VODIČ:

ZAŠTITA TAJNOSTI IZVORA INFORMA-CIJA

PRAVNI I TEHNIČKI ASPEKTI

SHARE FOUNDATION - 2015

vodič

"ZAŠTITA TAJNOSTI IZVORA INFORMACIJA - PRAVNI I TEHNIČKI ASPEKTI"
SHARE FONDACIJA
OKTOBAR 2015
UREDNICI: ĐORĐE KRIVOKAPIĆ, VLADAN JOLER
TEKSTOVI: NEVENA KRIVOKAPIĆ, BOJAN PERKOV, ANDREJ PETROVSKI
LEKTURA: MILICA JOVANOVIĆ
DIZAJN I PRELOM: OLIVIA SOLIS VILLAVERDE

ŠTAMPARIJA: NS PRESS DOO NOVI SAD
TIRAŽ : 200

PODRŠKA PROJEKTU:

CIVIL RIGHTS DEFENDERS

CIP - Каталогизација у публикацији
Библиотека Матице српске, Нови Сад
316.774:351.083.8(497.11)(036)
КРИВОКАПИЋ, Невена
Zaštita tajnosti izvora informacija - pravni i tehnički aspekti : vodič / [tekstovi Nevena Krivokapić, Bojan Perkov, Andrej Petrovski]. - Novi Sad : Share foundation, 2015 (Novi Sad : NS press). - 45 str. : ilustr. ; 16 cm

Tiraž 200.
ISBN 978-86-89487-05-3
1. Перков, Бојан [аутор] 2. Петровски, Андреј [аутор]
a) Медији - Извори информација - Заштита - Србија - Водичи
COBISS.SR-ID 302376967

ATTRIBUTION-SHAREALIKE CC BY-SA
This license lets others remix, tweak, and build upon your work even for commercial purposes, as long as they credit you and license their new creations under the identical terms. This license is often compared to "copyleft" free and open source software licenses. All new works based on yours will carry the same license, so any derivatives will also allow commercial use. This is the license used by Wikipedia, and is recommended for materials that would benefit from incorporating content from Wikipedia and similarly licensed projects.

UVOD

Profesionalno, odgovorno i etičko novinarstvo počiva na prikupljanju informacija od nezavisnih i kompetentnih izvora, kako bi novinari na istinit, nepristrasan i pošten način informisali građane o tekućim događajima. Kao jedna od tekovina medijskih sloboda, novinarima je na raspolaganju pravo da zaštite identitet svojih izvora, tj. da objavljuju informacije koje potiču od izvora koji iz određenih razloga žele da ostanu anonimni. Pozivanje na anonimne izvore je od ključnog značaja za izveštavanja o pitanjima od javnog interesa, sa kojima javnost na drugi način ne bi mogla da bude upoznata. Neke od najvećih afera u istoriji novinarstva (npr. afera "Votergejt" u SAD) otkrivene su upravo zahvaljujući saznanjima dobijenim od anonimnih izvora. Ipak, kako izmišljanje i zloupotreba anonimnih izvora predstavljaju grube prekršaje profesionalnih i etičkih standarda, u ovom vodiču ćemo pokušati da odgovorimo na najčešće nedoumice u vezi sa pravom na zaštitu anonimnosti izvora, kroz razmatranje propisa, preporuka, međunarodnih standarda i sudske prakse.

U eri digitalnih komunikacija, informisanje javnosti više nije rezervisano samo za novinare tradicionalnih medijskih organizacija - brojne internet platforme, poput blogova, foruma, društvenih mreža i nezavisnih onlajn portala, omogućavaju građanima da i oni izveste javnost o određenim društvenim pojavama i problemima. Pošto se može reći da na određeni način imaju ulogu sličnu novinarima, da li u određenim slučajevima treba da uživaju i prava koja imaju profesionalni novinari, npr. da zaštite svoje izvore? Debata o definisanju novinara u Srbiji je ponovo aktuelna[1], pa ćemo jedan deo vodiča posvetiti i razmatranju ove teme.

Na kraju ćemo se posvetiti merama tehničke zaštite koje preporučujemo novinarima i istraživačima za bezbedan prijem poverljivih informacija od izvora koji žele da ostanu anonimni, naročito ako je reč o uzbunjivačima. Govorićemo o uzbunjivačima u širem smislu, a ne samo u kontekstu domaćeg Zakona o zaštiti uzbunjivača. Saradnja novinara i uzbunjivača je od ključnog značaja za ukazivanje na zloupotrebe i demokratsku kontrolu rada državnih institucija. Uzbunjivači obično trpe različite vidove sankcija, od otkaza na poslu do krivičnog gonjenja, te je stoga važno da njihov identitet ostane poznat samo novinarima i urednicima sa kojima žele da sarađuju. SHARE Fondacija je stoga razvila DataLeaks.rs, sigurnu platformu za uzbunjivanje koja je jednostavna za korišćenje i garantuje da će osoba koja dostavlja informacije ostati anonimna.

1 http://www.mc.rs/licencama-u-zastitu-profesije.6.html?eventId=19123

ZAŠTITA NOVINAR-SKIH IZVORA U REPUBLICI SRBIJI

ZAKONSKE OSNOVE ZA ZAŠTITU IZVORA

Ukoliko ne žele da otkriju izvor informacije, novinari mogu da se pozovu na član 52 (Novinarska tajna) Zakona o javnom informisanju i medijima, u kome se jasno navodi:

"Novinar nije dužan da otkrije izvor informacije, osim podataka koji se odnose na krivično delo, odnosno učinioca krivičnog dela za koje je kao kazna propisan zatvor u trajanju od najmanje pet godina, ako se podaci za to krivično delo ne mogu pribaviti na drugi način."

Dakle, novinar ima zakonsku obavezu da otkrije identitet svog izvora informacije samo u slučaju da je reč o podacima koji se odnose na krivična dela za koja je zaprećena kazna zatvora od najmanje pet godina, odnosno na učinioce tih krivičnih dela. Prema odredbama Krivičnog zakonika Republike Srbije, to su uglavnom teži, kvalifikovani oblici krivičnih dela: ubistvo, zatim otmica, prinuda, iznuda ili ucena izvršena od strane organizovane kriminalne grupe, kao i oružana pobuna, ratni zločin protiv civilnog stanovništva, genocid itd. Dodatni uslov koji mora da bude ispunjen jeste da se podaci o određenom krivičnom delu ne mogu pribaviti na drugi način, osim da novinar otkrije svoje izvore informacija.

Zaštitu novinarima, ali i urednicima, izdavačima, štamparima i proizvođačima, pruža član 41 (Zaštita izvora informacija) Krivičnog zakonika, tako da se oni "neće smatrati izvršiocem krivičnog dela zbog toga što sudu ili drugom nadležnom organu nisu otkrili identitet autora informacije ili izvor informacije, osim u slučaju da je učinjeno krivično delo za koje je kao najmanja mera kazne propisan zatvor u trajanju od pet ili više godina, ili je to neophodno da bi se izvršenje takvog krivičnog dela sprečilo." Važno je napomenuti da se novinari i urednici, ali i drugi koji su uključeni u poslove javnog informisanja, poput izdavača, ne mogu krivično goniti ukoliko ne žele da

otkriju autore ili izvore informacija, izuzev ako je reč o pomenutim krivičnim delima.

Kao što se može videti iz navedenog, uslovi su identični u Zakonu o javnom informisanju i medijima i Krivičnom zakoniku, što bi značilo da samo pod izuzetnim okolnostima može doći do toga da novinar bude dužan da sudu ili drugom nadležnom organu otkrije izvor informacije.

PRAKSA, ETIČKI STANDARDI I ISKUSTVA DRUGIH ZEMALJA

U Srbiji, jedan od poznatijih slučajeva pritiska državnih organa na novinare da otkriju izvore informacija odigrao se 2011. godine, kada je Osnovno javno tužilaštvo u Novom Sadu podiglo optužnicu protiv novinarke i urednika lista "Nacionalni građanski" zbog objavljivanja teksta "Državni organi potpuno nespremni za rat". Novinarki Jeleni Spasić i uredniku Miloradu Bojoviću stavljeno je na teret da su ugrozili bezbednost Srbije otkrivanjem informacija iz strogo poverljivog dokumenta Ministarstva odbrane, kao i da nadležnim organima nisu otkrili identitet osobe koja im je dostavila izveštaj. Nedugo po podizanju optužnice, dok nije stupila na pravnu snagu, tužilaštvo je proširilo istragu na nepoznata službena lica, za koja se sumnjalo da su odala državnu tajnu. Prema rečima novinarke Spasić iz oktobra 2015, "do danas nije dobila dokument sa odlukom tužilaštva da odustaje od krivičnog gonjenja".[2]

Etički standardi profesije sadržani u Kodeksu novinara Srbije predviđaju da su novinari dužni da poštuju anonimnost izvora, ukoliko to izvor od njih traži. Izmišljanje anonimnih izvora prema Kodeksu predstavlja težak prekršaj standarda profesionalnog postupanja novinara. Kao preporuka se navodi da se korišćenje anonimnih izvora generalno ne preporučuje i da se na njih treba pozivati samo ukoliko ne postoje drugi načini da se saznaju informacije od značaja za javnost. Takođe, obaveza urednika je da sa novinarom proveri opravdanost pozivanja na anonimne izvore, te je iz tog razloga neophodno da bar jedan urednik zna i štiti identitet anonimnog izvora. Ukoliko izvor ne pristaje da novinar otkrije njegov identitet uredniku, takav zahtev izvora treba odbiti. U slučaju da novinar uredniku u mediju u kome je zaposlen, ne želi da otkrije identitet izvora, urednik može da donese odluku da ne objavi informaciju koja je dobijena od njemu nepoznatog izvora - takav postupak se prema Kodeksu novinara ne smatra cenzurom.[3]

Zaštita novinarskih izvora u okruženju postoji u medijskim zakonima kao standard, sa različitim manjim odstupanjima. Zanimljivo je da su u Makedoniji i Hrvatskoj novinari obavezani zakonom da pre objavljivanja obaveste urednike da je informacija potekla od neimenovanog izvora. Na Kosovu je usvojen poseban Zakon o zaštiti novinarskih izvora, koji reguliše pravo novinara da zaštite svoje izvore. Prema članu 8, ako se odluče da se pozovu na pravo da ne otkriju svoje izvore informacija, novinari i drugi medijski profesionalci ne mogu biti krivično gonjeni za korišćenje dokumenata i materijala koje su treća lica pribavila na nezakonit način.[4]

ZAŠTITA TAJNOSTI SREDSTAVA KOMUNIKACIJE

U ovom delu skrećemo pažnju na zakonske odredbe koje štite građane Srbije, pa samim tim i novinare, od neovlašćenog presretanja elektronskih komunikacija, odnosno prisluškivanja. Tajnost sredstava komunikacije je zagarantovana članom 41 Ustava Republike Srbije, a odstupanja su dozvoljena isključivo na osnovu sudske odluke, na određeno vreme i za potrebe vođenja krivičnog postupka ili zaštite nacionalne bezbednosti. Krivični zakonik u dva člana (čl. 142 - Povreda tajnosti pisama i drugih pošiljki i čl. 143 - Neovlašćeno snimanje i prisluškivanje) propisuje novčane i

2 O ovom slučaju možete da pročitate više na sledećim linkovima: A. Petrović, "Uzbunjivači moraju da budu zaštićeni od odmazde", Politika Online: http://www.politika.rs/sr/clanak/341436/Drustvo/Uzbunjivaci-moraju-da-budu-zasticeni-od-odmazde i T. Tagirov, "Poroci tajni, vrline javne", Vreme br. 1086: http://www.vreme.com/cms/view.php?id=1016693

3 Videti Kodeks novinara Srbije, poglavlje VI - Odnos prema izvorima informisanja, dostupno na: http://www.savetzastampu.rs/doc/Kodeks _ novinara _ Srbije.pdf

4 Kosovski zakon o zaštiti novinarskih izvora: http://www.kuvendikosoves.org/common/docs/ligjet/Law%20on%20the%20protection%20of%20the%20journalism%20sources.pdf

zatvorske kazne za povredu tajnosti komunikacije, uz strože sankcije ukoliko navedena krivična dela izvrši službeno lice u vršenju službe, npr. pripadnik policije ili bezbednosnih službi. Zaštita od povrede tajnosti komunikacije presudna je za novinare, koji svakodnevno dolaze do poverljivih informacija razgovarajući sa velikim brojem ljudi i razmenjujući informacije sa njima, među kojima su i izvori koji ne žele da se njihov identitet javno otkrije.

U presudi Evropskog suda za ljudska prava u slučaju Roman Zaharov protiv Rusije, iz decembra 2015. godine, konstatuje se da je nadzorom komunikacija glavnog urednika magazina o avijaciji, došlo do kršenja člana 8 Evropske konvencije o ljudskim pravima (pravo na poštovanje privatnog i porodičnog života). Slučaj se odnosi na tajni sistem prisluškivanja mobilne telefonije i komunikacija u Rusiji. Kršenje člana 8 se sastoji u tome da su operatori mobilne mreže dužni da po zakonu instaliraju opremu koja omogućava državnim službama da obavljaju pretrage aktivnosti i da bez dovoljno zakonskih garancija presreću i prisluškuju razgovore korisnika mobilnih mreža. Sud je utvrdio da Zaharov ima pravo da tvrdi da je žrtva kršenja Evropske konvencije o ljudskim pravima, iako nije mogao da dokaže da su njegovi razgovori praćeni i prisluškivani. Uzimajući u obzir da ne postoji dovoljan broj pravnih lekova i pošto se prisluškivanje odnosi na sve korisnike mobilnih mreža, sud je zaključio da Zaharov nije morao da dokaže da je čak bio u riziku od prisluškivanja razgovora. S obzirom da tajni nadzor može narušiti principe demokratije, sud je morao da se uveri da nije postojala adekvatna i efikasna garancija protiv zloupotrebe. Zaključak suda jeste da zakonske odredbe koje regulišu tajni nadzor ne obezbeđuju dovoljne garancije protiv zloupotrebe takvog sistema, te je utvrdio nedostatke u sledećim oblastima: okolnosti u kojima su nadležni organi ovlašćeni da koriste tajni nadzor, trajanje takvih mera, okolnosti u kojima treba da budu prekinute, i proces skladištenja i uništavanja podataka dobijenih iz tajnog nadzora. [5]

05 Evropski sud za ljudska prava, slučaj Roman Zaharov protiv Rusije, 4. decembar 2015. Dostupno na: http://hudoc.echr.coe.int/eng?i=001-159324

MEĐUNARODNI STANDARDI ZAŠTITE NOVINARSKIH IZVORA I SUDSKA PRAKSA

MEĐUNARODNI STANDARDI ZAŠTITE NOVINARSKIH IZVORA I SUDSKA PRAKSA

Kao jedan od najznačajnijih standarda novinarske profesije, zaštita identiteta izvora nalazi se u mnogim međunarodnim dokumentima i deklaracijama, potvrđena je i preporukama međunarodnih organizacija koje se bave zaštitom slobode izražavanja i medija i ima utemeljenje u presudama međunarodnih i nacionalnih sudova. U Rezoluciji o novinarskim slobodama i ljudskim pravima, donetoj na Evropskoj ministarskoj konferenciji o politici masovnih medija, u Pragu decembra 1994. godine, navodi se da "zaštita poverljivosti novinarskih izvora omogućava očuvanje i razvoj istinske demokratije."

Izveštaji o zaštiti novinarskih izvora međunarodne organizacije "Article 19", koja se bavi slobodom govora, takođe obrađuju teme otkrivanja i zaštite novinarskih izvora, kao i vidove zaštite koji su novinarima na raspolaganju. Nezavisno novinarstvo zavisi od slobodne razmene informacija između medija i građana. Pojedini građani (izvori) mogu da istupe sa tajnim ili veoma osetljivim informacijama, oslanjajući se na novinare da će ih proslediti široj javnosti radi obaveštavanja o pitanjima od javnog interesa.[7] "Media Legal Defence Initiative" (MLDI), organizacija koja se bavi pravnom zaštitom novinara, objašnjava da je u velikom broju slučajeva anonimnost preduslov za otkrivanje poverljivih informacija, zbog straha od ugrožavanja sigurnosti, slobode ili izvora prihoda. Upravo zbog toga novinari su dužni da garantuju anonimnost radi zaštite od pravnih rizika - u suprotnom, izvori im neće preneti informacije.[8] U ovim slučajevima, novinari bi trebalo da imaju pravo da odbiju zahtev za otkrivanje imena izvora i prirode informacije dobijene u poverenju. Bez garanci-

07 Article 19, Briefing Paper on Protection of Journalists' Sources: https://www.article19.org/data/files/pdfs/publications/right-to-protect-sources.pdf

08 Media Legal Defence Initiative (MLDI), Training manual on international and comparative media and freedom of expression law: http://www.mediadefence.org/news/mldi-publishes-manual-freedom-expression-law

je poverljivosti izvora, ugrožena je sama mogućnost otkrivanja informacija od javnog interesa, poput korupcije javnih funkcionera. Većina novinara je profesionalnim kodeksom obavezana da se suzdrži od odavanja poverljivih izvora, čak i u sudskim postupcima.[9]

Jedna od najvažnijih presuda povodom zaštite novinarskih izvora je presuda Evropskog suda za ljudska prava 1996. u slučaju Gudvin protiv Ujedinjenog Kraljevstva, na koju se oslanjaju brojne preporuke evropskog "mekog prava". U ovom slučaju, vezanom za objavljivanje poverljivih podataka o finansijskom statusu jedne kompanije, Evropski sud za ljudska prava je odlučio da je pokušaj da se novinar primora da otkrije svoj izvor, predstavljao kršenje člana 10 Evropske konvencije o ljudskim pravima. Iako je kompanija imala legitiman interes da identifikuje "nelojalnog" zaposlenog, prevagu nad ovom potrebom ipak je odnela sloboda štampe u demokratskom društvu.[10]

U ODLUCI EVROPSKOG SUDA NAGLAŠAVA SE:

"Zaštita novinarskih izvora jedan je od osnovnih uslova za slobodu štampe [...] Odsustvo takve zaštite moglo bi odvratiti izvore od pomaganja štampi da informiše javnost o stvarima od javnog interesa. Na taj način bi se narušila vitalna nadzorna uloga štampe, i ugrozili njeni kapaciteti za pružanje tačnih i pouzdanih informacija. Imajući u vidu značaj zaštite novinarskih izvora za slobodu štampe u demokratskom društvu, i moguće obeshrabrujuće dejstvo (chilling effect) koje bi naredba da se otkrije izvor imala na ostvarivanje te slobode, takva mera ne može biti u skladu sa članom 10 Konvencije, ukoliko nije opravdana pretežnijim zahtevom u interesu javnosti."[11]

Prema analizi organizacije "Article 19", u većini pravnih sistema "strana koja traži obelodanjivanje izvora će morati da pokaže da je odavanje tražene informacije od dovoljno velike važnosti da se opravda nalog za otkrivanje izvora, što znači da će sudovi morati da odmere posledice otkrivanja izvora po slobodu izražavanja."[12]

Pravo na zaštitu tajnosti izvora nije apsolutno, baš kao i većina ljudskih prava koja su zagarantovana međunarodnim konvencijama i nacionalnim propisima, tako da u određenim slučajevima ovo pravo može biti ograničeno u skladu sa tripartitnim testom za ograničenje prava na slobodu izražavanja. Ograničenja prava na slobodu izražavanja moraju biti:

- Propisana zakonom;
- Namenjena postizanju nekog od sledećih ciljeva: poštovanje prava i reputacije drugih, zaštita nacionalne bezbednosti, javnog reda, zdravlja ili morala;
- Neophodna za postizanje navedenog cilja, uključujući i to da ne postoji alternativna mera koja bi bila manje štetna po slobodu izražavanja. [13]

Principi Preporuke Saveta Evrope o pravu novinara da ne otkriju svoje izvore informacija (2000)[14] detaljno razrađuju tripartitni test koji se primenjuje prilikom zaštite izvora, posebno njegov deo o neophodnosti. Deklaracija o principima slobode izražavanja u Africi (2002)[15] se takođe oslanja na suštinske tačke navedene Preporuke Saveta Evrope. Kao najvažnije tačke u ovim dokumentima relevantna tumačenja izdvajaju:

- Novinaru se može naložiti da otkrije identitet izvora samo ukoliko postoji opravdan zahtev u interesu javnosti i kada su okolnosti od vitalne važnosti. U Preporuci Saveta Evrope se navodi da bi ovo mogao da bude slučaj samo ukoliko je otkrivanje izvora neophodno da bi se zaštitio ljudski život, sprečilo teško krivično delo, ili za odbranu osobe optužene da je počinila teško krivično delo;
- Uvek treba izbalansirati interes za otkrivanje izvora nasuprot negativnim posledicama naredbe za otkrivanje izvora po slobodu izražavanja;

09 Article 19, Briefing Paper on Protection of Journalists' Sources: https://www.article19.org/data/files/pdfs/publications/right-to-protect-sources.pdf

10 Media Legal Defence Initiative (MLDI), Training manual on international and comparative media and freedom of expression law: http://www.mediadefence.org/news/mldi-publishes-manual-freedom-expression-law

11 Evropski sud za ljudska prava, slučaj Gudvin protiv Ujedinjenog Kraljevstva, 27. mart 1996. Dostupno na: http://hudoc.echr.coe.int/eng?i=001-57974

12 Article 19, Briefing Paper on Protection of Journalists' Sources: https://www.article19.org/data/files/pdfs/publications/right-to-protect-sources.pdf

13 Više o tripartitinom testu i analiza organizacije Article 19 dostupni na: https://www.article19.org/pages/en/limitations.html

14 Preporuka Saveta Evrope: http://www.coe.int/t/dghl/standardsetting/media/doc/cm/rec(2000)007&expmem _ EN.asp

15 Deklaracija o principima slobode izražavanja u Africi: http://www.achpr.org/sessions/32nd/resolutions/62/

- Otkrivanje izvora može se naložiti samo po zahtevu pojedinaca ili organa koji imaju neposredan, legitiman interes, a koji su prethodno iscrpili sve razumne alternativne mere da zaštite taj interes;
- Isključivo sudovi bi trebalo da imaju ovlašćenje da narede otkrivanje izvora informacija;
- Sudovi ne bi smeli da nalože otkrivanje identiteta izvora u postupcima povodom povrede časti i ugleda;
- Otkrivanje identiteta izvora bi trebalo da bude ograničeno koliko je to moguće, npr. da se informacije o izvoru dostave samo osobama koje su tražile otkrivanje, a ne široj javnosti;
- Odluku o sankcijama protiv novinara koji su odbili da otkriju identitet izvora treba da donese samo nepristrasan sud nakon pravičnog suđenja, uz mogućnost žalbe sudu više instance.[16]

Prilikom vođenja sudskih postupaka mogu se javiti problemi u vezi sa otkrivanjem izvora, posebno kada je novinar tužena strana (npr. u slučajevima povrede časti i ugleda). Otkrivanje izvora informacije može ići u korist novinaru, iako etički kodeksi nalažu da treba sačuvati anonimnost izvora. Organizacija "Media Legal Defence Initiative" (MLDI) je opisala slučaj Džefrija Njarote, urednika iz Zimbabvea koji je otkrio slučaj korupcije u vezi sa kupovinom i prodajom automobila u koji su bili umešani ministri i visoko rangirani članovi vladajuće partije. Jedan od ministara je potom tužio Njarotu za povredu časti i ugleda. Iako su mu advokati savetovali da otkrije svoj izvor za priču koju je objavio, Njarota je to odbio i zbog toga izgubio na sudu.[17] U ovom slučaju se čini da je novinar istrajao u očuvanju tajnosti identiteta izvora, kako se ne bi narušio etički princip i njegov kredibilitet kao novinara. Smatramo da pravne posledice po novinare zbog insistiranja na očuvanju tajnosti izvora mogu da umanje medijske slobode, izuzev u slučajevima kada je interes javnosti da se sazna izvor informacije pretežniji u odnosu na pravo novinarske tajne, u skladu sa tripartitnim testom.

Iako je u SAD pravo na slobodu govora znatno šire određeno nego u Evropi, pre svega zbog Prvog amandmana na Ustav SAD, zanimljivo je da su 49 država i Distrikt Kolumbije (DC) usvojili takozvane "zaštitne zakone" (shield laws) ili sudsku praksu, koji omogućavaju medijima različite vidove zaštite od sudskih poziva (eng. subpoenas), kojima bi se novinarima moglo naložiti da otkriju identitet svojih izvora u sudskim postupcima. Ipak, na federalnom nivou ne postoji zaštitni zakon.[18] Američki Komitet reportera za zaštitu štampe ("Reporters Committee for Freedom of the Press") navodi da neki zaštitni zakoni štite novinare od prisilnog otkrivanja poverljivih izvora vesti, ali ne i neobjavljenih materijala. Ostali zakoni pružaju apsolutnu ili kvalifikovanu zaštitu prema vrsti pravnog procesa (krivični ili prekršajni) ili prema ulozi novinara (okrivljeni ili nezavisna treća strana). U državama koje nisu usvojile zaštitne zakone, državni sudovi su usvojili određenu vrstu kvalifikovanih privilegija. U ostalim slučajevima, državni ustavi mogu uključiti odredbe o slobodi štampe (free press provisions) koje su slične Prvom amandmanu Ustava SAD.[19]

16 Article 19, Protection of sources: https://www.article19.org/pages/en/protection-of-sources-more.html

17 Media Legal Defence Initiative (MLDI), Training manual on international and comparative media and freedom of expression law: http://www.mediadefence.org/news/mldi-publishes-manual-freedom-expression-law

18 Society of Professional Journalists, Shield Law 101: Frequently Asked Questions: http://www.spj.org/shieldlaw-faq.asp

19 Reporters Committee for Freedom of the Press, Legislative protection of news sources: http://www.rcfp.org/first-amendment-handbook/introduction-legislative-protection-news-sources-constitutional-privilege-a

KO SE MOŽE SMATRATI NOVINA-ROM?

KO SE MOŽE SMATRATI NOVINA-ROM? DA LI BLOGERI I SLIČNI ON-LAJN AKTERI MOGU UŽIVATI NOVI-NARSKU ZAŠTITU IZVORA?

POSTOJI LI UNIVERZALNA "DEFINICI-JA" NOVINARA?

Pošto se u ovom vodiču bavi-mo primarno novinarskim aktiv-nostima, važno je znati kako su definisani termini poput novinara, blogera i drugih lica koja objavljuju informacije i da li oni uživaju ista prava, kao i koje mehanizme imaju za zaštitu svojih izvora.

Za početak, napominjemo da ne postoji univerzalna definicija novi-nara, što je veoma značajno za očuvanje slobode medija, ali i prava da se informacije slobodno primaju i šalju. Stroge definicije mogu da dovedu do restriktivnog tumače-nja pojma "novinar", što ugroža-va novinarstvo kao slobodnu pro-fesiju.

Prilikom debate o definisanju poj-ma novinara, svakako treba uzeti u obzir preporuku Predstavnice OEBS-a za slobodu medija Du-nje Mijatović iz 2014. godine da bi države trebalo da se uzdrže od svakog pokušaja definisanja ko je novinar.[20]

Takođe, Preporuka Komiteta Ministara Saveta Evrope R (2000) 7, koja se upravo odnosi na pravo novinara da ne otkriju svoje izvore informacija, daje sledeće određe-nje novinara:

"Pojam 'novinar' označava svako fizičko ili pravno lice koje se redov-no ili profesionalno bavi sakuplja-njem i diseminacijom informacija javnosti putem bilo kog sredstva masovnog komuniciranja".[21]

Kada razmatramo druge komu-nikacione aktere, poput blogera,

20 Recommendations by OSCE Representative on Freedom of the Media on Open Journal-ism: http://www.osce.org/fom/118873?download=true

21 Preporuka dostupna na: http://www.coe.int/t/dghl/standardsetting/media/doc/cm/rec(2000)007&expmem _ EN.asp

takođe ne postoji univerzalno prihvaćena definicija. U najosnovnijem smislu, kako navodi organizacija "Article 19", bloger je svako lice koje piše, dodaje materijale, ili održava blog (dnevnik objavljen na Internetu). Blogovi omogućavaju svakom licu da objavljuje informacije na Internetu bez prednodne montaže i bez učestvovanja posrednika (urednik novina). Takođe, blog može biti anoniman ukoliko bloger tako želi. Blog odražava lični stav autora, može se odnositi na razne teme (od politike do mode) i može se razlikovati po dužini. Blogovi obično daju mogućnost čitaocima da ostave komentar i omogućavaju blogerima da se uključe u virtuelnu komunikaciju sa čitaocima. U nekim zemljama termin "bloger" se odnosi na slobodne novinare, što doprinosi konfuziji oko pravnog statusa blogera i pravila koja se na njih odnose. "Article 19" se zalaže da blogeri treba da uživaju isti vid zaštite koji je novinarima zagarantovan međunarodnim pravom.[22]

U svom opštem komentaru br. 34 na član 19 Međunarodnog pakta o građanskim i političkim pravima (Slobode mišljenja i izražavanja), Komitet UN za ljudska prava definiše novinarstvo na sledeći način: "Novinarstvo je funkcija u čijem vršenju učestvuje veliki broj aktera, uključujući profesionalne reportere i analitičare, kao i blogere i druge koji se bave formom samoobjavljivanja u štampi, na Internetu ili negde drugde."[23] Komitet UN za ljudska prava i Savet Evrope dali su okvirne definicije novinara i blogera, i prepoznali su da važnu ulogu u prikupljanju i širenju informacija imaju građansko novinarstvo i blogeri.

Inter-američka komisija za ljudska prava usvojila je zaštitu novinarskih izvora kao deo Deklaracije o principima o slobodi izražavanja:

"Svaki društveni komunikator ima pravo da poverljivim čuva njegove/njene izvore informacija, beleške i lične i poslovne arhive".[24]

Smatramo da je ova definicija naročito povoljna po onlajn komunikacione aktere, jer pojam "društveni komunikator" obuhvata širok skup pojedinaca koji se mogu baviti objavljivanjem informacija od značaja za javnost, tako da se pravo na očuvanje poverljivosti izvora proširuje sa profesionalnih novinara i na građanske reportere, npr. blogere. Na ovaj način se u obzir uzima razvoj tehnologije i novih komunikacionih platformi.

Komitet ministara Saveta Evrope u Preporuci o novom poimanju medija (2011) ističe da u novom medijskom ekosistemu zaštita izvora treba da se proširi do zaštite identiteta bilo koje osobe koja učini dostupnim sadržaj od javne važnosti u kolektivnom onlajn prostoru, te da ovaj prostor uključuje i platforme za deljenje sadržaja kao i društvene mreže.[25] Visoki sud Irske[26] je u slučaju Kornek protiv Morisa i drugih priznao da bloger ima pravo da štiti svoj izvor, jer bi primoravanje blogera da otkrije svoje izvore ugrozilo pravo da se informiše i utiče na javno mnjenje, što je u samom srcu slobode izražavanja.

Smatramo da striktne zakonske definicije novinara i blogera nisu dobre, te da prema navedenim međunarodnim smernicama u svakom pojedinačnom slučaju treba sagledati okolnosti i oceniti da li određeni onlajn komunikator može da uživa posebne vidove zaštite za profesionalne novinare, među kojima je i pravo da se ne otkrije identitet izvora.

STUDIJA SLUČAJA: ISPITIVANJE DANILA REDŽEPOVIĆA, UREDNIKA PORTALA "TELEPROMPTER"

Debata o tome ko se sve u Srbiji može smatrati novinarom ponovo je pokrenuta u oktobru 2015. godine, posle slučaja policijskog ispitivanja glavnog i odgovornog urednika portala "Teleprompter" (teleprompter.rs) Danila Redžepovića. Krajem septembra 2015, na portalu je objavljen tekst o navodnom prisluškivanju telefonskog razgovora predsednika opozicione Demokratske stranke Bojana Pajtića i Lidije Udovički, supruge vlasnika američke kompanije "Continental Wind Partners"[27] (CWP). Iako je Bojan Pajtić potvrdio

22 Article 19, Right to Blog: https://www.article19.org/data/files/medialibrary/3733/Right-to-Blog-EN-WEB.pdf

23 Opšti komentar br. 34 dostupan na: http://www2.ohchr.org/english/bodies/hrc/docs/gc34.pdf

24 Opšti komentar br. 34 dostupan na: http://www2.ohchr.org/english/bodies/hrc/docs/gc34.pdf

25 Preporuka dostupna na: https://wcd.coe.int/ViewDoc.jsp?id=1835645

26 Presuda Visokog suda Irske u slučaju Kornek protiv Morisa i drugih: http:// www.bailii.org/ie/cases/IEHC/2012/H376.html

27 http://www.teleprompter.rs/afera-reketiranje-procureo-prisluskivani-razgovor- izmedu-bojana-pajtica-i-lidije-udovicki.html

autentičnost transkripta razgovora, predstavnici državnih organa su demantovali da je transkript potekao od njih.[28]

U toku još jedne od brojnih dnevno-političkih afera, urednik "Telepromptera" je u oktobru 2015. dva puta pozivan u policiju na razgovor, pritom odbivši da se podvrgne poligrafskom testiranju. Redžepović je detaljno opisao tok ispitivanja, koje je prema njegovim rečima sprovedeno sa ciljem da se otkrije ko je izvor informacija o transkriptu. Redžepović tokom saslušanja nije hteo da saopšti identitet izvora informacije, pozivajući se na odredbe Zakona o javnom informisanju i medijima.[29] Prilikom drugog saslušanja prisutan je bio i tužilac za visoko-tehnološki kriminal Branko Stamenković, koji je sa inspektorima pokušavao da argumentuje stav da "Teleprompter" nije medij, jer nije upisan u Registar medija Agencije za privredne registre, kao i da Redžepović nije novinar, odnosno da se samim tim ne može pozivati na novinarsku tajnu. Tvrdnje da Redžepović nije novinar su zasnivali, između ostalog, i na njegovom priznanju da nije član nijednog novinarskog udruženja.[30] Policija je zbog ovog slučaja dolazila u prostorije tri najpoznatija novinarska udruženja (Udruženje novinara Srbije, Nezavisno udruženje novinara Srbije i Nezavisno udruženje novinara Vojvodine) kako bi došla do informacije da li je Danilo Redžepović njihov član, što udruženja nisu potvrdila.

Može se reći da je slučaj ispitivanja Danila Redžepovića, urednika portala koji nije zvanično registrovan kao medij, uticao na ponovno otvaranje debate o tome ko se sve može smatrati novinarom u Srbiji. Državni sekretar u Ministarstvu kulture i informisanja Saša Mirković je oktobru 2015. izjavio da bi trebalo "ozbiljno razmisliti" o definisanju novinara, što novinar Nedim Sejdinović (Nezavisno udruženje novinara Vojvodine) smatra veoma opasnim predlogom, jer se može koristiti u represivne svrhe. [31]

Zahvaljujući napretku tehnologije i sve većoj dostupnosti onlajn servisa, pojedinci mogu da objavljuju informacije od javnog interesa na mnogo načina - posredstvom blogova, društvenih mreža, onlajn portala itd. Kako bi izražavanje ideja, informacija i mišljenja bilo što slobodnije, akterima u digitalnom okruženju treba ostaviti mogućnost da registracijom steknu status medija ukoliko to žele, kako je i predviđeno Zakonom o javnom informisanju i medijima. Ipak, blogeri i drugi članovi onlajn zajednice koji se bave informisanjem o pitanjima od javnog interesa bi u određenim okolnostima trebalo da uživaju zaštitu kao i novinari zaposleni u medijskim organizacijama, ali je to bolje ostaviti za razmatranje u svakom slučaju ponaosob.

28 Preporuka dostupna na: https://wcd.coe.int/ViewDoc.jsp?id=1835645

29 Presuda Visokog suda Irske u slučaju Kornek protiv Morisa i drugih: http://www.bailii.org/ie/cases/IEHC/2012/H376.html

30 http://www.teleprompter.rs/drugo-saslusanje-urednika-telepromptera- novinarska-tajna-ne-vazi-za-tebe-posto-nisi-novinar.html

31 http://www.autonomija.info/mirkovic-definisati-ko-je-novinar.html

TEHNIČKA ZAŠTITA UZBUNJI-VAČA

TEHNIČKA ZAŠTITA UZBUNJIVAČA

U situacijama kada pojedinci koji su zaposleni u okruženju u kojem dolaze u kontakt sa izuzetno po-verljivim informacijama (vojska, policija, pravosudni organi i druge državne institucije, privatni sektor...) često imaju potrebu da ih podele sa javnošću i tako ukažu na potencijalne zloupotrebe. Najčešći nazivi za ove pojedince jesu uzbunjivači ili "duvači u pištaljku" (eng. whistleblowers) i bez njih se savremeno istraživačko novinarstvo gotovo ne može zamisliti. Svakako najpoznatiji uzbunjivač današnjice je Edvard Snouden, bivši analitičar američke Agencije za nacionalnu bezbednost (NSA), koji je novinaru Glenu Grinvaldu dostavio veliki broj strogo poverljivih dokumenata koji su ukazali na masovni nadzor digitalnih komunikacija građana.

Kada javnost sazna za njihove dojave, uzbunjivači mogu biti mete različitih pritisaka i pravnih posledica zbog svojih postupaka. U Srbiji je u novembru 2014. usvojen Zakon o zaštiti uzbunjivača, koji uzbunjivačima i sa njima povezanim licima pruža sudsku zaštitu od eventualne odmazde poslodavaca (otkaz, mobing...).[32] Napominjemo da se naše preporuke u ovom vodiču odnose na uzbunjivače u širem smislu, dakle i na one pojedince koji ne ispunjavaju formalne uslove propisane Zakonom o zaštiti uzbunjivača.

AKTIVNOSTI SHARE FONDACIJE U SFERI TEHNIČKE ZAŠTITE

SHARE Fondacija u okviru SHARE Labs-a sprovodi više istraživanja koja se odnose na arhitekturu Interneta, privatnost korisnika, razumevanje automatizovanih sistema i pretnje koje vrebaju u sajber prostoru. Takođe, SHARE Fondacija aktivno sarađuje sa novinarima, aktivistima, medijskim i građanskim organizacijama u borbi protiv sajber napada i pruža im tehničku i pravnu pomoć. Iz tog iskustva formirana je baza znanja i preporuka, objavljenih u

32 "Usvojen Zakon o zaštiti uzbunjivača", Blic online: http://www.blic.rs/vesti/politika/usvojen-zakon-o-zastiti-uzbunjivaca/3pr3jrp

seriji vodiča o različitim aspektima tehničke i pravne zaštite medija.

Što se tehničkih priručnika tiče, objavili smo dva vodiča. Prvi je "Osnove digitalne bezbednosti" i namenjen je individualnoj zaštiti novinara, medijskih radnika i individualnim korisnicima uopšte. Fokus tog vodiča su osnovni principi zaštite privatnosti u digitalnom okruženju i zaštite od digitalnih napada različitih vrsta. Vodič "Osnove digitalne bezbednosti" je odlična polazna tačka za sve korisnike Interneta koji drže do svoje privatnosti i zaštite svojih podataka.

Drugi vodič koji je SHARE Fondacija objavila, "Bezbednost organizacija u digitalnom okruženju", namenjen je tehničkoj posadi informacionih sistema u medijskim i građanskim organizacijama, koji imaju potrebu da uobičajena znanja o hardveru i softveru dopune lekcijama o njihovoj zaštiti.

Nema univerzalnog rešenja za tehničku bezbednost organizacija, usled činjenice da se novi alati i strategije za napad razvijaju gotovo svakodnevno. Pojedine organizacije imaju različite potrebe koje tehnički administratori dobro poznaju i kojima će lako prilagoditi opšti pregled zaštite ključnih tačaka sistema iz vodiča.

Oba vodiča su dostupna na sajtu SHARE Fondacije.[33]

Za istraživanja SHARE Labs-a posetite www.labs.rs.

PREPORUKE ZA BEZBEDNO UZBUNJIVANJE

U nastavku ćemo predstaviti preporuke za uzbunjivače. Proces uzbunjivanja je veoma kompleksan i treba ga sagledati iz više aspekata. Uzbunjivači su najčešće ljudi koji su insajderi i mogu da snose posledice ukoliko se njihov identitet otkrije. Oni su uglavnom zaposleni ili saradnici kompanije/organizacije na koju se dojava odnosi, tako da je anonimnost u uzbunjivanju od ključne važnosti. Samim tim što na uzbunjivanje utiče veliki broj faktora, često se dešava da se uzbunjivanje vrši na pogrešan način. Postoji više vrsta uzbunjivanja, počevši od slanja informacija poštom, pa sve do onlajn uzbunjivanja, koje je jedan od bezbednijih načina, ukoliko se postupa na pravi način. Da bismo olakšali proces slanja dojava, sastavili smo

33 http://www.shareconference.net/sh/content-type/publication

kratko uputstvo koje ima za cilj da svede rizike na minimum:

- Razmislite da li su informacije koje posedujete relevantne primaocu dojave. Postoje različite uzbunjivačke platforme, a prvi korak je da odlučite kome ćete poslati dojavu.
- Pri izboru uzbunjivačke platforme proverite kome zapravo šaljete dojavu. To možete uraditi putem WHOIS pretrage web sajta platforme (http://who.is/). Ukoliko WHOIS registri nisu otvoreni, razmislite o tome da možda nađete drugu platformu.
- Anonimnost je bitna. Nemojte nikome govoriti da planirate da šaljete dojavu i nemojte preterano otvoreno ispoljavati svoje nezadovoljstvo prema predmetu dojave. Ukoliko ipak imate potrebu da nekome kažete, recite nekoj bliskoj osobi kojoj verujete.
- Dojave nemojte slati mejlom, naročito ne sa službene adrese ili sa adrese koju često koristite za privatnu komunikaciju. Ukoliko baš morate dojavu poslati mejlom, možete napraviti privremenu email adresu koja će se deaktivirati posle 10 minuta (http://10minutemail.com/). Koristite "Tor pretraživač" (Tor Browser) kada šaljete dojavu mejlom (https://www.torproject.org/).
- Nemojte dojavljivati sa službenog ili privatnog telefona. U slučaju da je neophodno da dojava bude dostavljena telefonskim putem, uradite to sa javnog telefona, ali vodite računa o tome da veliki broj telefonskih govornica ima video-nadzor.
- Pristupajte veb platformama za uzbunjivanje preko Tor pretraživača.
- Pripremite dokumentaciju. Materijalni dokazi su veoma bitni, pa je dobro da imate fotokopije ili skenove svih relevantnih dokaza (dokumenata). Dokaze mogu predstavljati i fotografije, audio ili video-zapisi i sl.
- Posle slanja dojave, ponašajte se uobičajeno. Povedite računa da nemate nagle promene u ponašanju, jer tako možete lako da privučete pažnju. Ukoliko imate potrebu da razgovarate sa nekim, uradite to sa nekom vama bliskom osobom.

DATA LEAKS PLATFOR-MA

DATALEAKS PLATFORMA

U ovom poglavlju ćemo objasniti na koji način se koristi DataLeaks platforma i kako organizacije mogu da primaju anonimne dojave posredstvom DataLeaks-a. Ova uzbunjivačka platforma koristi GlobaLeaks softver, a anonimnost uzbunjivača se obezbeđuje pomoću Tor mreže. Tor je najsavremenije rešenje kada je reč o digitalnoj zaštiti anonimnosti. GlobaLeaks je prva open source, bezbedna i anonimna uzbunjivačka platforma koji je razvio Hermes centar za transparentnost i digitalna ljudska prava (Hermes Center for Transparency and Digital Human Rights).[34]

Tor je već integrisan u GlobaLeaks; na taj način vlasnik uzbunji- vačke platforme ne može da zna tačnu lokaciju i identitet uzbunjivača. Ipak nikad ne možete biti sigurni da neko neće da uradi dublje istraživanje o vašoj dojavi, pa prema tome preporučujemo maksimalni nivo bezbednosti. Najlakši način da očuvate svoju anonimnost jeste da koristite Tor - anonimni pretraživač (https://www.torproject.org/).

Potpuna bezbednost nikad ne može da bude garantovana. Ipak, tehnologija ove platforme je dizajnirana imajući u vidu situacije u kojima je život uzbunjivača u opasnosti. Eksperti za IT bezbednost su izvršili brojna testiranja softvera kako bi identifikovali i rešili potencijalne nedostatke. Štaviše, izvorni kod GlobaLeaks platforme je otvorenog tipa, tako da svako može da analizira i proveri da li je sam softver bezbedan. Ovo je najbolji način da se osigura bezbednost aplikacije.

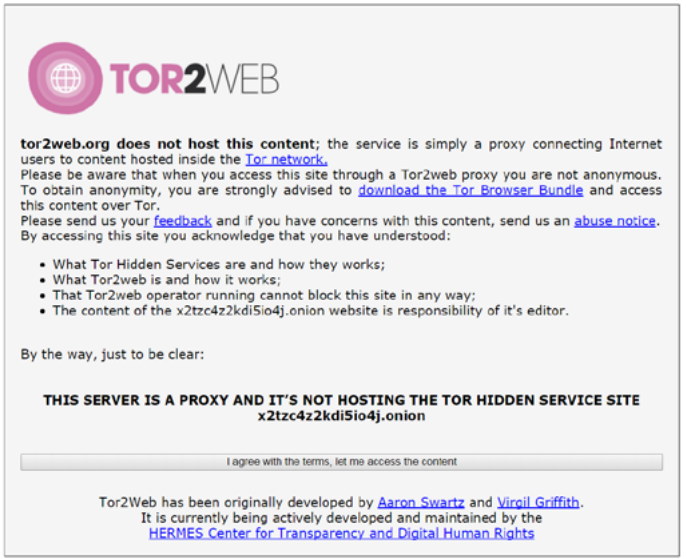
Ukoliko ste zainteresovani za detaljniju analizu bezbednosti GlobaLeaks platforme, posetite stranicu posvećenu bezbednosnom dizajnu i detaljima GlobaLeaks aplikacije. [35]

34 http://www.shareconference.net/sh/content-type/publication

35 https://docs.google.com/document/d/1SMSiAry7x5XY9nY8GAejJD75NWg7bp7M1P-wXSiwy62U/pub

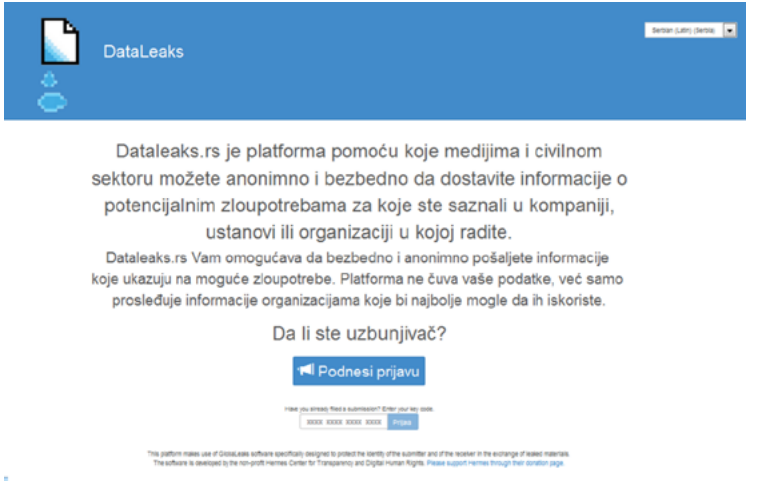
KAKO SE KORISTI DATALEAKS PLATFORMA

I pored činjenice da preporučujemo korišćenje Tor-a za slanje dojave bilo koje vrste, zbog unapređenja dostupnosti omogućili smo pristup platformi preko standardnog Interneta. Našu platformu možete posetiti na www.dataleaks.rs, pri čemu dobijate obaveštenje da je sajt hostovan u Tor mreži i da se preporučuje pristup kroz Tor, ali imate opciju da prihvatite uslove korišćenja i da pristupite platformi kroz običan pretraživač. Tor2Web proxy koristi TLS (HTTPS) bezbednost za pretraživače, što znači da je sadržaj koji šaljete kroz mrežu enkriptovan, odnosno nečitljiv trećim licima. Ipak, Tor2Web proxy ne može da zaštiti vaš identitet na mreži, odnosno ne može garantovati anonimnost podnosioca dojave.

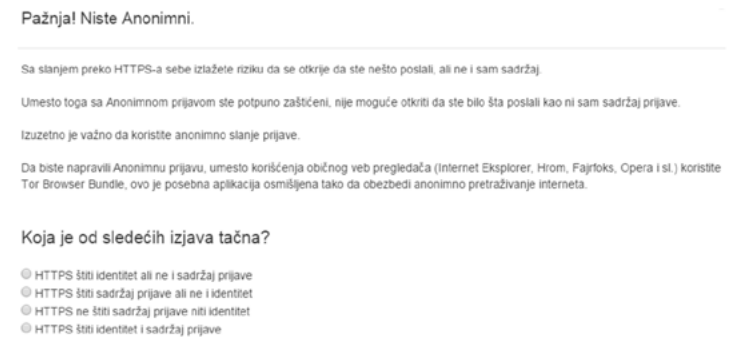


Ukoliko već koristite Tor, možete da unesete onion adresu (http://x2tzc4z2kdi5io4j.onion/#/) ili da ponovo koristite www.dataleaks.rs pri čemu ćete biti preusmereni na onion adresu. Onion adrese su posebne vrste adresa koje se koriste u okviru Tor mreže i ne može im se pristupiti direktno sa javnog Interneta, već samo kroz proxy servise kao što je Tor2Web.

U svakom slučaju, bilo da pristupate kroz Tor ili kroz običan pretraživač, dobićete istu početnu stranicu platforme DataLeaks koja izgleda ovako:

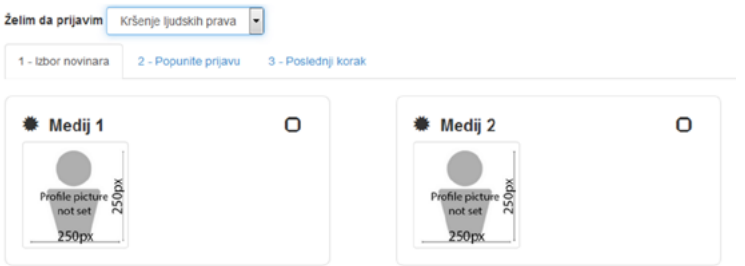


Ukoliko želite da podnesete prijavu, klikom na dugme "Podnesi prijavu" idete na prvi korak procedure. Korisnici koji ne koriste Tor za pristup platformi dobiće sledeće obaveštenje:

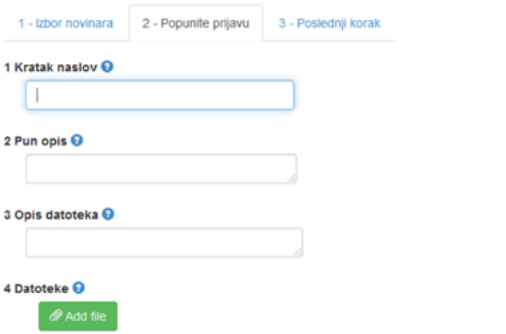


Već smo napomenuli da se korišćenjem Tor2Web za pristup DataLeaks platformi, uzbunjivačima obezbeđuje tajnost podataka koji se šalju, ali ne zaštita identiteta samog uzbunjivača, za šta se mora koristiti Tor.

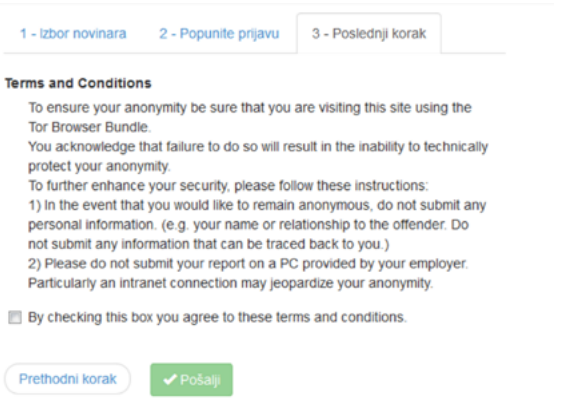
Prvi korak podnošenja dojave se sastoji u izboru oblasti na koju se odnosi dojava i izbor jednog ili više medija koji će biti primaoci dojave.



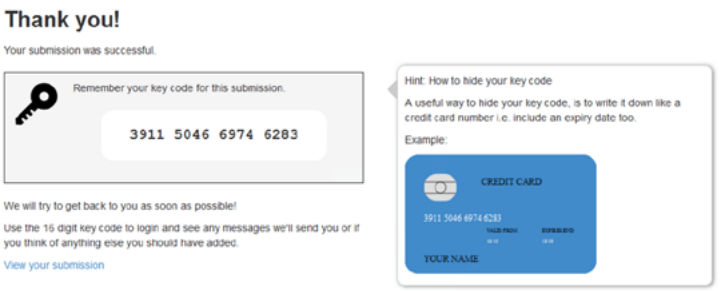
U drugom koraku podnošenja dojave se zapravo unose podaci koji su direktno vezani za samu dojavu; naslov dojave, opis dojave, opis podnetih datoteka i same datoteke (audio i video snimci, skenovi dokumenata itd):



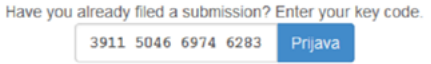
Da biste uspešno poslali dojavu, u trećem koraku, potrebno je da prihvatite uslove korišćenja platforme:



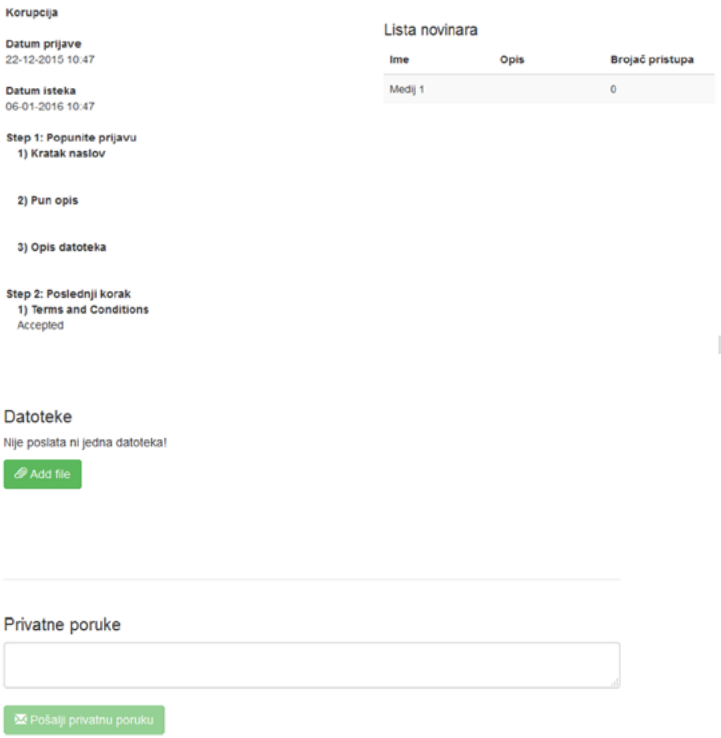
Kad konačno podnesete dojavu, dobićete informaciju koji je kod vaše dojave i savet kako da ga bezbedno čuvate. Na primer, zapišite ga kao da je broj kredite kartice, a pritom dodajte i datum isteka da bi bilo uverljivije.



Ovim je podnošenje dojave uspešno završeno. Ukoliko želite da vidite status vaše dojave, da dodate dokumenta, ili da bezbedno komunicirate sa medijem kojem ste poslali dojavu, možete da se vratite na početnu stranu gde imate polje u koje možete uneti vaš broj prijave:



Nakon unošenja ispravnog broja prijave dobijate prikaz vaše prijave i opcije za dodavanje datoteka i komunikaciju sa primaocem dojave:



KAKO POSTATI PRIMALAC DOJAVA KROZ DATALEAKS PLATFORMU

Nezavisne medijske organizacije i organizacije civilnog društva u Srbiji nemaju dovoljno kapaciteta da podižu individualne platforme za uzbunjivače. To je i bio jedan od motiva SHARE Fondacije da se postavi kao veza između potencijalnih uzbunjivača i organizacija kojima se dojave šalju. S druge strane, da bi se mogao garantovati kredibilitet destinacije i čitavog procesa uzbunjivanja, potrebno je da primalac dojave ispunjava niz tehničkih i ne-tehničkih uslova. Ne-tehnički uslovi su vezani za, medijski kredibilitet, odnosno mediji koji se smatraju neozbiljnim, propagandnim i slično ne mogu biti kredibilan primalac dojave. Takođe, transparentnost u radu i jasno zastupanje javnog interesa su prednosti koje bi uzbunjivača usmerile kome će da pošalje dojavu.

Tehnički uslovi se odnose na bezbednost same infrastrukture medijske organizacije ili organizacije civilnog društva. Platforma je tako postavljena da čak ni primalac dojave ne zna ko je izvor informacije. Ipak, ukoliko je sistem primalaca nebezbedan, može doći do gubitka ili preranog curenja podataka.

Tehnički preduslovi potrebni za bezbedno primanje i upravljanje dojavama podrazumevaju korišćenje anonimnog pretraživača i enkripciju elektronske komunikacije pomoću PGP.

Ukoliko ste medijska organizacija ili organizacija civilnog društva koja želi da prima dojave koristeći DataLeaks platformu SHARE Fondacije, možete da nam se obratite mejlom na info@sharedefense.org i mi ćemo vam pružiti svu potrebnu tehničku podršku.

ZAKLJUČAK

ZAKLJUČAK

Uzimajući u obzir pravnu i tehničku zaštiitu, kao i međunarodne standarde i praksu u vezi sa očuvanjem novinarskih izvora i rada sa uzbunjivačima, neophodno je imati u vidu da se bez garantovanja zaštite identiteta izvora novinari dovode u veoma nepovoljan položaj. Novinari i svi potencijalni izvori bi trebalo da budu svesni da u Srbiji postoje pravne odredbe koje mogu dovesti do otkrivanja identiteta izvora u sudskom postupku. Dakle, iako novinar primi određenu informaciju od izvora/uzbunjivača, mora da bude svestan kakve posledice to može imati po njega i njegove izvore, naravno ukoliko dođe do sudskog epiloga.

Na kraju, nekoliko saveta za novinare i uzbunjivače:

- Garantujte izvoru da će ostati anoniman samo ukoliko je to u skladu sa zakonom. U slučaju nedoumica, sigurnije je konsultovati se sa urednikom i pravnim savetnikom pre prihvatanja da se informacije objave;
- Vodite računa o posledicama po osobu koja je izvor u slučaju da budete primorani da otkrijete njen/njegov identitet na sudu;
- Trudite se da sa izvorom komunicirate na tehnički bezbedan način (enkriptovani mejlovi ili čet aplikacije) kako biste na minimum sveli mogućnost da treće strane otkriju identitet izvora i informacije koje šalje;
- Prema Kodeksu novinara Srbije, novinar ne sme slepo da veruje izvoru informacije, naročito ako izvor traži da ostane anoniman. U skladu sa standardima odgovornog novinarstva i novinarske pažnje, sve navode treba proveriti pre objavljivanja;
- Tehnički bezbedni načini za dostavljanje poverljivih informacija jesu dobra polazna tačka, ali svakako treba obratiti pažnju i na druge faktore koji mogu ukazati da ste uzbunjivač (npr. nagla promena ponašanja).

KORIŠĆENI MATERIJALI:

- Okrugli sto ''Profesionalni sertifikat ili licence novinarstvu'', Medija centar Beograd, april 2005: http://www.mc.rs/licencama-u-zastitu-profesije.6.html?eventId=19123
- A. Petrović, ''Uzbunjivači moraju da budu zaštićeni od odmazde'', Politika Online: http://www.politika.rs/sr/clanak/341436/Drustvo/Uzbunjivaci-moraju-da-budu-zasticeni-od-odmazde
- T. Tagirov, ''Poroci tajni, vrline javne'', Vreme br. 1086: http://www.vreme.com/cms/view.php?id=1016693
- Videti Kodeks novinara Srbije: http://www.savetzastampu.rs/doc/Kodeks _ novinara _ Srbije.pdf
- Kosovski zakon o zaštiti novinarskih izvora: http://www.kuvendikosoves.org/common/docs/ligjet/Law%20on%20the%20protection%20of%20the%20journalism%20sources.pdf
- Evropski sud za ljudska prava, slučaj Roman Zaharov protiv Rusije, 4. decembar 2015. Dostupno na: http://hudoc.echr.coe.int/eng?i=001-159324
- 4th European Ministerial Conference on Mass Media Policy - Prague, 7-8 December 1994: http://www.coe.int/T/E/Com/Files/Events/2002-09-Media/ConfMedia1994.asp
- Article 19, Briefing Paper on Protection of Journalists' Sources: https://www.article19.org/data/files/pdfs/publications/right-to-protect-sources.pdf
- Media Legal Defence Initiative (MLDI), Training manual on international and comparative media and freedom of expression law: http://www.mediadefence.org/news/mldi-publishes-manual-freedom-expression-law
- Evropski sud za ljudska prava, slučaj Gudvin protiv Ujedinjenog Kraljevstva, 27. mart 1996. Dostupno na: http://hudoc.echr.coe.int/eng?i=001-57974
- Article 19, Freedom of expression limitations: https://www.article19.org/pages/en/limitations.html
- Preporuka Saveta Evrope R (2000) 7: http://www.coe.int/t/dghl/standardsetting/media/doc/cm/rec(2000)007&expmem _ EN.asp
- Deklaracija o principima slobode izražavanja u Africi: http://www.achpr.org/sessions/32nd/resolutions/62/
- Society of Professional Journalists, Shield Law 101: Frequently Asked Questions: http://www.spj.org/shieldlaw-faq.asp
- Reporters Committee for Freedom of the Press, Legislative protection of news sources: http://www.rcfp.org/first-amendment-handbook/introduction-legislative-protection-news-sources-constitutional-privilege-a
- Recommendations by OSCE Representative on Freedom of the Media on Open Journalism: http://www.osce.org/fom/118873?download=true
- Article 19, Right to Blog: https://www.article19.org/data/files/medialibrary/3733/Right-to-Blog-EN-WEB.pdf
- Opšti komentar Komiteta UN za ljudska prava br. 34 na član 19 ICCPR: http://www2.ohchr.org/english/bodies/hrc/docs/gc34.pdf
- Inter-American Commission on Human Rights, Inter-American Declaration of Principles on Freedom of Expression, 108th session, 19 October 2000: https://www.cidh.oas.org/declaration.htm
- Preporuka Saveta Evrope CM/Rec(2011)7: https://wcd.coe.int/ViewDoc.jsp?id=1835645
- Presuda Visokog suda Irske u slučaju Kornek protiv Morisa i drugih: http://www.bailii.org/ie/cases/IEHC/2012/H376.html
- Teleprompter.rs, ''AFERA ''REKETIRANJE'': Procureo prisluškivani razgovor izmedu Bojana Pajtića i Lidije Udovički'': http://www.teleprompter.rs/afera-reketiranje-procureo-prisluskivani-razgovor-izmedu-bojana-pajtica-i-lidije-udovicki.html
- J. Štetin, ''Stefanović: Država nema veze sa prisluškivanjem Pajtića'', TV N1: http://rs.n1info.com/a96686/Vesti/Stefanovic-o-prisluskivanju-Pajtica.html
- D. Redžepović, ''MINISTRE, PRESTANI DA LAŽEŠ! Istina o saslušanju urednika Telepromptera'', Teleprompter.rs: http://www.teleprompter.rs/ministre-prestani-da-lazes-istina-o-saslusanju-urednika-telepromptera.html
- Teleprompter.rs, ''Drugo saslušanje urednika Telepromptera: ''Novinarska tajna ne važi za tebe pošto nisi novinar'''': http://www.teleprompter.rs/drugo-saslusanje-urednika-telepromptera-novinarska-tajna-ne-vazi-za-tebe-posto-nisi-novinar.html
- Autonomija.info, ''Sejdinović: predlog da se definiše ko je novinar je potencijalno veoma opasan'':
- http://www.autonomija.info/mirkovic-definisati-ko-je-novinar.html
- ''Usvojen Zakon o zaštiti uzbunjivača'', Blic online: http://www.blic.rs/vesti/politika/usvojen-zakon-o-zastiti-uzbunjivaca/3pr3jrp
- Publikacije SHARE Fondacije:
- http://www.shareconference.net/sh/content-type/publication
- Hermes Center for Transparency and Digital Human Rights: http://logiosshermes.org/
- GlobaLeaks Application Security Design and Details: https://docs.google.com/document/d/1SMSiAry7x5XY9nY8GAejJD75NWg7bp7M1PwXSiwy62U/pub

SHARE FOUNDATION - 2015