B FILM MONTENEGRO

Centar za građansko obrazovanje
Centre for Civic Education

SHARE FOUNDATION

IPFP

NOVINARSKI PRIRUČNIK ZA DIGITALNO DOBA:

tehnička i pravna zaštita

Ovaj projekat finansira Evropska unija

VLADA CRNE GORE
MINISTARSTVO JAVNE UPRAVE

NOVINARSKI PRIRUČNIK ZA DIGITALNO DOBA:
tehnička i pravna zaštita

Izdavač:
Centar za građansko obrazovanje (CGO)

Urednici:
Andrej Petrovski
Đorđe Krivokapić

Autori/ke:
Jelena Adamović
Anka Kovačević
Nevena Krivokapić Martinović
Filip Milošević
Bojan Perkov
Kristina Ćendić

Obrada teksta:
Milica Jovanović

Dizajn i produkcija:
Centar za građansko obrazovanje (CGO)

Tiraž:
170 primjeraka

ISBN 978-9940-44-021-3
COBISS.CG-ID 14114820

Vodič je dio projekta "Podrška lokalnim medijima – priče iz prve ruke! Podrška istraživačkom novinarstvu i medijskoj pismenosti na lokalnom nivou u Crnoj Gori " koji sprovode B-film Montenegro, Centar za građansko obrazovanje (CGO), SHARE fondacija i Institut za poslovnu i finansijsku pismenost. Projekat finansira EU posredstvom Delegacije Evropske unije u Crnoj Gori, a kofinansira ga Ministarstvo javne uprave Vlade Crne Gore.

NOVINARSKI PRIRUČNIK ZA DIGITALNO DOBA:

tehnička i pravna zaštita

Jul 2020.

SADRŽAJ

Uvod

Decentralizacija razmjene vijesti među građanima, od kojih je gotovo svaki tehnički dovoljno opremljen da može u trenutku da snimi, obradi i pošalje informacije na drugi kraj svijeta, postavila je novinarima težak izazov. Ima li danas ova profesija uopšte više smisla, kad je svako postao sam svoj medij? Mogu li se mediji izboriti za pažnju publike na tržištu prezasićenom informativnim i zabavnim sadržajima, svjesni da im nedostaje i resursa i znanja za snalaženje u digitalnom okruženju?

U vrijeme kada su mnoge javne i privatne aktivnosti prešle iz fizičkog u onlajn prostor, prikupljanje i provjera činjenica nalaže dobro poznavanje tehnologije. Potrebno je razumjeti novu logiku stvaranja i obrade podataka, nove parametre istraživanja koji važe na internetu, kao i različite bezbjednosne rizike koji u tim uslovima nastaju. Informatička prostranstva omeđena su, takođe, novim zakonskim normama koje bitno utiču na ulogu novinara u ostvarivanju javnog interesa.

Priručnik koji je pred vama pruža odgovore na neke od ključnih tehničkih i pravnih pitanja savremenog novinarstva, bilo da se ono realizuje u okviru medijske organizacije ili samostalno.

Šta je internet?

Internet infrastruktura Crne Gore

Otkad je 2016. godine u Crnoj Gori započela realizacija nacionalne Strategije razvoja informacionog društva, ostvaren je napredak u razvoju infrastrukture i mreža za brzi pristup internetu. Prema

podacima Ministarstva ekonomije, 80 odsto crnogorskih domaćinstava ima aktivan širokopojasni priključak na internet. U izvještaju Agencije za elektronske komunikacije i poštansku djelatnost (EKIP) o stanju tržišta elektronskih komunikacija za april 2020. godine za internet, ukupan broj širokopojasnih priključaka, nezavisno od tehnologije koja se upotrebljava za pristup iznosi 181.483 (1.021 priključaka više nego u martu). U odnosu na mart, broj širokopojasnih priključaka je veći za 0,57%, a u odnosu na isti period prošle godine, broj širokopojasnih priključaka je veći za 12,72%.

Domen *.me*

Nacionalni internet domen Crne Gore jeste .ME domen. Ovaj domen je nacionalni internet domen najvišeg nivoa (ccTLD) koji je globalno dostupan za registraciju, što znači da ga bilo ko može registrovati - dostupan je široj javnosti. Domen .ME može se registrovati od jula 2008. godine i registranti su kako iz Crne Gore, tako i iz SAD, Kine, Kanade, Velike Britanije, Francuske i Njemačke. Ipak, postoje domeni trećeg nivoa otvoreni samo za građane Crne Gore, kao što su gov.me, edu.me, co.me, net.me, org.me, priv.me i its.me. Godine 2016. dostignuto je milion domena, najviše zbog rasta tržišta za domen imena u Kini. Taj broj je 2017. godine pao na 900.000 domena, jer neki nisu obnovljeni, pa je rast usporen. Od te godine, bilježi se stalni rast od 6% godišnje.

Internet paket

Internet je globalna mreža uređaja, a svaki uređaj, bilo da je server, ruter, tablet, računar ili mobilni, koji je povezan na internet ima IP adresu. Sve informacije koje se prenose putem interneta, između rutera, servera i drugih hostova dijele se na manje komade

podataka, poznate kao internet paketi. Svaki paket se sastoji od zaglavlja i sadržaja. Zaglavlja (eng. headers) predstavljaju jedan tip metapodataka. Ruter internet provajdera utvrđuje adresu odredišta svakog paketa i određuje gdje da ga pošalje. Internet paket treba da stigne do određene lokacije za jednu sekundu i za to vrijeme prelazi ogromna prostranstva. Internet paket počinje da "putuje" od kućnog rutera, preko glavnog gradskog rutera, pa do glavnog data centra internet provajdera u zemlji. Dalje, paket prelazi iz određene države do najvećih "internet raskrsnica" (Internet Exchange Point – IXP) na kontinentu – u slučaju Evrope to je Frankfurt. Ako je željeni internet sadržaj hostovan u Sjevernoj Americi, paket će podvodnim kablovima preći okean, da bi stigao do data centra u kojem će biti skladišten.

Za samo jednu sekundu, internet paket prelazi hiljade kilometara i brojne državne granice, prebacuje se sa jednog internet provajdera na drugi, koji rade pod različitim pravnim regulativama i komercijalnim interesima, skače sa jedne internet raskrsnice na drugu i ostavlja trag svog postojanja na svakoj tački puta.

Kada internet paket dođe do konačne destinacije, on će biti skladišten i čekati da bude predmet analize algoritama. Ali, paket neće biti skladišten samo na tom mjestu. Tokom svog putovanja, on je na više mjesta bio kloniran i skladišten, u nekim drugim data centrima, serverima za zadržavanje podataka internet provajdera, u različitim zemljama i kod različitih državnih agencija ili privatnih kompanija.

Na kraju, paket će biti korišćen na više načina, kao djelić velike slagalice analize ponašanja, preferencija i interesovanja korisnika, ili mali dio koji će nekoga obilježiti kao potencijalnog teroristu ili razlikovati se od njega.

Tokovi podataka na internetu

Analiza putanje podataka na internetu je važna da bi se stvorila slika o protoku informacija kroz globalnu mrežu, kao i da bi se mapirale ključne lokacije i igrači. Saobraćaj podataka iz jedne države odlazi na nekoliko tačaka i zapravo se sve više centralizuje. Tačke centralizacije su tačke moći i što se više rutera ili provajdera sreće u jednoj tački, to je veći značaj te tačke, rutera ili servera.

Bitno je znati ko kontroliše te entitete, jer oni imaju kontrolu nad internetom u zemlji i mogu zloupotrebiti tu moć. Što se tiče odlaska podataka iz zemlje, slično centralizaciji lokalnog toka podataka kroz jedan ruter, podaci prolaze kroz nekoliko glavnih tačaka prije napuštanja zemlje.

Internet nije tako decentralizovan kakvim se na prvi mah čini, prije svega jer ga čine glavne lokacije za tranzit i hostovanje podataka, tzv. "prijestonice" protoka podataka koje su smještene u svega 13 zemalja. Ova struktura se danas veoma razlikuje od prvobitno zamišljene decentralizovane mreže, ideje sa začetka interneta. Internet provajderi se mogu posmatrati i kao kontrolori. Svaka potencijalna cenzura, filtriranje ili usporavanje internet saobraćaja će se najčešće izvesti u saradnji sa provajderima. Mapiranje tačaka spajanja nacionalnih i međunarodnih provajdera i analiza topologije mreže omogućava bolje razumijevanje ključne tačke ove infrastrukture, te gdje bi se potencijalna cenzura, filtriranje ili usporavanje saobraćaja mogli dogoditi.

Analiza protoka podataka za 100 najposjećenijih sajtova korisnika interneta u Srbiji, povezanih preko SBB mreže, pokazala je da, poslije par lokalnih skokova, sav saobraćaj odlazi na nekoliko tačaka, te

da 63% internet paketa napušta zemlju. Za razliku od evropskih država, poput Mađarske, Češke, Nemačke, Holandije ili Britanije, kroz koje podaci iz Srbije najčešće samo prolaze, skladištenje (hosting) podataka odvija se uglavnom u Sjevernoj Americi, tačnije u SAD.

Internet u doba koronavirusa

Izbijanje pandemije uslovilo je rast korišćenja elektronskih komunikacionih usluga, pa time i značajan porast telekomunikacionog saobraćaja, kako je saopštila Agencija za elektronske komunikacije i poštansku djelatnost (EKIP). Najveći porast desio se u drugoj polovini marta, kada je internet saobraćaj uvećan za oko 25%. Ukupno je za mjesec mart ostvareno 54% više internet saobraćaja nego u istom mjesecu prošle godine. Elektronske komunikacione mreže su u vrijeme epidemije preduzimale mjere da bi se povećanje korišćenja elektronskih komunikacionih usluga prevazišlo bez zagušenja i usporavanja saobraćaja.

Digitalna bezbjednost

Novinari i medijski radnici, čiji rad zavisi od povjerljivosti i bezbjednosti podataka, kao i izvora s kojima komuniciraju, moraju da vode znatno više računa o korišćenju tehnologije. Jedna kompromitovana tačka može ugroziti digitalnu bezbjednost čitave redakcije, ali i njihovih izvora. U današnje vrijeme, čitav novinarski rad je zasnovan na

korišćenju tehnologije - praktično sve povjerljive infomacije nalaze se u telefonima i kompjuterima.

Postoji mnogo faktora koji utiču na to da li će sistem biti bezbjedan ili ne. Prije svega, to su tehnološki faktori, tj. da li je sistem tehnološki kompromitovan ili ranjiv i koji je nivo bezbjednosti koji sami uređaji i programi koji su instalirani pružaju. Međutim, postoje i ljudski faktori, kao što su navike korisnika, koji su veoma bitni.

Opšte pravilo glasi da bezbjednost nije urođena karakteristika digitalnih sistema, već se na njihovoj bezbjednosti mora aktivno raditi. Prednost digitalne sredine leži u tome što korisnici donekle mogu da utiču na zaštitu sebe i drugih. Najvažnije bezbjednosne mjere dostupne su profesionalnim novinarima i svima koji se bave objavljivanjem informacija.

Enkripcija

Komunikacija u onlajn okruženju odvija se kanalima koje može da probije svako ko ima dovoljno znanja i resursa. Stoga je sadržaj komunikacije neophodno kodirati, ili enkriptovati, kako bi se osiguralo da će poruku pročitati samo oni kojima je namijenjena, odnosno koji imaju ključ za dekodiranje.

Važnost zaštite ličnih podataka, poslovnih tajni, ali i zaštite tajnosti novinarskih izvora, u savremenom digitalnom okruženju praktično podrazumijeva da je enkripcija postala sastavni dio svakodnevne rutine medijskog rada.

Većina informacionih sistema nije unaprijed enkriptovana, već se tome podvrgavaju njegovi pojedini segmenti po potrebi. Može

se enkriptovati komunikacija, odnosno sadržaj poruka koje se razmjenjuju, a mogu se enkriptovati i diskovi na kojima se podaci čuvaju. Enkripcija komunikacije se, prije svega, odnosi na servise za elektronsku poštu i tzv. četove, kao i na bezbjedno kretanje internetom.

Zaštita elektronske pošte

Tehnologija koja se nalazi u osnovi elektronske pošte ima dosta bezbjednosnih nedostataka, što znači da korisnik nema potpunu kontrolu nad pristupom metapodacima i sadržaju svojih mejlova, naročito kada se za to koriste javni servisi kao što je Gmail.

Jedan od najboljih načina za enkriptovanje sadržaja mejlova jeste PGP (Pretty Good Privacy). Nedostatak ovog programa ogleda se u implementaciji koja zahtijeva nešto naprednije digitalne vještine. Takođe, potrebno je da obje strane u komunikaciji koriste PGP da bi se program mogao uspostaviti kao mehanizam zaštićene komunikacije. Osim toga, postoje servisi, kao što su ProtonMail ili Tutanota, koji imaju ugrađenu enkripciju komunikacije između korisnika tih servisa.

Dok se digitalna pismenost šire javnosti ne podigne na viši nivo, teško je očekivati da će svi koristiti PGP, ali za specifične kontakte novinara, kao što su uzbunjivači ili javni službenici koji se bave osjetljivim pitanjima, poput nacionalne bezbjednosti, treba insistirati na uspostavljanju komunikacije enkriptovanim mejlovima na neki od dostupnih načina.

Pored mejla, za komunikaciju se koriste i različite čet usluge. Takve servise nerijetko koriste izvori da bi novinarima brzo prenijeli neku

nezvaničnu informaciju, nesvjesni rizika kojima se izlažu. Postoje, međutim, čet aplikacije koje omogućavaju enkriptovanu komunikaciju – Signal, Telegram, WhatsApp.

Bezbjedna pretraga interneta

Za pretraživanje interneta koriste se posebni programi (eng. browsers). Tehničko pretraživanje predstavlja pristupanje sadržaju na internetu pomoću odgovarajućih internet protokola. Postoje različita rješenja (Mozilla Firefox, Google Chrome, Brave Browser, Microsoft Edge) i svi na neki način obavljaju istu funkciju, ali da bi pretraživanje bilo bezbjedno, potrebno je podesiti dodatne parametre i instalirati dodatne komponente (eng. plugins) kao što je HTTPS Everywhere.

Osnovni nivo podrazumijeva korišćenje bezbjednih protokola kao što su SSL ili TLS. Ove tehnologije enkriptuju komunikaciju između klijenta i servera i tako efikasno štite od napada aktera "u sredini" (eng. Man-in-the-Middle). Na ovaj način je omogućen bezbjedan prenos osjetljivih podataka preko interneta kao što su korisnička imena, šifre ili povjerljivi lični podaci, poput brojeva ličnih dokumenata, podataka o platnim karticama, brojeva bankovnih računa, itd.

Enkripcija diskova

Velika količina podataka često se čuva na različitim uređajima, od kojih su za enkripciju relevantni lokalni diskovi i prenosivi uređaji (USB fleš memorije i eksterni hard diskovi).

Enkripcija diska podrazumijeva stvaranje sloja zaštite koji onemogućava neovlašćenim licima da pristupe sadržaju koji se nalazi na disku, ukoliko dođu u njegov posjed. Da bi se pristupilo

sadržaju potreban je unos šifre, a ponekad se postavljaju i dodatni parametari kao što su autentifikacija na dva nivoa, digitalni sertifikat ili biometrijski podaci.

Za enkriptovanje lokalnih i prenosivih diskova može se koristiti besplatan i otvoren softver VeraCrypt, koji posjeduje veliki broj funkcija u skladu sa potrebama korisnika.

U pojedinim slučajevima može biti potrebna hibridna enkripcija, Na primjer, kod USB fleš memorije, u jednoj transakciji javlja se potreba da se enkriptuje prenos sa nekog diska do fleš memorije i onda se enkripcija vrši na samoj memoriji. Cloud tehnologija sa druge strane, takođe, uslovljava posebne mehanizme enkripcije jer je sama tehnologija hibrid prenosa i skladištenja.

Ažuriranje softvera

Svakodnevno se razvijaju nove vrste tehnoloških napada i malicioznog softvera, te anti-malver aplikacije svakodnevno ažururaju svoje liste čime omogućavaju da program detektuje najnovije vrste malvera. Svaki sistem ima nedostatke koji se mogu iskoristiti da bi se ostvario neovlašćeni pristup sistemu. Sajber kriminalci konstantno rade na pronalaženju i istraživanju sistemskih nedostataka čijom bi se eksploatacijom omogućio upad u sistem. Zbog toga je bitno redovno ažurirati sve vrste aplikacija u okviru sistema, počev od operativnog sistema, preko anti-malver aplikacija do aplikacija koje se koriste svakodnevno. Preporučuje se da se aplikacije tako podese da samo obavještavaju korisnika da treba da ažurira softver, a da se ne dozvoljava da automatski preuzimaju ažurirane verzije programa.

Oprez od malvera

Malver je softver čija je namjena da pričini štetu informacionom sistemu. Najprepoznatljivija vrsta malvera su računarski virusi, ali postoje i druge vrste kao što su trojanci i crvi (eng. worms). Svaka vrsta malvera ima svoj način funkcionisanja, pa je zbog toga šteta koju nanosi svaki od njih različitog stepena. Malver može da izvodi različite operacije, od preusmjeravanja na lažne veb sajtove do destabilizacije čitavog sistema. Postoji i posebna vrsta malvera koji bilježi svaki unos preko tastature i zapise šalje trećim licima (eng. keylogger).

Takođe, postoji vrsta malvera koja ima mogućnost da šalje i po nekoliko hiljada mejlova sa zaraženog računara. Malver se distribuira na različite načine - najčešće ga korisnici sami preuzmu nekom svojom aktivnošću, mada napadači mogu iskoristiti i neki još neriješeni nedostatak instaliranih programa. Pored dobrog antimalver programa, potrebno je mijenjati navike - ne preuzimati nepouzdane aplikacije, ne otvarati sumnjive linkove i mejlove, ne posjećivati nepouzdane veb sajtove.

Kompleksnost šifre

Osnovno pravilo pri kreiranju šifri glasi da one ne treba da sadrže podatke o korisniku ni cijele riječi prirodnog jezika, jer se tako mogu lako otkriti metodom pokušaja i pogrešaka. Postoje generatori kompleksnih šifara sa nasumičnim karakterima, ali se te šifre teško pamte. Dobro rješenje je kreirati naizgled nasumične šifre koje se teško pogode, ali se lako pamte.

Takođe, bitno je konfigurisati i dobra sigurnosna pitanja za resetovanje

šifre. Treba povesti računa da odgovor na sigurnosno pitanje ne bude opšte poznat i da bude naizgled nasumičan.

Pored kompleksnih šifri, obavezno je aktivirati i autentifikaciju na dva nivoa (eng. two-step authentication) gdje god je to moguće. To je način autentifikacije koji pored unosa šifre zahtijeva i dodatni korak, najčešće unos koda koji se dobija putem SMS poruke ili mobilne aplikacije. Kvalitetna šifra i ostali mehanizmi zaštite pristupa neminovni su na putu ka bezbjednom sistemu, ali je podjednako bitan i način čuvanja. Nikako se ne preporučuje da se šifre zapisuju u sveske, na cjeduljice ili da se čuvaju u telefonu. Bezbjedan način čuvanja su softverska rješenja koja čuvaju šifre u bazi podataka u enkriptovanom formatu, tako da i u slučaju da je računar na kojem se šifre čuvaju meta napada, šifre ne gube svoj integritet. Primjeri softvera koji mogu da generišu nasumične i dugačke šifre i da ih čuvaju u zaštićenoj bazi na uređaju jesu KeePass i KeePassXC. Više o ovoj temi može se naći i u Vodiču "Osnove digitalne bezbednosti".

Sloboda izražavanja i onlajn mediji u digitalnom okruženju

Pravo na slobodu izražavanja zaštićeno je članom 10 Evropske konvencije za zaštitu ljudskih prava i osnovnih sloboda. U prvom stavu ovog člana navodi se da svako ima pravo na slobodu izražavanja, dok se u drugom stavu pojašnjava u kojim slučajevima to pravo

može biti ograničeno. Države članice Savjeta Evrope imaju pozitivne i negativne obaveze u vezi sa članom 10, odnosno pozvane su da aktivno unaprijeđuju zaštitu i poštovanje prava, ali i da se suzdrže od miješanja u ostvarivanje prava na slobodu izražavanja. Prema članu 10, stav 2, miješanje države u ovo pravo mora da zadovolji stroge kriterijume: ono mora biti propisano zakonom, neophodno u demokratskom društvu, kao i da ima legitimni cilj. Zaštita koju pruža član 10 pokriva i informacije i mišljenja koja mogu da šokiraju, uvrijede ili uznemire, pa prema tome sva ograničenja slobode izražavanja treba da se primjenjuju restriktivno.

Iako član 10 Konvencije ne pominje izričito slobodu medija, ona je sadržana u pravu na slobodu izražavanja. Uloga medija kao "psa čuvara" veoma je važna u svakom demokratskom i otvorenom društvu, a tu ulogu, dolaskom novih tehnologija, preuzima sve više aktera, jer se tradicionalno medijsko tržište u potpunosti promijenilo pojavom interneta uspostavljajući nove forme medija i komunikacije. Naime, digitalno okruženje predstavlja javni prostor koji je po svojim karakteristikama permanentno dostupan svim akterima, pružajući mogućnost da se neposredno učestvuje u razmjeni informacija na globalnom nivou.

Pored dobro poznatih tradicionalnih medija kao što su štampani mediji, radio i televizija kao i njihove internet stranice, sada su tu i mnogobrojni oblici onlajn medija. Teško je mapirati i klasifikovati nove oblike, ali najtipičniji su informativni portali, blogovi, servisi za pretraživanje sadržaja, društvene mreže, sajtovi za dijeljenje video sadržaja, agregatori vijesti i slično. Svi ovi oblici pružaju nam mogućnost da primamo i saopštavamo informacije, ali se postavlja pitanje koje internet forme treba smatrati "medijima" u smislu medijske regulative, te koja prava i odgovornosti u pojedinačnim

slučajevima postoje. Internet tako u potpunosti briše granice, mijenja uspostavljene sisteme i destabilizuje postojeća pravila javnog informisanja, što postavlja nove izazove kako regulatorima, tako i proizvođačima medijskog sadržaja.

Osnovni izazov s kojim se regulatori suočavaju jeste pitanje novinarskog statusa, odnosno pitanje ko jeste, a ko nije novinar i kako na tradicionalno razumijevanje profesije utiče savremeni koncept 'građanskog novinarstva'. Preporuke Komiteta ministara Savjeta Evrope iz 2011. godine utvrđuju šest kriterijuma za identifikaciju medija, dok je smjernice za status novinara dao 2012. godine tadašnji specijalni izvjestilac UN za slobodu izražavanja. Naime, Frank La Ru se u svom izvještaju opredijelio za tzv. funkcionalnu definiciju novinara po kojoj je to svako ko posmatra, opisuje, dokumentuje i analizira događaje, izjave, politike i bilo koji prijedlog koji može da utiče na društvo, sa svrhom sistematizovanja takvih informacija, sakupljanja činjenica i analize radi informisanja dijelova društva ili društva u cjelini. Digitalno okruženje nam samim prisustvom na mreži omogućava učešće u medijskoj sferi, što ranije nije bio slučaj. Internet se, takođe, smatra prostorom gdje svako može da kaže šta želi i u kojem ne važe pravila tradicionalnog novinarstva. U tom prostoru svi imaju istu šansu da prenesu informaciju i tako utiču na javno mnjenje, na isti način kao i etički školovano, urednički oblikovano novinarstvo koje poštuje sva pravila.

Ishod diskusije o novinarskom statusu u izmijenjenom okruženju direktno će uticati na utvrđivanje dometa nekih sloboda i prava, poput zaštite tajnosti izvora informacija ili prava na izuzetak od stroge primjene novog evropskog režima zaštite ličnih podataka. S druge strane to novo, digitalno okruženje dramatično utiče na položaj svakog ko se bavi informisanjem javnosti, profesionalno ili

povremeno. Digitalna pismenost, sajber bezbjednost i poznavanje tehnika i alata za prikupljanje informacija i zaštitu podataka u onlajn okruženju, postali su sastavni dio temeljnih novinarskih vještina.

Onlajn mediji i medijska regulativa

U Crnoj Gori je na snazi Zakon o medijima iz 2002. godine. U toku je postupak usvajanja u Skupštini novog Zakona, usklađenog sa nizom tehnoloških i društvenih promjena koje su se odigrale u međuvremenu, a od kojeg se očekuje da bitno unaprijedi medijsku sferu.

Za razliku od važećeg Zakona koji taksativno nabraja šta se smatra medijima (član 6), u prijedlogu novog Zakona ovakva jasna definicija izostaje. Umjesto toga, prijedlog novog Zakona navodi definiciju medijskih sadržaja pa se, između ostalog, u članu 6 navodi da se medijskim sadržajem smatra informacija, analiza, komentar, mišljenje i slično. Dodatno, u istom članu prijedloga navedena je nejasna odredba koja navodi da "mediji podrazumijevaju aktere uključene u proizvodnju i širenje medijskog sadržaja sa uređivačkom kontrolom ili nadzorom nad tim sadržajem namijenjenom neodređenom broju ljudi". Takođe, u članu 26 uvodi se pojam internetske publikacije i daje njena definicija: medij čiji se sadržaj širi putem interneta, a koji nije audiovizuelna medijska usluga. U skladu sa zadatim kriterijumima, to bi značilo da se internetskom publikacijom može smatrati svaka informacija, analiza, komentar, mišljenje i slično, proizvedena pod uređivačkom kontrolom ili nadzorom nad tim sadržajem i namijenjena neodređenom broju ljudi.

Ovako široka definicija internetske publikacije može dovesti do toga da se sve vrste onlajn medija, uključujući blogove, veb i mobilne platforme, forume, Tviter naloge, Fejsbuk stranice, kao i druge

internet servise koji se koriste za obavještavanje javnosti o pitanjima od javnog interesa, mogu smatrati medijima u skladu sa zakonom. Za razliku od aktuelnog Zakona o medijima, na ovaj način se prilično široko reguliše onlajn prostor, što može dovesti do velikih posljedica po slobodu izražavanja kao garantovanog prava, te po slobodnu razmjenu informacija.

U ranijim verzijama Nacrta zakona o medijima na samom početku se navodi značenje izraza, pa samim tim i šta su mediji, što se može vidjeti u Pravnom mišljenju i komentarima na nacrt zakona koje je naručila Misija OEBS-a u Crnoj Gori.

Sve u svemu, na onlajn medije u pogledu regulative treba gledati kao na sadržaje koje su uredrički oblikovani i koji imaju za cilj da informišu javnost o pitanjima od javnog interesa. Jedno od rješenja može biti da zakonodavac onlajn medijma ostavi opciju da se oni, ako to žele, registruju kao mediji i na taj način dobiju odgovarajući status sa svim pravima i obavezama. Neregistovani onlajn mediji moraju imati opciju da ostanu van opsega Zakona o medijima, iz razloga što medijski propisi nameću brojne odgovornosti koje mogu preopteretiti aktere koji nemaju ambiciju da budu medij u formalnom smislu. Drugim riječima, jedino i samo oni koji se svojevoljno registruju treba da budu smatrani medijem u smislu zakona koji uređuje ovu oblast. No, akteri koji odluče da se ne registruju ne ostaju u potpunosti van domašaja svih zakona - na njih se primjenjuju opšta zakonska pravila o naknadi štete ukoliko je prouzrokuju.

Nova etička pitanja

Novinari se različito odnose prema tehnološkim promjenama. Tako jedni zastupaju stav da je novinarstvo uvijek isto, bez obzira na to

kojim se sredstvima realizacije koristi, dok drugi danas već razlikuju "dron-novinarstvo" od ostalih, zasebnih vrsta koje podliježu različitim zakonitostima, poput štampanog, radijskog, televizijskog ili onlajn novinarstva.

U zavisnosti od uvjerenja o uticaju koji format može imati na medijske prakse, razlikuju se i pristupi etičkim standardima. Jedna struja ističe da će zahtjev tačnosti i cjelovitosti prenijete informacije ili odgovornosti za objavljenu neistinu uvijek odolijevati testu tehnoloških promjena, ma kako dramatične one bile. Druga struja smatra da su novi uslovi proizvodnje i distribucije vijesti radikalno promijenili već i same koncepte istine, privatnosti ili javnog interesa, te bi stoga i novinarski kodeks trebalo mijenjati.

Lista potencijalnih izazova koje pred novinare postavlja internet nije konačna, slično kao kada govorimo o uticaju informacionih tehnologija na društveno-političke ili ekonomske okolnosti. Mediji i novinari uče na vlastitim greškama, oslanjajući se na uhodane nivoe samoregulacije - od individualne novinarske pažnje, svijesti o sopstvenim ograničenjima i predrasudama, etičkim izazovima s kojima se suočavaju preko redakcijskih mehanizama (interni kodeksi, kazne i nagrade, urednička kontrola, čitalački ombudsman) do profesionalnih udruženja, nacionalnih i međunarodnih.

Neka od najvažnijih etičkih pitanja za onlajn novinarstvo zasad su grupisana oko provjere pouzdanosti izvora, korišćenja već objavljenih sadržaja sa stanovišta zaštite privatnosti i autorskih prava, transparentnosti i odgovornosti (ispravke grešaka, sukob interesa), kao i balansiranja komercijalnih i javnih interesa (prikriveno oglašavanje, osjetljivi sadržaji – nasilje, pornografija, govor mržnje).
Rast dva osnovna rizika po etičko novinarstvo - brzine i konkurencije

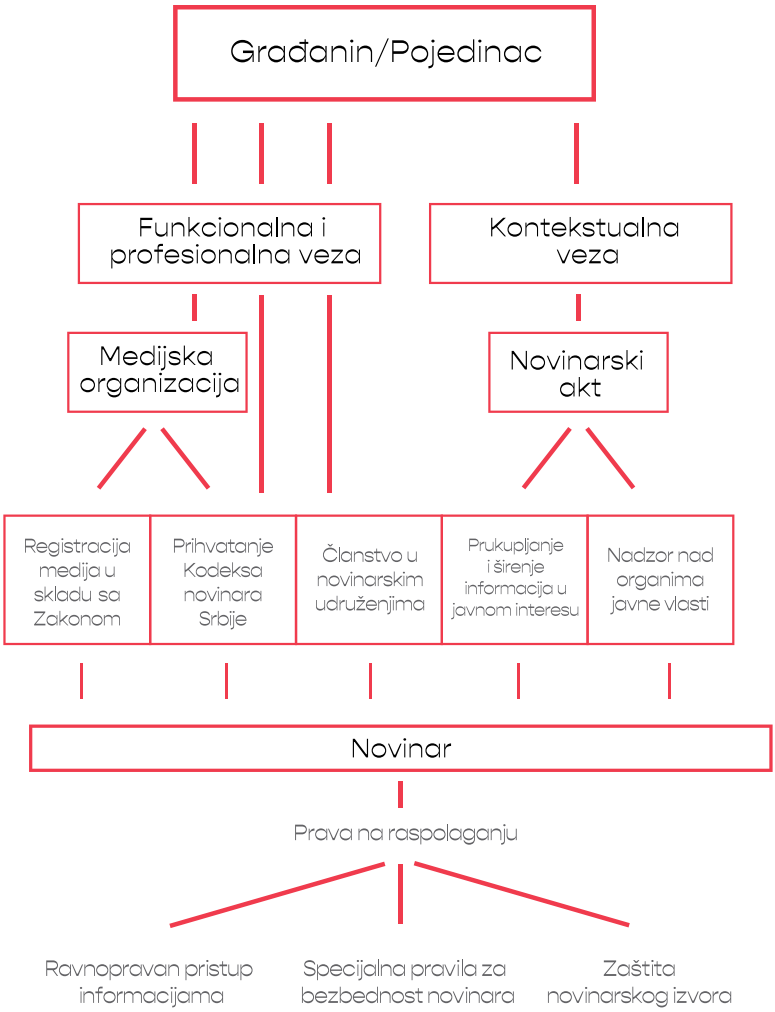
- znači da se profesionalni novinari u onlajn prostoru takmiče sa gigantskim korporacijama s jedne, i novinarima-amaterima s druge strane. U takvim uslovima ultimativni oslonac predstavlja novinarski integritet. Bez obzira da li koriste informacije publike (eng. crowdsourcing) u prikupljanju i provjeri tačnosti informacija, da li pišu blog u privatnom svojstvu ili kao zaposlleni u medijskoj organizaciji, lična odgovornost novinara biće na kraju i njihov reputacioni kapital na medijskom tržištu. Detaljna analiza poslovanja medija u novom tehnološkom i pravnom okruženju može se naći u priručniku "Regulatorni okvir i poslovni modeli onlajn medija".

Status novinara

Statusno pitanje je od izuzetne važnosti kada govorimo o dva prava - zaštita bezbjednosti novinara i zaštita izvora informacija. Često preovlađuje tumačenje prema kojem se posebna prava odnose samo na profesionalne novinare, članove strukovnih udruženja, odnosno osobe angažovane u nekom od medija upisanih u registar.

Međutim, s obzirom na drastične promjene medijskog okruženja, značajnu pažnju treba obratiti na usklađivanje postojećih standarda sa inoviranim načelom da novinarska zaštita pripada i učesnicima u javnoj komunikaciji koji nemaju formalni status novinara, ali stalno ili povremeno preduzimaju novinarski čin, odnosno izvještavaju javnost o pitanjima od javnog interesa.

Drugim riječima, pojedinci mogu imati privilegije i odgovornosti kada su profesionalno vezani za neku medijsku organizaciju, udruženje novinara ili samoregulatorno tijelo, što nam je sve dobro poznato, ili kroz sam novinarski čin, tj. prikupljanje i širenje informacija u cilju ostvarivanja javnog interesa i vršenja kontrole vlasti.



*Priručnik "Regulatorni okvir i poslovni modeli onlajn medija"

Pitanje se, dakle, može posmatrati kroz profesionalnu i kontekstualnu vezu. Razlika između ova dva aspekta leži u tome što se kod profesionalne veze novinarska zaštita pretpostavlja, dok je kod kontekstualne veze, ipak, na građanima da dokažu da preduzimaju novinarski čin koji im omogućava novinarske privilegije, pa samim tim i zaštitu.

Opšta pravila o privilegijama i odgovornostima

Postoje statusne razlike između registrovanih medija i neregistrovanih oblika izvještavanja, kojima se određuju pravila o privilegijama i odgovornostima u vezi sa objavljenim sadržajem. Osnovno pitanje jeste koji zakon će se primjenjivati, jer se na registrovane medije primjenjuje Zakon o medijima, dok se na neregistrovane aktere primjenjuje opšti režim u skladu sa Zakonom o obligacionim odnosima.

Kada govorimo o registrovanim medijima postoji niz privilegija, ali isto tako i odgovornosti koje su propisane Zakonom o medijima.

Privilegije

Zaštita izvora informacija

Jedan od najvažnijih standarda novinarske profesije jeste zaštita izvora informacija, kao tekovina medijskih sloboda i nalazi se u mnogim međunarodnim dokumentima, deklaracijama i preporukama. Novinari imaju pravo da zaštite identitet svojih izvora i objave informacije. Korišćenje ove privilegije je od ključnog značaja za izvještavanje o svim pitanjima od javnog interesa sa kojima javnost ne bi mogla da bude upoznata na drugi način.

Kao što navodi organizacija *Article 19* u publikaciji o zaštiti novinarskih izvora, nezavisno novinarstvo upravo zavisi od slobodne razmjene informacija između medija i građana. Pojedinci, tj. izvori, istupaju sa tajnim i osjetljivim informacijama, oslanjajući se na to da će ih novinari proslijediti široj javnosti radi obavještavanja o pitanjima od javnog interesa. Više o ovoj temi može se naći u vodiču "Zaštita tajnosti izvora informacija".

Trenutno važeći Zakon o medijima u članu 21, stav 3, navodi da novinar i druga lica koji tokom obavljanja novinarskog posla dođu do informacija koje mogu da ukažu na identitet izvora, nisu dužni da otkriju izvor informacije koji želi ostati nepoznat. Ako se ova odredba tumači ekstenzivno, može da se razumije na način da nema nikakvih ograničenja, tj. da je pravo na zaštitu tajnosti novinarskih izvora apsolutno.

Međutim, to nije slučaj sa prijedlogom Zakona (član 30, stav 1) koji kao osnovnu premisu ima istu stvar - da novinar nije dužan da otkrije izvor informacija - ali u sljedećem stavu se postavlja ograničenje da je novinar dužan da na zahtjev tužioca otkrije izvor informacija kada je to neophodno radi zaštite interesa nacionalne bezbjednosti, teritorijalnog integriteta, zaštite zdravlja i otkrivanja krivičnih dela zaprijećenih kaznom zatvora od pet i više godina.

Ovako široko definisani izuzeci mogu predstavljati opasnost po novinare, odnosno njihove izvore koji bi mogli trpjeti štetne posljedice ukoliko se njihov identitet otkrije na sudu. Posebno je problematično to što bi se ovaj član mogao koristiti za proganjanje novinara koji istražuju poslove javnih funkcionera i drugih moćnih ljudi, pod izgovorom "zaštite nacionalne bezbjednosti" i tome slično.

Pristup informacijama i akreditacije za izvještavanje

Formalna profesionalna veza koja jasno utvrđuje novinarski status značajno olakšava pristup informacijama i akreditacijama za izvještavanje. Poznat je princip da organizatori događaja raznih vrsta daju registrovanim medijima akreditacije za izvještavanje, dok ostali nisu u mogućnosti da budu akreditovani.

Pristup državnim fondovima – finansijska sredstva za ostvarivanje prava građana na informisanje

Kada govorimo o pristupu državnim fondovima i finansijskim sredstvima koja se dodjeljuju radi ostvarivanja javnog interesa, tj. prava građana na informisanje o pitanjima od značaja za njihovu zajednicu, po pravilu pravo na to imaju registrovani mediji. Entiteti koji nisu registrovani kao mediji u skladu sa Zakonom i u odgovarajućem javnom registru ne mogu da računaju na podršku iz javnih budžeta.

Trenutno važeći, ali i prijedlog novog Zakona, stoje manje više na istom stanovištu da se iz budžeta države odvajaju određena sredstva, a razlika je u tome za šta se sredstva dodjeljuju, tj. za koje sadržaje. Važeći Zakon odvaja sredstva za programske sadržaje koji su važni za razvoj nauke i obrazovanja, razvoj kulture, informisanje osoba oštećenog sluha i vida, kao i sredstva za navedene programske sadržaje na jezicima nacionalnih manjina (član 3). Prijedlog Zakona u članu 17 malo šire definiše ovu oblast, pa se finansiraju projekti u oblasti informisanja tako što država obezbeđuje finansijska sredstva za pružanje javnih usluga preko Fonda za podsticanje pluralizma i raznovrsnosti medija. Dodatno, država obezbjeđuje dio sredstava za medijske nekomercijalne sadržaje od javnog interesa, na jezicima manjinskih naroda i drugih manjinskih nacionalnih zajednica i

medijske nekomercijalne sadržaje od javnog interesa u štampanim neprofitnim medijima. U skladu sa oba akta, način i uslovi se dodatno propisuju aktom nadležnog organa za poslove informisanja ili Ministarstva za kulturu.

Odgovornosti

Obaveza novinarske pažnje – "odgovorno novinarstvo"

Osnovna obaveza novinara jeste da postupaju sa dužnom novinarskom pažnjom. To znači da ne smiju slijepo vjerovati izvorima informacija i prilikom izvještavanja dužni su da provjere informacije iz više nezavisnih izvora prije nego što ih objave. Ovo se posebno odnosi na društvene mreže i ostale izvore informacija na internetu - teorije zavjere i potpune izmišljotine koje završe u medijima obično nastaju u nekom zavučenom kutku interneta.

Važno je napomenuti da novinari, urednici i izdavači medija zbog nepoštovanja novinarske pažnje mogu pred sudovima odgovarati za naknadu štete.

Zanimljivo je da važeći Zakon predviđa samo odgovornost autora i osnivača medija, dok nije predviđena odgovornost glavnog i odgovornog urednika, što je dosta neuobičajeno u uporednoj praksi. To se mijenja u prijedlogu novog Zakona, jer se između ostalog navodi da su za štetu solidarno odgovorni osnivač, glavni i odgovorni urednik i novinar, ukoliko se dokaže da su postupali suprotno dužnoj novinarskoj pažnji. Odgovornost glavnog i odgovornog urednika u novinarskom poslu je neupitna, upravo zbog toga što su njegove osnovne uloge odabiranje i kontrola sadržaja koji će se objaviti u mediju.

Prijedlog unosi novinu izričitim opisom odgovornog novinarstva i kaže da je novinar dužan da "prije objavljivanja informacija o određenom događaju, pojavi ili ličnosti, sa dužnom novinarskom pažnjom, provjeri njeno porijeklo, istinitost i potpunost."

Takođe, kada govorimo o odgovornostima, prijedlog Zakona eksplicitno reguliše i uklanjanje komentara sa internetskih stranica. Prvenstveno se navodi da je komentar sadržaj koji je objavljen na internetskoj stranici od strane registrovanog korisnika. Budući da je definicija internetske publikacije izuzetno široko postavljena, razni oblici izražavanja na mreži se mogu podvesti pod ovu zakonsku formu. Odredba da komentar mora kreirati registrovani korisnik dovodi do dodatnih komplikacija: šta se dešava ukoliko onlajn medij nema obavezu registracije korisnika na svom sajtu?

Osnivač internetske publikacije, takođe, se obavezuje da ukloni komentar koji predstavlja očigledno nezakonit sadržaj i kojim se krše zakonom zaštićena prava, bez odlaganja a najkasnije u roku od 24 sata od trenutka saznanja ili prijave drugog lica. Ukoliko se to ne desi, lice na koje se odnosi komentar ima pravo da zahtijeva uklanjanje sadržaja od nadležnog suda.

U digitalnoj sferi, međutim, svake sekunde se objavljuje izuzetno velika količina sadržaja koju kreiraju sami korisnici, pa je praćenje svakog objavljenog komentara često nemoguće. Mehanizam propisan u prijedlogu Zakona je takozvana "notice and take down (NTD)" procedura koja opisuje postupak u kojem se sporni sadržaj uklanja nakon obavještenja zainteresovanog lica. Ova procedura se zasniva na odredbama Direktive Evropske unije o elektronskoj trgovini 2000/31/EC i prisutna je u svim zemljama EU, ali se implementira na različite načine. Pravnu neizvesnost stvara upravo

razlika u tumačenju prilikom procesa primjene na nacionalnom nivou.

U prijedlogu se navodi i da je internetska publikacija dužna da propiše pravila komentarisanja i da ih objavi. Pravila komentarisanja su veoma bitna za korisnike i neophodno je da oni budu obavješteni na koji način onlajn mediji postupaju sa komentarima, kao i koja se prava i obaveze odnose na sadržaj koji namjeravaju da postave. Savjet za štampu u Srbiji je izradio Priručnik za prilagođavanje pravila potrebama onlajn medija koji detaljnije govori o pravilima komentarisanja i raznim modelima koje onlajn mediji mogu primijeniti.

Da su postojeća rješenja još uvijek podložna različitim tumačenjima u odnosu na pravnu tradiciju, potvrđuje i odluka Ustavnog vijeća Francuske, doneta u junu 2020.godine, kojom su glavne odredbe tzv. Avia zakona proglašene neustavnim. Jedna od osporenih odredbi bila je obaveza pružalaca onlajn usluga da u roku od 24 sata uklone sadržaj koji korisnici prijave kao "očigledno nezakonit" u skladu sa prethodno definisanom listom pravnih povreda. Takođe je van snage stavljena odredba po kojoj su u slučaju terorističkih sadržaja i sadržaja koji se tiču seksualne eksploatacije dece, onlajn posrednici dužni da takve sadržaje uklone u roku od sat vremena od prijave koju podnose administrativni organi. Vijeće je u odluci navelo da ovakve odredbe ugrožavaju slobodu govora i komuniciranja, te da nisu proporcionalne, neophodne i prikladne.

Najveću neizvjesnost stvara vremenski rok i pitanje ko donosi odluku o tome šta predstavlja nezakonit sadržaj ili koja su to zaštićena prava u skladu sa Zakonom. Posebno treba uzeti u obzir i činjenicu da je za ovako nešto potrebno dodatnih resursa u okviru onlajn medija, odnosno neophodno je imati obučene ljude koji su u mogućnosti da

donose odluke ove vrste. Ukoliko se sadržaj ne ukloni, medij se izlaže riziku sudskog procesa; ukoliko se sadržaj ukloni, medij se izlaže riziku da postane cenzor koji ograničava pravo na slobodu izražavanja.

Pravo na odgovor i ispravku

Greške se u novinarstvu dešavaju, s lakšim ili težim posljedicama, ali u vrijeme kada je sadržaj gotovo nemoguće u potpunosti ukloniti sa interneta, posljedice grešaka mogu biti trajne.

Medijsko zakonodavstvo širom svijeta poznaje institute prava na odgovor ili ispravku informacije upravo da bi se omogućilo da strana koja je predmet izvještavanja dobije satisfakciju bez pokretanja sudskih postupaka ukoliko smatra da je oštećena.

Imajući u vidu da pravo na ispravku i odgovor otvara mogućnost zloupotrebe, medijsko zakonodavstvo uglavnom poznaje ograničenja u pogledu toga kada mediji nisu dužni da objave odgovor.

Važeći Zakon detaljno uređuje pravo na ispravku i odgovor, na način da svako lice ima pravo da zatraži objavljivanje ispravke i odgovora ukoliko je povrijeđeno neko njegovo pravo i to u roku od 30 dana od dana objavljivanja sadržaja. Propisano je na koji način se vrši objavljivanje, kao i kada medij nije dužan da objavi ispravku ili odgovor. Ukoliko medij ne objavi ispravku ili odgovor, a bio je dužan da to učini, regulisan je i postupak po tužbi.

Pored opštih odredbi, u prijedlogu Zakona se navodi da se u internetskim publikacijama odgovor i ispravka moraju objaviti najkasnije u roku od 12 sati od prijema i moraju biti povezani linkom sa medijskim sadržajem na koji se odnose.

Od velike važnosti je i to da onlajn mediji budu svjesni da se tradicionalne metode objavljivanja odgovora i ispravke moraju prilagoditi novom okruženju, pa je stoga neophodno da se uspostavi praksa na koji način će se to činiti kada je reč o vebsajtovima. Dobra polazna tačka su Smernice za primenu Kodeksa novinara Srbije u onlajn okruženju.

Posebni osnovi isključenja odgovornosti

Pored stvaranja originalnog sadržaja, mediji prenose i informacije ili tuđe navode od značaja za javnost. Iako načelno postoji odgovornost za sav sadržaj koji se u nekom mediju objavi, u određenim situacijama mediji se mogu pozvati na standarde isključenja od odgovornosti za nastalu štetu zbog prenetih informacija.

Jasan primjer je sporna informacija vjerno prenijeta s javnog skupa, ili objavljena u emisiji koja se emituje uživo, s tim da se u oba slučaja kao uslov postavlja da novinar mora postupiti s dužnom novinarskom pažnjom.

Važeći Zakon o medijima nema posebne odredbe koje se odnose na oslobođenje od odgovornosti, mada su one od izuzetnog značaja u pojedinim situacijama. Prijedlog Zakona to predviđa i to tako da solidarna odgovornost osnivača medija, glavnog urednika i novinara neće postojati ukoliko su sa dužnom novinarskom pažnjom objavili sadržaj koji je nanio štetu, a taj sadržaj je:

- vjerno prenijet sa rasprave na sjednici zakonodavne, izvršne ili sudske vlasti, organa državne i lokalne uprave, sa javnog skupa ili prenijet iz nekog akta organa, javne ustanove ili drugih lica kome su povjerena javna ovlašćenja;

- od javnog interesa i prenijet je kao citat iz drugog medija ili objavljen unutar intervjua, osim ako pojedini dijelovi sadrže očigledne uvrede i klevete;
- zasnovan na informacijama za koje su novinar i glavni urednik imali osnovan razlog da vjeruju da su potpune ili istinite, a postojao je opravdani interes javnosti da bude upoznata.

Samoregulacija

Poštovanje etičkih standarda novinarske profesije obaveza je svakog izvještavanja o temama od javnog interesa, bilo da je riječ o profesionalnim novinarima ili o građanima koji vrše novinarski čin.

Osnovni principi etičkog novinarstva praktično su univerzalni, kao što su istinitost, nepristrasnost, pravičnost ili odgovornost, sa različitim dopunama i pojašnjenjima iz lokalnog konteksta, istorijskog razvoja i iskustva. Tako pojedine odredbe kodeksa svjedoče o odbrani od komercijalnog pritiska u zapadnim društvima tokom druge polovine 20. vijeka, dok su izričite zabrane diskriminacije pratile borbu za društvenu inkluziju i ravnopravnost. Doba širenja lažnih vijesti i "alternativnih činjenica" danas predstavlja poseban izazov za princip istinitosti.

Etički kodeks novinara Crne Gore usvojen je 2002. godine, a dopunjen 2015. i 2018. godine, kada su uključene i smjernice za onlajn medije.

Samoregulatorna tijela

U Crnoj Gori ne postoji jedinstveno telo koje se bavi pitanjima novinarske etike i poštovanjem Kodeksa. Umjesto toga, tokom godina je osnovano

nekoliko tijela od kojih su neka još uvijek aktivna, dok su druga ugašena. Također, u pojedinim medijima postoji institut ombudsmana.

Mehanizam jedinstvene kolektivne samoregulacije u Crnoj Gori do sada nije uspostavljen. U početku je to bilo Novinarsko samoregulatorno tijelo, koje su zajedno osnovali novinarska udruženja i pojedini mediji, ali je ono prestalo sa radom 2010. godine. Zatim je nekoliko štampanih medija pokrenulo Medijski savjet za samoregulaciju, koji je pratio rad medija i odlučivao o žalbama, povremeno obustavljalo rad i ponovo nastavljalo. Nekoliko lokalnih i štampanih medija osnovalo je 2012. godine Samoregulatorni savjet za lokalnu štampu, koji je do danas objavio samo jedan izvještaj o radu medija, te nije jasno da li ovo tijelo i dalje postoji. Iste godine, osnovan je i Savjet za štampu, ali ovo tijelo nije nikad bilo aktivno. S druge strane, pojedini mediji su uspostavili ombudsmane koji su uglavnom i danas operativni – *ND Vijesti*, *Dan*, *Monitor*, *TV Vijesti* (samo do 2018. godine, prema dostupnim podacima).

Za razliku od važećeg, prijedlog novog Zakona o medijima prepoznaje značaj samoregulacije, te navodi da mediji mogu osnovati kolektivno samoregulatorno tijelo, ali i da svaki medij može osnovati interno samoregulatorno telo.

Mehanizmi samoregulacije su od vitalnog značaja za profesiju koja je nezavisna od državne kontrole, a koja svoje obaveze prema javnosti ispunjava stalnim preispitivanjem kvaliteta svog rada. Mada su interni mehanizmi izuzetno korisni za pojedinačne ili grupu srodnih medija, jedinstvena samoregulatorna platforma može značajno unaprijediti punu primjenu etičkih standarda u svakodnevnom izvještavanju. Mehanizam koji stalno provjerava kako se principi novinarskog kodeksa tumače u odnosu na izazove novog medijskog ekosistema, takođe je važan oslonac mladim onlajn medijima.

Mediji i zaštita podataka o ličnosti

Pravni okvir zaštite ličnih podataka

Bavljenje novinarstvom podrazumijeva i obradu različitih podataka o ličnosti, za različite svrhe i u različitim kontekstima. Bez obzira na to koju ulogu imaju u određenom mediju - novinari, urednici ili zaposlleni u administrativnoj podršci moraju biti upoznati sa svojim obavezama koje se tiču obrade ličnih podataka sa kojima imaju konktakt u svom radu. U suprotnom, za medij, a ponekad i za pojednice, mogu nastupiti negativne pravne posljedice i sankcije, uz veliki rizik i eventualnu štetu po njihov ugled.

U posljednjih nekoliko godina, zakonski okvir koji reguliše postupanje sa podacima o ličnosti pretrpio je velike promjene u skoro svim evropskim zemljama. Na nivou cijele Evropske unije, 25. maja 2018. godine, počela je da se primjenjuje Opšta uredba o zaštiti podataka (eng. General Data Protection Regulation, GDPR). Ovaj pravni akt je za sve države van Evropske unije važan iz dva razloga. Formalan razlog je taj da sam GDPR u članu 3(2) predviđa uslove pod kojima će se primjenjivati i na entitete koji nisu osnovani u EU, ali obrađuju podatke lica koji se nalaze u EU. Drugi razlog je to što države van EU u svoja nacionalna zakonodavstva uvode zakone koji propisuju iste visoke standarde - što u cilju približavanja evropskom tržištu, što u cilju proklamovanja visokih standarda u oblasti ljudskih prava, među kojima je i pravo na privatnost.

Otkako je GDPR počeo da se primjenjuje, postoje najave da će i u Crnoj Gori biti donijet novi Zakon o zaštiti podataka o ličnosti koji će nova pravila EU inkorporirati u domaće zakonodavstvo. Međutim, u trenutku pisanja ovog vodiča ne postoji javno dostupan nacrt takvog propisa.

Pitanje sprovođenja GDPR pravila je od posebnog značaja za rad novinara. Naime, GDPR u svom članu 85 posebno reguliše situacije obrade podataka kada se radi o obavještavanju javnosti. Popularno nazvan "novinarski izuzetak" koji je sadržan u ovom članu GDPR-a odnosi se na situacije kada novinari ne moraju da poštuju sva zakonska pravila prilikom obrade podataka o ličnosti, ukoliko je to neophodno za obavljanje novinarskog posla. Pravila poput "novinarskog izuzetka" nisu sadržana u trenutno važećem Zakonu o zaštiti podataka Crne Gore. Ova činjenica u određenim situacijama može biti izvor pravne nesigurnosti.

Osnovni koncepti iz oblasti zaštite ličnih podataka

Podatak o ličnosti ili lični podatak je širok pojam u kontekstu pravne regulative. Trenutno, crnogorski Zakon lične podatke jezgrovito definiše kao sve informacije koje se odnose na fizičko lice čiji je identitet utvrđen ili se može utvrditi. U osnovi te definicije stoji ideja da se ličnim podatkom smatra svaka informacija koja se odnosi na fizičko lice i koja može, samostalno ili sa drugim informacijama doprinijeti identifikaciji određenog lica. Neki podaci kao što su jedinstveni matični broj, otisak prsta ili ime i prezime, direktno doprinose identifikaciji. Međutim, ličnim se smatraju i svi oni podaci koji indirektno mogu da dovedu do istog rezultata, kao što su opis psiholoških karakteristika, lozinke i nalozi za poruke, mejl adrese, istorija aktivnosti na internetu, a pogotovo na društvenim mrežama

(metapodaci, šerovi, lajkovi, klikovi), istorija pretrage interneta, IP adresa kompjutera ili smartfona, i slično.

Ovako širok spektar informacija koje se smatraju ličnim podatkom posljedica je, između ostalog, sve raširenije digitalizacije sve većeg broja društvenih i ličnih aktivnosti. U onlajn okruženju mnogi takvi lični podaci postaju lako javno dostupni. Važno je istaći da su svi lični podaci, u principu, pod istom pravnom zaštitom. Drugim riječima, to što je neki podatak postao javan, čak i voljom samog lica, ne znači da ga zakon ne štiti i da treća lica mogu sa tim podatkom slobodno da raspolažu. Takođe, mediji u okviru svoje obrade ličnih podataka svakodnevno te podatke čine javno dostupnim. Zbog toga je od izuzetnog značaja da u obavljanju svog posla ne prelaze granicu kojom nepotrebno i nezakonito zadiru u privatnost lica koja imaju pravo na zakonsku zaštitu podataka o sebi.

Određeni podaci o ličnosti su po svojoj prirodi vrlo osjetljivi, jer se njihovom obradom dublje zadire u privatnost kao osnovno ljudsko pravo. Stoga, propisi tim podacima obezbjeđuju veći stepen zaštite, odnosno za obradu takvih podataka propisuju strože uslove. U **kategoriju posebnih podataka**, prema trenutnom crnogorskom Zakonu, spadaju podaci koji se odnose na rasno ili etničko porijeklo, političko mišljenje, vjersko ili filozofsko uvjerenje, članstvo u sindikalnim organizacijama, kao i podaci koji se odnose na zdravstveno stanje ili seksualni život.

Entitet prema kojem fizičko lice - nosilac podataka može da ostvaruje svoja prava naziva se **rukovalac**. Rukovalac može biti bilo koje pravne forme ili subjektiviteta, mada će u pravilu to biti pravna lica ili državni organi. Ono što jedan entitet čini rukovaocem jeste činjenica da je taj entitet odredio svrhu i način obrade ličnih podataka.

U medijskom prostoru, to je po pravilu sam medij, a ne pojedinačni novinari ili urednici. Međutim, i novinar koji, na primjer, ima svoj blog, mogao bi se smatrati rukovaocem pod određenim uslovima.

Pored rukovaoca, u obradi podataka često učestvuju i **obrađivači**. To su entiteti koji nisu odredili ni svrhu za koju se obrađuju podaci, niti su odredili način - ali su rukovaocu obezbijedili sredstva (npr. opremu, aplikaciju ili softver) koju rukovalac koristi prilikom obrade. Na primjer, obrađivač u kontekstu medija je IT kompanija koja je izradila sajt i koja održava kako sajt, tako i softverske programe koje novinari koriste u svakodnevnom radu. Uloga obrađivača je da, prije svega, obezbijedi da podaci budu sigurni, odnosno da se ne događaju incidenti kao što je "curenje" ili gubitak podataka. Oni se posebnim ugovorom sa rukovaocem obavezuju da oprema koja služi za obradu podataka o ličnosti bude sigurna i bezbjedna.

Osnovna pravila koja se moraju poštovati prilikom obrade ličnih podataka

Odgovornost da obrada podataka o ličnosti bude zakonita pripada rukovaocu (dakle, ne obrađivaču). Krug njegovih obaveza se načelno može podijeliti na materijalne i formalne obaveze. Materijalne obaveze se odnose na glavna pravila koja moraju da prate bilo koji proces obrade podataka, od početka do kraja, tj. od prikupljanja podataka do njihovog brisanja. Ta pravila su sadržana u GDPR načelima, ali ih propisuje i aktuelni crnogorski Zakon.

Logika ovih osnovnih pravila je sljedeća: (i) prije otpočinjanja obrade rukovalac mora jasno da **odredi i definiše svrhu** koja se želi postići obradom, pri čemu ta svrha mora biti opravdana i zakonita (ograničenost svrhom); (ii) kada je svrha definisana, mora

se odrediti **da li postoji pravni osnov** koji dozvoljava obradu za konkretnu svrhu, pri čemu su raspoloživi pravni osnovi regulisani samim zakonom (zakonitost); (iii) za definisanu svrhu mogu da se prikupljaju samo oni lični **podaci koji su zaista neophodni,** tj. bez kojih ostvarivanje svrhe ne bi uopšte bilo moguće (minimizacija); (iv) moraju se preduzeti potrebne mjere da bi podaci bili **tačni**, po potrebi ispravljeni i redovno ažurirani (tačnost); (v) kao i mjere koje su u konkretnim okolnostima potrebne da podacima pristupaju i u njih imaju uvid isključivo ona lica koja su za to ovlašćena i niko treći, da podaci **ne budu izgubljeni, uništeni ili oštećeni** (integritet i povjerljivost) (vi) podaci koji su prikupljeni za ostvarivanje konkretne svrhe **moraju biti obrisani ili anonimizovani** čim se ta svrha ostvari (ograničenje čuvanja); (vii) lica čiji se podaci obrađuju moraju **na jasan i lako pristupačan način biti informisana** o konkretnim obradama koje se na njih odnose, uz uvažavanje njihovih prava (transparentnost i poštenje).

Pored materijalnih pravila koja se moraju poštovati za svaki poseban proces obrade, rukovaoci imaju i određene formalne obaveze, kao što je obaveza da zaključe odgovarajuće **ugovore sa obrađivačima** i obaveza da vode **evidencije o obradama** koje vrše. Prema važećem crnogorskom Zakonu, postoji i obaveza registracije zbirki podataka kod Agencije za zaštitu ličnih podataka i slobodan pristup informacijama. Međutim, za očekivati je da će novi zakon u skladu sa GDPR ukinuti obavezu registracije i da će se ove zbirke tj. evidencije voditi samo interno kod rukovaoca. Cilj evidencija je da rukovalac na jednom mjestu ima pregled svih vrsta i procesa obrade koje vrši u okviru svoje djelatnosti, sa odgovarajućim informacijama koje opisuju te procese, iz kojih se može utvrditi da li rukovalac zaista poštuje osnovna pravila.

Ne postoji propisana obaveza da rukovalac ima **politiku privatnosti** tj. dokument kojim javno definiše svoj odnos prema privatnosti i ličnim podacima i obavještava građane o njihovim pravima. Međutim, propisi sadrže detaljna pravila u vezi sa time o čemu sve rukovaoci moraju da obavijeste lica čije podatke obrađuju. Praksa je pokazala da je politika privatnosti način da se ispuni obaveza obavještavanja. Za većinu medija prisutnih na internetu, dostupnost ovakvog dokumenta je stvar dobre prakse i već uspostavljenih standarda.

Novinarski izuzetak

Novi režim zaštite ličnih podataka tretira slobodu izražavanja i informisanja kao poseban slučaj obrade za koji važe nešto drugačija pravila. Obrada podataka o ličnosti, u ovom kontekstu, načelno je izuzeta od primjene određenih odredbi zakona koji se tiču principa obrade, prava građana i obaveza rukovalaca i obrađivača – pod uslovom da je u konkretnom slučaju to neophodno. Ovakva regulativa je potrebna da bi se u praksi izmirio sukob između dva fundamentalna prava: slobode izražavanja i informisanja s jedne, i prava na privatnost s druge strane. Svaki put kada ovaj sukob pretegne u korist slobode govora i interesa javnosti, novinarsko istraživanje i objavljivanje informacija u medijima biće oslobođeno obaveza zaštite ličnih podataka. Sa stanovišta primjene zakona koji štite lične podatke, ovakvo rješenje se obično naziva „novinarski izuzetak".

Konkretni slučajevi u kojima je moguće osloniti se na novinarski izuzetak tek će biti testirani u praksi, uglavnom po uzoru na primjenu GDPR-a zbog njegovog značaja u evropskom pravnom prostoru. Ipak, već je moguće predvidjeti potencijalne sukobe između zaštite podataka o ličnosti i samog novinarskog čina. Nedoumice i rizici

u primjeni izuzetka ogledaju se u tumačenju pojmova kao što su novinarstvo, novinar, mediji, javni interes i tome slično.

U tom smislu, osnovno i početno pitanje jeste - kome je namijenjen novinarski izuzetak? Pitanja poput onih ko je novinar, kakav sadržaj se može smatrati novinarstvom i šta je javni interes koji novinarstvo ispunjava - postaju sve važnija u kontekstu aktiviranja izuzetka u novinarske svrhe. Dakle, treba imati na umu da obrada ličnih podataka u ovom posebnom slučaju slobode izražavanja i informisanja ne znači blanko izuzetak za obradu podataka o ličnosti već, kako GDPR propisuje, samo ako su ova ograničenja neophodna da bi se pravo na zaštitu podataka o ličnosti uskladilo sa slobodom izražavanja i informisanja".

Medijskim organizacijama će, po pravilu, biti lakše da se oslone na izuzetak ako mogu da prikažu odgovarajuće interne politike i procedure, usklađivanje sa kodeksima i adekvatno vođenje baza podataka, dok sve to može biti veći izazov za novinarski rad u ličnom svojstvu (eng. freelancer) bez podrške medijske organizacije.

Prema praksi evropskih sudova, pojam "novinara" koji se može osloniti na novinarski izuzetak treba široko tumačiti, pri čemu je od ključne važnosti da li je u konkretnoj objavi svrha objave bila "objelodanjivanje informacije, mišljenja i ideja javnosti", kao što se može vidjeti u presudi Suda pravde Evropske unije u slučaju "Sergejs Buivids v. Datu valsts inspekcija" u kojoj je odlučeno da se ova pravila primjenjuju i na "jutjubere" kada su ispunjeni određeni uslovi.

U nedostatku konkretnijih smjernica na EU nivou, još uvijek su relevantne smjernice britanskog Povjereništva za primjenu stare evropske Direktive o zaštiti podataka koje daju konkretne prijedloge

za analizu novinarskog izuzetka koji se može razložiti na četiri elementa: (1) podaci se obrađuju samo za novinarstvo, umjetnost ili književnost, (2) sa ciljem objave određenog materijala, (3) uz razumno vjerovanje da je to objavljivanje u javnom interesu, i (4) uz razumno vjerovanje da usklađivanje nije kompatibilno sa novinarstvom.

Prikupljanje i obrada podataka o ličnosti je bitan dio novinarskog posla i, mada nova pravila podižu nivo zaštite ličnih podataka, položaj novinara koji poštuju pravne i profesionalne standarde ne bi trebalo značajno da se promijeni. Praktične implikacije može imati prenos tereta na novinare da utvrde da li legitimni interes javnosti prevazilazi pravo na privatnost, posebno u kontekstu istraživačkog novinarstva. Takođe postoji opasnost da se pravila o zaštiti podataka o ličnosti zloupotrebe u cilju represije nad "nepodobnim" medijima. Ipak, s obzirom na to da je ovaj problem već prepoznat, važno je zakonsko utemeljenje novinarskog izuzetka na osnovu kojeg novinari mogu da se suprotstave takvim praksama. U tom kontekstu, iako važeći crnogorski Zakon o zaštiti podataka o ličnosti u tekstu ne prepoznaje novinarski izuzetak kao takav, prema najavama da će GDPR pravila uskoro biti implementirana u domaći pravni sistem očekuje se da i ovo pitanje bude riješeno na odgovarajući način.

Evidencije radnji obrade koje su karakteristične za medije

U situacijama kada mediji i novinari moraju da primjenjuju zakone o zaštiti podataka o ličnosti, oni će imati status rukovaoca podacima i u tom svojstvu moraju da poštuju pravila koja se odnose na rukovaoce. Ipak, u okviru djelatnosti medija postoje određeni procesi obrade koji su karakteristični i specifični, i za koje će važiti slična pravila i sektorski standardi.

- S obzirom na to da su granice novinarskog izuzetka još uvijek nejasne, od značaja je pitanje u kojem su režimu lični **podaci o medijskim izvorima**, odnosno da li za njihovo prikupljanje, korišćenje i čuvanje važe sva pravila kao i za obradu drugih ličnih podataka. Kratak odgovor bi mogao da glasi: da, u velikoj mjeri. Suštinski, u odnosu na ove podatke medijska organizacija ima status rukovaoca, jer ona sama određuje za koje svrhe se mogu koristiti podaci o izvorima, koji se podaci prikupljaju, koliko dugo se čuvaju i na koji način se obezbjeđuje njihova sigurnost i povjerljivost. Kako bi poštovala propise o zaštiti ličnih podataka, medijska organizacija bi svojim internim pravilima trebalo da utvrdi sve svrhe za koje će koristiti podatke o izvorima, te da odredi odgovarajuće pravne osnove, vrstu i obim podataka koje prikuplja, kao i rokove čuvanja. Takođe, ukoliko smatra da se na ove podatke primjenjuje novinarski izuzetak - medijska organizacija bi to pitanje trebalo unaprijed da razmotri i analizira, te da interno predvidi pravila koja taj izuzetak mogu da opravdaju.
- Zakoni po pravilu ne propisuju obavezu rukovalaca da imaju **politike privatnosti**, odnosno dokument kojim organizacija javno definiše svoj odnos prema privatnosti i ličnim podacima. Pokazalo se da ovakav dokument predstavlja dobar način da se ispune obaveze transparentnosti i obavještavanja lica čiji se podaci obrađuju. Za korisnike onlajn medija, politika privatnosti dostupna na sajtu biće znak poštovanja uspostavljenih standarda.
- Prihodi onlajn medija se najčešće ostvaruju putem **targetiranja korisnika uz pomoć kolačića, odnosno trekera**. Onlajn mediji koriste ove alate da bi mjerili posjetu svojim sajtovima i pratili ponašanje posetilaca, za potrebe

analize internet saobraćaja, ali i za potrebe marketinga. Ipak, kolačići i trekeri koje korisnici pokupe prilikom čitanja onlajn medija dio su tehnologije koja podrazumijeva prikupljanje i obradu podataka o ličnosti. Stoga je važna potpuna transparentnost i po ovom pitanju, obično u okviru politike privatnosti ili posebne politike o kolačićima. S obzirom na to da je u pitanju tematika koja prosječnom korisniku može biti nejasna, medijska organizacija treba da posveti posebnu pažnju da pruži relevantne informacije o tehnologijama praćenja i korišćenoj analitici na jednostavan i lako razumljiv način. Takođe, ukoliko se na sajtu nalaze kolačići trećih strana, medijska organizacija bi trebalo da ima regulisan odnos sa svakom od njih.

- Pojedini mediji ostvaruju svoje prihode kroz **donacije direktno od čitalaca**. Vrsta podataka o ličnosti koja se prikuplja od čitalaca-donatora u velikoj mjeri će biti uslovljena zakonskim obavezama koje rukovaoci imaju prema računovodstvenim, poreskim ili deviznim propisima. Međutim, ukoliko prikupljanje ličnih podataka nije utemeljeno na zakonskoj regulativi, već rukovalac prikuplja dodatne lične podatke za svoje druge svrhe, na primjer statističke, analitičke ili marketinške, tada je potrebno da rukovalac za tu obradu pribavi drugi pravni osnov, što će po pravilu biti pristanak ili legitimni interes.
- Određeni mediji su kao svoj glavni biznis model odabrali pretplatu, koja se sprovodi u različitim modalitetima. Ovo podrazumijeva da se čitaoci u određenim okolnostima moraju registrovati i platiti za sadržaje koji na drugi način nisu dostupni. Tako mediji stvaraju **baze preplatnika** na koje se primjenjuju propisi o ličnim podacima sadržanim u tim bazama. Bez obzira na modalitet, pretplata znači da nastaje ugovorni odnos između medija i čitalaca - pretplatnika. Podaci

koji su potrebni za izvršenje ovog ugovora sa pretplatnikom će se uglavnom smatrati njegovim ličnim podacima, dok će pravni osnov za njihovu obradu biti izvršenje ugovora. Ukoliko će se podaci koristiti i za druge svrhe, potrebno je odrediti da li ta druga svrha podrazumijeva i traženje odgovarajućeg pristanka, na primjer za sprovođenje raznih anketa.

- Jedan od načina komunikacije sa postojećim i potencijalnim čitaocima može biti i putem **direktnog oglašavanja** koje, umjesto na široku publiku, usmjerava promotivnu poruku direktno na pojedinca - mejlom, konvencionalnom poštom, SMS porukama, telefonskim pozivima, itd. Pravni osnov je glavno pitanje za rukovaoce koji koriste direktan marketing, a u igri su najčešće pristanak ili legitimni interes. Na osnovu dosadašnje prakse čini se da preovlađuje stav da je slanje poruka sa reklamno-propagandnim oglasima radi sticanja novih korisnika moguće samo ako su korisnici pristali da primaju takve poruke. Međutim, ukoliko se promotivne poruke šalju već postojećim korisnicima, a sadržaj poruke je relevantan za odnos koji je sa njima već uspostavljen, onda je moguće koristiti kontakte korisnika za ovaj vid komunikacije i po osnovu legitimnog interesa. Ustanovljena praksa za komunikaciju mejlom jeste da se u svakoj poruci nalazi link ka stranici na kojoj korisnik može da povuče svoj pristanak (*unsubscribe link*).
- Značaj razumijevanja pravila o zaštiti ličnih podataka dolazi do izražaja u situacijama kada novinari u svom poslu koriste **velike baze podataka**, odnosno podatke iz javno dostupnih baza. Zakon štiti i takve lične podatke, te je bitno razumjeti obaveze i mjere koje novinari moraju preuzeti kada rukuju javnim i velikim bazama podataka. Obilje informacija u velikim bazama predstavlja ozbiljan izazov

za novinare prilikom razlikovanja podataka potrebnih za istraživanje i svih ostalih. Nerelevantni podaci osoba koje su predmet istraživanja ili podaci osoba koje nisu obuhvaćene istraživanjem, neće obezbjediti pravni osnov za obradu. S takvim podacima treba biti obazriv i oni se ne smiju koristiti, dijeliti, ostavljati nezaštićenim, i tome slično. Takođe, važno je podsjetiti da novinarski izuzetak pokriva samo podatke koji su deo konkretnog novinarskog zadatka. Posle objavljivanja, sirovi podaci se brišu ili anonimizuju. Za dalju obradu, kao što je čuvanje u arhivama, potreban je poseban pravni osnov.

- U principu, na podatke **zapošljenih u medijima** primjenjuju se ista pravila kao i na bilo koju drugu kategoriju lica.

Uvod u OSINT

Obavještajni rad sa otvorenim izvorima, OSINT je akronim za "Open Source Intelligence" što se definiše kao "pretraga, prikupljanje, analiza i korišćenje javno dostupnih i otvorenih podataka". Pored istraživačkih novinara, OSINT tehnike koriste i obavještajne službe, privatne detektivske agencije, hakeri, biznis analitičari, kao i analitičari u mirovnim operacijama Ujedinjenih nacija.

U doba prije digitalizacije, izvori javno dostupnih podataka su uglavnom bili tradicionalni mediji, arhive i javne evidencije državnih institucija. Danas živimo u svijetu prezasićenom digitalizovanim informacijama, u kojem se neprestano stvaraju, prenose i skladište ogromne količine podataka. Sve je više ličnih, tuđih, prisvojenih, izgubljenih, zaturenih,

procurjelih i zaboravljenih datoteka različitih tipova, sadržaja, veličina, namjena i primjena. Tako je za svako ozbiljnije saznanje, analizu i razumijevanje informacija, navigacija postala presudna veština za opstanak u prostranstvima jedinica i nula.

Bilo da je cilj stići do izvora nekog problema, otkriti zloupotrebu ovlašćenja ili pronaći smisao u istrazi, OSINT je značajan proces u radu svakog novinara, istraživača, aktiviste, uzbunjivača ili zabrinutog građanina koji samostalno želi da dođe do važnih informacija.

Etička pitanja

Prikupljanje i korišćenje podataka uvijek povlače različita pravna i etička pitanja. Šta treba raditi sa slučajnim otkrićima koja bi mogla da naude svedocima? Da li je objavljivanje informacija proporcionalno, da li zaista koristi javnom interesu? Bez obzira na to da li se legitimno pristupa samo dostupnim podacima iz otvorenih izvora, česte su sporne situacije u "sivoj zoni":

- upotreba lažnih naloga na društvenim mrežama je često prekršaj njihovih pravila, ali se koriste zbog zaštite privatnosti;
- korišćenje "procurjelih" podataka koji su u nekom trenutku ukradeni;
- napredna pretraga omogućava pristup nezaštićenim sistemima ili uređajima sa fabričkom šifrom za pristup, što tehnički nije neovlašćeni pristup, ali nije ni ovlašćen.

Pristup velikim količinama podataka povlači i veliku odgovornost. Tehnike pretrage mogu da unaprijede istraživački rad, ali mogu i da vode u zloupotrebe i ugroze tuđu privatnost. Stoga je važno

razumjeti kontekst na koji se podaci odnose i voditi se osnovnim principima novinarske etike.

Priprema i bezbjednost

Prije upotrebe većine OSINT alata i tehnika, potrebno je preduzeti određene mjere bezbjednosti i pripremiti sistem za rad. Istraživanje otvorenih izvora podrazumijeva daleko više aktivnosti nego što je uobičajeno. Osim ostavljanja digitalnog otiska i ličnih tragova intenzivnom navigacijom na internetu, otvaranje različitih vrsta datoteka i dokumenata nepoznatog porijekla povlači rizik od inficiranja sistema malverom koji može da prouzrokuje katastrofalne posljedice. To se podjednako odnosi na slučajne incidente koliko i na veoma česte slučajeve namjernog targetiranja istraživačkih novinara.

Kompartmentalizacija

Jedna od najvažnijih mjera je kompartmentalizacija, tj. odvajanje sistema za istraživanje od privatnog sistema za ličnu upotrebu. Ovde se, prije svega, misli na korišćenje posebnog računara za istraživačke djelatnosti sa kojeg će se izvoziti samo relevantni nalazi na druge računare ili sisteme u okviru organizacije. Ako je kompjuter inficiran, sistem se formatira i ponovo instalira uz minimizaciju štete.

U slučaju da ne postoje materijalni resursi za ovakvo rješenje, softversku kompartmentalizaciju je moguće izvesti na još dva načina:

Podešavanjem "virtualizacije" – instalacije posebnog operativnog sistema u okruženju odvojenom od osnovnog operativnog sistema. Popularan besplatni softver otvorenog koda za virtualizaciju je VirtualBox.
Upotrebom prenosnog operativnog sistema koji se pokreće sa

eksterne memorije (USB flash, SD kartica etc.) i radi nezavisno od osnovnog. Primjer ovakvog sistema je Tails.

Osim razdvajanja sistema za rad, kompartmentalizacija u istraživačkom radu uključuje i otvaranje namjenskih email adresa za registraciju na potrebne servise, i eventualnu registraciju pseudo-naloga na društvenim mrežama koji ni na koj način ne smiju da se povezuju sa privatnim. Za elektronsku poštu se trenutno preporučuju besplatni servisi ProtonMail i Tutanota, a zanimljiv servis za generisanje profilne slike nepostojećih ljudi je thispersondoesnotexist.com. Takođe, u nekim slučajevima će biti potrebna i neregistrovana prepaid SIM kartica.

Anonimnost

U većini slučajeva je napredna pretraga putem pretraživača slobodna. Međutim, pristup određenim adresama i dokumentima bi mogao da bude protivzakonit ili sumnjiv. Sav saobraćaj na internetu i upite pretrage bilježe pretraživači, internet provajderi, pa i obavještajne agencije, a potom ih i čuvaju na neodređeno vrijeme. Te informacije je moguće povezati sa identitetom i kasnije iskoristiti protiv osobe koja je pristupala spornim sadržajima.

TOR

Jedan od najsigurnijih načina za maskiranje internet saobraćaja i zaštitu identiteta tokom onlajn pretrage je servis za anonimnu komunikaciju Tor. Za razliku od popularnih programa kao što su Firefox i Chrome, Tor sav saobraćaj šalje kroz volontersku mrežu sastavljenu od više hiljada tačaka, čime lokacija postaje nedostupna onome ko nadgleda mrežu ili kontroliše saobraćaj. Tor enkriptuje

originalne podatke, uključujući i IP adresu, i šalje ih kroz virtuelno kolo koje obuhvata uzastopne, slučajno izabrane Tor etape.

Upotreba Tor-a je vremenom postala sve jednostavnija, ali su istovremeno i pojedini servisi počeli da traže CAPTCHA potvrdu zbog velike količine automatizovanih pretraga, što ponekad može da oteža i uspori procese. Takođe, neke od zemalja obilježavaju korišćenje Tor pregledača kao sumnjivu aktivnost, što ne spriječava anonimizaciju saobraćaja, ali ni utvrđivanje činjenice da se sajtovima i pretrazi pristupa kroz Tor mrežu.

VPN

Ako iz nekog razloga nije moguće koristiti Tor, alternativna ali i manje sigurna opcija je upotreba VPN (Virtual Private Network) servisa. Virtuelne privatne mreže prerušavaju IP adresu korisnika u drugu IP adresu koju posjeduje VPN provajder. Najveći problem kod ovih servisa je transparentnost, jer su to mahom privatne kompanije koje mogu da tvrde da čuvaju identitet korisnika, ali je to veoma teško dokazati.

Tehnike i alati

Dorkovanje i operatori (napredna pretraga)

Tokom istrage često postoji potreba da se prikupi što više informacija na određenu temu. Napredne tehnike pretrage na internetu mogu pomoći da se otkriju datoteke ili tragovi relevantni za pitanja na koje se traže odgovori. Primjera radi, to mogu biti poreski izvještaji ili troškovnici i budžeti lokalnih samouprava, informacije koje nisu vidljive na njihovim stranicama/prezentacijama, ili ne izlaze kao rezultati obične internet pretrage.

Dodatno, poznata i kao "Google hacking", Gugl dorkovanje je tehnika definisana 2002. godine, a koriste je redakcije, istraživačke organizacije, bezbjednosni revizori i tehnološki pismeni kriminalci (sajber-kriminalci) šaljući njome upite pretraživačima da bi pronašli neotkrivene informacije ili sigurnosne propuste i ranjivosti sistema. Ovu tehniku je moguće koristiti na većini pretraživača, pa je zato danas zovemo samo "dorkovanje".

Dorking praktično znači korišćenje pretraživača u njihovom punom potencijalu kako bi se otkrili rezultati koji nisu vidljivi uobičajenom pretragom. Ona omogućava da se finijom pretragom zaroni dublje u veb stranice i dokumenta dostupna onlajn. Za to nije potrebna sofisticirana oprema, softver ili posebno tehničko znanje, već se svodi na razumijevanje nekoliko ključnih riječi/parametara i simbola koji se koriste kao "operatori" i "filteri" za preciznije rezultate pretrage. Za efikasnost je, doduše, ponekad potrebno i malo upornosti, kreativnosti, strpljenja i sreće.

Uobičajena internet pretraga se oslanja na semantički način traženja informacija, tj. unošenjem direktnog pitanja ("Koliki je budžet Crne Gore?") ili biranjem ključnih reči ("Crna Gora budžet"). S druge strane, napredna pretraga bi precizirala taj upit kombinovanjem tehničkih i semantičkih elemenata kako bi se iskoristila prednost činjenice da se sadržaj na mreži konstantno očitava i indeksira mašinski. Tehničke elemente koji su u službi dodatnih filtera u ovoj tehnici nazivamo "operatorima".

Operator	Primjer	Opis
site:	auto-put mateševo site:vijesti.me	Prikazuje sve stranice na kojima se pominju zadate riječi u okviru definisanog sajta (vijesti.me)
filetype:	filetype:pdf site:mif.gov.me	Pretraga određenih tipova datoteka. Primjer prikazuje sve pdf dokumente indeksirane na sajtu Ministarstva finansija.
OR	site:gov.me budžet filetype:xls OR filetype:pdf	Širi pretragu na rezultate koji imaju jedan ili više zadatih upita. Primjer prikazuje sve Excel i pdf dokumente na domenu i pod-domenima Vlade Crne Gore.
AND	site:gov.me budžet AND 2020 filetype:xls OR filetype:pdf	Sužava pretragu prikazujući samo rezultate koji imaju obje (ili više) ključnih reči definisanih upitom. Primjer isključuje dokumenta budžeta pre 2020. godine.
cache:	cache:niksic.me	Prikazuje posljednju sačuvanu (keširanu) verziju sajta od strane pretraživača.
“ ”	"Službeni list CG br.21/09 i 40/11"	Pretraga tačno definisanog upita između navodnika isključuje ostale kombinacije zadatih pojmova.
-	budžet crne gore -zakon	Znak minus isključuje rezultate koji sadrže drugu (ili više) određenih reči.

Metapodaci, slike i lokacije

Sve digitalne datoteke, dokumenti, fotografije, muzika, mejlovi i drugi fajlovi osim svog osnovnog sadržaja imaju i svoje metapodatke, tj "podatke o podacima". Kod tekstualnih dokumenata to su, na primjer, vrijeme kreiranja i posljednje izmene, njegova veličina, zatim vlasništvo tj. autor koji je napravio dokument, itd. Originalne fotografije sa sobom često nose i podatke o lokaciji gde su napravljene, tako da metapodaci ponekad daju presudne informacije za utvrđivanje činjenica i otkrivanje detalja tokom istraživanja.

Međutim, postavljanjem fotografija na društvene mreže se briše većina metapodataka, pa je za provjeru izvora, vjerodostojnosti ili dodatne informacije potrebno pokušati tehnikama poput obrnute pretrage fotografija. Svi veći pretraživači imaju ovu opciju, a dovoljno je kopirati adresu fotografije na internetu ili je otpremiti sa računara. Gugl trenutno ima najveći broj opcija za analizu, Jandeks je često bolji u prepoznavanju lokacija, a ponekad vrijedi probati i druge servise kao što su Bing ili *TinEye*.

Za provjeru i utvrđivanje lokacija se koristi kombinacija mapa, uličnih i satelitskih snimaka, a pored popularnog *Google Maps* servisa koji nudi priličan broj opcija i nekoliko slojeva prikaza, postoji još nekoliko alata koji mogu da budu od koristi u specifičnim slučajevima. Desktop aplikacija servisa *Google Earth* nudi pregled satelitskih snimaka kroz vrijeme, a servis *DualMaps* olakšava prostornu navigaciju prikazujući mapu, satelitski snimak i uličnu perspektivu zadate lokacije istovremeno. Takođe, volonterski servis *OpenStreetmap* sadrži mnoge informacije koje su unosili sami građani, a kojima kompanije često nemaju pristup, što ih čini važnim faktorom u diversifikaciji prikupljenih podataka.

Istorija interneta i arhiviranje

Dva su razloga zbog kojih je arhiviranje interneta za novinare i istraživače od presudne važnosti:

1. Kada se pretragom stigne do linkova koji ne rade, stranica koje su promijenjene ili čitavih veb prezentacija koje više ne postoje.
2. Kada se pretragom stigne do stranica ili informacija koje su vrijedne, ali bi iz različitih razloga mogle da postanu nedostupne.

U prvom slučaju bi bilo idealno vratiti se kroz vrijeme i preuzeti kopiju stranice pre nego što joj se nešto desilo. U drugom slučaju bi bilo pametno arhivirati ih na vrijeme i spriječiti takav scenario.

Jedan od impresivnijih kulturnih poduhvata savremenog društva je *Internet Archive*, najveća onlajn biblioteka multimedijalnih sadržaja. Njen servis *Wayback Machine* funkcioniše kao digitalna vremenska kapsula i nudi upravo to – pristup velikom broju stranica kroz vrijeme i arhiviranje trenutno dostupnih sadržaja za buduće potrebe.

Uz pomoć automatizovanih procesa, *Wayback Machine* može da pristupi i arhivira praktično svaki javni vebsajt. Ipak, ne postoje definisani obrasci po kojima algoritam odlučuje koje adrese posjećuje i koliko to često radi zbog ograničenih resursa i drugih faktora koji na to utiču. Zbog toga nije uvijek moguće pronaći arhiviranu verziju nekog sadržaja baš određenog datuma, ali bez obzira na to, arhiva raspolaže neizmjernom količinom podataka koji su često nezamjenljiv resurs za istraživanje.

Pored jednostavnog pristupa arhivama, ovaj servis dozvoljava i ručno čuvanje specifičnih stranica u određeno vrijeme kojima posle i drugi mogu da pristupaju. Ovaj proces je važan jer dodaje element neutralnosti i povjerenja pri upućivanju na izvore informacija u poređenju sa stranicama i kopijama dokumenata sačuvanih na ličnim uređajima.

Druge tehnike i resursi

OSINT podrazumijeva još puno tehnika i alata koje mogu biti korisne za različite vrste istraživanja. Informacije o pojedincima, kompanijama, organizacijama, projektima, važnim lokalnim i globalnim događajima su sveprisutne, a osim nama poznatog "površinskog" interneta, moguće ih je tražiti i mnogo dublje, u daljim i mračnijim prostranstvima digitalne sfere. Za dalje istraživanje ovih tehnika i alata preporučujemo uputstva Exposing The Invisible Kit i Open Source Intelligence - Navigator for investigative journalists u čijem su pisanju učestvovali i autori ovog priručnika.


i
t
v
A


m
e
d
1
w