godine“, RATEL, https://www.ratel.rs/uploads/documents/empire_plugin/66c341c1c112c.pdf

43 Bojana Caranović, „POSLOVNA SARADNJA NIJE KARTEL: Šta zaista stoji iza sukoba SBB sa kompanijama ‘Telekom’ i ‘Telenor’“, Novosti, 31. januar 2021, https://www.novosti.rs/ekonomija/vesti/959930/poslovna-saradnja-nije-kartel-sta-zaista-stoji-iza-sukoba-sbb-kompanijama-telekom-telenor

44 Miloš Obradović, „Šta je Globaltel koji je Telekom kupio od Pinka Željka Mitrovića i kako posluje?“, Danas, 5. novembar 2023, https://www.danas.rs/vesti/ekonomija/sta-je-globaltel-koji-je-telekom-kupio-od-pinka-zeljka-mitrovica-i-kako-posluje/

45 „United Media i SBB podnele krivičnu prijavu protiv Telekoma i Telenora“, N1, 8. april 2021, https://n1info.rs/vesti/united-media-i-sbb-podnele-krivicnu-prijavu-protiv-telekoma-i-telenora/

46 „Advokatska kancelarija Tomanović: Da li je postupanje tužiteljke Savović protiv Telekoma Srbije uticalo na njenu smenu?“, Danas, 6. jun 2023, https://www.danas.rs/vesti/drustvo/advokatska-kancelarija-tomanovic-da-li-je-postupanje-tuziteljke-savovic-protiv-telekoma-srbije-uticalo-na-njenu-smenu/

47 Vojislav Milovančević, „Velika pobeda četiri kompanije United Grupe: Telekom izgubio spor od 80 miliona“, Nova S, 25. maj

2022, https://nova.rs/vesti/drustvo/velika-pobeda-cetiri-kompanije-united-grupe-telekom-izgubio-spor-od-80-miliona/

48 „Novi nedeljnik iza kog stoje donedavni novinari NIN-a zvaće se 'Radar'", Radio 021, 13. februar 2024, https://www.021.rs/story/Info/Srbija/367176/Novi-nedeljnik-iza-kog-stoje-donedavni-novinari-NIN-a-zvace-se-Radar.html

49 Tanja Maksić, „Pregled javne potrošnje u oblasti javnog informisanja, kulture, civilnog društva i omladine u periodu 2019-2021", BIRN, 16. maj 2022, https://birn.rs/izvestaji/javno-o-javnim-konkursima/

50 Nic Newman, „What do we know about the rise of alternative voices and news influencers in social and video networks?", Reuters Institute, 17. jun 2024, https://reutersinstitute.politics.ox.ac.uk/digital-news-report/2024/rise-alternative-voices-and-news-influencers-social-and-video-networks

51 Sanja Živanović, „Televizija i dalje najpopularniji medij, konstantan rast publike na internetu, ali mediji od toga nemaju mnogo koristi", Cenzolovka, 26. jul 2023, https://www.cenzolovka.rs/trziste/televizija-i-dalje-najpopularniji-medij-konstantan-rast-publike-na-internetu-ali-mediji-od-toga-nemaju-mnogo-koristi/

52 Snježana Milivojević, Danka Nikolić Slavnić i Snežana Bajčeta, „Informisanje u digitalnom okruženju u Srbiji", Centar za medijska istraživanja FPN, 2020, https://safejournalists.net/wp-content/uploads/2021/04/informisanje-u-digitalnom-okruzenju-2020-5-compressed-compressed-1.pdf

53 Mila Bajić i Snežana Bajčeta, „Izbori 2023 na informativnoj margini: Analiza predizborne kampanje u onlajn medijima", SHARE Fondacija, januar 2024, https://www.sharefoundation.info/wp-content/uploads/Izbori-na-informativnoj-margini-2023.pdf

54 Mapping Media Freedom, European Center for Press and Media Freedom (2016-2024), https://www.mapmf.org/explorer?q=Distributed+Denial+of+Service&f.type_of_incident=Hacking%2FDDoS&sort=timestamp%3Adesc

55 „2024 World Press Freedom Index – journalism under political pressure", Reporters Without Borders, 2024, https://rsf.org/en/2024-world-press-freedom-index-journalism-under-political-pressure

56 Ana Zdravković, „SLAPP tužbe ukratko", Slavko Ćuruvija Fondacija, decembar 2023, https://www.slavkocuruvijafondacija.rs/wp-content/uploads/2023/12/SLAPP-tuzbe-ukratko-Slavko-Curuvija-fondacija.pdf, str.3

57 Sofija Parojčić, „Suđenje KRIK-u po tužbi sudije kreće ispočetka", KRIK, 12. novembar 2024, https://www.krik.rs/sudjenje-krik-u-po-tuzbi-sudije-krece-ispocetka/

58 Milena Vasić i Kristina Todorović, „Zloupotreba Prava Analiza SLAPP Slučajeva i Zaštita Slobode Izražavanja na Internetu u Srbiji", Komitet pravnika za ljudska prava – YUCOM, mart 2024., https://yucom.org.rs/wp-content/uploads/2024/05/Analiza-SLAPP.pdf

59 Jelena Zorić, „Slučaj nuklearne inženjerke: Otkaz zbog politički nepodobnih tvitova", Vreme, 9. jun 2023, https://vreme.com/komentar/slucaj-nuklearne-inzenjerke-otkaz-zbog-politicki-nepodobnih-tvitova/

60 Ana Lalić, „KC Vojvodine pred pucanjem: Bez zaštite za medicinske sestre", Nova.rs, 1. april 2020, https://nova.rs/vesti/drustvo/kc-vojvodine-pred-pucanjem-bez-zastite-za-medicinske-sestre/

61 Marija Vučić, „Novinarki portala nova.rs određen pritvor od 48 sati", Raskrikavanje, 2. april 2020, https://www.raskrikavanje.rs/page.php?id=635

62 „Informacije o korona virusu ubuduće samo od Kriznog štaba, novinari ukazuju na prikrivenu cenzuru", Južne vesti, 1. april 2020, https://www.juznevesti.com/Drushtvo/Informacije-o-korona-virusu-ubuduce-samo-od-Kriznog-staba-novinari-ukazuju-na-prikrivenu-cenzuru.sr.html

63 „Novinarska udruženja Srbije traže povlačenje Vladinog zaključka o informisanju", Radio Slobodna Evropa, 1. april 2020, https://www.slobodnaevropa.org/a/30522236.html

64 Sava Majstorov, „Prekršajne prijave protiv novinara i aktiviste", SO Info, 12. april 2022, https://www.soinfo.org/vesti/vest/26608/prekrsajne-prijave-protiv-novinara-i-aktiviste/

65 „Aktivista iz Niša: Policija me probudila u 7h zbog poziva na protest na Fejsbuku", N1, 6. decembar 2021, https://n1info.rs/vesti/aktivista-iz-nisa-policija-me-probudila-u-7h-zbog-poziva-na-protest-na-fejsbuku/

66 @pricac_dpm, 19. decembar 2023, https://x.com/pricac_dpm/status/1737177868717715645?t=QhBueDLXclCNlji17i9eDw

67 Stefan Kosanović, „Za provladine medije srušila se 'stara nadstrešnica' Železničke stanice. Prethodno milioni evra uloženi u rekonstrukciju", Raskrikavanje, 1. novembar 2024, https://www.raskrikavanje.rs/page.php?id=Za-provladine-medije-srusila-se-stara-nadstresnica-Zeleznicke-stanice--Prethodno-milioni-evra-ulozeni-u-rekonstrukciju-1414

68 „Vesić: U Železničku stanicu Novi Sad uloženo 65 miliona evra", Srpska napredna stranka, 5. jul 2024, https://www.sns.org.rs/novosti/vesti/vesic-u-zeleznicku-stanicu-novi-sad-ulozeno-65-miliona-evra

69 @mirkotopalovic7, 1. novembar 2024, https://x.com/mirkotopalovic7/status/1852438856911798375

70 @SlavicaPlavsic, 5. novembar 2024, https://x.com/SlavicaPlavsic/status/1853770331267174873

71 @hijenailesinar, 1. novembar 2024, https://x.com/hijenailesinar/status/1852374790587179253

72 „Veliki protest u Beogradu u fotografijama", BBC News na srpskom, 23. decembar 2024, https://www.bbc.com/serbian/articles/c140v1e13r5o/lat

73 Mike Smeltzer and Alexandra Karppi, „Nations in Transit 2024: A Region Reordered by Autocracy and Democracy", Freedom House, 2024, https://freedomhouse.org/sites/default/files/2024-04/NIT_2024_Digital_Booklet.pdf

74 „Why Communication Metadata Matters", Electronic Frontier Foundation, 2024, https://ssd.eff.org/module/why-metadata-matters

75 Ewen MacAskill and Gabriel Dance, „NSA Files: Decoded", The Guardian, 1. novembar 2013, https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded

76 DIRECTIVE 2006/24/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, 15. mart 2006, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32006L0024

77 „SHARE istražuje: Ko (sme da) zna gde ste bili prošlog leta", SHARE Fondacija, 16. jun 2016, https://resursi.sharefoundation.info/sr/resource/share-istrazuje-ko-sme-da-zna-gde-ste-bili-proslog-leta/

78 „The Court of Justice declares the Data Retention Directive to be invalid", Court of Justice of the European Union, 8. april 2014, https://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054en.pdf

79 Ranija verzija Zakona o elektronskim komunikacijama, dostupna na: https://www.paragraf.rs/propisi/zakon_o_elektronskim_komunikacijama.html

80 Zakon o elektronskim komunikacijama, Sl. glasnik RS, br. 35/2023, https://www.paragraf.rs/propisi/zakon-o-elektronskim-komunikacijama.html

81 „Invisible Infrastructure: Surveillance Architecture", SHARE Lab, 9. mart 2015, https://labs.rs/en/invisible-infrastructures-surveillance-achitecture/

82 Odluka I⍰⍰-1245/2010, Ustavni sud Republike Srbije, 13. jun 2013, https://www.ustavni.sud.rs/sudska-praksa/baza-sudske-prakse/pregled-dokumenta?PredmetId=9081

83 Sascha Venohr, „The Tell-All Telephone", DataJournalism.com, https://datajournalism.com/read/handbook/one/case-studies/the-tell-all-telephone

84 „Zadržavanje podataka o komunikaciji u Srbiji: Koliko smo pod nadzorom? (2014-2016)", SHARE Lab, 29. avgust 2017, https://labs.rs/sr/zadrzavanje-podataka-o-komunikaciji-u-srbiji/; „Zadržavanje podataka o komunikaciji u Srbiji: Koliko smo pod nadzorom? Pregled stanja u 2017. godini", SHARE Fondacija, 26. decembar 2018, https://resursi.sharefoundation.info/sr/resource/zadrzavanje-podataka-o-komunikaciji-u-srbiji-koliko-smo-pod-nadzorom/

85 „Pristup bez transparentnosti – praksa zadržavanja podataka u 2018", SHARE Fondacija, 29. oktobar, 2019, https://www.sharefoundation.info/sr/pristup-bez-transparentnosti-praksa-zadrzavanja-podataka-u-2018/

86 Ninoslava Bogdanović, „Zadržani podaci o komunikacijama u 2020. godini: formalnost umesto kontrole", SHARE Fondacija, 27. avgust 2021, https://www.sharefoundation.info/sr/zadrzani-podaci-o-komunikacijama-u-2020-godini-formalnost-umesto-kontrole/

87 „BIA traži obaveznu registraciju svih pre-paid, post-paid i Internet korisnika", SHARE Fondacija, 27. decembar 2013, https://resursi.sharefoundation.info/sr/resource/bia-trazi-obaveznu-registraciju-svih-pre-paid-post-paid-i-internet-korisnika/

88 „Registracija korisnika pripejd kartica ponovo predložena", SHARE Fondacija, 6. decembar 2016, https://resursi.sharefoundation.info/sr/resource/registracija-korisnika-pripejd-kartica-ponovo-predlozena/

89 Pravilnik o tehničkim uslovima za registraciju pripejd korisnika, Ministarstvo informisanja i telekomunikacija Republike Srbije, 5. februar 2024, https://mit.gov.rs/vest/sr/3501/pravilnik-o-tehnickim-uslovima-za-registraciju-pripejd-korisnika.php

90 „The Crime Messenger: How Sky ECC Phones Became a Tool of the Criminal Trade", OCCRP, 22. oktobar 2024, https://www.occrp.org/en/project/the-crime-messenger; „Global Coalition Takes Down New Criminal Communication Platform", Europol, https://www.europol.europa.eu/media-press/newsroom/news/global-coalition-takes-down-new-criminal-communication-platform; Filip Milošević, „EncroChat: Kad policija hakuje", SHARE Fondacija,

30. jun 2023, https://www.sharefoundation.info/sr/encrochat-kad-policija-hakuje/

91 Zlatko Petrović, „Pazi snima se!", SHARE Fondacija, 27. novembar 2017, https://resursi.sharefoundation.info/sr/resource/pazi-snima-se/

92 „Da li su poznate lokacije novih kamera za nadzor i rizici po ustavna prava građana?", SHARE Fondacija, 22. mart 2019, https://www.sharefoundation.info/sr/da-li-su-poznate-lokacije-novih-kamera-za-nadzor-i-rizici-po-ustavna-prava-gradjana/

93 „Huawei zna sve o kamerama u Beogradu – i nije im teško da to i kažu!", SHARE Fondacija, 29. mart 2019, https://www.sharefoundation.info/sr/huawei-zna-sve-o-kamerama-u-beogradu-i-nije-im-tesko-da-to-i-kazu/

94 „Huawei Safe City Solution: Safeguards Serbia", Archive Today, 22. mart 2019, https://archive.li/pZ9HO#selection-10783.1-10789.57

95 „Share_TV – hiljade.kamera", SHARE Fondacija, https://www.youtube.com/watch?v=XlMldmOhYG8

96 Zakon o zaštiti podataka o ličnosti, Sl. glasnik RS, br. 87/2018, https://www.paragraf.rs/propisi/zakon_o_zastiti_podataka_o_licnosti.html

97 „MUP do daljeg da obustavi uvođenje sistema za pametan video nadzor", SHARE Fondacija, 18. novembar 2019, https://www.sharefoundation.info/sr/mup-do-daljeg-da-obustavi-uvodenje-sistema-za-pametan-video-nadzor/

98 „Kamere bez upotrebne dozvole / procena uticaja 2.0", SHARE Fondacija, 31. jul 2020, https://www.sharefoundation.info/sr/kamere-bez-upotrebne-dozvole-procena-uticaja-2-0/

99 „Povlačenje nacrta korak ka moratorijumu na biometrijski nadzor", SHARE Fondacija, 23. septembar 2021, https://www.sharefoundation.info/sr/povlacenje-nacrta-korak-ka-moratorijumu-na-biometrijski-nadzor/

100 „Vulin: Na molbu Vučića, povučen Nacrt zakona o unutrašnjim poslovima", N1, 23. septembar 2021, https://n1info.rs/vesti/vulin-na-molbu-vucica-povucen-nacrt-zakona-o-unutrasnjim-poslovima/

101 „Poverenik sproveo postupak nadzora u MUP, povodom sumnji na upotrebu tehnologije za prepoznavanje lica (Facial Recognition Technology)", Poverenik za informacije od javnog značaja i zaštitu podataka o ličnosti, 18. februar 2022, https://goto.now/CAV8C

102 „Biometrija ponovo u Nacrtu zakona o unutrašnjim poslovima", SHARE Fondacija, 8. decembar 2022, https://www.sharefoundation.info/sr/biometrija-ponovo-u-nacrtu-zakona-o-unutrasnjim-poslovima/

103 „Druga runda bitke protiv masovnog biometrijskog nadzora", SHARE Fondacija, 9. januar 2023, https://www.sharefoundation.info/sr/druga-runda-bitke-protiv-masovnog-biometrijskog-nadzora/

104 „Ko bi mogao da bude novi direktor policije: Tri imene u vrhu liste kandidata", 021, 2. novembar 2024, https://www.021.rs/story/Info/Srbija/392109/Ko-bi-mogao-da-bude-novi-direktor-policije-Tri-imena-u-vrhu-liste-kandidata.html

105 „Projekat Pegasus: Šta se dogodilo i kako se zaštititi", SHARE Fondacija, 22. jul 2021, https://www.sharefoundation.info/sr/projekat-pegasus-sta-se-dogodilo-i-kako-se-zastititi/

106 Stephanie Kirchgaessner, Paul Lewis, David Pegg, Sam Cutler, Nina Lakhani and Michael Safi, „Revealed: leak uncovers

global abuse of cyber-surveillance weapon", The Guardian, 18. jul 2021, https://www.theguardian.com/world/2021/jul/18/revealed-leak-uncovers-global-abuse-of-cyber-surveillance-weapon-nso-group-pegasus

107 Phineas Rueckert, „Pegasus: The new global weapon for silencing journalists", Forbidden Stories, 18. jul 2021, https://forbiddenstories.org/pegasus-the-new-global-weapon-for-silencing-journalists/

108 Sam Jones, „Use of Pegasus spyware on Spain's politicians causing 'crisis of democracy'", The Guardian, 15. maj 2022, https://www.theguardian.com/world/2022/may/15/use-of-pegasus-spyware-on-spains-politicians-causing-crisis-of-democracy

109 Nektaria Stamouli, „Greek prosecutor closes spyware scandal probe, infuriating opposition and victims", Politico, 30. jul 2024, https://www.politico.eu/article/greek-prosecutor-closes-spyware-scandal-probe-infuriating-opposition/

110 Wojciech Kość, „Poland launches Pegasus spyware probe", Politico, 19. februar 2024, https://www.politico.eu/article/poland-pegasus-spyware-probe-law-and-justice-pis-jaroslaw-kaczynski/

111 Hendrik Mildebrath, „Greece's Predatorgate The latest chapter in Europe's spyware scandal?", European Parliament Research Service (EPRS), https://www.europarl.europa.eu/RegData/etudes/ATAG/2022/733637/EPRS_ATA(2022)733637_EN.pdf

112 „BLASTPASS NSO Group iPhone Zero-Click, Zero-Day Exploit Captured in the Wild", Citizen Lab, 7. septembar 2023, https://citizenlab.ca/2023/09/blastpass-nso-group-iphone-zero-click-zero-day-exploit-captured-in-the-wild/

113 „Forensic Methodology Report: How to catch NSO Group's Pegasus", Amnesty International, 18. jul 2021, https://www.amnesty.org/en/latest/research/2021/07/forensic-methodology-report-how-to-catch-nso-groups-pegasus/

114 „Wikileaks: Softver za nadzor i u Srbiji", SHARE Fondacija, 11. septembar 2013, https://resursi.sharefoundation.info/sr/resource/wikileaks-softver-za-nadzor-i-u-srbiji/

115 „Uvoz i upotreba opreme za nadzor u Srbiji: Slučaj Trovicor", SHARE Fondacija, 28. novembar 2013, https://resursi.sharefoundation.info/sr/resource/uvoz-i-upotreba-opreme-za-nadzor-u-srbiji-slucaj-trovicor/

116 „Hacking Team : 'Italijanski posao' srpskih službi bezbednosti", SHARE Labs, 13. jul 2015, https://labs.rs/sr/501/

117 Bill Marczak, John Scott-Railton, Siddharth Prakash Rao1, Siena Anstis, and Ron Deibert, „Running in Circles – Uncovering the Clients of Cyberespionage Firm Circles", Citizen Lab, 1. decembar 2020, https://citizenlab.ca/2020/12/running-in-circles-uncovering-the-clients-of-cyberespionage-firm-circles/

118 Clement Lecigne i Christian Resell, „Protecting Android users from 0-Day attacks", Google Threat Analysis Group (TAG), 19. maj 2022, https://blog.google/threat-analysis-group/protecting-android-users-from-0-day-attacks/

119 Bill Marczak, John Scott-Railton, Bahr Abdul Razzak, Noura Aljizawi, Siena Anstis, Kristin Berdan, and Ron Deibert, „Pegasus vs. Predator: Dissident's Doubly-Infected iPhone Reveals Cytrox Mercenary Spyware", Citizen Lab, 16. decembar 2021, https://citizenlab.ca/2021/12/pegasus-vs-predator-dissidents-doubly-infected-iphone-reveals-cytrox-mercenary-spyware/

120 „About Apple threat notifications and protecting against mercenary spyware", Apple Support, 24. oktobar 2024, https://support.apple.com/en-us/102174

121 „Otkriveni pokušaji špijunskih napada na mobilne uređaje pripadnika civilnog društva", SHARE Fondacija, 20. novembar 2023, https://www.sharefoundation.info/sr/otkriveni-pokusaji-spijunskih-napada-na-mobilne-uredaje-pripadnika-civilnog-drustva/

122 „Serbia: Civil society threatened by spyware", Amnesty International, 28. novembar 2023, https://securitylab.amnesty.org/latest/2023/11/serbia-civil-society-threatened-by-spyware/

123 „Spyware in Serbia: civil society under attack", Access Now, 28. novembar 2023, https://www.accessnow.org/spyware-attack-in-serbia/

124 John Scott-Railton, Bill Marczak, Bahr Abdul Razzak, Siena Anstis, and Ron Deibert, „Spyware Targeting Against Serbian Civil Society", Citizen Lab, 23. novembar 2023, https://citizenlab.ca/2023/11/serbia-civil-society-spyware/

125 Bill Marczak, John Scott-Railton, Bahr Abdul Razzak, and Ron Deibert, „Triple Threat

NSO Group's Pegasus Spyware Returns in 2022 with a Trio of iOS 15 and iOS 16 Zero-Click Exploit Chains", *Citizen Lab*, 18. april 2023, https://citizenlab.ca/2023/04/nso-groups-pegasus-spyware-returns-in-2022/

126 Stephanie Kirchgaessner, „Critics of Serbia's government targeted with 'military-grade spyware'", The Guardian, 28. novembar 2023, https://www.theguardian.com/technology/2023/nov/28/critics-of-serbias-government-targeted-with-military-grade-spyware

127 „'A Digital Prison': Surveillance and the suppression of civil society in Serbia", Amnesty International, 16. decembar 2024, https://www.amnesty.org/en/documents/eur70/8813/2024/en/

128 „Forensic Methodology Report: How to catch NSO Group's Pegasus", Amnesty International, 18. jul 2021 https://www.amnesty.org/en/latest/research/2021/07/forensic-methodology-report-how-to-catch-nso-groups-pegasus/

129 Mobile Verification Toolkit, Amnesty International, jul 2021, https://docs.mvt.re/en/latest/

130 About Lockdown Mode, Apple Support, 16. septembar 2024, https://support.apple.com/en-us/105120

131 Krivični zakonik, Sl. glasnik RS, br. 94/2024, https://www.paragraf.rs/propisi/krivicni-zakonik-2019.html

132 Zakon o zaštiti podataka o ličnosti, Sl. glasnik RS, br. 87/2018, https://www.paragraf.rs/propisi/zakon_o_zastiti_podataka_o_licnosti.html

133 Zakonik o krivičnom postupku, Sl. glasnik RS, br. 62/2021, https://www.paragraf.rs/propisi/zakonik_o_krivicnom_postupku.html

134 Zakon o kritičnoj infrastrukturi, Sl. glasnik RS, br. 87/2018, https://www.paragraf.rs/propisi/zakon-o-kriticnoj-infrastrukturi.html

135 Prevedeno i adaptirano iz: Soledad Antelada Toledano, „Critical Infrastructure Security: Cybersecurity lessons learned from real-world breaches", Packt Publishing Ltd., jun 2024, ISBN: 978-1-83763-356-2, pp. 39-42.

136 Zakon o informacionoj bezbednosti, Sl. glasnik RS, br. 6/2016, 94/2017 i 77/2019 https://www.paragraf.rs/propisi/zakon_o_informacionoj_bezbednosti.html

137 „Bezbednost. Korisničko iskustvo. Digitalizacija. Tim redosledom", SHARE Fondacija, 26. septembar 2018, https://www.sharefoundation.info/sr/bezbednost-korisnicko-iskustvo-digitalizacija-tim-redosledom/

138 „Neovlašćeno objavljeni podaci o ličnosti više od 5 miliona građana Srbije", SHARE Fondacija, 15. decembar 2014, https://resursi.sharefoundation.info/sr/resource/neovlasceno-objavljeni-podaci-o-licnosti-vise-od-5-miliona-gradana-srbije/

139 „Agencija za privatizaciju – jedinstven slučaj", SHARE Fondacija, 24. mart 2016, https://resursi.sharefoundation.info/sr/resource/agencija-za-privatizaciju-jedinstven-slucaj/

140 Maja Nikolić, „Zastareo postupak za curenje podataka iz Agencije", N1, 12. januar 2017, https://n1info.rs/vesti/a220880-curenje-podataka-iz-agencije-za-privatizaciju-zastarelo/

141 Porezna uprava RH, „Što je OIB i zašto je uveden?", https://www.porezna-uprava.hr/HR_OIB/Stranice/sto_je_OIB.aspx

142 Zakon o zaštiti podataka o ličnosti, Sl. glasnik RS, br. 87/2018 https://www.paragraf.rs/propisi/zakon_o_zastiti_podataka_o_licnosti.html

143 Sajber kultura u Srbiji, Nacionalni CERT Republike Srbije, decembar 2020. godine, https://www.cert.rs/files/shares/Sajber%20Kultura%20Ratel%20web%20V0.5.6.pdf

144 Bojan Perkov, „Dan posle pandemije: idemo li ka distopiji nadzora", SHARE Fondacija, 2. april 2020, https://www.sharefoundation.info/sr/dan-posle-pandemije-idemo-li-ka-distopiji-nadzora/

145 „Tokovi podataka u Informacionom sistemu Covid-19", SHARE Fondacija, 30. april 2020, https://www.sharefoundation.info/sr/tokovi-podataka-covid-19/

146 „Pandemija jedne lozinke. Kako je šifra za Covid-19 završila na internetu?", SHARE Fondacija, 20. april 2020, https://www.sharefoundation.info/sr/pandemija-jedne-lozinke/

147 „Opomena Batutu zbog bezbednosnog incidenta sa ličnim podacima građana", SHARE Fondacija, 31. jul 2020, https://www.sharefoundation.info/sr/opomena-batutu-zbog-bezbednosnog-incidenta-sa-licnim-podacima-gradana/

148 Kimberly Wood, „Cybersecurity Policy Responses to the Colonial Pipeline Ransomware Attack", The Georgetown Environmental Law Review, 7. mart 2023, https://www.law.georgetown.edu/environmental-law-review/blog/cybersecurity-policy-responses-to-the-colonial-pipeline-ransomware-attack/

149 Ninoslava Bogdanović, „Kako je Novi Sad otet i zaključan", SHARE Fondacija, 11. jun 2021, https://www.sharefoundation.info/sr/kako-je-novi-sad-otet-i-zakljucan/

150 „IT infrastruktura RGZ-a meta intenzivnog hakerskog napada", Republički geodetski zavod, 15. jun 2022, https://www.rgz.gov.rs/vesti/5028/vest/it-infrastruktura-rgz-a-meta-intenzivnog-hakerskog-napada

151 „Podaci o nepokretnostima su pouzdani i neoštećeni", Republički geodetski zavod, 24. jun 2022, https://www.rgz.gov.rs/vesti/5131/vest/podaci-o-nepokretnostima-su-pouzdani-i-neo%c5%a1te%c4%87eni

152 Bill Cozens, „A deep dive into Phobos ransomware", ThreatDown, 24. jul 2019, https://www.threatdown.com/blog/a-deep-dive-into-phobos-ransomware/

153 „Polovina službi za katastar nastavila sa radom", Republički geodetski zavod, 4. jul 2022, https://www.rgz.gov.rs/vesti/5148/vest/polovina-slu%c5%bebi-za-katastar-nastavila-sa-radom

154 „Od ponedeljka katastar radi u punom kapacitetu", Republički geodetski zavod, 9. jul 2022, https://www.rgz.gov.rs/vesti/5168/vest/od-ponedeljka-katastar-radi-u-punom-kapacitetu

155 „Poverenik okončao vanredni inspekcijski nadzor nad Republičkim geodetskim zavodom“, Poverenik za Informaci e od avnog Znača a i Zaštitu Podataka o Ličnosti, 18. jul 2022, https://shorturl.at/uSOHG

156 Zapisnik o nadzoru RGZ, https://www.sharefoundation.info/wp-content/uploads/Nadzor-RGZ-Zapisnik.pdf

157 Natalija Jovanović, „Još se ne zna da li su u hakerskom napadu na RGZ ugroženi lični podaci građana“, BIRN, 23. jun 2022, https://birn.rs/jos-se-ne-zna-da-li-su-u-hakerskom-napadu-na-rgz-ugrozeni-licni-podaci-gradana/

158 „Sistem i podaci bezbedni“, Elektroprivreda Srbije, 19. decembar 2023, https://www.eps.rs/lat/vesti/Stranice/eps-hakerski-napad.aspx

159 „Đedović Handanović:Hakerski napad na EPS nije ugrozio proizvodnju ni podatke“, Politika, 5. februar 2024, https://www.politika.rs/scc/clanak/597593/dedovic-handanovic-hakerski-napad-na-eps-nije-ugrozio-proizvodnju-ni-podatke

160 „Od jutros ponovo moguće platiti račune za struju na šalterima EPS-a“, Danas, 19. februar 2024, https://www.danas.rs/vesti/ekonomija/od-jutros-ponovo-moguce-platiti-racune-za-struju-na-salterima-eps-a/

161 Natalija Jovanović, „Elektroprivreda Srbija pod ucenom hakera“, Radio Slobodna Evropa, 28. decembar 2023, https://www.slobodnaevropa.org/a/srbija-elektroprivreda-hakeri-ucena/32751103.html

162 Natalija Jovanović, „Ucenjivači objavili navodna dokumenta Elektroprivrede Srbije na dark vebu“, Radio Slobodna Evropa, 19. januar 2024, https://www.slobodnaevropa.org/a/elektroprivreda-srbije-dark-web-ucenjivanje-dokumenta/32783800.html

163 Bojan Perkov, „Internet v. Deep web v. Dark web“, SHARE Fondacija, 9. jun 2023, https://www.sharefoundation.info/sr/internet-v-deep-web-v-dark-web/

164 „Elektroprivreda Srbije u prijavi Povereniku tvrdi da su sačuvani lični podaci“, Radio Slobodna Evropa, 22. januar 2024, https://www.slobodnaevropa.org/a/srbija-eps-podaci-poverenik/32787022.html

165 „Poverenik o hakerskom napadu na EPS: Nema informacija da su ugroženi podaci o ličnosti građana“, Insajder, 29. januar 2024, https://insajder.net/prenosimo/poverenik-o-hakerskom-napadu-na-eps-nema-informacija-da-su-ugrozeni-podaci-o-licnosti-gradana

166 Christopher Bing, „Exclusive: U.S. to give ransomware hacks similar priority as terrorism“, Reuters, 4. jun 2021, https://www.reuters.com/technology/exclusive-us-give-ransomware-hacks-similar-priority-terrorism-official-says-2021-06-03/

167 Anđela Milivojević, „Rodno zasnovano digitalno nasilje u Srbiji: Pregled trendova“, SHARE Fondacija, septembar 2024, https://www.sharefoundation.info/wp-content/uploads/Rodno-zasnovano-digitalno-nasilje-u-Srbiji.pdf

168 „2023 State Of Deepfakes: Realities, Threats, and Impact“, Security Hero, 2023, https://www.securityhero.io/state-of-deepfakes/

169 „Online zlostavljanje i proganjanje devojaka iz Batajnice još uvek bez adekvatne reakcije nadležnih organa“, Zoomer, 29. avgust 2023, https://zoomer.rs/online-zlostavljanje-i-proganjanje-devojaka-iz-batajnice-jos-uvek-bez-adekvatne-reakcije-nadleznih-organa/

170 „Online and ICT-facilitated violence against women and girls during COVID-19“, UN Women, 2020, https://www.unwomen.org/sites/default/files/Headquarters/Attachments/Sections/

Library/Publications/2020/Brief-Online-and-ICT-facilitated-violence-against-women-and-girls-during-COVID-19-en.pdf

171 „O koroni i grudima", Vreme, 12. novembar 2024, https://vreme.com/projekat/o-koroni-i-grudima/

172 Ana Novaković, „Nedozvoljen pornografski sadržaj deli se na Telegramu, javnost uznemirena", N1, 9. mart 2021, https://n1info.rs/vesti/nedozvoljen-pornografski-sadrzaj-deli-se-na-telegramu-javnost-uznemirena/

173 Hristina Cvetinčanin Knežević, „'Nečija ćerka': Strašan nekažnjen danak osvetničke pornografije na Balkanu", Balkan Insight, 18. oktobar 2021, https://balkaninsight.com/sr/2021/10/18/necija-cerka-strasan-nekaznjen-danak-osvetnicke-pornografije-na-balkanu/

174 Anđela Milivojević, „'Bila sam nemoćna': Ispovesti žena i devojaka širom Srbije o užasnim posledicama osvetničke pornografije", Balkan Insight, 14. mart 2023, https://balkaninsight.com/sr/2023/03/14/bila-sam-nemocna-ispovesti-zena-i-devojaka-sirom-srbije-o-uzasnim-posledicama-osvetnicke-pornografije/

175 Ana Zdravković, Nikolina Tomašević i Staša Ivković, „Telegram iza senke: incest, dečija i osvetnička pornografija", Osnažene, 2024, https://osnazzene.org.rs/blog/telegram-iza-senke-incest-decija-i-osvetnicka-pornografija/

176 Anđela Milivojević, „Rodno zasnovano digitalno nasilje u Srbiji: Pregled trendova", SHARE Fondacija, septembar 2024, https://www.sharefoundation.info/wp-content/uploads/Rodno-zasnovano-digitalno-nasilje-u-Srbiji.pdf, str.8

177 „Javna rasprava o izmenama Krivičnog zakonika: Zloupotreba intimnih sadržaja ne sme ostati nekažnjiva", SHARE Fondacija, 30. oktobar 2024, https://www.sharefoundation.info/sr/javna-rasprava-o-izmenama-krivicnog-zakonika-zloupotreba-intimnih-sadrzaja-ne-sme-ostati-nekaznjiva/

178 Saopštenje povodom navoda u medijima u vezi sa javnom raspravom o nacrtima zakona o izmenama i dopunama Krivičnog zakonika i Zakonika o krivičnom postupku, Ministarstvo pravde Republike Srbije, 1. novembar 2024, https://www.mpravde.gov.rs/vest/44678/saopstenje-povodom-navoda-u-medijima-u-vezi-sa-javnom-raspravom-o-nacrtima-zakona-o-izmenama-i-dopunama-krivicnog-zakonika-i-zakonika-o-krivicnom-postupku.php

179 William Spindler, „2015: The year of Europe's refugee crisis", UNHCR, 8. decembar 2015, https://www.unhcr.org/news/stories/2015-year-europes-refugee-crisis

180 Petra Molnar, „Technological Testing Grounds: Migration Management Experiments and Reflections from the Ground Up", EDRi and the Refugee Law Lab, novembar 2020, https://edri.org/wp-content/uploads/2020/11/Technological-Testing-Grounds.pdf

181 Joshua Askew, „'Mass surveillance, automated suspicion, extreme power': How tech is shaping EU borders", Euronews, 6. april 2023, https://www.euronews.com/next/2023/04/06/mass-surveillance-automated-suspicion-extreme-power-how-tech-is-shaping-the-eus-borders

182 „Illegal Pushbacks and Border Violence Report", Border Violence Monitoring Network, mart 2021, https://borderviolence.eu/app/uploads/BVMN-Monthly-Report-March-21.pdf

183 „Surveillance Technologies at European Borders: Serbia", Border Violence Monitoring Network, 8. novembar 2024, https://borderviolence.eu/app/uploads/Surveillance-tech-in-Serbia.pdf

184 Kristina Korte, 2023, „'So, if you ask whether fences work: they work'—the role of border fortifications for migration control

and access to asylum", Comparative Migration Studies 11(1), pp. 1-18, https://doi.org/10.18452/28381

185 Mila Bajić, „Balkanskom rutom do Beograda: Teorije zavere o naseljavanju migranata u Srbiji za vreme koronavirusa", rad predstavljen na Saboru politikologa „Političke posledice pandemije" (2020), 2020, str. 19, http://www.upns.rs/sites/default/files/2021-05/The%202020%20SPSA%20Abstracts_0.pdf

186 Kari Paul, „'It let white supremacists organize': the toxic legacy of Facebook's Groups", The Guardian, 4. februar 2021, https://www.theguardian.com/technology/2021/feb/04/facebook-groups-misinformation

187 „Podnete prekršajne prijave protiv Fejsbuka i Gugla", SHARE Fondacija, 4. decembar 2019, https://www.sharefoundation.info/sr/podnete-prekrsajne-prijave-protiv-fejsbuka-i-gugla/

188 „Član Levijatana automobilom upao u migrantski prihvatni centar u Obrenovcu", Mašina, 7. maj 2020, https://www.masina.rs/clan-levijatana-automobilom-upao-u-migrantski-prihvatni-centar-u-obrenovcu/

189 Dunja Savanović, „Profil na Instagramu širi rasizam u Srbiji: Fotografišu ljude afričkog porekla, pa objave vreme i lokaciju", N1, 31. januar 2024, https://n1info.rs/vesti/profil-na-instagramu-siri-rasizam-u-srbiji-fotografisu-ljude-africkog-porekla-pa-objave-vreme-i-lokaciju/

190 Laura Bates, „Facebook's 'Spotted' pages: everyday sexism in universities for all to see", The Guardian, 31. januar 2014, https://www.theguardian.com/lifeandstyle/womens-blog/2014/jan/31/facebooks-spotted-pages-everyday-sexism-universities

191 Sanja Ilić, „RT Balkan istražuje TikTok nasilje: Da li je moguće ukidanje društvenih mreža u Srbiji?", RT, 10. maj 2023, https://lat.rt.rs/srbija-i-balkan/30503-drustvene-mreze-i-nasilje/

192 „Analiza uvođenja filtriranja Interneta u Srbiji", SHARE Fondacija, 18. decembar 2014, https://resursi.sharefoundation.info/sr/resource/analiza-uvodenja-filtriranja-interneta-u-srbiji/

193 https://monitoring.labs.rs/data?caseId=766

194 Aleksandra Trajković Arsić, „Filter na Tiktoku veliča masovno ubistvo u 'Ribnikaru', ko treba da reaguje", RTS, 9. jul 2023, https://www.rts.rs/lat/vesti/drustvo/5205271/tik-tok-izazov-filter-pucnjava-zrtve-.html

195 Hristina Cvetinčanin Knežević, „Deca i mladi na internetu: Šta znamo o rizicima onlajn odrastanja", SHARE Fondacija, avgust 2023, https://www.sharefoundation.info/wp-content/uploads/Deca-i-mladi-na-internetu.pdf

196 „Dečaci od slika devojčica i nastavnica sa društvenih mreža pravili eksplicitni sadržaj", N1, 9. februar 2024, https://n1info.rs/vesti/na-novom-beogradu-decaci-od-slika-devojcica-i-nastavnica-sa-drustvenih-mreza-pravili-eksplicitni-sadrzaj/

197 „Novi napadi na Prajd info centar u Beogradu", Radio Slobodna Evropa, 27. februar 2024, https://www.slobodnaevropa.org/a/napadi-prajd-info-centar-beograd/32837734.html

198 @ginalash__, 7. januar 2024, https://x.com/ginalash__/status/1744054303017369694?t=CMm_LC4QkDMGe4kdSVyVlw

199 @dasezna, 10. mart 2024, https://x.com/dasezna/status/1766816518501810346

200 „Reditelj dobija PRETNJE zbog svađe sa Viktorom Savićem oko Parade ponosa: Ono što je glumac uradio nakon RASPRAVE

iznenadilo mnoge", Blic, 29. avgust 2022, https://www.blic.rs/zabava/stevan-filipovic-dobija-pretnje/xjdjng1

201 „UNS: Osuđujemo izveštavanje 'Srpskog telegrafa' o Noi Milivojev i objavljivanje uznemirujućih fotografija", Cenzolovka, 10. jul 2023, https://www.cenzolovka.rs/etika/uns-osudjujemo-izvestavanje-srpskog-telegrafa-o-noi-milivojev-i-objavljivanje-uznemirujucih-fotografija/

202 @dasezna, 6. jul 2023, https://x.com/dasezna/status/1676979327173271552?t=6fy-eoIWOgGolV_rQ_k6tA&s=35

203 Tamara Evdokimova, „The global rise of anti-trans legislation", Coda, 10. jul 2023, https://www.codastory.com/waronscience/lgbtq-trans-rights-2023/

204 „Raskrinkavanje SNS u Kraljevu", Ozonpress, 26. novembar 2024, https://www.ozonpress.net/politika/raskrinkavanje-sns-u-kraljevu/

205 „Deljenje novca iz budžeta – pomoć ili kupovina glasova", Insajder, 30. novembar 2023, https://insajder.net/teme/deljenje-novca-iz-budzeta-pomoc-ili-kupovina-glasova-video

206 „Budžetski bankomat ponovo radi: Koliko novca je vlast za četiri godine podelila starima, mladima i ostalima?", Danas, 3. novembar 2023, https://www.danas.rs/vesti/ekonomija/koliko-je-novca-drzava-podelila-gradjanima-srbije-za-cetiri-godine/

207 „Počinje primena Zakona o socijalnoj karti", Pravni portal, 22. februar 2022, https://www.pravniportal.com/pocinje-primena-zakona-o-socijalnoj-karti/

208 (Anti) socijalne karte, Inicijativa A11, https://antisocijalnekarte.org/

209 Ibid.

210 Elettra Bietti, „How the Free Software and the IP Wars of the 1990s and 2000s Presaged Today's Toxic, Concentrated Internet", Promarket, 28. januar 2022, https://www.promarket.org/2022/01/28/digital-platforms-regulation-free-software-ip-wars-concentration-internet/

211 Richard Salis, „A Look at how U.S Based Yahoo! was Condemned by French Law", Juriscom.net, 10. novembar 2000, http://lthoumyre.chez.com/txt/jurisfr/cti/yauctions.htm

212 Mila Bajić, „Beograd je Net – Razgovor sa Slobodanom Markovićem", SHARE Fondacija, 23. oktobar 2020, https://www.sharefoundation.info/sr/beograd-je-net/

213 Arhivirani sajt ETF-a o protestima 96. godine https://web.archive.org/web/20070611085519/http://galeb.etf.bg.ac.yu/~protest96/

214 Upotreba IKT-a, pojedinci, 2024, Republički zavod za statistiku, 25. oktobar 2024, https://www.stat.gov.rs/sr-latn/vesti/20241025-upotreba-ikt-a-pojedinci-2024/?s=2702

215 SHARE Fondacija, „Uvedeno filtriranje interneta u Srbiji", 30. oktobar 2020, https://www.sharefoundation.info/sr/uvedeno-filtriranje-interneta-u-srbiji/

216 Carole Cadwalladr and Emma Graham-Harrison, „Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach", The Guardian, 17. mart 2018, https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election

217 Mark Scott, „Cambridge Analytica helped 'cheat' Brexit vote and US election, claims whistleblower", Politico, 27. mart 2018, https://www.politico.eu/article/cambridge-analytica-chris-wylie-brexit-trump-britain-data-protection-privacy-facebook/

218 Carole Cadwalladr and Stephanie Kirchgaessner, „Revealed: the US adviser who tried to swing Nigeria's 2015 election", The Guardian, 18. februar 2023, https://www.theguardian.com/world/2023/feb/18/cambridge-analytica-staff-leaked-emails-team-jorge-nigeria-election-sam-patten-tal-hanan

219 Zach Schonfeld, „Supreme Court drops Facebook's appeal of investor suit in Cambridge Analytica scandal", The Hill, 22. novembar 2024, https://thehill.com/regulation/court-battles/5004496-supreme-court-facebook-cambridge-analytica/

220 „EU introduces new rules on transparency and targeting of political advertising", Council of the European Union, 11. mart 2024, https://www.consilium.europa.eu/en/press/press-releases/2024/03/11/eu-introduces-new-rules-on-transparency-and-targeting-of-political-advertising/

221 Jess Weatherbed, „Google says it will stop serving political ads in the EU", The Verge, 14. novembar 2024, https://www.theverge.com/2024/11/14/24296510/google-dropping-political-ads-in-the-eu-ttpa

222 Annette Kroeber-Riel, „Five considerations for the EU's new political ads rules", Google, 23. februar 2023, https://blog.google/around-the-globe/google-europe/five-considerations-for-the-eus-new-political-ads-rules/

223 Hortense Goulard, „Facebook accused of censorship of 'Napalm girl' picture", Politico, 9. septembar 2016, https://www.politico.eu/article/norwegian-prime-minister-facebook-wrong-to-censor-vietnam-war-picture/

224 „Tviter nalog Danasa nakon sedam dana ponovo aktivan", Danas, 23. septembar 2019, https://www.danas.rs/zivot/tehnologije/tviter-nalog-danasa-nakon-sedam-dana-ponovo-aktivan/

225 „Myanmar: Facebook's systems promoted violence against Rohingya; Meta owes reparations", Amnesty International, 29. septembar 2022, https://www.amnesty.org/en/latest/news/2022/09/myanmar-facebooks-systems-promoted-violence-against-rohingya-meta-owes-reparations-new-report/

226 Dell Cameron, Shoshana Wodinsky, Mack DeGeurin and Thomas Germain, „Read the Facebook Papers for Yourself", Gizmodo, 18. april 2022, https://gizmodo.com/facebook-papers-how-to-read-1848702919

227 „LEAK: France & Germany demand more censorship from internet companies", EDRi, 7. jun 2018, https://edri.org/our-work/leak-france-germany-demand-more-censorship-from-internet-companies/

228 „Preventing 'Torrents of Hate' or Stifling Free Expression Online?", The Future of Free Speech, maj 2024, https://futurefreespeech.org/wp-content/uploads/2024/05/Preventing-Torrents-of-Hate-or-Stifling-Free-Expression-Online-The-Future-of-Free-Speech.pdf

229 Jelena Adamović, Mila Bajić, Snežana Bajčeta, Bojan Perkov i Tijana Stevanović, „DSA, DMA, AIA and Western Balkans", SHARE Fondacija, 2024, https://www.sharefoundation.info/wp-content/uploads/SHARE_DSA-DMA-AIA-STUDY.pdf

230 „DSA Enforcement Tracker", The Future of Free Speech, 30. novembar 2023, https://futurefreespeech.org/tracker-of-dsa-enforcement/

231 „SHARE: Prijave protiv 16 globalnih tehno kompanija", SHARE Fondacija, 2. oktobar 2020, https://www.sharefoundation.info/sr/share-prijave-protiv-16-globalnih-tehno-kompanija/

232 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

233 „Meta promenila Politiku privatnosti: Naši podaci kao materijal za trening AI", SHARE Fondacija, 12. jul, 2024, https://www.sharefoundation.info/sr/meta-promenila-politiku-privatnosti-nasi-podaci-kao-materijal-za-trening-ai/

234 Alex Hern, „Facebook: no current plans to make 'catastrophic' news feed change worldwide", The Guardian, 24., oktobar 2017, https://www.theguardian.com/technology/2017/oct/24/facebook-no-plans-news-feed-change-worldwide

235 Mila Manojlović, „Mediji u Srbiji oznaku 'saradnici Vlade' vide kao Tviter 'žigosanje'", Radio Slobodna Evropa, 17. avgust 2021, https://www.slobodnaevropa.org/a/31414785.html

236 „Demostatov monitoring: RTS – cenzura kritičkog mišljenja", N1, 1. mart 2024, https://n1info.rs/vesti/demostat-monitoring-rts/

237 Mila Bajić i Milica Jovanović, „Kad podaci procure: za i protiv neovlašćenog otkrivanja", SHARE Fondacija, 22. april 2021, https://www.sharefoundation.info/sr/kad-podaci-procure/

238 „Pandemija jedne lozinke. Kako je šifra za Covid-19 završila na internetu?", SHARE Fondacija, 20. april 2020, https://www.sharefoundation.info/sr/pandemija-jedne-lozinke/

239 Mila Bajić, „Zašto je svake godine sve teže pratiti izbornu kampanju na mrežama?", SHARE Fondacija, 13. novembar 2023, https://www.sharefoundation.info/sr/zasto-je-svake-godine-sve-teze-pratiti-izbornu-kampanju-na-mrezama/

240 Andrew Hutchinson, „Twitter's New API Access Charges Could Price Many Apps and Researchers Out of Their Projects", Social Media Today, 12. mart 2023, https://www.socialmediatoday.com/news/twitters-new-api-access-charges-could-price-many-apps-and-researchers-out/644775/#:~:text=%E2%80%9CThe%20cheapest%2C%20Small%20Package%2C,%24125%2C000%20and%20%24210%2C000%20a%20month.

241 Rebecca Bellan, „Meta axed CrowdTangle, a tool for tracking disinformation. Critics claim its replacement has just '1% of the features'", TechCrunch, 15. avgust 2024, https://techcrunch.com/2024/08/15/meta-shut-down-crowdtangle-a-tool-for-tracking-disinformation-heres-how-its-replacement-compares/