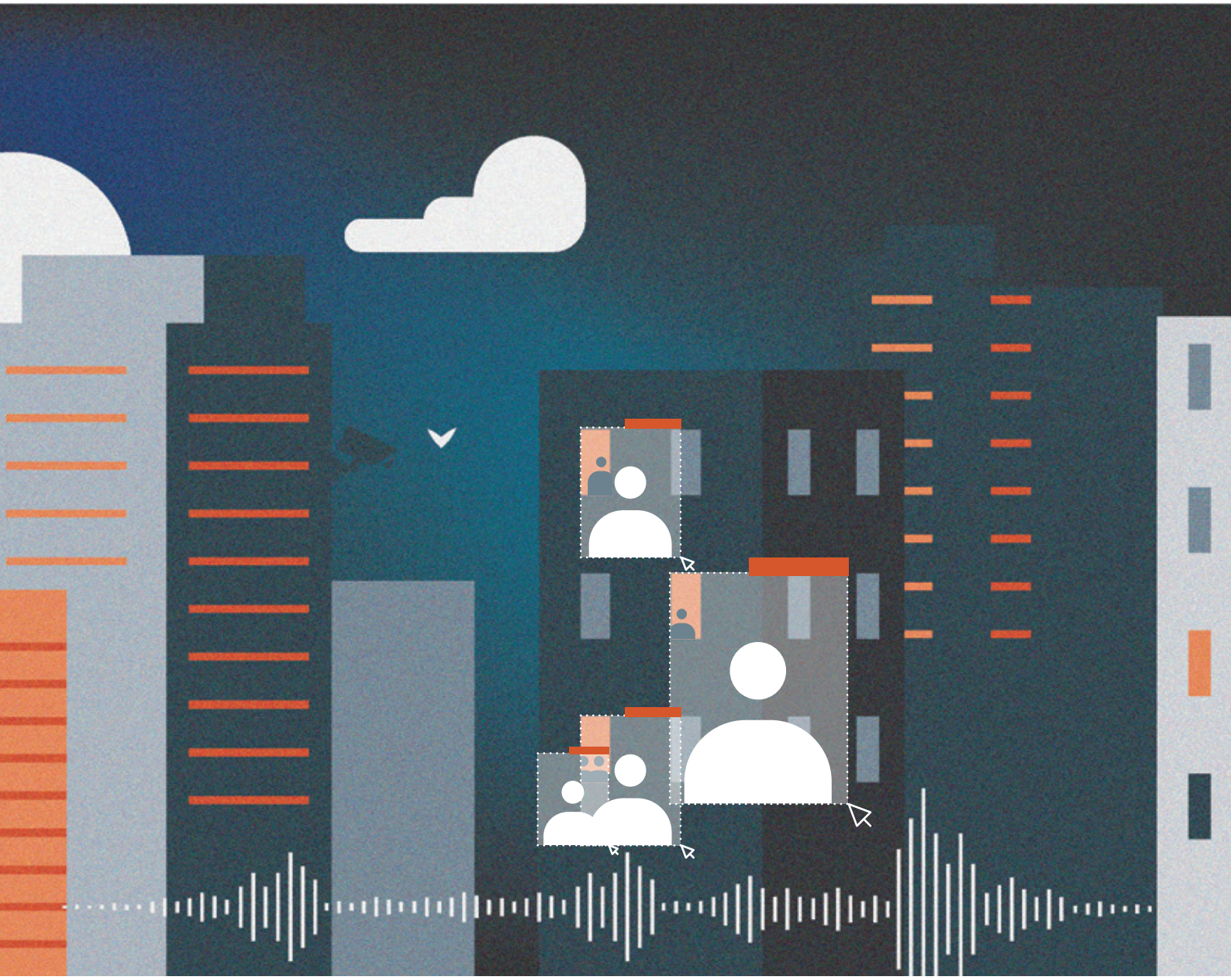
Zaštita novinarskih izvora u digitalnom okruženju: pravo i medijska praksa

Praviš se da živiš normalno



OEBS Organizacija za evropsku bezbednost i saradnju
Misija u Srbiji

#ЕУ ЗА ТЕБЕ

Zaštita novinarskih izvora u digitalnom okruženju: pravo i medijska praksa

Praviš se da živiš normalno

Bojana Kostić i Tanja Maksić, 2025.

Organizacija za evropsku bezbednost i saradnju
Misija u Srbiji

#ЕУ ЗА ТЕБЕ

Napomena: Ova analiza izrađena je uz finansijsku pomoć Evropske unije. Stavovi izrečeni u ovom izveštaju pripadaju isključivo autorima i njihovim saradnicima i ne predstavljaju nužno zvaničan stav Misije OEBS-a u Srbiji i nužno ne odražavaju stavove Evropske unije.

Sadržaj

Rezime 5

Uvod 9

Metodologija, predmet analize i struktura 11

2. Medijska praksa 17

Društveni kontekst 17

Medijski sistem Srbije 21

Važnost zaštite novinarskih izvora 24

Nalazi istraživanja 27

3. Pravni okvir zaštite novinarskih izvora 46

Normativni okvir i uporednopravna rešenja 46

Međunarodni standardi i regulativa Evropske unije 54

4. Diskusija 64

5. Zaključci 72

6. Preporuke 78

1. Mediji i novinari *kontinuirano* da rade na podizanju kapaciteta, unapređenju znanja i „digitalne higijene" 78
2. Sprovesti istrage u vezi sa digitalnim nadzorom nad novinarima i procenu zaštite novinarskih izvora 79
3. Zaštita novinarskih izvora iz Zakona o javnom informisanju i medijima ne treba da bude predmet izmena u datim političkim okolnostima 80
4. Obezbediti zaštitu novinarskih izvora kroz druge zakonske propise 81
5. Harmonizacija sa članom 4. Akta o medijskim slobodama (EMFA) mora biti odložena dok se ne ispune prethodno navedene preporuke 82
6. Ojačati ulogu suda u procesu odlučivanja o zahtevu za sprovođenje posebnih dokaznih radnji i mera digitalnog nadzora 82
7. Transparentne javne nabavke i kontrolni mehanizmi 83

Rezime

Studija „Zaštita novinarskih izvora u digitalnom okruženju: pravo i medijska praksa" mogla bi se svesti na jedan upečatljiv citat koji je dao novinar intervjuisan tokom rada na studiji: „Cele službe su stavljene u svrhu nadzora. Međutim, ono što je opasno je da mi ne znamo ko za koga radi – oni su razbili sistem, i ne znamo jel` neko radi za službu ili za mafiju, sve je isprepletano."

Potreba za ovom studijom proizilazi ne samo iz Strategije razvoja sistema javnog informisanja u Republici Srbiji 2020-2025, koja je prepoznala probleme zaštite novinarskih izvora, već i zbog sve učestalijih napada na novinare korišćenjem digitalnog nadzora i špijunskih softvera. Utisak medijskih radnika je da „ako država ima interes da te prati, nema šanse da se odbraniš." Do ovog zaključka dolaze i međunarodne studije koje zaštitu novinarskih izvora u digitalnom okruženju sve više vide kao pitanje zaštite podataka do kojih dolaze novinari, a ne isključivo njih samih.

Razgovori koji su vođeni sa novinarima u okviru pripreme ove studije govore o visoko razvijenoj svesti o važnosti zaštite izvora, ali i o ograničenim internim resursima, suženom prostoru za delovanje nezavisnih medija i nepovoljnim uslovima rada, u kom su stalni pritisci i svest o nadzoru - normalnost. Svedočanstva govore o lepezi nelegalnih praksi nadzora, koji variraju od fizičkog praćenja, prisluškivanja i upotrebe spyware-a, zaplene opreme, SLAPP tužbi i sl. Ona takođe govore i o duboko ukorenjenom nepoverenju novinara u institucije, „ćutanju" administracije i nedovoljno razvijenim mehanizmima zaštite.

U ovako opisanom okruženju, zaštita novinarskih izvora okosnica je poverenja između novinara, izvora i javnosti. Ovaj institut poznaje i Zakon o javnom informisanju i medijima– član 58. koji sa malo reči, pruža osnovne garancije zaštite, odnosno pravo novinara da ne otkrije izvor informacije osim u veoma usko definisanim uslovima. Fokus ove studije je prevas-

hodno na pitanju da li ova zakonska norma vrši svoju zaštitnu funkciju, i to kroz prizmu povezanih zakonskih propisa (na primer, Zakonik o krivičnom postupku i drugih zakona koji regulišu rad službe bezbednosti, Zakon o elektronskim komunikacijama), kao i kroz institucionalna postupanja u praksama digitalnog nadzora.

Kako svaka mera digitalnog nadzora ograničava ljudska prava, ona mora biti odobrena od strane suda ili drugog nezavisnog organa – samo u izuzetnim situacijama – srazmerno cilju koji se želi postići, neophodnosti u demokratskom društvu i u skladu sa zakonom. Prakse digitalnog nadzora, analizirane u studiji, mapiraju netransparentnost u njihovom korišćenju, nejasne razloge i opravdanost potrebe za njihovim korišćenjem, ukazujući na jačanje krivično-pravnog otiska i pritiska. Zbog toga ne čudi utisak novinara koji zaključuje da je „najvažnija stvar što postoji veliki strah, čak i za najbanalnije stvari, pukla negde cev ili tako nešto, a ljudi ne smeju da o tome pričaju pod punim imenom i prezimenom."

Zakonodavna rešenja u Srbiji ostavljaju (skoro) neograničen pristup policijskim službenicima i radnicima bezbednosnih službi novinarskim podacima i tako im omogućavaju da zaobiđu zaštitu izvora. Ne postoje eksplicitna zakonodavna rešenja ni uputstva za postupanje u slučajevima digitalnog nadzora, niti u situacijama pretresa ili oduzimanja uređaja. Poređenja radi, belgijski zakon, kao i Preporuke Saveta Evrope i praksa Evropskog suda za ljudska prava, predviđaju i obavezu minimizacije prikupljanja podataka, definisanje opsega i mera za zaštitu od arbitrarnog, neograničenog i intruzivnog pristupa. Studija dodatno obrađuje i član 4. EU Akta o medijskim slobodama, koji se fokusira na slučajeve digitalnog nadzora nad novinarima i zaključuje da u procesu evropskih integracija, Srbija mora otići više koraka dalje - ne samo kako bi usaglasila krivično-procesne radnje sa institutom zaštite izvora, već i sprečila korišćenje intruzivnog softvera (spyware-a).

Zbog toga studija, u preporukama, izlaže niz koraka koji se moraju ispuniti kako bi se omogućio adekvatan nivo zaštite izvora. Prvo, potrebno je sprovesti nezavisnu istragu u vezi sa dosadašnjim slučajevima korišćenja špi-

junskog softvera i digitalnog nadzora nad novinarima, uz učešće medijske zajednice i novinara čija su ljudska prava na ovaj način direktno prekršena. Kroz analizu podataka iz istrage biće moguće utvrditi slabe karike sistema i zakonske praznine, koje u drugom koraku treba dodatno analizirati, a pre svega kroz povezane zakonske norme koje se moraju usaglasiti tako da omogućuju poštovanje zaštite izvora. Treće, usaglašavanje sa članom 4. Akta o medijskim slobodama treba odložiti dok se ne ispune prethodna dva koraka i ne steknu društveni uslovi, pre svega na nivou stabilnosti i vladavine prava. Treba poći od jasne činjenice da špijunski softver stoji u suprotnosti sa principima zaštite ljudskih prava, što je indikator da mora postojati jasna zakonska zabrana korišćenja ovih alata i mera. Osim toga, u izmenama zakonodavstva potreban je sveobuhvatni pristup, koji uzima u obzir ceo proces digitalnog nadzora i digitalnih rizika po zaštitu novinara i izvora. Uređenje sistema javnih nabavki, primena mera nadzora nad novinarima, kontrolna funkcija sudova - zaštita novinara i njihovih izvora mora biti „ukorenjena" u svaki segment ovog procesa. Samo jačanje člana 58. ZJIM neće biti dovoljno ako proces nabavke, upotrebe i nadzora nad ovim tehnologijama ostane bez ozbiljnih sistema kontrole i korekcije.

Uvod

Novinarstvo je profesija rada u javnom interesu, a svaka novinarska priča uključuje ukrštanje i iznošenje tačnih i proverenih činjenica iz više izvora i predstavljanje različitih perspektiva. Bez novinarskih izvora i ljudi koji su spremni da podele informacije bez otkrivanja svog identiteta široj javnosti, bez pouzdanih podataka ili relevantnih dokumenata, novinarstvo ne bi imalo funkciju četvrte grane vlasti, one koja poziva na odgovornost one na poziciji moći. Koliki je značaj izvora i njihova zaštita jasno je samo kada se pogleda rad istraživačkih novinara na lokalnom, regionalnom i međunarodnom nivou. Istraživačke priče poput čuvene 3P serije - Panama, Pandora i Paradise[1] - koje su otkrile veze između globalnih političkih i biznis elita, njihovih koruptivnih dogovora i štetnih posledica, ne bi bile moguće bez novinarskih izvora.

Pitanja demokratije usko su povezana sa pitanjem medijskih sloboda i nezavisnosti medija. Demokratije, koje po izveštajima Freedom House-a već 18. godinu za redom beleže pad, sa 2024. godinom doživljavaju najviši nivo demokratskog proklizavanja.[2] Od urušavanja izbornih procesa, do oružanih sukoba (uključujući i one na granici Evrope), do sve većeg uplitanja države u nezavisnost medija - demokratske vrednosti, institucionalni okviri zaštite i vladavina prava ozbiljno se urušavaju. Većina odgovora na ove navedene strukturne demokratske rizike uglavnom ukazuje na važnost medijskih sloboda, medijskog pluralizma, i bezbednost novinara.

Pitanje medijskih sloboda je krucijalno za zaštitu novinarskih izvora. Novinari imaju i „globalnu etičku obavezu da izbegavaju otkrivanje svojih

1 OCCPR, Panama Papiri, OCCPR dostupno na: https://www.occrp.org/en/project/the-panama-papers Pandora, dostupno na: https://www.icij.org/investigations/pandora-papers/ i Paradise, dostupno na: https://www.icij.org/investigations/paradise-papers/

2 Freedom House. 2024 Year in Review. Dostupno na: https://freedomhouse.org/impact/2024

izvora."[3] Analiza će pokazati i da je u nekim zemljama, kao što je Švedska,[4] otkrivanje izvora, u određenim uslovima, kažnjivo. Pravo zaštite novinarskih izvora, i sa njom korelativno povezana obaveza državnih organa da poštuju ovo pravo i da se suzdrže od radnji koje mogu otkriti novinarske izvore, spada u okvir slobode izražavanja, i uže u korpus tzv. novinarskih privilegija. Privilegija koje su sticane decenijama upravo u cilju kreiranja uslova u kojima medijske slobode, među kojima je i zaštita izvora i informacija, omogućavaju novinarima i medijskim radnicima da rade u javnom interesu i interesu očuvanja demokratije i vladavine prava.[5] Većina evropskih zemalja, među njima i Srbija, ima jasnu, zakonski predviđenu, zaštitu novinarskih izvora.[6] U Srbiji je to član 58. Zakona o javnom informisanju i medijima (ZJIM[7]), koji pod naslovom Novinarska tajna, određuje da:

„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."

Ovaj član, detaljno analiziran u sledećim poglavljima, je okosnica ove studije, koja teži da ispita, razume i preporuči mere i politike za očuvanje i osnaživanje normativne i institucionalne prakse zaštite novinarskih izvora ili novinarske tajne. Potreba za ovom studijom proističe iz više osnova.

Prvo, Strategija razvoja sistema javnog informisanja u Srbiji 2020-2025 (Medijska Strategija[8]), a posebno tačka 1.3. Zaštita novinarskih izvora, prepoznala je višestruke probleme s kojima se novinari u svom radu sreću. To je pre svega „neovlašćeno presretanje komunikacije i pristup tzv. zadrža-

3 J. Posseti, Zaštita novinarskih izvora u digitalnom okruženju, UNESCO (2017), str.11

4 Ibid., vidi isto: D. Banisar, Silencing sources: An International Survey of Protections and Threats to Journalists' Sources, Privacy International (2007)

5 N. Mugosa i S.Gazivoda, Zaštita novinarskih izvora, Centar za građansko obrazovanje, 2021, str.5

6 J. Posseti, Zaštita novinarskih izvora u digitalnom okruženju, UNESCO (2017), str.18

7 Zakon o javnom informisanju i medijima, "Službeni glasnik RS", br. 92/2023 od 27. oktobra 2023.

8 Strategiju razvoja sistema javnog informisanja u Republici Srbiji za period 2020–2025. godina „Službeni glasnik RS", broj 11 od 7. februara 2020.

nim podacima[9], koji mogu da dovedu do otkrivanja novinarskih izvora, *čak i kada novinar to sam ne čini* [...]. Problem je utoliko veći što državni organi neovlašćeno pristupaju *sadržini komunikacije* i zadržanim podacima.[10]"

Drugo, i pet godina kasnije, ova praksa nadzora je dodatno proširena, tako da su danas pojedini novinari i aktivisti za ljudska prava izloženi, pored pristupa zadržanim podacima i sadržini komunikacije[11], agresivnijim oblicima pristupa kroz tzv. intruzivni softver (spyware), detaljnije analiziran u nastavku.

Treće, i najvažnije, zaštita izvora ili novinarske tajne u ZJIM predstavlja pravno-normativni okvir zaštite, svi drugi „povezani" zakoni, kao što su Zakon o unutrašnjim poslovima, Zakon o elektronskim komunikacijama (ZEK), koji predviđa okvir za zadržavanje podataka, Zakonik o krivičnom postupku (ZKP), i drugi zakoni, moraju biti usaglašeni sa ovom normom.

Metodologija, predmet analize i struktura

Ova uvodna razmatranja pokazuju pravnu logiku i važnost razumevanja šireg normativnog okvira koji je osnov ove analize. Pored toga, analiza detaljno ukazuje na različite prakse koje novinari i medijski radnici koriste u Srbiji u cilju zaštite izvora, očuvanja profesionalnog poverenja i integriteta, i na kraju dana, medijskih sloboda. Analiza takođe ukazuje na ne mali broj slučajeva digitalnog nadzora i pristupa uređajima kroz špijunski softver (spyware), domaće i inostrane proizvodnje.[12] Važno je naglasiti da, bez obzira što u ovim slučajevima cilj digitalnog nadzora nije uvek direktno bio povezan sa otkrivanjem izvora, sama činjenica da je na ovaj način

9 Zadržani podaci su oni podaci o komunikaciji, koje operatori moraju da čuvaju. Uglavnom je reč o meta-podacima (podaci sa baznih stanica, trajanje, početak i kraj komunikacije, vrsta, lokacija i sl.), a koji su posebno definisani u članu 128. ZEK-a.

10 Ibid.

11 Vidi detaljno o tome u sledećem poglavlju.

12 Amnesty International Serbia: "A Digital Prison": Surveillance and the suppression of civil society in Serbia, Amnesty International, 2024. Dostupno na: https://www.amnesty.org/en/documents/eur70/8813/2024/en/

i indirektno mogao biti otkriven izvor odnosno izvori, samo po sebi već predstavlja moguće kršenje člana 58.[13]

Zaštita novinarskih izvora u digitalnom okruženju, suštinski, sve više je *pitanje zaštite podataka* novinara koji su pohranjeni na različitim uređajima kao i tokom njihovog prenosa kroz mrežu, nego što je samo pitanje zaštite novinara, redakcija i domova. Svakako, ova binarna perspektiva ima isključivo praktičnu i ilustrativnu vrednost - da ukaže na značaj oživljavanja člana 58. i sa njim povezanih zakonskih rešenja, na način na koji se može „kontrolisati" uticaj digitalnog nadzora kao što je tajni nadzor komunikacije, pristup zadržanim podacima, kao i korišćenje špijunskog softvera, na medijske slobode, privatnosti i druga ljudska prava novinara i medijskih radnika.

Glavno istraživačko pitanje je - da li je postojeći pravni okvir zakonske zaštite novinarskih izvora u digitalnom represivnom i rizičnom okruženju pruža dovoljan nivo garancija zaštite izvora? Studija dolazi do odgovora kroz unakrsnu procenu tri među-povezana nivoa: i. Pozitivno normativnog okvira u Srbiji, međunarodnih rešenja i evropskog zakonodavstva, ii. Lokalnih institucionalnih dinamika, iii. Medijskog okruženja i prakse. U skladu sa svim navedenim:

1. Normativni okvir obuhvata analizu pozitivno pravnih rešenja u oblasti zaštite izvora, sa posebnim akcentom na norme predviđene u ZJIM, ZKP,[14] ZEK[15], Zakona o bezbednosno-informativnoj agenciji (ZBIA[16]). Pored toga, uporednopravna analiza pojedinih evropskih nacionalnih zakonodavstva, kao i međunarodnih standarda, omo-

13 J. Posetti, Zaštita novinarskih izvora u digitalnom okruženju, UNESCO (2017), str.12 Protecting journalism sources in the digital age; UNESCO series on internet freedom; 2017 - 248054eng.pdf

14 Zakonik o krivičnom postupku, „Službeni glasnik RS", br. 72/2011, 101/2011, 121/2012, 32/2013, 45/2013, 55/2014, 35/2019, 27/2021 i 62/2021

15 Zakon o elektronskim komunikacijama, „Službeni glasnik RS", br. 44/2010, 60/2013 – odluka US, 62/2014, 95/2018 – dr. zakon i 95/2021

16 Zakon o Bezbednosno-informativnoj agenciji, „Službeni glasnik RS", br. 42/2002, 111/2009, 65/2014 – odluka US, 66/2014 i 36/2018

gućava uvid u širu sliku i „mesto" pravnog okvira zaštite novinarskih izvora u Srbiji.

2. Institucionalni okvir pruža uvid u dinamike između novinara, medijskih organizacija, s jedne, i institucija sistema, sa druge strane. Razumevanje ove dinamike je važno zato što su pojedini državni organi, pre svega policija, tužilaštva, sudovi, imaju značajna zakonodavna ovlašćenja, kao i ograničenja u pogledu zaštite novinarskih izvora.

3. Medijsko okruženje i praksa ukazaće na uobičajene prakse rada medija i novinara u cilju zaštite svojih izvora u sistemu koji karakterišu različiti oblici nedemokratskog delovanja i pritisaka na medijski i novinarski rad.

Oblasti koje nisu direktno konvergentne sa pitanjima zaštite izvora, iz uskog ugla zaštite medijskih sloboda i zaštite novinara, nisu obrađivane, iako su važne. Tako, oblasti kao što su javne nabavke opreme za pristup podacima i komunikaciji[17], politike koje ove tehnologije donose kroz različite oblike javno-privatnih partnerstava[18], tehničke specifikacije tehnologija digitalnog nadzora, ostaju van okvira ove analize.[19] Ove teme informisale su rad na ovoj analizi, a naročito saznanja iz oblasti uticaja biometrijskog nadzora na medijske slobode,[20] policijske istražne radnje koje se oslanjaju na pristup podacima na društvenim mrežama, i policijske i tužilačke radnje koje pristupaju podacima kroz različite oblike zloupotrebe ovlašćenja.[21]

17 J. Roberts et al., Mythical beasts and where to find them: Mapping the global spyware market and its threats to national security and human rights, Atlantic Council (2024), S. Woodhams, Spyware: An unregulated and escalating threat to indepedent media, CIMA (2021), B. Marczak,Triple Threat: NSO Group Pegasus Spyware Returns in 2022 with a Trio of iOS15 and iOS16 Zero-Click Exploit Chains, The Citizen Lab (2023)

18 E. Jakubovska et al., Beyond the face: Biometrics and society, Share Foundation (2023), B. Kostić Nekontrolisani nadzor, nekontrolisane posledice, OEBS Misija u Srbiji (neobjavljeno)

19 Ibid., fn. 16

20 B. Kostić Nekontrolisani nadzor, nekontrolisane posledice, OEBS Misija u Srbiji (neobjavljeno)

21 Informacije na ove teme dobijene su uglavnom kroz intervjue, ali i usko-stručnu literaturu praksi drugih zemalja.

Analiza zaštite novinarskih izvora u digitalnom okruženju oslanja se na dva metodološka instrumenta. Normativnopravna analiza će biti zasnovana na desk istraživanju akademske i stručne literature, kao i pravnonormativnog okvira zemalja Evropske unije, EU zakonodavstva, međunarodnih propisa, posebno imajući u vidu bogatu jurisprudenciju Evropskog suda za ljudska prava. Kroz uporednopravnu analizu biće identifikovana različita zakonodavna rešenja, sa posebnim akcentom na digitalne politike država i osvrtom na član 4. Evropskog Akta o medijskim slobodama (EMFA[22]) koji posebno normira obavezu država da zaštite novinarske izvore i novinare od intruzivnih tehnologija digitalnog nadzora, uključujući i špijunskog softvera (spyware-a). Međunarodni standardi zaštite novinarskih izvora postoje, ali, kao i većina standarda, „pate" od neodređenosti, te će oni biti navedeni, ali i obrađivani u onom delu u kom su važni za razumevanje digitalnog aspekta, sa akcentom na presude Evropskog suda za ljudska prava.

Ovako identifikovan pravnonormativni okvir zaštite ukazaće na uporednopravnu logiku i težnje zakonodavaca. Paralelno sa analizom pozitivnopravnog okvira, skicirana je i mapa institucija koje, na jedan ili drugi način, imaju ulogu u zaštiti novinarskih izvora. Njihove normativne obaveze, naročito one koje se odnose na krivično procesno postupanje, su, oslanjajući se na drugi metodološki instrument - intervjue, analizirane kako bi se utvrdio stepen usaglašenosti između normativne obaveze institucija i njihovog stvarnog postupanja. Važno je pojasniti da, iz ugla zaštite novinarskih izvora, nije nužno svaka radnja institucija sistema, ne samo policije, direktno povezana sa namerom otkrivanja novinarskih izvora. U velikom broju slučajeva reč je, zapravo, o zastrašivanju, koje kreira mogućnosti nadzora nad dnevnim aktivnostima novinara koje neminovno uključuju, zbog prirode posla, komunikaciju sa izvorima. *Zbog toga, „ukupan uticaj nadzora na zaštitu izvora i novinarstvo, koje je zavisno od tajnosti izvora, je pod snažnim uticajem presretanja, ‚zarobljavanja' i dugotrajnog skla-*

22 Predlog Evropskog akta o slobodi medija (EMFA), COM(2022) 457 final, Predlog uredbe Evropskog parlamenta i Saveta o uspostavljanju zajedničkih pravila za zaštitu pluralizma i nezavisnosti medija u Uniji i o uspostavljanju Evropskog odbora za medijske usluge.

dištenja podataka od strane posrednika.[23]" U tim okolnostima, pravne mere zaštite izvora koje štite novinara od otkrivanja izvora mogu se zaobići *kroz „backdoor" pristup podacima.*

Drugi metodološki instrument koji je korišćen su polu-strukturirani, dubinski intervjui. Oni su organizovani online i uživo (prema raspoloživosti intervjuisanih) i uključili su 17 aktera iz medijskog sektora: novinare, urednike, medijsko pravne eksperte i predstavnike civilnog sektora. Okvirna pitanja za intervjue su obuhvatala mapiranje praksi rada novinara sa izvorima, a naročito digitalnih alata koji se koriste u ove svrhe; samoprocene o znanju, resursima i interim kapacitetima; svest o upotrebi spyware-a i drugih tehničkih alata za nadzor; uticaj na izbor tema i sagovornika; praksa zaštite izvora u kontekstu policijskih ili drugih istraga i sudskih postupaka; primena zakonodavnih mera i sl. Sagovornici za intervjue birani su među novinarima i urednicima koji rade u nezavisnim medijima u Srbiji, poznatim po kritičkom i istraživačkom uređivačkom pristupu. Odabrani su jer se, zbog prirode tema kojima se bave, s pravom može pretpostaviti da bi mogli biti meta digitalnog nadzora i drugih oblika pritisaka. Sagovornici su, takođe, iskusni medijski radnici, sa zavidnim iskustvom. Svi njihovi citati i izjave su anonimizovani, kao garancija da svoja iskustva mogu slobodno da podele tokom razgovora i učešća u istraživanju. Među njima je devet muškaraca i osam žena, međutim, svi su u izveštaju obeleženi muškim rodom kako bi se dodatno zaštitio njihov identitet.

Na tako zasnovanim podacima, kroz perspektivu tri navedena okvira, formulisane su preporuke u vezi sa pravnim okvirom zaštite novinarskih izvora u digitalnom okruženju. U najkraćem, analiza će odgovoriti na pitanje da li je potrebno izmeniti pravnu normu iz ZJIM i osnažiti je tako da prepozna i odgovori na izazove digitalnog okruženja. To se prvenstveno odnosi na nadzor u javnom i privatnom prostoru, presretanje digitalne komunikacije, korišćenje intruzivnog softvera (spyware) i sa njima povezane oblike zastrašivanja i pritisaka kao što su targetiranje novinara kroz

23 J. Posetti, Zaštita novinarskih izvora u digitalnom okruženju, UNESCO (2017), str.23

javne nastupe političkih elita, policijska saslušanja, kao i saslušanja od strane pripadnika državne bezbednosti.[24] Iako je možda valjalo navesti na početku, neka ostane za kraj uvoda da se digitalno okruženje ne sme posmatrati izolovano od „fizičkog" prostora - već sveobuhvatno kao međusobno prožimajući splet tehnologije, institucija, novinarskog rada i praksi medijskog izveštavanja naspram kojih stoji horizontalna pravna norma iz ZJIM, i sa njom druge povezane pozitivnopravne norme.

Analiza, nakon uvoda, predstavlja prakse digitalnog nadzora nad novinarima i posredno izvorima, kao i mehanizme zaštite koje novinari primenjuju, ukazujući na stepen razumevanja sveprožimajućeg nadzora i njegovih posledica. Pravna razmatranja, u trećem poglavlju, analiziraju uže normu iz člana 58. ZJIM, a zatim njenu povezanost, šire sa drugim pravnim normama, a kroz prizmu prakse digitalnog nadzora. Kroz analizu, uporednopravnu i međunarodnu, ova pravna razmatranja biće stavljena u normativni kontekst korekcije i kontrole mera digitalnog nadzora. Te mere su tek u povoju i teško mogu da odgovore na narušavanja slobode medija i bezbednosti novinara kojima Srbija svedoči. Zbog toga, poslednje poglavlje, u delu zaključci i preporuke samo *podvlači moguće putanje kretanja u ovoj oblasti,* a detaljnije preporuke i strateški principi zaštite, u skladu sa ustavno-pravnim garancijama i vladavinom prava, mogu biti predloženi kada se Srbija svrsishodno i u dobroj veri posveti izgradnji zaštite medijskih sloboda i bezbednosti novinara - kao stubu demokratije i vladavine prava.

24 O napadima na novinare, vidi monitoring Safe Journalists Mreže, dostupno na: https://safejournalists.net/sr/

2. Medijska praksa

Društveni kontekst

Aktuelni politički sistem Srbije se u relevantnim međunarodnim dokumentima obično opisuje kao sistem oslabljenih demokratskih kapaciteta i ograničenih prava i sloboda građana[25]. Politička moć se sve više centralizuje u rukama izvršne vlasti i političkog vrha, dok moć institucija, naročito onih kontrolnih, ali i parlamenta i sudstva, rapidno slabi, pokazuju brojni nezavisni izveštaji.

Ovaj politički kontekst karakteriše i duboka polarizacija društva, u kojoj se politički neistomišljenici i kritičari vlasti označavaju kao neprijatelji, a javna debata o suštinski važnim pitanjima gotovo da potpuno izostaje[26]. Ograničeni mehanizmi kontrole dodatno otežavaju otkrivanje i osporavanje zloupotreba moći, na šta upozoravaju godišnji izveštaji o napretku u EU integracijama[27], ali i druge međunarodne institucije poput Freedom House[28], Reporters Without Borders[29] ili Instituta V Dem[30]. Upravo ovakav

25 O stanju političkog sistema Srbije, videti više u godišnjem izveštaju Evropske Komisije za 2024. godinu, dostupno na: https://enlargement.ec.europa.eu/document/download/3c8c2d7f-bff7-44eb-b868-414730cc5902_en?filename=Serbia%20Report%202024.pdf

26 Govor Komesara UN za ljudska prava (2025), dostupno na: https://serbia.un.org/en/294822-statement-un-high-commissioner-human-rights-conclusion-his-visit-serbia

27 Evropska komisija, Godišnji izveštaj o napretku Srbije za 2024. godinu. Dostupno na: https://enlargement.ec.europa.eu/document/download/3c8c2d7f-bff7-44eb-b868-414730cc5902_en?filename=Serbia%20Report%202024.pdf

28 Freedom House, Izveštaj "Freedom of the World" za 2025. godinu, sekcija za Srbiju. Dostupno na: https://freedomhouse.org/country/serbia/freedom-world/2025

29 Reporters Without Borders, izveštaj za Srbiju za 2025. godinu. Dostupno na: https://rsf.org/en/country/serbia

30 Institute V Dem, izveštaj "Democracy Report" 2025. Dostupno na: https://www.v-dem.net/documents/61/v-dem-dr__2025_lowres_v2.pdf

kontekst omogućava lakše uvođenje i širenje tehnologija nadzora, koje se mogu koristiti za dalje jačanje političke kontrole i suzbijanje kritičkih glasova, predstavljajući tako dodatni izazov i za demokratiju i ljudska prava u Srbiji.

Brojna istraživanja medija i civilnog društva svedoče o značajnoj ekspanziji upotrebe tehnologija digitalnog nadzora u Srbiji u poslednjih nekoliko godina. Na primer, Share fondacija je detaljno mapirala uvođenje biometrijskog nadzora saobraćajnica[31] i postavljanje Huawei kamera[32] sa mogućnošću prepoznavanja lica u gradskim sredinama. Nacrt Zakona o unutrašnjim poslovima je nakon instaliranja kamera sa biometrijskim mogućnostima pokušao da zakonski uokviri ovaj proces, ali i da proširi ovlašćenja policije u ovom domenu[33], sa nedovoljno razvijenim mehanizmima kontrole. Nacrt Zakona je povučen iz rasprave dva puta[34], ali kamere sa mogućnošću biometrijskog nadzora su i dalje prisutne na ulicama.

BIRN-ov izveštaj o javnim nabavkama[35] pokazao je milionske investicije različitih državnih institucija u sofisticirane sisteme nadzora, uključujući softvere za praćenje komunikacija, analitiku i video nadzor koji se postavlja na javnim površinama, saobraćajnicama, pijacama, školama, prosvet-

31 Share fondacija, projekat Hiljade kamera. Dostupno na: https://hiljade.kamera.rs/sr/pocetna/

32 Share fondacija, Huawei zna sve o kamerama u Beogradu – i nije im teško da to i kažu!. Dostupno na: https://sharefoundation.info/huawei-zna-sve-o-kamerama-u-beogradu-i-nije-im-tesko-da-to-i-kazu/

33 NUNS, Nacrt Zakona o unutrašnjim poslovima ugrožava širok korpus ljudskih prava, NUNS, 2021, dostupno na: https://nuns.rs/nacrt-zakona-o-unutrasnjim-poslovima-ugrozava-sirok-korpus-ljudskih-prava

34 I. Krstić, Šta predlaže novi zakon o policiji? Biometrijski nadzor, pretresi bez naloga i primena sile bez povoda, Mašina, 2022, dostupno na: https://www.masina.rs/sta-predlaze-novi-zakon-o-policiji-biometrijski-nadzor-pretresi-bez-naloga-i-primena-sile-bez-povoda/

35 BIRN Srbija, izveštaj Nadzor bez kontrole: Javne nabavke tehnologija za digitalni nadzor u Srbiji (2025). Dostupno na: https://birnsrbija.rs/nadzor-bez-kontrole-javne-nabavke-tehnologija-za-digitalni-nadzor-u-srbiji/

nim i zdravstvenim ustanovama i sl. Istraživanje nedeljnika Radar[36] donosi svedočenja o nabavci opreme uz zloupotrebu finansija javnih preduzeća, pa se tako govori o nabavci „minijaturnih audio-snimača, dronova, kamera visoke osetljivosti opremljenih senzorima, kamera za prepoznavanje lica, GPS lokatora, ometača signala, softvera za analizu ličnih podataka“, kao i o upadima na naloge na društvenim mrežama.

Ovako ubrzana implementacija nadzornih tehnologija bez adekvatne javne rasprave, zakonodavnog okvira i institucionalne kontrole, kulminirala je krajem 2024. godine, kada su se u javnosti prvi put pojavili dokazi o upotrebi spyware-a, jednog od najintruzivnijih alata za praćenje i kontrolu komunikacija.

U decembru 2024. godine izveštaj BIRN-a i forenzička analiza međunarodne organizacije Amnesty International[37], otkrili su da je srpska Bezbednosno-informativna agencija (BIA) nezakonito otključavala telefone novinara i aktivista koje je pozivala ili privodila na razgovore, a potom na te uređaje instalirala spyware – maliciozni kompjuterski softver dizajniran tako da tajno nadgleda, prikuplja i prenosi podatke o aktivnostima korisnika bez znanja ili pristanka (vidi više o spyware i regulaciji u sledećem poglavlju). Kako je pokazala forenzička analiza Amnesty International-a[38], mobilni telefoni četvorice građanskih aktivista i jednog novinara, najpre su „otključavani“ izraelskim softverom Cellebrite, a zatim je na njih instaliran domaći špijunski softver NoviSpy koji je sa njihovih telefona preuzimao veliku količinu ličnih podataka, fotografija, kontakata, poruka i sl.

36 Milan Radonjić, Kako vlast nadzire i kontroliše građane, nedeljnik Radar (2025). Dostupno na: https://radar.nova.rs/drustvo/alternativni-centri-moci-zvucni-top-mup-bia/

37 Aleksa Tešić, Dokazano: BIA hakuje telefone aktivista, BIRN (2024). Dostupno na: https://birn.rs/hakovanje-telefona-bia-spijunaza-aktivista/

38 Amnesty International, izveštaj A Digital Prison (2024). Dostupno na: https://www.amnesty.org/en/wp-content/uploads/2024/12/EUR7088132024ENGLISH.pdf

Osim toga, tehnički dokazi Amnesty International-a[39] pokazuju i da je tokom jednog meseca generisano i potencijalno instalirano više od 20 različitih uzoraka NoviSpy softvera, što ukazuje na mnogo širi obim nadzora.

Samo tri meseca kasnije, dve novinarke BIRN-a[40] bile su mete neuspelog pokušaja instalacije špijunskog softvera Pegasus na njihove telefone. Poruka na srpskom jeziku, sa zaraženim linkom, poslata je putem Vibera, koja je naizgled ličila na obraćanje izvora, ali je zapravo sadržala linkove ka malicioznom softveru. Napad, na sreću, nije bio uspešan jer novinarke nisu kliknule na pomenuti link.

Moćne tehnologije digitalnog nadzora u rukama nedemokratskih vlasti postaju sredstvo kontrole nad društvom i „utišavanja" kritičkih glasova, kako pokazuju rezultati istraživanja u zemljama u kojima su ranije otkriveni slučajevi zloupotrebe spyware-a[41]. Ovakva tehnologija omogućava vlastima da prate komunikaciju, prikupljaju informacije, identifikuju izvore i unapred uguše ili diskredituju inicijative koje bi mogle mobilisati javnost. Upravo zato su najčešće žrtve špijunskog softvera aktivisti za ljudska prava, demonstranti, opozicioni političari i nezavisni novinari, čiji je rad usmeren na razotkrivanje zloupotreba i kritiku vlasti.

Nadzor se često intenzivira upravo u trenucima kada raste građanski otpor, jer vlasti nastoje da preduprede ili uguše mobilizaciju i kritiku. To se jasno vidi i u kontekstu aktuelnih studentskih i građanskih protesta, kada se pojačava praćenje komunikacija i fizičkog kretanja[42], identifikacija

39 Ibid.

40 A. Tešić, Dve novinarke BIRN-a mete Pegazus špijunskog programa, BIRN (2025). Dostupno na: https://birn.rs/birn-novinarke-meta-pegazus-spijunaza/

41 Amnesty International, The Pegasus Project. Dostupno na: https://securitylab.amnesty.org/case-study-the-pegasus-project/

42 J. Zorić, G. Andrić, Protesti u Srbiji: Kako i zašto informacije o kritičarima režima cure u tabloide, BIRN (2024). Dostupno na: https://birn.rs/zasto-cure-informacije-o-kriticarima-vlasti/

organizatora protesta[43], snimanje učesnika i prisustvo nadzornih kamera na mestima okupljanja, kao i privođenje i oduzimanje tehničke opreme[44].

Medijski sistem Srbije

U dostupnoj literaturi, medijski sistem Srbije opisuje se kao „zarobljen" (engl. captured)[45], što znači da je pod strogom, institucionalnom i finansijskom kontrolom političkih ili ekonomskih centara moći. Umesto da služe javnom interesu, tako kontrolisani mediji selektivno izveštavaju, i rade u službi određenih centara (moći), dok nezavisni i kritički glasovi bivaju sistemski marginalizovani, finansijski pritisnuti ili diskreditovani. Aktuelna vlast posebno ima uticaj na televizije s nacionalnom frekvencijom i tabloidnu štampu, što se vidi po direktnim i indirektnim vlasničkim vezama, kao i plasiranom sadržaju i uređivačkim politikama[46].

U relevantnim međunarodnim i domaćim izveštajima mogu se naći brojni opisi i ocene ovakvog stanja medijskog sistema Srbije. Na primer, Reporteri bez granica u svom godišnjem izveštaju o stanju slobode medija za 2025. godinu,[47] srpskom medijskom sistemu daju 53 boda, što je do sada najmanje zabeleženi broj bodova. Slično tome, istraživanje Media Pluralism

43 N1 Beograd, "Novosti" ugrožavaju bezbednost studenata (2025). Dostupno na: https://n1info.rs/vesti/novosti-ugrozavaju-bezbednost-studenata/

44 A. Tešić, Nova žrtva špijunskog nadzora: Student priveden na šest sati, telefon mu hakovan, BIRN (2025). Dostupno na: https://birn.rs/student-spijunski-nadzor-hakovan-telefon/

45 MFFR Serbia Mission Report, izveštaj Findings and recommendations following the MFRR solidarity mission to Serbia in April 2025. Dostupno na: https://ipi.media/wp-content/uploads/2025/05/MFRR-Serbia-Mission-Report-May-2025.pdf

46 Istraživanja Media Ownership Mintor za Srbiju, Global Media Registry i BIRN (2023). Dostupno na: https://serbia.mom-gmr.org/en/

47 Reporters Without Borders, izveštaj za Srbiju za 2025. godinu. Dostupno na: https://rsf.org/en/country/serbia

Monitor za 2025. godinu[48] mapira visok nivo rizika u tri od četiri ključne oblasti: tržišni pluralizam, politička nezavisnost i društvena uključenost.

Digitalni prostor smatra se generalno otvorenim i slobodnim, zahvaljujući čemu i opstaje veliki broj nezavisnih medija, ali ni on nije bez limita. Algoritamsko okruženje[49] pogoduje brzom i nekvalitetnom novinarstvu, dok su vodeći mediji, koji ostvaruju najveći deo prihoda na tržištu digitalnog oglašavanja, prilagodili proizvodnju i distribuciju sadržaja logici velikih platformi.

Aktuelna vlast na različite načine pokušava da utiče i na taj segment informisanja i koristi ga kao alat za kontrolu narativa i suzbijanje kritičkih glasova, najpre, oslanjajući se na mreže tzv. „botova" i „trolova" koje orkestrirano šire propagandne poruke, često preko anonimnih profila[50]. Sadržaji koji nastaju u digitalnom prostoru brzo se prelivaju i u analogni – kroz tabloidnu štampu, televizije sa nacionalnom frekvencijom i kampanje diskreditacije koje podstiču visoko rangirani političari – čime se efekat propagande dodatno pojačava[51].

Upravljanje finansijskim resursima pokazalo se kao jedan od najefikasnijih mehanizama kontrole medija. Nezavisni i istraživački mediji suočavaju se s finansijskim pritiscima, ograničenim pristupom oglašivačima i javnim fondovima. Javna preduzeća i državne institucije često koriste javne konkurse i državno oglašavanje kao mehanizam nagrađivanja „prijatelj-

48 I. Milutinović, izveštaj Media Pluralism Monitor za 2025. godinu za Srbiju, European University Institute (2025). Dostupno na: https://cadmus.eui.eu/entities/publication/e176c784-969b-4b57-bbad-829df1e44cbe

49 B.Kostić i T. Maksić, Algoritmi, mreže i održivost medija: Igra velikih brojki, BIRN (2023). Dostupno na: https://birnsrbija.rs/algoritmi-mreze-i-odrzivost-medija-igra-velikih-brojki/

50 Videti, na primer, akciju kompanije Twitter koja je sa svoje mreže uklonila preko 8.500 naloga koji su orkestrirano promovisali vladajuću stranku (2020.). Dostupno na: https://www.rferl.org/a/serbia-twitter-vucic-sns-serbian-progressive-party/30526199.html

51 FoNet, Botovi SNS-a na Fejsbuku imali 5.374 profila: Objavljen izveštaj Mete o gašenju provladinih naloga u Srbiji, Kubi i Boliviji, Danas (2023). Dostupno na: https://www.danas.rs/vesti/politika/botovi-sns-a-na-fejsbuku-imali-5-374-profila-objavljen-izvestaj-mete-o-gasenju-provladinih-naloga-u-srbiji-kubi-i-boliviji/

skih“ i sankcionisanja kritičkih medija. Istraživanja BIRN-a o distribuciji novca kroz konkurse[52] i javne nabavke[53] pokazuje favorizovanje dodeljivanja projekata i ugovora medijima koji su bliski vlasti[54]. Do sličnih zaključaka došla su i istraživanja Asocijacije nezavisnih elektronskih medija (ANEM)[55], Udruženja novinara Srbije[56] kao i brojna saopštenja Koalicije za slobodu medija[57].

Duboka polarizacija i podela očituje se kroz medijski sadržaj, koji je generalno niskog kvaliteta i ne doprinosi javnom diskursu i demokratskoj debati. Kako konstatuje izveštaj Novosadske novinarske škole[58], nedostatak pluralizma i monopol na objavljivanje informacija je dugogodišnji problem koji opterećuje sferu javnog informisanja.

Bezbednost novinara i medijskih radnika, u takvom okruženju, često je ugrožena – i u fizičkom i u digitalnom prostoru, kao i učestalim tzv. SLAPP tužbama. Baza napada na novinare[59] Nezavisnog udruženja novinara Srbije pokazuje da je u prvoj polovini 2025. godine bilo čak 135 zabeleženih napada i pritisaka (što je bio ukupni skor za neke od prethodnih

52 BIRN Srbija, izveštaj Pregled projektnog finansiranja u oblastima medija, civilnog društva, kulture i omladine u periodu od 2019. do 2024. godine: između podrške i pritiska (2025). Dostupno na: https://birnsrbija.rs/javno-o-javnim-konkursima-2019-2024/

53 BIRN Srbija, izveštaj Transparentnost pod lupom: Javne nabavke za medijske usluge (2025). Dostupno na: https://birnsrbija.rs/transparentnost-pod-lupom-javne-nabavke-za-medijske-usluge/

54 Cenzolovka, odabrani tekstovi o projektnom sufinansiranju u Srbiji. Dostupno na: https://www.cenzolovka.rs/tag/projektno-sufinansiranje-medija/

55 ANEM, sekcija posvećena praćenju i analizi konkursa za projektno sufinansiranje medija. Dostupno na: https://anem.org.rs/sr/projektno-sufinansiranje/analize-projektno-sufinansiranje

56 UNS, sekcija posvećena praćenju sprovođenja javnih konkursa, dostupno na: https://uns.org.rs/sr/desk/akcija.html

57 Koalicija za slobodu medija, Publikacije, dostupno na: https://koalicijazaslobodumedija.rs/publikacije/

58 Novosadska novinarska škola, izveštaj Monopol prisutan – pluralizam odsutan (2025). Dostupno na: https://novinarska-skola.org.rs/publication/monopol-prisutan-pluralizam-odsutan/

59 NUNS, Baza napada na novinare. Dostupno na: https://nuns.rs/baza-nuns/?keyword=&gender=&type_of_incident=&life_threat_type=&physical_attack_type=&organisation_attack_type=&organisation_threat_type=&pressure_type=&type_of_media=&incident_year=& page=1

godina), a da je od tog broja čak 19 fizičkih napada na novinare. Ovako veliki broj napada posledica je, prvenstveno, intenziviranih studentskih i građanskih protesta na kojima je posebno ugrožena bezbednost novinara. Monitoring Share Fondacije[60] je za prethodnih deset godina zabeležio 427 povreda prava medija i novinara u digitalnom prostoru, od toga 19 u prvoj polovini 2025. godine. Ove povrede uključuju različite vrste pretnji, manipulacije sadržajem, verbalne napade, tehničke napade i sl.

Porastu broja slučajeva ugrožavanja bezbednosti, među koje spada i digitalni nadzor, pogoduje i neadekvatna reakcija institucija, pre svega, policije i tužilaštva i veliki nivo nekažnjivosti. Dostupni izveštaji Stalne radne grupe za bezbednost novinara[61] govore da nadležna tužilaštva formiraju relativno mali broj predmeta, a da još manji broj završi sudskom odlukom. Ovakvo ponašanje institucija ne doprinosi u dovoljnoj meri tzv. „efektu odvraćanja“ potencijalnih izvršilaca, iako se zakonska norma koja reguliše ovu oblast smatra u dobroj meri adekvatnom.

Važnost zaštite novinarskih izvora

Zaštita novinarskih izvora jedno je od ključnih novinarskih prava i profesionalnih privilegija, koje garantuje slobodu informisanja. Ono podrazumeva pravo „anonimizacije“ sagovornika tj. pravo novinara da ne otkriju identitet osoba koje su im poverile informacije, naročito kada su te informacije ključne za ostvarivanje javnog interesa u informisanju. Ovo pravo je posebno važno za forme novinarstva poput istraživačkog, jer omogućava izvorima da bez straha od odmazde ili posledica (u ličnom ili profesionalnom životu) podele važne podatke, dokumenta i svedočenja o korupciji, zloupotrebama vlasti ili drugim temama od interesa za društvo.

60 Share Fondacija, Praćenje povreda digitalnih prava i onlajn povreda u Srbiji. Dostupno na: https://monitoring.labs.rs/

61 N. Jovanivić, V. Matić i M. Janković, Izveštaj o radu Stalne radne grupe za bezbednost novinara za 2023. godinu, OSCE (2024). Dostupno na: https://www.osce.org/files/f/documents/c/f/564302.pdf

Digitalne komunikacije i okruženje fundamentalno su promenili ne samo novinarske prakse rada, već i njihov odnos prema zaštiti izvora. Ključni problem leži u gotovo neograničenim mogućnostima tehnologija digitalnog nadzora naročito u okruženjima gde su medijske slobode i nezavisno novinarstvo na udaru, kao što je slučaj u Srbiji.

Problem digitalnog nadzora povezan je sa konceptom „skupa nadzornih instrumenata" (engl. „surveillance assemblage")[62]. Prema autorima ovog koncepta, digitalni nadzor ne podrazumeva tehnički nepovezane elemente, već dinamični i stalno promenljivi sistem koji oblikuju politički, ekonomski, društveni i kulturni faktori.

U praksi, zaštita izvora obuhvata tehničke, pravne, i etičke mere koje novinari i redakcije primenjuju kako bi sačuvali identitet izvora i poverljivost komunikacije. To uključuje korišćenje sigurnih i šifrovanih kanala komunikacije, čuvanje dokumentacije na sigurnim digitalnim uređajima, ali i spremnost da se odbije zahtev suda, policije ili drugih organa vlasti za otkrivanje izvora.

Zaštita izvora u tesnoj je vezi sa nekoliko fundamentalnih principa slobode medija. Najpre, u bliskoj je vezi sa poverenjem. Bez poverenja da će njihov identitet ostati zaštićen, izvori ne bi bili spremni da podele osetljive informacije sa novinarima. Kada se poverenje naruši, bilo kroz curenje informacija ili prinudno otkrivanje izvora, to ne utiče samo na jedan slučaj, već dugoročno podriva ulogu novinarstva kao kontrolora vlasti i čuvara javnog interesa.

Drugi temeljni princip je bezbednost, i podrazumeva garancije zaštite i za novinare i za njihove izvore. Kada je identitet izvora zaštićen, smanjuje se rizik od pretnji, pritisaka i nasilja, posebno u sistemima u kojima je moć koncentrisana ili ne postoje dovoljno čvrste institucionalne garancije zaštite. Za novinare, ove garancije znače i njihovu sopstvenu bezbednost

62 Videti više u P. di Salvo, Digital Journalism, (2024)

– jer očuvanje poverljivosti izvora štiti i njih same od sudskih pritisaka, nadzora ili kriminalizacije rada.

Zaštita novinarskih izvora direktno doprinosi principu medijskog pluralizma jer omogućava novinarima iz različitih medija – velikih, malih, nezavisnih ili lokalnih – da slobodno istražuju i izveštavaju o temama od javnog značaja. Kada izvori znaju da će njihov identitet biti zaštićen, spremniji su da se obrate i manje uticajnim ili kritički nastrojenim medijima, čime se jača raznovrsnost glasova i perspektiva u javnom prostoru. Zaštita izvora tako postaje preduslov za postojanje otvorenog, pluralističkog i demokratskog medijskog okruženja.

Poverljivost podrazumeva i princip odgovornosti novinara da zaštiti identitet izvora koji su tražili anonimnost i upravo zbog toga je deo šireg, etičkog okvira rada novinara i ključni element profesionalnog integriteta. Kodeks novinara i novinarki Srbije[63] (izmenjen i dopunjen u decembru 2024) posvećuje celu glavu VIII odnosu novinara i izvora, navodeći, između ostalog, da „anonimnost treba omogućiti samo izvorima koji mogu da pruže važne podatke ili informacije iz prve ruke, odnosno dokumenta od javnog interesa“.

Iako je ova zaštita prepoznata u različitim pravnim i zakonskim odredbama, ona često zavisi od primene pravnog okvira, volje institucija sistema, pravosudnih organa i vlasti da poštuju norme, i kapaciteta novinara da prepoznaju i odgovore na digitalne i institucionalne pretnje, kao što će u nastavku pokazati i rezultati ovog istraživanja.

63 Savet za štampu, Kodeks novinara i novinarki Srbije, dopunjeno izdanje (2025). Dostupno na: https://savetzastampu.rs/wp-content/uploads/2024/12/KODEKS-novinara-i-novinarki-2025-korekcija.pdf

Nalazi istraživanja

U ovom delu izveštaja predstavljeni su glavni nalazi istraživanja o praksama zaštite novinarskih izvora, dobijene kroz direktne razgovore i intervjue sa novinarima i urednicima domaćih medija. Indirektni dokazi o ovim praksama dobijeni su kroz razgovore sa advokatima i pravnicima koji ih zastupaju na sudu ili pružaju pravne savete, kao i sa predstavnicima civilnog društva.

Ovi razgovori donose svedočanstva o visoko razvijenoj svesti predstavnika medija o potrebi očuvanja identiteta izvora, naročito u kontekstu „zarobljenih" medija i strogo kontrolisanog informacionog prostora, ali i o porastu pritisaka i nelegalnih praksi u pokušajima njihovog otkrivanja.

A. Digitalni alati i porast nepoverenja

Promene tehnološkog okvira funkcionisanja medija fundamentalno su izmenile procese rada medija (prikupljanje i distribucija informacija, odnos sa publikom) i dodatno su uticale na promenu načina komunikacije novinara sa izvorima. Digitalni kanali doneli su bržu, neposredniju i dvosmernu razmenu informacija, ali su istovremeno otvorili nova pitanja bezbednosti i poverljivosti.

Elektronska komunikacija i digitalni tragovi postali su potencijalna slaba tačka koja se može iskoristiti za identifikaciju i kompromitaciju izvora ili pak samih novinara i njihove privatnosti. Dostupna tehnologija, lako upravljanje aplikacijama za nadzor, velika količina dobijenih podataka kao i podaci dostupni na društvenim mrežama („*gledaju šta like-uješ, like je kao virus, reklame koje pratiš...*") zapravo omogućavaju profilisanje potencijalnih „meta" – bilo da su oni novinari ili njihovi izvori. Upravo zato je potreba za razumevanjem i primenom mera bezbednosti i tzv. „digitalne higijene" postala sastavni deo profesionalne odgovornosti novinara.

Gotovo svi sagovornici navode aplikaciju Signal, kao jedan od najsigurnijih digitalnih alata pogodnu za neposrednu komunikaciju ili razmenu osetljivih podataka ili dokumenata sa izvorima („*pokazala se kao najjednostavnija, a do sada se nije pokazalo da ima neke probleme ili bagove*“).

Osim pomenutog Signala, postoji čitav niz manje ili više razvijenih praksi zaštićene komunikacije sa izvorima.

> *„Imamo trostruku proveru izvora. Prvo se preko Signala dogovorimo da se nađemo negde, onda se tamo sretnemo, usmeno se dogovorimo za detalje gde, kada i kako da se sretnemo, pa se onda treći put viđamo sa izvorima (Sagovornik 14).”*

Razlike u praksama rada sa izvorima potiču, najpre, zbog prirode samih medija (lokalni, nacionalni ili istraživački mediji) kao i njihovih različitih potreba (da li se bave dnevnim informisanjem ili temama poput crne hronike ili korupcije i sl. u kom su izvori po pravilu „osetljiviji“). Očekivano, istraživački mediji prednjače po razvijenosti praksi digitalne bezbednosti, zaštite komunikacije i dokumenata.

> *„Mi imamo svoju javnu i internu verziju bezbednosnog pravilnika. Javna verzija pravilnika je ono što mogu da ispričam tebi ili na televiziji, a to je da enkriptujemo sve poverljive podatke, koristimo Signal itd. Interna verzija se odnosi na to kako jedni sa drugima komuniciramo, ko je za šta nadležan iz te oblasti, kako pazimo jedni na druge itd. (Sagovornik 3).”*

Sa druge strane, potrebe lokalnih medija su nešto drugačije. Teme kojima se oni bave tiču se lokalnih prilika, koje nemaju veliki uticaj na nacionalnom nivou, pa je i rizik od nadzora ili otkrivanja izvora nešto umanjen.

> *„Najčešće šta se dešava je da nas kontaktira neko, da li putem društvenih mreža, putem mejla ili zove na telefon. Ukoliko osetimo da je u pitanju nešto osetljivije, onda uglavnom zovemo da se vidimo uživo sa ljudima, da nam ništa ne šalju. A ukoliko je neki komunalni problem, onda kažemo šaljite na mejl." (Sagovornik 5)*

Poverenje građana u lokalne medije meri se poverenjem građana da im javljaju osetljive informacije, naročito u trenucima kada institucionalni mehanizmi zakažu.

> *„Mi imamo na sajtu rubriku ‚prijavi problem'. Na početku su tu građani prijavljivali komunalne probleme, međutim, sad nam stiže sve više škakljivih tema. Jednom sam tako dobio anonimnu prijavu o trgovini glasova za vreme izbora (Sagovornik 14)."*

Svest o gotovo sveprisutnom digitalnom nadzoru mnoge sagovornike je navela da se zapravo odreknu digitalnih praksi i komunikaciju sa izvorima obavljaju bez elektronskih uređaja. Sama mogućnost praćenja poruka, poziva ili lokacije dovela je do opreza koji podrazumeva povratak na lične susrete, angažovanje posrednika i prenošenje informacija „uživo".

Mnogi sagovornici tako navode da uopšte ne nose mobilni telefon kada idu na razgovor sa poverljivim izvorom, da stavljaju „naočare i kačket", da izvori ostavljaju dokumenta u „radnji", da nekad moraju da idu u drugi grad, pa čak i to da se sa „*ljudima srećemo u parkovima, na grobljima, na takvim nekakvim neverovatnim mestima*".

> *Imali smo situacije gde se nalazimo sa osobom, naravno bez telefona. Praksa je da dogovorimo susret na nekom mestu, ali često se desi da se dogovorimo za jedno mesto, a onda sa tom osobom odemo na neko drugo. Važno je stignemo prvi i da sednemo tako da imamo pregled cele prostorije, kao i da na kraju ne odemo zajedno (Sagovornik 1)."*

Osim susreta sa izvorima, izbegava se i slanje poverljivih dokumenata elektronskim putem, osim ako je neophodno, a tada se koriste enkripcija ili fizički prenos (USB, štampana kopija (engl. hard copy)).

> *„Naši uređaji su redovno ažurirani... Dokumente koji su poverljive prirode čuvamo na kriptovanim diskovima, a koristimo i sigurne servise za deljenje fajlova kada je to neophodno. Radimo redovne bekape, i vodimo računa o tzv. digitalnoj higijeni – dakle, ne otvaramo fajlove iz neproverenih izvora, ne radimo s javnih Wi-Fi mreža, i svesni smo gde ostavljamo tragove (Sagovornik 2).”*

Ovakav oblik neposredne komunikacije, iako sigurniji, usporava novinarski rad i otežava pristup izvorima, ali i govori o krupnijem problemu – *da je poverenje u bezbednost digitalne komunikacione mreže ozbiljno narušeno.* Narušenom poverenju doprinose i vrlo dalekosežne i uznemirujuće posledice otkrivanja identiteta izvora, koje vrlo slikovito opisuju slučajevi uzbunjivača. Uzbunjivač Aleksandar Obradović[64] je pomogao novinarima da razotkriju aferu Krušik i zbog toga bio uhapšen i izložen javnoj diskreditaciji. Uzbunjivačica, policajka Katarina Petrović iz Valjeva[65], suspendovana je nakon što su informacije o policijskom (ne)postupanju o slučaju visoko pozicioniranog političara dospele u medije.

Svi sagovornici imaju visoko razvijenu svest o zaštiti izvora, što nije samo rezultat profesionalne i etičke interne kulture u redakcijama, već i posledica specifičnog okruženja u kojem rade. Naime, za nezavisne medije vrata institucija često su „zatvorena", pa do informacija ne mogu doći redovnim ili zakonskim putem, poput zahteva za pristup informacijama od javnog značaja. U takvim uslovima, poverenje izvora postaje ključno, jer su upravo oni često jedini način da se dođe do podataka od javnog interesa i razotkriju teme koje bi inače ostale skrivene od javnosti.

---

64 J. Veljković, odabrani tekstovi BIRN-a o Aleksandru Obradoviću. Dostupno na: https://birn.rs/tag/aleksandar-obradovic/

65 N1 Beograd, odabrani tekstovi o Katarini Petrović. Dostupno na: https://n1info.rs/tag/katarina-petrovic/

> *„Najvažnija stvar je što postoji veliki strah, čak i za najbanalnije stvari... pukla negde cev ili tako nešto, a ljudi ne smeju da o tome pričaju pod punim imenom i prezimenom... Ja svima pričam da sam na merama već deset godina i da treba da vodimo računa o čemu razgovaramo, ali takođe kažem da od nas nikad ništa nije ‚iscurilo'. Kad bi se to desilo jedanput, dvaput, ja bih mogao da zatvorim firmu (Sagovornik 6)."*

Sistematsko zatvaranje institucija prema medijima i uskraćivanje zvaničnih informacija primorava novinare da se oslanjaju na izvore kao ključan izvor podataka od javnog značaja. Međutim, pritisci, ucene i pretnje upućene tim izvorima pokazuju koliko je njihova bezbednost ugrožena, a rizik koji preuzimaju realan i ozbiljan.

> *„Mi smo lokalni medij koji godinama nije dobio izjavu od funkcionera ili direktora javnih preduzeća... pokušali smo da dobijemo odgovore preko odborničkih pitanja, pa je i to prestalo, na neke događaje smo dolazili nepozvani...onda smo se dovijali na različite načine, a jedan od tih načina su insajderi iz javnih preduzeća. Onda su te ljude počeli da, na osnovu naših tekstova, zovu, uslovljavaju, prete (Sagovornik 17)."*

B. (Ne)legalne prakse institucija sistema

Razgovori sa novinarima i urednicima mogu se čitati i kao svedočenja o brojnim (ne)legalnim praksama ugrožavanja bezbednosti novinara i otkrivanja identiteta izvora. Oni variraju od upotrebe špijunskog softvera (spyware-a), presretanja komunikacija i prisluškivanja, pristupa zadržanim podacima, do „curenja podataka" koji obično završe u provladinim tabloidima, otkrivanja izvora kroz policijske ili istražne radnje, pa čak i podnošenja tzv. SLAPP tužbi. Sve ove prakse biće detaljnije opisane u nastavku, a mapirane su kroz sprovedene intervjue.

Prema svedočenjima pojedinih novinara, u nadzor su, pretpostavlja se, umešane policija i bezbednosne službe, a podrazumevaju „*tehničko praćenje, praćenje preko kamera po gradu, fizičko praćenje, a ukoliko ne znaju iz koje službe je izvor informacija krenuo, objave čak i fiktivnu informaciju da je izvor uhapšen da bih ja zvao i proverio da li je to tačno... dakle, koriste i neke sofisticiranije metode*“ *(Sagovornik 4).*

Istraživanjem je mapirano nekoliko anegdotskih slučajeva koji ilustruju ovakve nelegalne prakse. Ovi slučajevi su vrlo slikoviti, a daju tek naznake o dubini problema. Većina novinara ima svest o gotovo stalnom nadzoru („*toliko sam se već navikao da je to postala normalnost*“) i tome prilagođava svoje prakse rada. Obrada i izbor tema, međutim, ne trpe – novinari i urednici se vode javnim interesom i od tema ne odustaju lako.

Spyware – novi alat u arsenalu nadzora

„*Jednog dana, jedna koleginica je u redakcijskoj Signal grupi prijavila čudnu poruku koju je dobila. Nekoliko minuta kasnije, druga koleginica je javila da je primila gotovo identičnu poruku sa istog broja. Odmah nam je bilo jasno da to nije slučajnost.*“ Ovako urednik BIRN-a opisuje trenutak kada je redakcija inicijalno posumnjala na hakerski napad za koji će se kasnije (digitalnom forenzičkom analizom Amnesty International-a) ispostaviti da je mogući neuspeli pokušaj instalacije spyware-a. „*Nismo bili iznenađeni – naš posao nosi rizik, i računali smo da će se ovako nešto kad-tad desiti. Ali kada zaista dođe taj trenutak, shvatite da nijedna priprema ne može da ukloni neprijatnost koju to saznanje nosi*“, dodaje on.

Sa druge strane, novinaru Slaviši Milanovu iz lokalnog portala Far iz Dimitrovgrada, telefon je oduzet tokom rutinske kontrole saobraćajne policije i bez njegovog znanja instaliran spyware NoviSpy, čiji tragovi vode do BIA, kako je pokazala forenzička analiza Amnesty International-a. Po svedoče-

nju koje je Milanov ispričao portalu Raskrikavanje[66], on je, najpre, primetio da nešto nije u redu sa njegovim telefonom. Telefon je bio otključan bez prethodne saglasnosti novinara, mobilni internet bio je isključen, baterija se brzo praznila, aplikacije koje nije koristio bile su aktivne, a forenzička analiza Amnesty International-a je potvrdila da je jedan deo podataka sa telefona preuzet. Ista forenzička analiza potvrdila je prisustvo špijunskog softvera domaće proizvodnje. Instalacija ovog softvera je nelegalna bez naredbe suda. Odgovori institucija na slučaj Slaviše Milanova, međutim, izostaju. Do trenutka objavljivanja ovog izveštaja, nije se oglasilo nadležno tužilaštvo, kao ni Zaštitnik građana niti Poverenik za zaštitu podataka o ličnosti, kojima su se Milanov i nekoliko organizacija civilnog društva takođe žalili[67]. Novinar je, uz pomoć Nezavisnog udruženja novinara Srbije, još u martu 2025. godine Višem javnom tužilaštvu podneo krivičnu prijavu protiv NN lica u Policijskoj stanici Pirot, a kasnije je tu prijavu i dopunio. Unutrašnju kontrolu u policiji je sproveo načelnik PU Pirot. U odgovoru PU koji je dostavljen advokatu Milanova navodi se da je kroz razgovor sa policajcima utvrđeno da nije bilo povreda prava u slučaju zadržavanja. Unutrašnja kontrola, ipak, ni u jednom segmentu svog postupanja nije se referisala na oduzimanje telefona, iako su Milanov i njegov advokat insistirali upravo na tome.

Imajući u vidu da Milanov, kao ni celokupna redakcija Far, nema aktivne tužbe niti naznaka bilo kakve nelegalne aktivnosti, medijskoj i široj javnosti i dalje ostaju nepoznati motivi ovako intruzivnog kršenja prava. Njegova pretpostavka je pokušaj zastrašivanja, otkrivanja izvora ili pak pritisak kako bi se određene novinarske priče zaustavile.

66 V. Radojević, Državni nadzor: Novinaru tajno instaliran špijunski softver u telefon tokom ispitivanja u policijskoj stanici, Raskrikavanje/KRIK (2024). Dostupno na: https://www.raskrikavanje.rs/page.php?id=Drzavni-nadzor-Novinaru-tajno-instaliran-spijunski-softver-u-telefon-tokom-ispitivanja-u-policijskoj-stanici-1427

67 Mašina, Srbija nezakonito špijunira svoje građane, institucije ćute: Organizacije civilnog društva podnele dopune krivične prijave (2025). Dostupno na: https://www.masina.rs/srbija-nezakonito-spijunira-svoje-gradane-institucije-cute-organizacije-civilnog-drustva-podnele-dopune-krivicne-prijave/

Jedina konkretna posledica ovog, i ostalih slučajeva otključavanja telefona i upotrebe spyware-a u Srbiji, je ta da je izraelska kompanija Cellebrite sprovela „internu istragu i donela odluku o obustavljanju upotrebe svojih proizvoda od strane određenih korisnika u Srbiji", navodi se u izveštaju BIRN-a.[68] U saopštenju za javnost koje je kompanija izdala krajem januara 2025. godine, navodi se da kompanija „ozbiljno shvata optužbe o mogućoj zloupotrebi njene tehnologije od strane korisnika" na način koji bi bio u suprotnosti sa izričitim i implicitnim uslovima navedenim u našem ugovoru o krajnjem korisniku." U javnosti, međutim, nema dostupnih informacija o tome kojim entitetima/institucijama su ukinute licence, da li su one ukinute potpuno ili samo delimično, da li je zabrana pristupa uređajima trajna ili samo privremena i sl.

Stručnjaci za bezbednost koji su intervjuisani u toku istraživanja, navode da je spyware nekad lako, nekad teško detektovati – to zavisi od same tehnologije, koliko je ona sofisticirana (nekad je dovoljno da kliknete na link ili poruku i da uopšte ne znate da je tu), ali i od same svesti novinara. Što se tiče NoviSpy, spyware-a domaće proizvodnje, on nije dovoljno sofisticiran prema oceni Amnesty International-a, i baš zato su oni koji su bili predmet njihovog izveštaja i posumnjali da se eventualno nešto dešava. Taj spyware i svi alati koji su pravljeni sa malo resursa lakši su za detekciju. Skuplji alati, poput Pegasusa, za koje je potrebno stotine hiljada evra za pristupne licence, teže se otkrivaju. Na primer, u slučaju domaćeg alata potrebno je da „mete" budu fizički odvojene od telefona da bi bio instaliran, dok se Pegasus instalira „na daljinu", a radi po principu snimanja ekrana i onoga što se na njemu dešava. Sa druge strane, organizacije koje otkrivaju spyware-e (poput Citizens Lab ili Amnesty International), bave se analizom što većeg broja telefona, na taj način identifikuju određene indikatore prisustva ove tehnologije i prave svoju bazu – dok proizvođači onda dalje razvijaju tehnologiju i te indikatore zaobilaze („*to je bukvalno*

68 A.Tešić, Cellebrite obustavlja saradnju s pojedinim korisnicima u Srbiji nakon otkrića BIRN-a i Amnestija o zloupotrebama, BIRN (2025). Dostupno na: https://birn.rs/cellebrite-obustavlja-saradnju-sa-srbijom-zbog-zloupotrebe-tehnologija/

igra mačke i miša“). Kako konstatuje jedan od sagovornika „*kombinacija spyware-a i biometrije je smrt slobodnog novinarstva*“ (Sagovornik 8).

Osim navedenih tehničkih aspekata, jedan od ključnih problema upotrebe spyware-a je ne samo njegova invazivnost, već i obim podataka koji on preuzima, a analiza pravnog okvira u nastavku pokazaće da ne postoje jasna uputstva za ograničen pristup podacima. Pravnici koji su intervjuisani tokom istraživanja, ali i međunarodni standardi, insistiraju na striktno definisanom obimu podataka koji se preuzimaju od novinara sužavajući se na one koji su neophodni za istragu, jer se upravo u velikoj količini neselektivno preuzetih podataka mogu naći i oni koji identifikuju izvor.

Pristup uređajima, praćenje i prisluškivanje

Osim spyware-a, istraživanjem je detektovano i nekoliko slučajeva u kojima su prava novinara povređena drugačijim, nešto „tradicionalnijim“, ali jednako delotvornim metodama nadzora. Digitalni alati i mere, prepliću se sa onim u fizičkom prostoru. „*Ako država ima interes da te prati, nema šanse možeš da se odbraniš*“ konstatovalo je nekoliko sagovornika tokom istraživanja. Sagovornicima nije uvek bilo jasno da li su „na merama“ (kolokvijalni izraz za posebne dokazne mere i dokazne radnje za čije sprovođenje je potrebna odluka suda), ali im je jasno da objavljivanje tekstova pokreće određene mehanizme nadzora. Kada je reč o analiziranim slučajevima, nedostaje jasna dokumentacija i informacije koje bi novinarima omogućile da razumeju razloge za nadzor.

Pripadnici različitih službi bezbednosti ponekad koriste manipulativne tehnike kako bi pristupili podacima i uređajima. Pojedini sagovornici su naveli da im je oprema (kompjuter, telefon) oduzimana kao deo redovne policijske istrage. Krajnji rezultat je bio da su praktično odustajali od korišćenja takve opreme, sumnjajući na potencijalno kompromitovanje informacija i izvora.

> *„Oni su meni zaplenili laptop i dva telefona. Tražili su mi da otključam telefone, što ja po savetu advokata nisam hteo... Čovek, mislim, policajac, je izvadio neke uređaje, jako male. I samo je, bukvalno, prevukao par puta preko ekrana i taj ekran je jednom počeo da radi, kao neki silni bar kodovi da trče. I to je bilo to (Sagovornik 13).”*

> *„Imali smo situaciju pre nekoliko godina da je naša novinarka dobila pretnju. Došla je policija i zaplenila je računar. Držali su ga jedno, dva, tri dana, onda su ga vratili, ali zato smo mi posle toga taj računar liferovali (Sagovornik 5).”*

Opremu novinarima ponekad oduzima i obezbeđenje većih javnih skupova. U ovim slučajevima zabrinjava činjenica da policija retko reaguje na ovu vrstu povrede prava.

> *„Kada sam bio na jednom javnom događaju odakle sam izveštavao, neko iz obezbeđenja mi je uzeo telefon na 40 minuta. Ne znam šta je sa njim radio. Ne postoji zapisnik da mi je telefon oduzet, ne postoji zapisnik da mi je telefon vraćen, ne postoji prijava, ništa bukvalno ne znam. Kontaktirali smo pravnu pomoć novinarskog udruženja, jednom mi se javio tužilac i jednom mi je prišao jedan inspektor da kaže da će pokrenuti istragu, ali se od tada ponašaju kao da se ništa nije desilo (Sagovornik 14).”*

Krađa opreme bez tragova nasilnog ulaska, nedostupne kamere i sumnja na koordinisane upade u prostorije u kojima rade mediji ukazuju na visok stepen organizovanosti i moguće učešće službi bezbednosti, zaključuje se iz razgovora. Takođe, curenje podataka i informacija o neobjavljenim tekstovima i poverljivim razgovorima direktno potvrđuje postojanje nadzora i pritisaka usmerenih na zastrašivanje redakcija.

> *„Na automobilu iz kog su mi ukrali kompjuter bili su obrisani svi tragovi, čak i moji. To je potvrdila forenzika... lopov bi obio bravu, a auto je otvoren tako da nije obijen. Nisu radile kamere, tu ima nekoliko kamera u kraju. Bio je dan i lepo vreme, bila je gotova škola i*

> *puno ljudi, znači sve je obavljeno za nekoliko minuta. Ono što je mene moglo da ošteti je imenik, ali nisam imao ništa što je bilo važno za tekst (Sagovornik 4).”*

Ozbiljan oblik pritiska na novinare je (vidljivo i upadljivo) fizičko praćenje i zastrašivanje.

> *„Imali smo i fizičko praćenje. Snimili smo neki ogroman džip jedne paravojne formacije, imamo mi tu fotografiju. Bukvalno on nas prati tu od redakcije. Prijavila sam policiji, čisto da postoji pisan trag, ali odgovor je bio da policija nema ta saznanja, niko od građana nije prijavio i to je to (Sagovornik 17).”*

Sudski postupci i identitet izvora

Pojedini novinari svedoče da su se suočavali sa pritiscima da otkriju svoje izvore čak i tokom sudskih postupaka, gde su ih sudije ili advokati direktno ispitivali o identitetu izvora. Takva iskustva su retka, ali dodatno ilustruju manjak razumevanja i poštovanja prava na zaštitu izvora čak i unutar pravosudnog sistema.

> *„Zabrinjava i to što postoji veliko nerazumevanje... a to sam video na suđenju BIRN-u, kada je sudija pitala novinara ‚ko vam je izvor', umesto da zaustavi pitanje, kao da nije bila svesna šta je zapravo pitala (Sagovornik 3).”*

> *„Mi smo nekoliko puta bili pozivani u tužilaštvo zbog nekih naših tekstova. Međutim, tu je postojala procedura, bio je nalog suda. Pitanja jesu išla u pravcu toga ko vam je dao podatke i kako ste došli do tih informacija, ali smo se uvek ‚pokrili' zahtevom za pristup informacijama od javnog značaja. Izvor smo u tom slučaju potpuno anulirali. Dolaze nam ovde i policajci, nekoliko puta traže snimke sa naše kamere, a kažu da kamere u gradu ne rade (Sagovornik 7).”*

> *„Dva ili tri puta smo imali takav zahtev i ponudu onoga ko nas tuži da će da povuče tužbu ako otkrijemo ko nam je izvor. Nismo to mogli da prihvatimo i izgubili smo sporove, to su bili postupci za uvredu i klevetu. Ali, to je bila cena da sačuvamo izvore. Drugi slučaj je bio*

> *kada je jedna opština takođe tražila da otkrijemo ko nam je izvor, jer smo objavili dokumenta za koja su oni smatrali da predstavljaju neku vrstu službene tajne. Tužilaštvo je obavilo istragu tim povodom, ali nismo dobili informaciju da li nastavljaju dalje sa postupkom (Sagovornik 6).”*

Osim toga, jednom lokalnom mediju dešavalo se da im se obraćaju advokati zbog komentara na sajtu.

> *„Imali smo situaciju u kojoj su nam se ljudi obraćali, da li zbog nečega što smo objavili ili čak i zbog komentara na sajtu. Praktično su nas zvali advokati tih ljudi i oni su tražili informaciju ‚otkud vam ovo' ili, na primer, ‚jel znate ko je napisao taj komentar'. Mi nemamo, zapravo, uvid u celu IP adresu, pa ne znamo, i u tim slučajevima odgovor bi bio da ne možemo da im kažemo to i da jedino što mogu da urade je da preko tužilaštva pokušaju da zatraže takvu informaciju, a mi ćemo sa našim advokatima videti kako da postupimo dalje (Sagovornik 5).”*

Pojedini mediji u Srbiji suočili su se sa tzv. SLAPP tužbama koje nisu imale za cilj dokazivanje stvarne štete, već pritisak da se tokom sudskog postupka otkrije identitet izvora.

> *„Mi smo videli da su nas pojedinci, policijski komandiri, tužili da bi došli do informacija ko je to tačno pričao o njima sa novinarima, ali se jasno videlo šta je namera. Sve te slučajeve smo dobili i nismo otkrili svoje izvore (Sagovornik 3).”*

C. Zastrašivanje i kontrola informacija

Novinari opisuju ove vrste pritisaka kao deo šire strategije zastrašivanja i kontrole širenja informacija. Kompromitovanjem izvora šalje se poruka novinarima da odustanu od priča, ali i potencijalnim izvorima da ne otkri-

vaju informacije medijima. Primeri navedeni u ovom izveštaju i identifikovani tokom sprovođenja intervjua ukazuju na to da ugrožavanje poverljivosti nije izolovan incident, već sistemski obrazac zastrašivanja.

> *„Nekad se vidi da me prate, ali ja ne znam da li je to zbog ljudi sa kojima se srećem, da njih upozoravaju što pričaju sa mnom ili zbog mene. Nekad je to vrlo upadljivo, vidi se da je parkiran auto tamo gde mu nije mesto i sede neka dvojica...nekad i ne primećujem... nekad sam morao da menjam mesto sastanka sa izvorima (Sagovornik 4).”*

> *„Policajci su bili su vrlo uporni, rekli su mi ‚kaži ko su, mi ćemo ionako saznati', a ja odgovaram ‚u tom slučaju moraćete da objasnite kako ste do njih došli, jer ja neću da vam kažem, ne moram po zakonu' (Sagovornik 13).”*

Sagovornici generalno dele utisak da postoji ukorenjeno nepoverenje institucija prema novinarima i nerazumevanje njihove uloge u društvu. Stalno ispitivanje o izvoru informacija otkriva pretpostavku da novinar ne istražuje samostalno, već da mu neko „namešta“ podatke, čime se umanjuje njegov profesionalni kredibilitet.

> *„Koga god da zovem, nekog odgovornog iz institucija, redovno pitaju, ‚a odakle ti to'...Kod nas generalno postoji svest da novinar samo prenosi informacije koje je dobio, kao da on sam ne ume nešto da istraži ili da pronađe podatke, i zato uvek postoji ta svest da mu neko nešto namešta (Sagovornik 1).”*

Posledice nekontrolisanog nadzora i nelegalnih praksi praćenja i prisluškivanja novinara višestruke su i duboko zabrinjavajuće. Novinari često moraju da menjaju opremu (*„Ja sam taj telefon prosto prestao da koristim. Mislim, služio mi za slikanje i da pitam mamu šta kuva. Tako da sam se opremom pozdravio...” Sagovornik 13*) koja je kompromitovana i neupotrebljiva, prinuđeni su da menjaju kancelarije za koje sumnjaju da su prisluškivane, dok deo izvora, u strahu za sopstvenu bezbednost, prestaje da komunicira s njima.

Ove okolnosti zahtevaju uvođenje složenijih bezbednosnih procedura i usložnjavaju svakodnevni rad redakcija, usporavajući i otežavajući istraživački rad. Uz to, novinari se suočavaju sa izolovanjem i efektivnim onemogućavanjem da obavljaju svoj posao, dok se posledice osećaju i na psihološkom planu.

> *„Mnogo smo pažljiviji, biramo način na koji ćemo komunicirati. Sve nam to usložnjava posao, komunikacija u redakciji sad ima slojeve, nije nekad jednostavna... naša relanost je sada takva da stalno mislimo na nas i na izvore (Sagovornik 3).”*

U razgovorima sa novinarima uočava se da se deo izvora, suočen sa sve prisutnijim nadzorom i strahom od odmazde, povlači i odustaje od saradnje, čak i kada raspolaže informacijama od velikog javnog značaja. S druge strane, postoje i oni koji uprkos rizicima odlučuju da progovore, vođeni osećajem odgovornosti ili ličnog integriteta.

Broj izvora i njihova spremnost na saradnju često zavise od šire društveno-političke klime – u trenucima kada kontrola vlasti jača, pritisci rastu i izvori se povlače, dok se u otvorenijim okolnostima prostor za poverljivu komunikaciju širi. Ključnu ulogu, međutim, igra i sam pristup novinara – njihova dosledna primena zakona, spremnost da štite izvor po svaku cenu i izgradnja međusobnog poverenja često su presudni faktori koji odlučuju da li će neko podeliti informacije ili se povući.

> *„Od tri moja izvora, dvoje je izvedeno pred komisiju da utvrde da li su pričali za medije, i počelo je šikaniranje na poslu... treća osoba nije imala nikakve veze sa mnom i pričom, ali su je nekako pogrešno povezali sa mnom, jer su je pratili na društvenim mrežama. Neki izvori su se povukli, jer su se opravdano plašili. Gotovo godinu dana nisam dobio ni mejl ni iz jedne institucije. Ali sam, sa druge strane, dobio neke nove izvore, jer se pokazalo da sam dobro postupio... bilo je čak i izvora koji su hteli da pričaju, ‚peru biografiju', na šta ja ne pristajem (Sagovornik 13).”*

„Ima pritisaka na cele organizacije, kad nešto izađe u medije, oni se ne ustručavaju da izvrše pritisak na celu službu, jer ne znaju odakle je izašla informacija. Cele službe su stavljene u svrhu nadzora. Međutim, ono što je opasno je da mi ne znamo ko za koga radi – oni su razbili sistem, i ne znamo jel neko radi za službu ili za mafiju, sve je isprepletano (Sagovornik 4).”

Edukovanje samih izvora važan je aspekt novinarskog rada. Ova edukacije se ne odnosi samo na tehnike bezbednog komuniciranja, već i na to šta znači „moć medija“ i povećana pažnja javnosti.

> *„Moramo da ih edukujemo šta sam izlazak u javnost znači za izvore. Čini mi se da je naša praksa da mi njima objasnimo šta bi bila posledica za njih, da se ne desi da mi objavimo neku priču i bude nam super, a izvori posle kažu ‚nisam znao da će se ovo dogoditi’ (Sagovornik 5).”*

Jedna od ključnih poruka svih sprovedenih intervjua je da je oprez neophodan, ali da je najvažnije da novinari ne upadaju u „paranoju“ i autocenzuru.

> *„Ne upadamo u paranoju i autocenzuru – u jednom momentu su svi mislili da nas stalno prisluškuju... odbijam da budem žrtva, uhvatim sebe da se stalno osvrćem, gledam tablice, pazim kojim ulicama se krećem i ostalo... odbijam da tako živim.(Sagovornik 13)”*

> *„Jednostavno, uvek sam na oprezu. To znači ne u paranoji, to je jako bitno, jer onda sve postaje besmisleno, i bavljenje ovim poslom, ali biti stalno oprezan i voditi računa, to definitivno treba. Naravno, ne treba da nas sprečava da se bavimo temama za koje mislimo da su važne (Sagovornik 1).”*

> *„Sistem iznenađenja u stvari ‚pali’ najviše. Oni smatraju kad naprave neko to zastrašivanje, čak i taj fizički napad, da ćemo mi odustati, prestati da pišemo, da dolazimo, da pitamo, a mi odemo, pa pitamo. Baš, namerno. Ja sam odlazio na konferencije sa strahom, tresem se, ali odem. Ali u jednom trenutku ta količina straha u kojoj čovek živi,*

> *dovede do ravnodušnosti. Pa kao u redu, ajde sad, baš me briga. Počneš da živiš jednostavno normalno, zato što mozak ne može konstantno da ima taj pritisak i onda samo odbaciš sve i praviš se da živiš normalno (Sagovornik 17).”*

Važan nalaz je da opisane okolnosti nisu dovele do promena u izboru tema. Svi sagovornici ističu da teme biraju isključivo na osnovu javnog interesa i to se nije menjalo uprkos okolnostima.

> *„Svest o digitalnom nadzoru ne utiče na izbor tema – jer mi biramo teme po važnosti za javnost, a ne po tome koliko su ‚bezbedne’ za nas. Ono što se jeste promenilo jeste to što još pažljivije pristupamo komunikaciji, a sve više i sami istražujemo prakse digitalnog nadzora nad građanima (Sagovornik 2).”*

D. Širi društveni kontekst pritiska na nezavisne medije

Prethodno opisane forme digitalnog nadzora predstavljaju samo jedan segment šire lepeze pritisaka kojima su nezavisni mediji u Srbiji izloženi. Novinari nisu uvek prva meta nadzora, ali nadzor je toliko neselektivan da su novinari i njihovi izvori neka vrsta „kolateralne štete“.

> *„Digitalni nadzor koji se zloupotrebljava i politički pritisak idu ruku pod ruku. Ja mislim da oni ne koriste nadzor za kontrolu kriminalnih aktivnosti, nego ga koriste neselektivno i u svrhu kontrole, a to vidim i iz slučajeva otvorenog nadzora aktivista i organizatora protesta... izlazili su snimci sa aerodroma, slike aktivista na sastancima ispred ambasada. Trenutno vlast nema nikakav problem da kontroliše novinare, aktiviste i opozicionare, a zaštita izvora je ostala na nama (Sagovornik 3).”*

> *„Mi imamo i veći problem na lokalu, jer se svi znamo. Oni lako mogu da, prema vrsti informacija, otkriju ko je od 5 ljudi koji imaju pristup toj informaciji, ko je potencijalni izvor (Sagovornik 15).”*

Uskraćivanje zvaničnih informacija i izbegavanje komunikacije od strane državnih organa dodatno otežava profesionalni rad, dok bezbednosne pretnje i različiti oblici zastrašivanja stvaraju okruženje stalnog pritiska i nesigurnosti.

Različitim oblicima ugrožavanja rada nezavisnih medija treba dodati i snažan finansijski pritisak, koji se ogleda u uskraćivanju pristupa javnim sredstvima i oglašivačima, kao i u otežanom pristupu donatorskim fondovima. Paralelno s tim, nezavisni novinari i redakcije svakodnevno se suočavaju sa javnim kampanjama diskreditacije, u kojima se targetiraju kao „neprijatelji države", „plaćenici" ili „strani agenti".

Sve zajedno, gore navedeno, govori o društvenom kontekstu u kom je nezavisno novinarstvo ozbiljno ugroženo, a sa njim i širi okvir prava građana na informisanje.

E. Kako se grade interni kapaciteti?

Interni kapaciteti medija nesrazmerni su obavezama koje su im nametnute, još jedan je od važnih zaključaka istraživanja. Različite redakcije zato primenjuju nekoliko strategija u podizanju sopstvenih kapaciteta – unapređenje tehničke zaštite, organizovanje obuka i rad sa stručnjacima, sprovođenje posebnih projekata koji su usmereni na pitanja bezbednosti i sl.

> *„Najvažnije je znanje. Novinari moraju da znaju kako funkcionišu digitalni napadi, kako izgleda kompromitovan uređaj, kako da to prepoznaju i kome da se obrate. Tehnička podrška je važna, zakoni su takođe važni – ali ako nema znanja, ni najbolji zakon neće pomoći. (Sagovornik 2)"*

Podizanje bezbednosne kulture u redakcijama ključno je za zaštitu i privatnosti novinara i poverljivosti izvora sa kojima sarađuju. Uvođenje jasnih protokola, redovne edukacije i odgovorno upravljanje digitalnim alatima doprinosi prevenciji nadzora, upada i curenja informacija. Kako navodi

jedan od sagovornika, bezbednosne provere bi trebalo raditi redovno, a ne samo u slučajevima kada nešto iskrsne ili se dese nepredviđeni događaji.

> *„Jako je bitno da novinari postanu svesni da to što trenutno nemaju šta da kriju, ne znači da treba da koriste ‚običan' telefon. Bez obzira na temu na kojoj rade, uvek, po pravilu, treba da komuniciraju na bezbedan način, jer informacija može da iskrsne u bilo kom trenutku razgovora. Obuke su neophodne, jer se oblast menja. Kolege treba da znaju da ne moraš da nosiš telefon u policiju, da ako te privedu odmah ugasiš telefon, svi treba da znaju da apsolutno ne moraš da kažeš ko ti je izvor ni u policijskoj ni u tužilačkoj istrazi, jer nas štiti zakon, imaš kod sebe broj urednika i advokata,....ako nisu prošli obuku neće znati šta su im prava (Sagovornik 3)."*

Otežavajuća okolnost je ta da domaći mediji ne raspolažu dovoljnim resursima da se dodatno posvete podizanju kapaciteta digitalne bezbednosti. Tokom razgovora iskrsli su komentari poput „*mi smo previše mala redakcija da bismo imali posebne ljude koji bi se samo time bavili*" ili „*nisam tehnički potkovan, više sam živeo u prošlom veku nego ovom, ali imam ljude koji mi pomažu da budem u toku*".

Obuke o bezbednosnoj kulturi u redakcijama je prošao deo onih koji su učestvovali u istraživanju. Obuke su mahom jednokratne i finansirane kao deo određenih projektnih aktivnosti. Međunarodna saradnja se takođe pokazala vrlo korisnom, jer postoje internacionalni timovi koji detaljno prate ovu oblast i šalju obaveštenja i najnovije savete, a ponekad organizuju i obuke za domaće medije. Novinarima je takođe bila vrlo korisna i pravna pomoć i pravni saveti koje dobijaju od novinarskih udruženja, a ona se pokazala naročito dragocenom u okolnostima ograničenih resursa koje mediji imaju.

> *„Mislim da nažalost u trenutnom stanju, u današnje vreme, kako se stvari rade i kako funkcionišu, da jako fali tih resursa. Novinari, redakcije, mediji, oni nemaju vremena za usavršavanje, za prilagođa-*

> *vanje itd. Brzina informacija i svega što se dešava, ...oni ne mogu da stignu i nemaju dovoljno resursa (Sagovornik 8).”*

Izlazak u javnost i dosledno pridržavanje profesionalnih standarda, pokazale su se kao dve uspešne strategije zaštite. Najpre, jer se tako podstiče podrška šire javnosti i solidarnost, a dodatno pokazuje legitimitet i poverljivost, pokazujući da novinari koriste dobijene informacije isključivo u javnom interesu, nepokolebljivo štiteći identitet izvora.

U zaključku ovog dela istraživanja, može se konstatovati da su pouzdani izvori kritično važni u situacijama kada su institucije zatvorene. Nivo zaštite zavisi od tri ključna faktora: samih novinara i bezbednosne kulture u redakcijama, društvenog konteksta i tehnološkog okvira. Različiti oblici digitalnog nadzora, koji su mahom bez adekvatnih sudskih naloga, su u porastu, a kulminiraju sa upotrebom spyware-a. Ovo istraživanje je mapiralo nekoliko važnih iskustvenih slučajeva koji govore i o praćenju komunikacija, nadzoru u javnom prostoru, curenju informacija i sl. Mediji imaju veliku odgovornost čuvanja izvora, ali i ograničene resurse (tehničke, materijalne, neophodno znanje) kojima ne mogu da se suprotstave moćnom državnom aparatu. Duboko ukorenjeno nepoverenje prema institucijama i adekvatna primena zakona takođe se čitaju kao jedan od zaključaka. Posledice nekontrolisanog digitalnog nadzora mogu se posmatrati kroz promene i prilagođavanje praksi novinarskog rada, promene u načinu komunikacije sa izvorima, bezbednosnim protokolima i sl., ali ne i na planu izbora tema koje su uvek vođene javnim interesom. Zbog toga je nadzor, u kontekstu šireg, političkog pritiska na nezavisne medije, postao samo još jedan njegov alat.

3. Pravni okvir zaštite novinarskih izvora

Normativni okvir i uporednopravna rešenja

Zaštita izvora može biti apsolutna ili kvalifikovana, što znači da se može ograničiti samo pod određenim uslovima. U skladu sa standardima Saveta Evrope, Evropskog suda za ljudska prava, međunarodnih dokumenata i relevantne literature korišćene u ovoj analizi, takva ograničenja su generalno dozvoljena isključivo ako ispunjavaju trodelni test ograničenja slobode izražavanja: ograničenje mora biti propisano zakonom, proporcionalno legitimnom cilju koji se želi postići i neophodno u demokratskom društvu.

Kada se posmatra domaća norma iz člana 58. ZJIMA, ona predviđa kvalifikovanu zaštitu. U osnovi, pravilo je da novinar nije dužan da otkrije izvore. Osim ako je reč o krivičnom delu ili učiniocu za koji je *zaprećena kazna od najmanje pet godina* i *ako se podaci o delu ili učiniocu ne mogu pribaviti na drugi način* – što predstavlja izuzetak od pravila i pretpostavlja kumulativno ispunjenje oba uslova. U nastavku, biće ukazano na niz međunarodnih standarda (preduslova) koji se moraju ispuniti kako bi zaštita izvora bila potpuna i svrsishodna.

Ova norma sa malim brojem reči na veoma kompaktan način, ipak, uspeva da obuhvati osnovne postulate zaštite novinarskih izvora, tako štiteći ne samo informacije koje mogu da otkriju izvore i da ih identifikuju, već i neobjavljene informacije.[69] Koliko je poznato autorkama ove analize,

69 D. Banisar, Silencing sources: An International Survey of Protections and Threats to Journalists' Sources, Privacy International (2007), str. 28

sudske prakse, kada je konkretno reč o zaštiti izvora, nema. Još važnije, po saznanjima medijsko-pravnih stručnjaka sa kojima je razgovarano u pripremi, represivni organi su, do sada, poštovali ovu normu. Dakle, ova norma iz člana 58. ZJIM i dalje „obavlja" svoju zaštitnu funkciju.

Problem nastaje usled neusaglašenosti „povezanih" pravnih propisa i praksi institucija sistema. Praksi koje zbog intruzivnosti, obimne ekstrakcije podataka i zabeleženog nivoa digitalnog nadzora - definisan kao sredstva i tehnologije za otkrivanje, praćenje, presretanje, obradu i zadržavanje podataka o ličnosti ili komunikaciji pojedinaca[70] – ugrožavaju bezbednost novinara i principe zaštite novinarskih izvora. Pored problema sa različitim oblicima nadzora, Zakonik o krivičnom postupku ne predviđa,

1. Mogućnost da novinari *odbiju da svedoče,* ako postoji mogućnost da će otkriti izvor, kao u Francuskoj.[71]

2. Ne postoje, kao u Belgiji, posebna pravila o pretresu redakcija i njihovih domova, što može ostaviti velika ovlašćenja policiji.

3. Ne postoje ni *posebna pravila o pretresanju novinara i zadržavanju uređaja,* što otvara mogućnost za zloupotrebe i pristup neograničenom broju podataka, pa tako i o izvorima.

U Belgiji, i slično u Austriji, propisi o zaštiti izvora *zabranjuju bilo koju meru detekcije ili istražne radnje protiv novinara ili redakcije,* osim u veoma specifičnim situacijama, a vezi sa izvršenjem krivičnog dela i ako su ispunjeni ostali uslovi, kao što je postojanje sudske odluke, ozbiljnost krivičnog dela, svrsishodnost i proporcionalnost, da je ova istražna radnja poslednje sredstvo i da su ostale mere iscrpljene, što je uslov i u članu 58. ZJIM. Belgijski zakon predviđa i obavezu minimizacije prikupljanja podataka, a

70 M .Pisarić, Špijunski softver protiv novinara u ed. J. Kostić i M.M. Bošković, Mediji Kazneno Pravo i Pravosuđe, Tematski zbornik radova međunarodnog značaja, Institut za uporedno pravo, (2024), str.444

71 D. Banisar, Silencing sources: An International Survey of Protections and Threats to Journalists' Sources, Privacy International (2007), str.29

čak i kada je pretres sproveden - *mora se uložiti trud da se minimizira rizik od identifikacije izvora.*

U Belgiji, zakon ide i korak dalje i predviđa ovu vrstu zaštite novinarskih izvora i za situacije digitalnog nadzora, kao što je *sudski odobreno prisluškivanje i presretanje komunikacije* na drugi način. Nemačka ima delimičnu zaštitu gde krivični zakon zabranjuje korišćenje akustičnog nadzora nad novinarima, ali ova mera se ne odnosi na telekomunikacije. U Srbiji, član 166. Zakonika o krivičnom postupku predviđa da, na obrazloženi predlog javnog tužioca, sud *može odrediti nadzor i snimanje komunikacije telefona, elektronske i druge komunikacije* prema licu za koje postoji osnovi sumnje da je izvršilo određena (teža) krivična dela[72], a da se dokazi ne mogu pribaviti na drugi način ili bi prikupljanje bilo znatno otežano. Pri tome, „organ postupka će posebno *ceniti da li bi se isti rezultat mogao postići na način* kojim se manje ograničavaju prava građana."[73] To su važne garancije za zaštitu novinara i novinarskih izvora čije primena i zaštitna funkcija treba biti predmet posebne analize.

Naredba mora sadržati tačno definisane podatke o licu koje se nadzire kao i informacije koje se odnose na *„obim i trajanje*" posebne dokazne radnje.[74] U kontekstu zaštite izvora, a u cilju smanjenja mogućnosti da se kroz nad-

72 Obuhvata niz krivičnih dela koja novinari u svom poslu redovno prate i izveštavaju javnost, a o čemu podatke neretko dobijaju od strane izvora, uključujući, zloupotrebu položaja odgovornog lica (član 227. Krivičnog zakonika), zloupotrebu u vezi sa javnom nabavkom (član 228. Krivičnog zakonika), primanje mita u obavljanju privredne delatnosti (član 230. Krivičnog zakonika), davanje mita u obavljanju privredne delatnosti (član 231. Krivičnog zakonika), falsifikovanje novca (član 241. st. 1. do 3. Krivičnog zakonika), pranje novca (član 245. st. 1. do 4. Krivičnog zakonika)

73 ZKP, član 161.

74 Naredba sadrži raspoložive podatke o licu prema kojem se tajni nadzor komunikacije određuje, zakonski naziv krivičnog dela, označenje poznatog telefonskog broja ili adrese osumnjičenog, odnosno telefonskog broja ili adrese za koju postoje osnovi sumnje da je osumnjičeni koristi, razloge na kojima se zasniva sumnja, način sprovođenja, obim i trajanje posebne dokazne radnje, član 167, stav 2.
lako razmatranje sudske prakse u pogledu načina na koji sudovi definišu obim nadzora nad komunikacijama i, još važnije, načina na koji se on primenjuje u praksi prevazilazi okvir ove analize, ipak je – uprkos istraživačkim izazovima – od suštinskog značaja razumeti kako sudovi i policija sprovode digitalni nadzor u stvarnosti.

zor otkriju izvori, po uzoru na Belgiju, važno je da o*bim nadzora bude inicijalno određen kao minimalan i takav da ne zaobiđe zaštitu izvora, kao i da budu jasno definisani opseg i mere za zaštitu od arbitrarnog, neograničenog i intruzivnog pristupa.*[75] Trenutno zakonsko rešenje tajnog nadzora komunikacije u Srbiji ne predviđa ovakav poseban vid zaštite novinarskih izvora, iako ostavlja prostora za proširenje i nadgradnju. Naime, zakon predviđa da naredba mora sadržati procenu obima nadzora, kao i da se nakon sprovedenog nadzora, sudiji za prethodni postupak dostavljaju materijali kao i prateći podaci, *„i ocena o svrsishodnosti i rezultatima primene nadzora"*.[76] Ostaje nejasno, šta se dešava u situacijama kada sud utvrdi da nadzor nije bio svrsishodan. Nakon ovog dela procesa, „sav materijal dobijen sprovođenjem tajnog nadzora komunikacije dostaviće se javnom tužiocu."[77]

Važno je napomenuti da ukoliko javni tužilac ne pokrene krivični postupak u roku od 6 meseci od upoznavanja sa materijalom ili ako odluči da ga ne koristi u postupku, sudija za prethodni postupak donosi rešenje o uništavanju materijala.[78] O tome, javni tužilac može obavestiti lice koje je bilo pod nadzorom. Trenutne predložene izmene ZKP predviđaju da javni tužilac mora da obavesti lice, što će biti značajno za slučajeve nadzora nad novinarima, doduše samo one oblike nadzora koji se sprovode nakon stupanja na snagu izmenjenog ZKP.[79] U slučaju neregularnosti prilikom prikupljanja materijala, na prikupljenim podacima se ne može zasnivati sudska odluka. [80] Međutim, trenutno predložene izmene ZKP[81] i ZK[82] donose i novine u pogledu širenja opsega nadzora i to kroz širenje spiska krivičnih dela za koje se mogu odrediti posebne dokazne radnje, uključujući i tajni nadzor.[83] Predložene izmene ZK ukazuju da se pojam „računarskog

75 Szabó i Vissy protiv Mađarskee, App No 37138/14, Presuda ESLJP, (12.1. 2016.), para. 65
76 ZKP, član 170.
77 ZKP, član 170, stav 2.
78 ZKP, član 163, stav 1.
79 Vidi više na: https://ekonsultacije.gov.rs/topicOfDiscussionPage/529/4, Član 163, izmene Zakonika o krivičnom postupku
80 ZKP, član 163.
81 Vidi više na: https://ekonsultacije.gov.rs/topicOfDiscussionPage/529/4
82 Vidi više na: https://ekonsultacije.gov.rs/topicOfDiscussionPage/529/4
83 Član 162, stav 1, tačka 2, izmene Zakonika o krivičnom postupku

virusa" oslanja na subjektivne elemente, zahtevajući nameru ugrožavanja ili nanošenja štete.

Naredbu izvršava kako policija, tako i Bezbednosno-informativna agencija (BIA) ili Vojnobezbednosna agencija (VOA), o čemu se sačinjavaju dnevni zapisnici koji se dostavljaju javnom tužiocu ili sudiji za prethodni postupak, na njihov zahtev.[84] Pored tajnog nadzora iz ZKP koji mogu sprovoditi pripadnici BIA ili VOA, BIA[85] ima veoma slične nadležnosti u okviru delokruga svog posla i delovanja odnosno praćenja, suzbijanja organizacija i lica usmerenih ka vršenju organizovanog kriminala sa elementom *inostranosti,* unutrašnjeg i međunarodnog terorizma, krivičnih dela protiv čovečnosti i međunarodnog prava i *protiv ustavnog poretka i bezbednosti zemlje.*[86]

Član 13. Zakona o BIA (ZBIA) tako omogućava tajni nadzor, snimanje komunikacije, uključujući i na javnim mestima, statistički elektronski nadzor komunikacije i informacionih sistema, kao i računarsko pretraživanje već obrađenih ličnih i drugih podataka. Direktor Agencije BIA podnosi sudu predlog, koji izdaje naredbu koja, između ostalog, sadrži i informacije o primeni, *obimu,* i trajanju mere.

ZBIA definiše takođe da sprovođenje ove mere mora biti poslednje sredstvo, te da *„okolnosti slučaja"* (postavljeno veoma široko) ukazuju da se te radnje drugačije ne bi mogle sprečiti, otkriti, dokazati ili bi izazvale nesrazmerne teškoće. Radnici Agencije *'će posebno voditi računa"* (bez detaljnijih uputstava) o određivanju i trajanju mere, o obimu neophodnom da se svrha postigne i postizanju rezultata na drugi način.[87] Ukoliko prilikom primene posebne mere BIA prikupi materijal o krivičnom delu za koje su mogu sprovesti i posebne mere iz ZKP, a reč je velikom broju različitih

84 ZKP, član 168.

85 Radi preciznosti, važno je navesti da i Vojnobezbednosna agencija ima ovlašćenja u ovom domenu koja su veoma slična rešenjima u ZBIA. Vidi više: Zakon o Vojnobezbednosnoj agenciji i Vojnoobaveštajnoj agenciji, „Službeni glasnik RS", br. 88/2009, 55/2012 – odluka Ustavnog suda, 17/2013

86 ZBIA, član 12.

87 ZBIA, član 14.

krivičnih dela[88], Agencija materijal dostavlja javnom tužilaštvu koje mora zahtevati sprovođenje posebne dokazne radnje i nastaviti gonjenje po pravilima krivičnog postupka.[89]

Zakonska rešenja iz ZKP i ZBIA - na uštrb vladavine prava i podele vlasti - pokušala su da ukrste nadležnosti i ovlašćenja ZBIA koja se odnose na posebne mere sa posebnim dokaznim radnjama iz ZKP, što kreira dodatni pritisak na zaštitu izvora. Po ZBIA, službenici Agencije mogu sprovoditi posebnu dokaznu meru u trajanju od tri meseca, a „može se produžiti najviše još tri puta u trajanju od po tri meseca."[90] Ukupno, ova mera može trajati 12 meseci, dok se posebna dokazna radnja sprovodi tri meseca uz mogućnost produženja za još tri meseca.[91] Imajući u vidu da posebnu dokaznu meru koju sprovodi BIA odobrava Predsednik Višeg suda u Beogradu[92], a dokazne radnje iz ZKP, sudija za prethodni postupak u zavisnosti od mesta izvršenja krivičnog dela, Agencija, čini se, na jednostavniji i centralizovan način može sprovoditi posebne dokazne mere. Mera se sprovodi u cilju zaštite nacionalnih interesa (od organizovanog kriminala, terorizma, do zaštite ustavnog poretka i nacionalne bezbednosti), ostavljajući prostora za različita i široka tumačenja, a samim tim i primenu ove mere. Zbog toga se otvara niz pitanja u vezi sa zakonskim i institucionalnim polugama kontrole nad sprovođenjem ovih posebnih dokaznih mera koje je *neophodno dalje analizirati kroz prizmu zaštite novinara i novinarskih izvora.*[93]

Posebne mere i posebne dokazne radnje u svojoj suštini ograničavaju ljudska prava i imaju intruzivan karakter, zbog čega moraju biti odobrene

88 Vidi član: 161, stav 1. i 2. ZKP

89 ZBIA, član 15, Posebne dokazne radnje se izuzetno mogu odrediti i prema licu za koje postoje osnovi sumnje, okolnosti slučaja ukazuju da se na drugi način krivično delo ne bi moglo otkriti, sprečiti ili dokazati ili bi to izazvalo nesrazmerne teškoće ili veliku opasnost.

90 ZBIA, član 15a, stav 3

91 Detaljnije regulisano članom 166. ZKP, stav 3. Osim za teža krivična dela iz člana 162. stav 1., tačka 1. kad se može produžiti još najviše dva puta u trajanju od po tri meseca.

92 ZBIA, član 15, stav. 3

93 Ovo je takođe naglašeno od strane eksperata koji su učestvovali u intervju procesu i kojima se i ovim putem zahvaljujemo na izdvojenom vremenu.

od strane suda ili drugog nezavisnog organa, samo u izuzetnim situacijama, srazmerno cilju, neophodnosti u demokratskom društvu i svrsishodnosti. Prakse digitalnog nadzora, analizirane u prethodnom poglavlju, netransparentnost u korišćenju ovih mera, često neutvrđenost razloga i opravdanost potrebe za njihovim korišćenjem, ukazuju na jačanje krivičnopravnog otiska i pritiska. *Ovakvo ukrštanje nadležnosti represivnih organa, u zemljama sa ograničenim demokratskim kapacitetima i vladavinom prava, veoma verovatno dovodi do obima nadzora koji je nesrazmeran cilju koji se želi postići. Posledično, takav nadzor*[94] *dovodi ograničavanja slobode izražavanja, odnosno ugrožavanja bezbednosti novinara i izvora.* Trenutno predviđena kontrolna uloga suda ni normativno ni u praksi ne može da obezbedi nivo zaštite koji se zahteva po međunarodnim standardima.[95]

Pored navedenog, represivni organi, policija i BIA, takođe u okviru svojih ovlašćenja mogu pristupati i zadržanim podacima, uz odobrenje suda i uz ispunjenost uslova koji se odnosi na dokazne radnje i dokazne mere. *Zadržani podaci*[96] su oni koje telekomunikacioni operatori moraju da čuvaju, a uglavnom je reč o meta-podacima (podaci sa baznih stanica, trajanje, početak i kraj komunikacije, lokacija i sl.), a koji su definisani ZEK.[97] Prema Pravilniku[98] koji definiše zahteve za uređaje i podršku u sprovođenju pristupa zadržanim podacima kao i presretanja komunikacije određuje se

94 Više o sličnim navodima vidi, pored Amnesty International izveštaja koji je citiran u istraživanju: Izjava nakon misije u Srbiji, Savet Evrope, april 2025, dostupno na: https://www.coe.int/en/web/commissioner/-/serbia-authorities-should-ensure-safety-of-demonstrators-and-improve-working-environment-for-civil-society-and-human-rights-defenders, Evropska komisija, Izveštaj o vladavini prava za 2025. godinu – Poglavlje o Srbiji, dostupno na sajtu Evropske komisije, 8.7.2025., str.13, dostupno na: https://commission.europa.eu/publications/2025-rule-law-report-communication-and-country-chapters_en

95 Srbija nije usamljena u ovome, vidi više o presudama Evropskog suda za ljudska prava i Evropskog suda pravde, Privacy International, PI's guide to international law and surveillance, Privacy International, 2024

96 ZEK, član 129.

97 Operator je dužan da omogući zakonito presretanje na osnovu odluke suda i da tehnički obezbedi potrebne uređaje i programsku podršku o svom trošku. Nadležni organ i operator moraju voditi evidencije o svakom presretanju (pravni osnov, datum, vreme) i čuvati ih kao tajnu. ZEK, član 127. 2 i 3.

98 Pravilnik o zahtevima za uređaje i programsku podršku za zakonito presretanje elektronskih komunikacija i tehničkim zahtevima za ispunjenje obaveze zadržavanja podataka o elektronskim komunikacijama. 49, „Sl. glasnik RS", 88/2015

uspostavljanje „monitoring centra", koji se do uspostavljanja novog, nalazi u prostorijama BIA. Imajući u vidu široka ovlašćenja BIA u kontekstu posebnih dokaznih mera, monitoring centar koji se i dalje nalazi u njihovim kancelarijama predstavlja kritičan rizik ograničavajući prostor za nadzor i kontrolu rada ovog organa vlasti.

Kao što i Medijska Strategija navodi, ovim podacima pristupalo se veoma često i, čini se, nesrazmerno. Iako podataka iz prethodnog perioda nema, malo je razloga koji ukazuju da se sa ovom praksom prestalo. Rešenja iz drugih evropskih zemalja nema previše, jer su zemlje mahom anulirale ove odredbe nakon odluke Evropskog suda pravde iz 2016. godine, kojom je Direktiva o zadržanim podacima oglašena nevažećom zbog neproporcionalnog mešanja u pravo na privatnost.[99] Određeni broj zemalja je zadržao ovu odredbu, sličnu kao u Srbiji. Nije poznato da li postoje posebna pravila za postupanje policijskih organa u slučaju pristupanja zadržanim podacima novinara. Zbog toga presude Evropskog suda za ljudska prava igraju važnu ulogu, jer ukazuju na važnost jasno artikulisane odluke suda, koja, između ostalog, mora da sadrži ne samo ocenu ispunjenosti uslova za ograničenje koje zakon predviđa, već i obrazloženje, kao i *definisan obim pristupa*, na način na koji *onemogućava pristup podacima koji nemaju veze s istragom odnosno nepotrebno zadiru u privatnost novinara*.[100]

Međutim, nedostatak pravnih rešenja na nacionalnom nivou ne znači da je ovde reč o pravnoj praznini. Evropski sud za ljudska prava je kroz veliki broj presuda definisao standarde koji se odnose kako na digitalni nadzor

99 Sud pravde Evropske Unije doneo je odluku (Digital Rights Ireland45) da se EU Direktiva o zadržanim podacima, na neproporcionalan način, meša u privatnost i druga prava svih ljudi koji žive u Evropi, da propisuje pravila koja prevazilaze neophodne mere, čime je ona prestala da važi, Judgement of the Court (Grand Chamber), 8 April 2014.
Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others., Joined Cases C293/12 and C594/12. (ECLI:EU:C:2014:238). Vidi više ovde: https://www.europarl.europa.eu/legislative-train/theme-area-of-justice-and-fundamental-rights/file-data-retention-directive

100 M. Pisarić, Špijunski softver protiv novinara u ed. J. Kostić i M.M. Bošković, Mediji Kazneno Pravo i Pravosuđe, Tematski zbornik radova međunarodnog značaja, Institut za uporedno pravo, (2024), str. 461. Vidi isto u poglavlju Diskusija, niže.

nad novinarima, tako i na situacije oduzimanja uređaja, pretresa novinara, novinarskih redakcija i domova. Ovo je posebno važno u kontekstu Srbije, imajući u vidu slučajeve pretresanja novinara i njihovih domova bez postojanja jasnih zakonskih mera koje bi onemogućile zaštitu izvora. Oduzimanje telefona novinaru bez jasnog, zakonitog osnova, otvara mogućnost uvida u njegove komunikacije, kontakte i poverljive informacije.[101] S druge strane, Belgija predviđa da mere nadzora, kao i pretres, *ne mogu biti korišćeni tako da se zaobiđe pravo na zaštitu novinarskih izvora,* osim, ako postoji nalog suda i ako je reč o krivičnom delu terorizma, postojanju ozbiljne pretnje po fizički integritet i ukoliko su iscrpljene sve ostale mere.[102] Ako se informacije dobiju mimo ovog okvira, sudovi *ne mogu koristiti te informacije kao dokaz* osim u vrlo izuzetnim okolnostima.

Međunarodni standardi i regulativa Evropske unije

Zbog različitih međunarodnih instrumenata koji se ukrštaju kroz oblast zaštite novinarskih izvora, ovaj deo izveštaja će ukazati na pojedine segmente i instrumente koji su važni za razumevanje rizika digitalnog okruženja. To su, pre svega, osnovni „standardi" zaštite izvora, ali i „povezane" oblasti kao što su, recimo, prakse pristupa zadržanim podacima i presretanje komunikacije, sa detaljnijom regulatornom analizom upo-

101 Slučaj novinara Zoomera, Darka Gligorijevića, kojem je određeno zadržavanje zbog snimka koji je zabeležio, a na kojem se vidi kako u studentskom domu jure Miloša Pavlovića, koji je u tom trenutku već bio javno dostupan. Tom prilikom policija mu je oduzela telefon. Iako ga je sudija za prekršaje već sutradan odmah pustila, telefon je u policiji zadržan još nekoliko dana, navodno po nalogu tužioca. Vidi više o tome na: ANEM, Slučaj Darka Gligorijevića (Zoomer): Kako je priveden novinar dok je radio svoj posao,ANEM,2025, dostupno na: https://anem.org.rs/sr/strane/slucaj-darka-gligorijevica-zoomer-kako-je-priveden-novinar-dok-je-radio-svoj-posao. Vidi takođe slične slučajeve: NUNS: Pritvaranje urednika "Slavije info" predstavlja opasnu praksu koja se može negativno odraziti na slobodu izražavanja, NUNS, 2025, dostupno na: https://nuns.rs/nuns-pritvaranje-urednika-slavija-info-predstavlja-opasnu-praksu-koja-se-moze-negativno-odraziti-na-slobodu-izrazavanja/,

102 D. Banisar, Silencing sources: An International Survey of Protections and Threats to Journalists' Sources, Privacy International (2007), str.73

trebe špijunskog softvera (spyware) iz člana 4. Akta o medijskim slobodama Evropske unije.

Međunarodni standardi i praksa, iako mnogobrojni,[103] predstavljaju samo generalni okvir zaštite novinarskih izvora koji, uopšteno govoreći, zaštitu izvora predstavlja kao neophodan, esencijalan element ili preduslov slobode medija, tako da novinar može biti pozvan da otkrije izvore samo u izvanrednim okolnostima,[104] upravo onako kako to predviđa i norma u ZJIM. Preporuke i rezolucije UN-a prepoznaju probleme u vezi sa pristupom podacima, komunikaciji, čak i upotrebi špijunskog softvera, i preporuke iz ovih dokumenata insistiraju na poštovanju testa zakonitosti, proporcionalnosti, neophodnosti, a kao takve su važne za zaštitu novinarskih izvora.[105] Iako pravno neobavezujući, ovi standardi imaju značajnu funkciju, kao baza za nadogradnju, a naročito su korisni za Srbiju. Posebno imajući u vidu okolnost da je UN Komitet za zaštitu ljudskih prava u izveštaju za Srbiju prepoznao da uvođenje biometrijskog nadzora mora biti usaglašeno sa zaštitom ljudskih prava. To, pre svega, podrazumeva zakonski okvir koji predviđa adekvatne pravne mehanizme zaštite, kao i redovnu sudsku reviziju, uključujući i *za online nadzor,* a naročito onaj koji se *odnosi na sprovođenje krivičnih istraga*, gde lični podaci iz izveštaja moraju ostati zaštićeni. Komitet poziva da situacije u kojima su „podaci iz istraga curili od autoriteta do medija budu istraženi."[106]

Kao što se i navodi u izveštaju za Srbiju, UN politike zahtevaju od država da redovno vrše reviziju procedura, praksi i zakonskog osnova za nadzor

103 J. Posetti, Zaštita novinarskih izvora u digitalnom okruženju, UNESCO (2017)

104 D. Banisar, Silencing sources: An International Survey of Protections and Threats to Journalists' Sources, Privacy International (2007), str.14, vidi isto: Ujedinjene nacije, Savet za ljudska prava. (2020). *Rezolucija 45/18: Bezbednost novinara i pitanje nekažnjivosti* (A/HRC/RES/45/18)

105 Na primer, UN General Assembly Resolution on the Right to Privacy in the Digital Age, UN Doc A/RES/77/211 (15.12.2022), Vidi više o UN dokumentima na ovu temu: Privacy International, PI's guide to international law and surveillance, Privacy International, 2024 str.6

106 Komitet za zaštitu ljudskih prava, Zaključna zapažanja u IV periodičnom izveštaju za Srbiji (CCPR-C-SRB-CO-4) (3.5.2024), para.37

komunikacija u cilju zaštite privatnosti[107], da zakon mora biti jednostavan, dostupan, jasan, precizan, razumljiv i nediskriminatoran,[108] uz izbegavanje blanketnih normi koje nisu neophodne i proporcionalne, i mera koje mogu ugroziti online sigurnost.[109] Neophodno je da postoje nezavisna nadzorna tela (engl. oversight mechanisms) koja su odvojena od nadležnih domaćih organa, koja imaju ulogu proaktivne istrage i nadgledanja aktivnosti, pri čemu treba da imaju pristup alatima za nadzor, koje analiziraju kroz periodične izveštaje.[110]

Počevši od 1996.[111] godine, Evropski sud za ljudska prava ukazao je na važnost zaštite izvora i postavio standarde za domaće sudove. Oni su dužni da jasno ukažu na ograničenja koja se moraju poštovati prilikom izvršavanja radnji koje mogu dovesti do povrede prava na zaštitu izvora, *zato što državni organi mogu imati široka ovlašćenja te steći uvid u veliki broj informacija i izvora.*[112] Evropski sud u nizu naknadnih presuda dalje razrađuje standarde zaštite pokrivajući različite situacije, uključujući i digitalni nadzor.

Na ovoj bogatoj sudskoj praksi, Preporuke Komiteta Ministara, koju je podržala i Srbija, postavile su standarde, koji iako iz 2000. godine[113] i dalje stoje kao okosnica za regulisanje ovog pitanja. One predviđaju da identifikacija izvora može biti zasnovana samo na članu 10. Evropske Konven-

107 UN Human Rights Council Resolution on the Right to Privacy in the Digital Age, UN Doc A/HRC/RES/54/21 (12 October 2023), para.9

108 UN Human Rights Council Resolution on Terrorism and Human Rights, UN Doc A/HRC/RES/51/24 (7 October 2022), para 16. Vidi isto: Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, UN Doc A/HRC/41/35 (28 May 2019), para. 24 i 25.

109 Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, UN Doc A/HRC/29/32 (22 May 2015)

110 Report of UNGA, United Nations High Commissioner for Human Rights on the Right to Privacy, A/HRC/51/17, 4 avgust 2022, dostupno na: https://docs.un.org/en/A/HRC/51/17

111 Goodwin protiv Velike Britanije, - 17488/90 [1996] ECHR 16 (27.31996)

112 Vidi više o tome: Roemen i Schmit protiv Luksemburga - 51772/99 [2003] ESLJP 102 (25.2.2003). 24 Ernst i Drugi protiv Belgije - 33400/96 [2003] ESLJP 359 (153.2003). 2De Haes i Gijsels protiv Belgije[1997] 25 E.H.R.R. 1.

113 Savet Evrope, Preporuka br. R (2000) 7 Komiteta ministara Saveta Evrope državama članicama o pravu novinara da ne otkriju svoje izvore informacija, usvojena 8. marta 2000. godine.

cije o zaštiti ljudskih prava[114] i ograničenjima predviđenim stavom 2, što predstavlja marginu delovanja država članice. Pored toga, što, kao što je slučaj u Srbiji, zemlja mora predvideti pravni osnov zaštite. Zaštita važi ne samo za novinare, već i urednike i redakcije, i spoljne organizacije i saradnike. Otkrivanje izvora neće biti smatrano neophodnim, osim ako se ne može sa *sigurnošću utvrditi* da razumne alternativne mere ne postoje ili su već iscrpljene i da je legitimni javni interes pretežniji, a taj interes mora biti dokazan, dok okolnosti moraju ozbiljne, te da postoji velika društvena potreba za rešenjem slučaja. Ovi uslovi moraju biti ispunjeni tokom svih faza postupaka.[115]

Takođe, novinari ne bi smeli biti primorani da otkriju svoje poverljive izvore u slučajevima klevete ili bilo kom drugom postupku „zbog navodne povrede časti ili ugleda neke ličnosti, nadležni organi treba da razmotre, radi utvrđivanja istinitosti ili neistinitosti tih tvrdnji, sve dokaze koji im stoje na raspolaganju na osnovu nacionalnog procesnog prava i ne treba u tom cilju da zahtevaju od novinara da otkrije informacije koje mogu da ukažu na identitet izvora."[116]

Predlog za pokretanje postupka radi otkrivanja identiteta izvora može podneti samo nadležni organ, koji mora obavestiti novinare o pravu da ne otkriju izvor, kao i o ograničenjima tih prava. Takođe, sankcije za neotkrivanje smeju biti donošene od strane viših sudova, a novinar mora imati mogućnost nezavisnog preispitivanja ovakve odluke. U slučajevima kada se novinar odazove pozivu da otkrije izvor, sudovi bi trebalo da preduzmu mere kako bi se ograničilo otkrivanje izvora na razumnu meru, uz zaštitu od samodiskriminacije - pravo da se ne iznose dokazi protiv sebe u postupcima.

114 Konvencija Saveta Evrope o zaštiti ljudskih prava i osnovnih sloboda, potpisana 4. novembra 1950. u Rimu, na snazi od 3. septembra 1953. (ETS br. 5)

115 Načelo 3, ibid. 83

116 Načelo 4, ibid.83

U kontekstu Srbije važno je da se prisluškivanje, presretanje komunikacije, i sudski pretresi i zaplene *ne smeju koristiti kao sredstvo za zaobilaženje zaštite poverljivosti izvora*.[117] Savet Evrope, u istoj Preporuci iz 2000. godine, navodi radnje koje *ne bi trebalo primenjivati* ukoliko postoji mogućnost otkrivanja izvora:

„i. nalozi za *presretanje* ili radnje koje se odnose na komunikaciju ili prepisku novinara ili njihovih poslodavaca,

ii. nalozi za *nadzor* ili radnje koje se odnose na novinare, njihove kontakte ili njihove poslodavce, iii. nalozi za *pretres ili zaplenu*, ili radnje koje se odnose na privatne ili poslovne prostorije, lične stvari ili prepisku novinara ili njihovih poslodavaca, ili *lične podatke povezane s njihovim profesionalnim radom.*“

Ukoliko su informacije koje identifikuju izvor pravilno pribavljene od strane policijskih ili pravosudnih organa primenom bilo koje od gore navedenih radnji — iako to možda nije bio cilj tih radnji — moraju se preduzeti mere kako bi se sprečila njihova naknadna upotreba kao dokaza pred sudovima, *osim ako bi njihovo otkrivanje bilo opravdano*.[118] Imajući u vidu ova jasna ograničenja, zakonodavni okvir Srbije, pre svega ZKP i ZBIA, ne pruža zadovoljavajući nivo garancija zaštite izvora, iz jednostavnog razloga – *zato što ih ne prepoznaje eksplicitno*. Takođe, teško je sa sigurnošću utvrditi na koji način i koliko efikasno sudska odobrenja pružaju mogućnost targetiranog pristupa podacima i komunikaciji, na način na koji se štite novinarski izvori, i u kojoj meri se institucije sistema pridržavaju ovih sudskih uputstava. Sasvim drugo je pitanje da li je sa tehničkog aspekta ovako targetiran pristup uopšte moguć.

Na nivou Evropske Unije, posebno je važan Evropski akt o medijskim slobodama (EMFA). Po prvi put, ovaj Akt, sa dejstvom direktne primene u državama članicama, ne samo da reguliše oblasti poput nezavisnosti jav-

117 Ibid.
118 Ibid. Princip 6

nih servisa, transparentnosti vlasništva u medijima, posebnih mera za moderaciju medijskog sadržaja i sl., već se posebno bavi zaštitom medijskih sloboda kroz prizmu zaštite izvora. Radi efikasne zaštite novinarskih izvora i poverljive komunikacije, ovaj Akt uvodi zajedničke *minimalne standarde zabrane prinudnih mera država članica,* uključujući upotrebu intruzivnog softvera (npr. špijunskih programa) prema medijima, novinarima, urednicima i osobama povezanim s njima. Takve mere, navodi se u Aktu, ugrožavaju poverenje između novinara i izvora i sužavaju slobodan protok informacija, što šteti i kvalitetnom informisanju javnosti i slobodi medijskog tržišta u EU. Novinari, uključujući i frilensere, moraju biti zaštićeni od nadzora koji može uključivati tajno snimanje, praćenje lokacije, pristup šifrovanim podacima i druge oblike digitalnog nadzora.

EMFA pruža široku definiciju špijunskog softvera, kao proizvoda sa digitalnim elementima specijalno dizajniranim da iskoristi manjkavosti drugog proizvoda sa digitalnim elementima, a koji omogućava prekriveni nadzor kroz nadgledanje, ekstrakciju, prikupljanje i analizu podataka fizičkih i pravnih lica.[119] Ova definicija, nedovoljno je precizirala elemente i funkcionalnosti ovakvih sistema nadzora, zbog čega je studija Evropske organizacije za zaštitu digitalnih prava (EDRI) korisna.

Špijunski softver je svaki softver: 1. koji je: instaliran ili korišćen na uređajima bez saglasnosti korisnika, 2. koji ima mogućnost da kompromituje uređaj privremeno ili stalno, 3. čije korišćenje je omogućeno kroz iskorišćavanje postojećih ili kreiranih manjkavosti digitalnog sistema, kao što je društveni inženjering, fizičko instaliranje, mehanizmi prethodne instalacije, kao i kroz obmanjujuće reklame. Jednom instaliran, spyware može imati mogućnost pristupa i nadgledanja uređaja u realnom vremenu, prikupljanja ličnih podataka, naknadnog filtriranja i deljenja sa trećim stranama, kontrole i manipulacije podataka, menjanje i fabrikovanje informacija, poruka, fajlova, kao i podmetanje dokaza.[120]

119 EMFA, član 2(2)

120 EDRI, Spyware and state abuse, The case for an EU wide ban, EDRI (2025), str. 7,8

U skladu sa ovom EDRI studijom „ili-ili" pristup je važan: alat ne mora da ispunjava sve ove radnje kumulativno da bi bio kvalifikovan kao softver. „Svaki softver koji ispunjava ključne karakteristike i ima jednu ili više navedenih funkcionalnosti može se kvalifikovati kao spyware, i s toga treba da potpadne pod okvire zabrane", uključujući komercijalni softver, softver razvijen od strane države, spyware za privatne svrhe kao što je recimo proganjanje partnera, kao i softveri za otkrivanje šifri i logova, kao i za ekstrakciju senzitivnih informacija.[121]

Akt je počeo sa primenom na nivou EU u avgustu 2025. godine[122], a zemlje kandidati bi trebalo da imaju dovoljno vremena da, učeći iz iskustva država članica, domaćeg društvenog i političkog konteksta, medijskih praksi, naročito analiziranih u prethodnom poglavlju, osiguraju adekvatan, efikasan zakonski okvir i, još važnije, različite mehanizme zaštite utemeljene na vladavini prava, zaštiti ljudskih prava i medijskih sloboda. Rešenja predstavljena u članu 4. Prava pružaoca medijskih usluga predstavljaju samo *minimalne*[123] standarde; Srbija mora otići (više) koraka dalje, pre svega zbog postojanja jasnih indicija o korišćenju ovih tehnologija u nadzoru nad novinarima, a i zbog već objašnjenih ukrštanja, pa i proširenja nadležnosti policije i BIA u kontekstu digitalnog nadzora. Ova ovlašćenja nisu praćena efikasnim i delotvornim mehanizmima zaštite ljudskih prava, pa i novinarskih izvora - što je inače namera evropskog zakonodavca.

Akt u preambuli objašnjava zakonodavni cilj, a to je uniformna zaštita izvora u svim državama članicama i garancije koje države moraju pružiti zbog toga što su „izvori od nesagledive važnosti kao ‚sirovi materijali' novinarima: oni su osnova produkcije medijskog sadržaja, naročito vesti i dnevnih dešavanja." Navode se, u članu 4, radnje koje države članice ne smeju primenjivati:

121 Ibid., str. 8, 9

122 https://www.europarl.europa.eu/news/de/press-room/20250725IPR29818/media-freedom-act-enters-into-application-to-support-democracy-and-journalism

123 EMFA, Recital (23)

1. *Obavezivati pružaoce medijskih usluga da otkriju informacije* u vezi sa ili one koje mogu da otkriju izvore i tajnost komunikacije, kao i osobe povezane sa pružaocem usluga (stav 1).

2. *Pritvoriti, sankcionisati, presresti ili pretresati* pružaoce medijskih usluga ili uredničkog osoblja, kao i njihove poslovne ili privatne prostore, *staviti pod nadzor ili izvršiti pretres i zaplenu* u cilju pribavljanja informacija koje se odnose na ili mogu otkriti novinarske izvore ili poverljivu komunikaciju (stav 2).

3. *Koristiti intruzivne nadzorne softvere* na materijalima, digitalnim uređajima, alatima koje koriste pružaoci medijskih usluga, kao i lica profesionalno povezanih sa njima (stav 3).

Lica profesionalno povezana sa pružaocem mogu se smatrati licima koja bi zbog njihovog redovnog ili profesionalnog odnosa mogla imati takve informacije ili bi mogla podvrgnuti njih ili njihove korporativne ili privatne prostorije nadzoru ili pretresu i zapleni u svrhu pribavljanja takvih informacija.

Od ovog osnovnog i primarnog pravila mogu se napraviti izuzeci i to u slučaju kada je reč o zadržavanju i presretanju (stav 2), ako postoji zakonski osnov, ako je u skladu sa trodelnim testom ograničenja ljudskih prava, ako je opravdano u svakom pojedinačnom slučaju u cilju zaštite javnog interesa[124] i srazmerno cilju koji se želi postići. Mora postojati odobrenje suda ili drugog nezavisnog tela. U pojedinim urgentnim i izuzetnim situacijama može se „naknadno odobriti od strane takvog tela bez nepotrebnog odlaganja.[125]"

124 Misli se pre svega na zaštitu javnih politika (policy), bezbednosti (security), sigurnosti (safety), zdravlje. Vidi više: Jan Erik Kermer, Član 4. Evropskog akta o slobodi medija: propuštena prilika? Procena nedostataka u zaštiti novinarskih izvora, Centar za pluralizam i slobodu medija, Dostupno na: https://cadmus.eui.eu/server/api/core/bitstreams/88a04e9e-60cc-5d21-97b2-f7283429d28b/content, str.200

125 EMFA, član 4(4)

Pored ispunjenosti ovih uslova, za korišćenje intruzivnog softvera (stav 3), mora biti reč o ozbiljnom krivičnom delu kao što je terorizam, trgovina ljudima, seksualna eksploatacija dece iz Okvirne Odluke o evropskom nalogu za hapšenje i postupcima predaje između država članica[126] – ili druga krivična dela za koje se u državama članicama može izreći kazna od najmanje pet godina. Zahteva se i da *„nijedna druga manje intruzivna mera ne bi bila dovoljna i adekvatna da dovede do otkrivanja informacije"* (paragraf 26).

Postavlja se još niz uslova koji se moraju ispuniti za primenu ovih mera:

1. Postepeni pristup: zabranjuje se korišćenje špijunskog softvera, ako se informacija može pribaviti korišćenjem manje intruzivnih mera kao što je ispitivanje (stav 1) ili presretanje i pretresanja (stav 2) - tzv. iznuđeno otkrivanje (engl. forced disclosure).[127]

2. Sprovođenje redovne sudske procene ispunjenosti uslova tokom trajanja mere.

3. Primenu zaštitnih mera, kao što je pravo lica na informacije i pristup ličnim podacima koji se obrađuju. Ove mere primenjivaće se na svaku obradu ličnih podataka sprovedenu u kontekstu primene mera nadzora. Ova zaštita se odnosi na i druga prava lica navedena u Direktivi o zaštiti fizičkih lica u procesu obrade podataka od strane nadležnih tela u svrhe krivično pravne zaštite.[128]

126 Evropska Unija, Okvirna Odluka od 13 juna 2002. o evropskom nalogu za hapšenje i postupcima predaje između država članica - Izjave određenih država članica o usvajanju okvirne odluke,2002/584/JHA, dostupno na: https://eur-lex.europa.eu/eli/dec_framw/2002/584/oj/eng

127 EMFA,. fn.49, p.194

128 Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (OJ L 119, 4.5.2016, p. 89).

4. Pravo na *efikasnu* sudsku zaštitu za pružaoce medijskih usluga, njihov urednički tim ili povezana lica. Države članice moraju poveriti *nezavisnom telu ili organu sa relevantnom stručnošću zadatak da pruži pomoć osobama u cilju ostvarivanja prava*. Ukoliko takvo telo ili organ ne postoji, te osobe mogu zatražiti pomoć od samoregulatornog tela ili drugih mehanizama.

5. Ostale odgovornosti država članica detaljno su regulisane najvišim pravnim aktima EU, a koji se odnose pre svega na zaštitu nacionalnih interesa i očuvanje osnovnih državnih funkcija.[129]

Ovako postavljena norma, ipak, po nekim autorima, predstavlja udar na zaštitu izvora pred nominalnim ciljem zaštite pretežnijeg interesa, koji je ostao na državama članicama da definišu u okviru strogo zadatih uslova (na primer, težina krivičnog dela) u svakom konkretnom slučaju. Bez obzira na činjenicu da će Akt, i član 4, tek zaživeti na prostoru EU, analiza iz poglavlja 2, u vezi sa medijskim praksama, gotovo jasno ukazuje da *„karakteristike i mogućnosti (spyware) ga čine inherentno inkompatibilnim sa principima neophodnosti, proporcionalnosti, i pravne sigurnosti,"*[130] te izrazite kompleksnosti i pravne virtuoznosti koja se zahteva u cilju institucionalne kontrole digitalnog nadzora. U nastavku, sledeće poglavlje ukazuje na niz dodatnih kritičnih tačaka i manjkavosti rešenja iz člana 4, kroz prizmu standarda koje je postavio Evropski sud za ljudska prava, kao drugih međunarodnih rešenja.

129 Recital 8, EMFA

130 Ibid, fn.47, str. 11

4. Diskusija

Države imaju pozitivnu obavezu da zaštite novinare i druge medijske aktere od zastrašivanja, pretnji i nasilja, bez obzira na to da li oni dolaze iz vladinih, sudskih, verskih, biznis ili kriminalnih izvora. Ova obaveza jasno je potvrđena u Preporuci CM/Rec(2016)4 Komiteta Ministara Saveta Evrope, kojom se države članice pozivaju da osiguraju bezbedno i povoljno okruženje za slobodno i nezavisno novinarstvo.[131] Savet Evrope je još 2000. godine usvojio Preporuku br. R(2000)7 o pravu novinara da ne otkriju svoje izvore informacija, potvrđujući posvećenost država članica zaštiti slobode izražavanja kao zajedničke evropske vrednosti. Posebno se u Načelu 6 naglašava da se mere nadzora nad komunikacijama, prisluškivanja, praćenja, kao i sudskih naloga za pretres ili zaplenu ne smeju koristiti sa ciljem da se zaobiđe pravo novinara na zaštitu svojih izvora. Takve radnje — uključujući prisluškivanje komunikacija novinara, nadzor njihovih kontakata, ili pretrese njihovih prostorija, ličnih stvari i poslovne prepiske — predstavljaju ozbiljan rizik za poverljivost izvora i time direktno ugrožavaju novinarsku slobodu i bezbednost. Ova načela zajedno čine *temelj za zaštitu novinarstva u demokratskim društvima i postavljaju jasne granice državnim intervencijama* koje bi mogle ugroziti slobodno i odgovorno informisanje.

Posebno kada je reč *o pretresanju prostorija i oduzimanju uređaja*, ovlašćenja policije su veoma široka, omogućavajući im gotovo neograničen pristup ličnim i profesionalnim dokumentima i podacima. Evropski sud za ljudska prava, stao je na stanovište da domaći organi treba da predvide *nivo garancije u vidu prethodne kontrole od strane suda ili drugog nezavisnog organa*. U slučaju nepostojanja ove prethodne kontrole, Evropski sud za ljudska prava zaključuje da ne postoji dovoljan nivo zaštitnih mera, što

131 Savet Evrope, Komitet ministara, Preporuka CM/Rec(2016)4 državama članicama o zaštiti novinarstva i bezbednosti novinara i drugih medijskih aktera, usvojena 13. aprila 2016.

posledično dovodi do kršenja slobode izražavanja.[132] *Francuski Krivični zakonik nalaže sudu da prilikom izdavanja odobrenja za pretres prostorija i uređaja ne smeju biti korišćene radnje kojima bi se zaobišlo pravo na zaštitu izvora, i da transkripcija komunikacije novinara tako pristupljenim podacima ne sme da uključi komunikaciju sa izvorima.*[133]

Domaći sud mora imati mogućnost da *odbije da izda naredbu za sprovođenje digitalnog nadzora,* ili da izda *ograničeno odobrenje* kako bi se zaštitili izvori. U hitnim situacijama, krizama i povišenim tenzijama u društvu, treba predvideti proceduru za *identifikaciju i izolaciju materijala od strane vlasti koji bi mogli otkriti izvor*.[134] Slično je i sa oduzimanjem i pretresanjem elektronskih uređaja - moraju postojati proceduralne garancije protiv neograničenog pristupa materijalu i arbitrarnog mešanja. U slučaju S.Sorokin protiv Rusije[135], Evropski sud navodi da prilikom izdavanja naredbe, sud nije dovoljno precizno objasnio razloge zbog kojih je potrebno pretresanje, niti je obrazloženje ukazalo na sprovođenje testa ograničenja prava u smislu zaštite pretežnijeg interesa. Pored toga, *domaći sud nije izdao uputstva za sužavanje obima pristupa podacima i onemogućio pristup nepovezanim licima i profesionalnim podacima.*[136] U Srbiji, domaći sud može da odbije da izda nalog, ali je potrebno uraditi dodatne analize, u saradnji sa sudovima u tom procesu, kako bi se utvrdilo da li i u kojim situacijama sud koristi ovo pravo. Po saznanjima autorki ove analize, *u Srbiji ne postoje posebna uputstva,* makar ne javno dostupna, za policijske službenike i zaposlene u BIA u vezi sa postupanjem prilikom pretresa prostorija ili oduzimanja uređaja, što ukazuje na mogućnost pristupa velikom broju nepovezanih i privatnih podataka. Uz to, *trenutni nivo ukrštanja proceduralnih ovlašćenja* BIA-e i policije, iz mnogih razloga koji prevazilaze okvire ove analize,

132 M. Pisarić, Špijunski softver protiv novinara u ed. J. Kostić i M.M. Bošković, Mediji Kazneno Pravo i Pravosuđe, Tematski zbornik radova međunarodnog značaja, Institutu za uporedno pravo, (2024), str. 455

133 Savet Evrope, Kako zaštiti novinarske izvore?, Savet Evrope, (2023), str.25

134 M. Pisarić, Špijunski softver protiv novinara u ed. J. Kostić i M.M. Bošković, Mediji Kazneno Pravo i Pravosuđe, Tematski zbornik radova međunarodnog značaja, Institutu za uporedno pravo, (2024), str. 455

135 Sergej Sorokin protiv Rusije, br. 52808/09, stavovi 62–64, presuda od 30. avgusta 2022, Evropski sud za ljudska prava.

136 Ibid., p.456

ozbiljno može narušiti postojeće mehanizme zaštite slobode medija i vladavine prava. Drugim rečima, ovakvo zakonsko ukrštanje nadležnosti otvara mogućnost zloupotrebe, nejasnoća i nedorečenosti.[137]

Sličan nivo garancija i zaštite se zahteva i u situacijama pristupa *zadržanim podacima* i presretanju komunikacije. Spomenuta Preporuka Saveta Ministara iz 2000. godine navodi radnje kojima ne treba pribegavati, osim pod određenim uslovima. Ako policija tokom sprovođenja tih radnji dođe do saznanja o izvorima, *„treba preduzeti mere koje će sprečiti korišćenje te informacije."*[138] U skladu sa osnovnim uslovima za ograničenje prava novinara, *naredba suda mora biti "jasna, sa detaljnim pravila koja ukazuju na opseg i način primene mera.[139]"* Sud mora posebno odrediti obim pristupa, i to uzimajući u obzir stepen intruzivnosti mere i cilj koji se želi postići, a odluka mora biti obrazložena, kako bi pokazala pravovaljane razloge za pristup zadržanim podacima.[140] Provejava utisak kroz intervjue rađene za potrebe ove studije, kao i analizu medijskih praksi i izrazito problematičnih slučajeva digitalnog nadzora, a kao što je i navedeno u Medijskoj Strategiji, da je u Srbiji, pristup zadržanim podacima ponekad arbitraran, sa indicijama o neispunjenosti zakonskih uslova, kao što je postojanje sudske odluke koja treba da ukaže na dozvoljeni opseg intruzije na način na koji se *ne prikupljaju podaci koji nisu u konkretnoj vezi sa slučajem, a koji kasnije mogu biti upotrebljeni u druge svrhe.*[141] *Zato je i kontrolna funkcija suda važna, da*

137 Vidi više o tome: S. Beljanski, Prisluškivanje i dokazivanje, Peščanik (4.7.2025), dostupno na: https://pescanik.net/prisluskivanje-i-dokazivanje/

138 Načelo 6, Preporuka Komiteta Ministara (2000)

139 Podchasov protiv Rusije, App No 33696/19,ESLJP (13.2.2024), para. 63

140 Evropski sud za ljudska prava ukazao je na sledeće procene koje domaći organ treba da uzme u razmatranje: prirodu i težinu relevantnih krivičnih dela; nivo stvarnog mešanja u pravo na poštovanje privatnog života; obim i primenu sistema za čuvanje podataka; period zadržavanja podataka; mogućnost preispitivanja; mere zaštite od zloupotrebe; kao i garancije usmerene na regulisanje pristupa trećih strana i zaštitu integriteta i poverljivosti podataka. Vidi više: N.F. i drugi protiv Rsijem Apps Nos 3537/15, ESLJP, (12.9.2023), para.46

141 Ibid., fn.58, str.458, vidi isto: *Sedletska protiv Ukrajne*, Application No. 42634/18, ESLJP (1.4.2021)

zaštiti privatnost i slobodu izražavanja novinara i pore toga, zaštiti izvore.[142] U veoma sličnom slučaju, Evropski sud pravde zaključuje da francusko zakonodavstvo koje daje mogućnost generalnog i nediskriminatornog pristupa zadržanim podacima u cilju suzbijanja ozbiljnih krivičnih dela, ali bez limitiranja prikupljanja na striktno neophodne podatke, ne može se smatrati opravdanim u okvirima demokratskog društva.[143]

Iako je EMFA detaljno regulisala načine i uslove za upotrebu špijunskog softvera, postojeća ograničenja u Aktu, nejasnoće i zakonske praznine ostavljaju prostora za zloupotrebe. Posebno su rizične za zemlje u kojima ne postoji dovoljan nivo nezavisnosti sudova i drugih tela koja treba da odobre radnje digitalnog nadzora iz člana 4. Pored toga, na državama članicama i kandidatima je da *odrede mere za procenu institucionalne nezavisnosti i mehanizam zaštite od donošenja odluka sa ovako dalekosežnim posledicama tela koja suštinski nisu nezavisna.* Najviše prostora za zloupotrebe ostavlja *ex post odobrenje suda* rezervisano samo za izuzetne i urgentne situacije, koje je niti bliže objašnjeno, niti je predviđen period za ovo naknadno odobravanje. Povrh svega „otvara se mogućnost ugrožavanja novinarskih prava pre nego što je pravna zaštita dostupna."[144] Pitanje je šta se dešava u situacijama kada sud odluči da je prethodna radnja nadzora bila ilegalna, a prava novinara su već prekršena.

---

142 Presude Evropskog Suda pravde pružaju uvid u niz uslova, procesa i procena koje se moraju sprovoditi u svakom pojedinačnom slučaju kako bi se zaštitila privatnost. Iako se odnose na fizička lica, podjednako su primenjivi i na zaštitu novinara i izvora. Vidi više: Privacy International, PI's guide to international law and surveillance, Privacy International, 2024, str. 36-38

143 La Quadrature du Net, French Data Network, Fédération des fournisseurs d'accès à Internet associatifs, Igwan.net v de l'Intérieur, Ministre des Armées; Ordre des barreaux francophones et germanophone, Académie Fiscale ASBL, UA, Liga voor Mensenrechten ASBL, Ligue des Droits de l'HommeASBL, VZ, WY, XX v Conseil des ministers (C-511/18, C-512/18 and C-520/18), Judgment, Grand Chamber, Court of Justice of the European Union (6 October 2020), para. 141

144 Jan Erik Kermer, *Član 4. Evropskog akta o slobodi medija: propuštena prilika? Procena nedostataka u zaštiti novinarskih izvora*, Centar za pluralizam i slobodu medija, Research Associate, PhD. Dostupno na: https://cmpf.eui.eu/article-4-of-the-european-media-freedom-act-a-missed-opportunity, str.199

Problematičan je i veliki broj krivičnih dela iz člana 4. stav 4(2) koji se odnosi na sva dela za koje je zaprećena kazna od najmanje 5 godina, što obuhvata različita krivična dela u različitim državama, pa je teško postići dovoljan nivo pravne sigurnosti. Pored toga, reč je o nesrazmerno velikom broju krivičnih dela, iako i pravna norma iz ZJIM koristi isti kriterijum. Problem nije zaprećena kazna i njena visina, nego blanko uključivanje velikog broja krivičnih dela. U kontekstu Srbije, problematičan je i nedostatak jasnih zakonskih ograničenja i smernica za postupanje institucija sistema koje treba, pre svega, da se uzdrže od ovih radnji.

Upravo ovi nedostaci, uz činjenicu da je reč o minimalnim standardima, *kreiraju mogućnost da se ova norma upotpuni* standardima Evropskog suda za ljudska prava, Saveta Evrope i nacionalnih zakonodavstava koja pružaju veći stepen zaštite.[145] Ovo tim pre, što je nakon Pegasus skandala,[146] EU Parlament formirao Istražni odbor koji je zaključio da ne samo da su pojedine EU države koristile, nego su postale i značajna karika u lancu trgovine ovim tehnologijama. Pored činjenica slabog odaziva država za saradnju sa odborom, Parlament je u Preporukama zaključio da postoji „nezrelost, nespremnost, nepodobnost institucija EU", što može „predstavljati indiciju za procenu adekvatnosti EU da reaguju na korišćenje špijunskog softvera."[147] Ova ocena se može pripisati i institucijama u Srbiji, koje pored toga što nisu sprovele dubinsku istragu prethodnih slučajeva korišćenja intruziv-

145 Ibid., str.202

146 Pegazus projekat (nazvan po „fajlu" tj. „virusu"), koji u mobilnom telefonu, bez interakcije sa zaraženim fajlom, počinje da sakuplja sve podatke, uključujući one koji se dele u realnom vremenu. Identifikovan je kod novinara i boraca za ljudska prava iz Azerbejdžana, Mađarske, Meksika, Francuske, Španije, Velike Britanije, Turske, Kazahstana, itd. Istraga je pokazala da je i telefon ubijenog novinara Jamala Khashoggija, 2018. godine bio zaražen, kao i telefon meksičkog novinara Cecilia Pineda, koji je ubijen dva sata nakon što je objavio informaciju o povezanosti lokalnih vlasti sa narko kartelom. Vidi više: Amnesty International, Forensic Methodology Report, How to Catch NSOs Group Pegasus, Amnesty International (18.7.2021), dostupno na: https://www.amnesty.org/en/latest/research/2021/07/forensic-methodology-report-how-to-catch-nso-groups-pegasus/ i Access Now, Pegasus Archive, dostupno na: https://www.accessnow.org/tag/pegasus-project/

147 M. Pisarić, Špijunski softver protiv novinara u ed. J. Kostić i M.M. Bošković, Mediji Kazneno Pravo i Pravosuđe, Tematski zbornik radova međunarodnog značaja, Institutu za uporedno pravo, (2024), str. 451

nog softvera, sve više pretenduju da prošire nadzor i krivičnopravni otisak kroz ukrštanje nadležnosti represivnih organa nad građanima, novinarima, aktivistima, pa tako i nad novinarskim podacima i izvorima. Kao što je objašnjeno, svaka radnja policije, u slučaju Srbije i BIA, koja po svom obimu i trajanju prevazilazi ograničenja postavljena standardima i domaćim normama, može zaobići zaštitu novinarskih izvora.

Poslednja dešavanja na svetskom i evropskom nivou idu u pravcu širenja nadzora i kontrole, a u cilju jačanja ideje o očuvanju nacionalne bezbednosti. Tako se trenutno u EU razgovora o pravičnom i efektivnom pristupu podacima građana za potrebe vršenja policijskih poslova. Evropska Komisija će ove godine sprovesti procenu uticaja u cilju *utvrđivanja značaja zadržanih podataka za policijske organe*. Na ovaj način, otvara se mogućnost za ponovno uspostavljanje pravnog okvira o zadržanim podacima, koji je Evropski sud pravde pre 11 godina proglasio nevažećim. Svaka nova regulativa moraće da poštuje kriterijume koje je ova presuda postavila u smislu prikupljanja striktno neophodnih podataka u cilju istraga ozbiljnih krivičnih dela – što je u skladu i sa članom 4. EMFA. Pored toga, već postojeći mehanizam omogućava razmenu e-dokaza među policijama država članica, ali ne i presretanje u realnom vremenu, sa posebnim problemom u vezi sa enkripcijom koja navodno otežava istrage, pa se i ona stavlja u okvir analize kroz tzv. Mapu puta koju Evropska Komisija razvija u ove svrhe.[148] I pre ovih najava, a u periodu nakon anuliranja Direktive o zadržanim podacima, države koje su zadržale ove odredbe, nisu precizno odredile mere koje policija i drugi organi moraju poštovati u cilju zaštite izvora. Samo navođenje, kao što je recimo slučaj Belgije, da nadzor ne sme zaobići pravo na zaštitu izvora, nije dovoljno jasno. *Nedostaju (saznanja) i pravne prakse, uputstva i moguća zakonska rešenja koja i sa tehničkog i institucionalnog aspekta*

148 Evropska komisija. *European Commission publishes its plan to enable more effective law enforcement access to data*. Inside Privacy. (2023). Dostupno na: https://www.insideprivacy.com/data-privacy/european-commission-publishes-its-plan-to-enable-more-effective-law-enforcement-access-to-data/

preciziraju proces od početka do kraja. Zakon o zaštiti podataka o ličnosti pruža odličan početan okvir, kao i presude Evropskog suda za ljudska prava.[149]

Dodatni problematičan aspekt nadzora u Srbiji su i javne nabavke opreme i softvera. Krovni dokument kojim se reguliše nabavka tehnologija u ovoj oblasti jeste Uredba o javnim nabavkama u oblasti odbrane i bezbednosti, koja praktično predstavlja podzakonski akt donet radi operacionalizacije Zakona o javnim nabavkama.[150] Uredbom se uređuju vrste postupaka javnih nabavki u oblasti odbrane i bezbednosti, uslovi i način njihovog sprovođenja, kao i komunikacija u postupcima javnih nabavki. Javne nabavke u oblasti odbrane i bezbednosti, u skladu sa referentnim zakonom su nabavke: 1) vojne opreme, uključujući i bilo koji njen sastavni deo, komponentu ili sklop; 2) bezbednosno osetljive opreme, uključujući i bilo koji njen sastavni deo, komponentu ili sklop; 3) dobara, usluga ili radova direktno povezanih sa prethodno navedenom opremom; 4) usluga i radova isključivo za vojne namene; 5) bezbednosno osetljivih radova i bezbednosno osetljivih usluga.

Ovako postavljene norme ne pružaju bliži uvid u to koja bi konkretno oprema mogla biti nabavljena, odnosno, mogu predstavljati prostor za zloupotrebu, te upotrebu nabavljene tehnologije protiv prava i sloboda građana, uključujući tu i novinare i njihove izvore. Iako je neosnovano tražiti potpunu transparentnost organa bezbednosti, odgovornost u pružanju makar nekih konkretnijih informacija mora postojati, odnosno, mora biti zakonski bolje predviđena i definisana.

U celini posmatrano, novinari su danas - uzimajući u obzir ceo „asortiman" mera digitalnog nadzora od pristupa zadržanim podacima, do pretresanja prostorija, oduzimanja uređaja i instaliranja špijunskog softvera, primorani da rade pod sistemskom pretnjom koja deluje prikriveno, podrivajući njihovu bezbednost, a da pritom ne ostavlja vidljive tragove svog delovanja. „Cilj nadzornih alata, poput špijunskog softvera, jeste

149 J. Posetti, Zaštita novinarskih izvora u digitalnom okruženju, UNESCO (2017), str.25

150 Zakon o javnim nabavkama, "Službeni glasnik RS" br. 91/2019 i 92/2023

maksimalna invazivnost uz minimalnu vidljivost, a takva dinamika podseća na koncept ‚crne kutije', koji se obično primenjuje na tehnologije čije tehničke sposobnosti i unutrašnja logika nisu lako podložne nadzoru ili odgovornosti." Koncept crne kutije vezuje se za algoritme i način „kretanja" informacija kroz platformizovane sisteme, poput društvenih mreža. Ipak, i sam špijunski softver, s obzirom na broj nepoznanica, nevidljivost, i uopšte digitalni nadzor - zbog same netransparentnosti, nedostupnosti informacija, načina i obima pristupa, a sa veoma jasnom svešću o nesagledivim posledicama, postaje „tehno-magla" koja otežava procenu pretnji i prirodu kršenja ljudskih prava.[151]

151 P.Di. Salvo, Dealing with the blackbox: European Journalists and threats of Spyware, Digital Journalism (2024), p.15

5. Zaključci

Šire posmatrano, svaki oblik nekontrolisanog digitalnog nadzora *suštinski predstavlja napad na slobodu izražavanja i privatnost, kao i na druga ljudska prava.* Bilo da je reč o pristupu podacima i presretanju komunikacije, ili o korišćenju špijunskog softvera (engl. spyware) – ove prakse u svojoj osnovi ne samo da imaju efekat zastrašivanja i sa njima povezanih posledica, već je, i kako nalazi istraživanja pokazuju, reč o radnjama koje se sa stanovišta zaštite slobode izražavanja, čiji je element i zaštita izvora, *teško mogu opravdati i sagledati kao pravno dozvoljen način ograničavanja ovog prava.*

Nedostaju zakonski osnovi visokog kvaliteta u Srbiji, zasnovani na vladavini prava, kao i efikasne institucionalne mere zaštite od arbitrarnog i nesrazmernog nadzora. Norme moraju biti jasne, dostupne, na način na koji lica mogu da predvide posledice radnje predviđene zakonom, sa jasnim garancijama protiv zloupotreba.[152] Domaći zakoni, pre svega ZBIA i ZKP, ali i ZEK, ostavljaju prostora za različita tumačenja, sa širokim ovlašćenjima za institucije sistema, a bez jasne i izričite garancije o zaštiti od zloupotreba.[153] *Kritično nedostaju odredbe o zaštiti novinarskih izvora kroz ova zakonska rešenja.* Nedostaju i zakonske norme kao i podzakonski akti za organe koji će jasno odrediti o*pseg diskrecionog ovlašćenja nadležnih organa*[154], a novinarima nije ostavljena mogućnost naknadnog ispitivanja odluke. Ovo su samo neke od manjkavosti koje treba uzeti u razmatranje prilikom analize medijske prakse iz poglavlja 2, kao i u budućim pravnim razmatranjima i multisektorskim diskusijama.

Kada je reč o špijunskom softveru, *potrebno je krenuti od pretpostavke da ne može postojati špijunski softver koji je dizajniran u skladu sa poštovanjem ljudskih prava, jer sama činjenica da zloupotrebljava manjkavosti uređaja i da*

152 Potoczká iAdamčo protiv Slovačke,, App No 7286/16, ESLJP (12.1.2023), para. 71
153 Na primer, Uzun protiv Germany, App No 35623/05, ESLJP (2.9.2010), para. 63
154 Szabó i Vissy protiv Mađarske, App No 37138/14, ESLJP (12.1.2016), para.65

postoji mogućnost manipulacije podacima stoji u suprotnosti sa principima zaštite ljudskih prava,[155] *što je jasan indikator da mora postojati jasna zakonska zabrana korišćenja ovih alata i mera.*

U kontekstu Srbije, a u skladu sa standardima Evropskog suda za ljudska prava i slično sa Aktom o medijskim slobodama (EMFA), u svakom pojedinačnom slučaju nadležni organ mora:

1. Sprovesti test dozvoljenosti (u skladu sa zakonom), srazmernosti (u odnosu na cilj koji se želi postići kroz određivanje opsega i primene mera, uz postojanje minimalnih mehanizama zaštite) i neophodnosti u demokratskom društvu (policija i organ koji izdaje odobrenje).

2. Razumljivo ukazati kako legitimni interes za zaštitu javnog interesa odnosi prevagu nad ograničenjem prava na zaštitu novinara.[156]

3. Utvrditi da li je informacija u neposrednoj vezi sa konkretnim krivičnim delom, uzimajući u obzir ozbiljnost svih okolnosti.

4. Proceniti da li postoje alternativni načini otkrivanja ili su iscrpljene sve mogućnosti („poslednje sredstvo").

5. Nedvosmisleno utvrditi da li pristup podacima, i u kom obimu, može otkriti izvor i onemogućiti (filtriranjem ili na drugi način izolovati) pristup tim podacima.

6. Mora biti jasno da je informacija **ključna** za rešenje slučaja, dakle ne za nastavak istrage.

155 EDRI, Spyware and state abuse, The case for an EU wide ban, EDRI (2025), str. 13

156 U svojoj bogatoj praksi, Evropski Sud za ljudska prava doneo je veliki broj presuda koje su sve, na jedan ili drugi način, ili u određenoj meri posebno pažnju posvetile ovom pitanju. Buduće analize treba posebno da se pozabave ovom temom, kako bi sudijama približile proces balansiranja. Više o jurisprudeniciji suda: Privacy International, PI's guide to international law and surveillance, Privacy International, 2024

7. Omogućiti efikasan pristup adekvatnim pravnim lekovima, kao i oformiti nadzorna tela koja su nezavisna od organa koji sprovodi nadzor.[157]

Pored toga, *svaki zahtev nadležnog organa mora doći samo od organa koji se usko bavi poslovima krivičnopravne zaštite,* dakle organ sa mandatom da zahteva pristup ovim podacima u okviru određene institucije, a ne neodređeni broj lica i odeljenja. U Velikoj Britaniji su to samo viši policijski službenici koji moraju dobiti dozvolu od svojih nadređenih. Službenik mora prvo sprovesti tripartitni test dozvoljenosti ograničenja slobode izražavanja koji će pokazati da li je digitalni nadzor u skladu sa zakonom, da li teži legitimnom cilju, i da li je neophodan u demokratskom društvu. Budući da je svaki pristup podacima i svaki zadržani podatak u svojoj osnovi ograničavanje prava na slobodu izražavanja i privatnost, službenici su, u skladu sa prirodom policijskog delovanja, dužni da sprovedu one radnje koje najmanje ograničavaju slobode i prava.

Svako ograničenje mora se *usko, ciljano i svrsishodno tumačiti i pristupiti ograničenju samo „ako se na ubedljiv način može utvrditi ispunjenost uslova"*[158]*,* jer to su namere zakonodavca koji novinarima pruža veći stepen krivično-pravne zaštite, kao i garancije zaštite i uživanja medijskih sloboda. U suprotnom, bez ove zaštite izvora, fizička bezbednost novinara je ozbiljno ugrožena, što se kosi sa obavezom države da garantuje zaštitu novinara. Bez zaštite izvora, novinari mogu biti prisiljeni da otkriju izvore od strane policije, ili tokom sudskih postupaka, i zbog toga Savet Evrope preporučuje da novinari ne treba da budu prinuđeni da predaju beleške, fotografije, audio zapise, video materijale u situacijama krize, kao što su višemesečni protesti u Srbiji, kako bi osigurali svoju bezbednost. [159]

157 Szabó i Vissy protiv Mađarske, App No 37138/14, ESLJP (12.1.2016), para. 85 (između ostalih presuda)

158 Načelo 3 (b), Komitet Ministara Saveta Evrope, Preporuka o pravu novinara da ne otkriju svoje izvore informacija No. R(2000)7

159 Smernice Komiteta ministara Saveta Evrope o zaštiti slobode izražavanja i informisanja u vremenima krize. Usvojene od strane Komiteta ministara 26. septembra 2007

Zaštita novinarskih izvora u digitalnom okruženju se mora *posmatrati višeslojno i inter-sektorski povezano sa drugim problemima i politikama bezbednosti novinara.* Ova višeslojnost podrazumeva sveobuhvatni pristup, koji uzima u obzir ceo proces digitalnog nadzora i digitalnih rizika po zaštitu novinara i izvora. Od javnih nabavki, primene mera nadzora nad novinarima, do sudske i tužilačke uloge, zaštita novinara i njihovih izvora mora biti „ukorenjena" u svaki segment ovog procesa. Buduće rasprave na ove i slične teme moraju uzeti u obzir ceo „skup nadzornih instrumenata" (engl. surveillance assemblage), *politike, institucije, načela vladavine prava,* pre nego što se uže fokusiraju na pitanje zaštite novinarskih izvora. Jednostavnije rečeno, ne može biti dovoljno samo jačati normu zaštite izvora, pa čak i povezanih normi iz drugih zakona, ako je proces nabavke, upotrebe i nadzora nad ovim tehnologijama bez ozbiljnih sistema kontrole i korekcije.

Zaštita ličnih podataka uređena posebnim zakonom je takođe važan okvir zaštite. Osnovni principi obrade podataka, a naročito obaveza *minimalne obrade,* koja je takođe naglašena u presudama Evropskog suda za ljudska prava i pojedinim domaćim zakonodavstvima u odnosu na policijske istražne radnje, bilo da je reč o pristupu zadržanim podacima, pretresu prostorija ili novinara, ukazuju na važnost dosledne primene Zakona o zaštiti ličnih podataka. Ovaj krovni zakon mora se direktno primeniti u cilju zaštite izvora i bezbednosti novinara, jer pruža normativni okvir rada za policiju, radnike BIA, sudove i tužilaštvo. Naime, svi oni se smatraju *rukovaocima podacima* po ovom Zakonu kada sprovode posebne dokazne radnje i posebne mere, ako je reč o Agenciji.

Važnu ulogu u procesima digitalnog nadzora imaju i *internet posrednici, operatori, pružaoci digitalnih usluga*, druge kompanije koje se nalaze u lancu obrade podataka sa različitim funkcijama. Iako su obavezni da zadržavaju podatke i omoguće sprovođenje posebnih dokaznih radnji i mera, u skladu sa zakonskim ograničenjima i načelima poštovanja ljudskih prava, privatni akteri takođe treba da odgovaraju na ove zahteve u skladu sa istim načelima. Organizacija Global Network Initiative (GNI) decenijama već pomaže kompanijama, uključujući operatore, platforme poput Mete,

i druge internet posrednike i gigante, da odgovore na zahteve institucija sistema. Kompanije koje su članice GNI moraju kroz procene rizika uticaja na ljudska prava da razviju interne procedure za postupanje po zahtevima institucija, pa tako održavaju registar zahteva za pristup podacima i zahtevima za ograničavanje slobode izražavanja, kao i da omoguće pristup pravnim lekovima za korisnike čija prava su ugrožena. Posebno se obavezuju kompanije da državni zahtevi budu u skladu sa domaćim zakonom, međunarodnim standardima, transparentni, *usko specifični (dakle, ne blanko).* Potrebno je da svaki zahtev sadrži, pored zakonski propisanih uslova, osnov za ograničenje prava, *kao i naziv organa, ime i prezime, poziciju i potpis osobe koja zahteva pristup*. U slučajevima kada se kompanije suočavaju sa preširokim zahtevima, one mogu da zahtevaju od država objašnjenje, specifikaciju i *sužavanje obima,* ukazujući na neusaglašenost sa domaćim i međunarodnim propisima.[160]

Uključivanje kompanija u proces razvoja širih zakonskih rešenja i smernica za postupanje organa i privatnih aktera podjednako je važno kao i uključivanje novinara i medijskih organizacija, jer su kompanije - privatni akteri - *čuvari podataka, i njihovo postupanje je vođeno i ekonomskim i političkim interesima*. Zbog toga je, za kraj zaključka, važno podvući da u izmene zakonske norme ZJIM ne treba ulaziti ne samo zbog političkih tenzija, nego zbog toga što je *potrebno jasno razumevanje praksi privatnih aktera i institucija sistema u procesima digitalnog nadzora.* Analiza i izmena ZJIM, u skladu sa zaštitom ljudskih prava i uz poštovanje prava i sloboda zagarantovanih u svim relevantnim zakonima i drugim propisima, ne bi trebalo da se uzmu u razmatranje bez još *većih i dubinskih izmena „povezanih" zakonskih propisa* (ZKP, ZBIA, ZK, ZVOA, itd.), kao i njihovo dodatno usaglašavanje sa ZZLP, ZEK, Zakon o unutrašnjim poslovima. Takva izmena jednostavno ne vodi popunjavanju identifikovanih praznina u zaštiti izvora i, još važnije, zaštiti podataka novinara čija obrada može da dovode do otkrivanja izvora. Potrebno je, takođe, razmisliti i o smernicama i uputstvima za zaštitu izvora tokom sprovođenja posebnih dokaznih radnji i mera, edukaciji pra-

160 Global Network Initiative(GNI), Smernice za primenu principa o slobodi izražavanja i privatnosti, dostupno na: https://globalnetworkinitiative.org/gni-principles/implementation-guidelines/

vosudnih organa, a naročito policije i BIA, kako bi se *holistički, višeslojno i smisleno pristupilo ovoj oblasti*. Primer Crne Gore, koja je izmenila normu iz Zakona o medijima[161] tako što je predvidela niz izuzetaka u kojima se može zahtevati otkrivanje izvora, kao i uslova koji se moraju poštovati[162], a da pritom nije ujedno osigurala zaštitu novinarskih podataka i izvora u drugim zakonima kojima se može zaobići norma iz člana 30. ovog Zakona - govori u prilog ovoj tezi. Delimične izmene nisu put ka adekvatnoj i sveobuhvatnoj zaštiti izvora i ličnih podataka novinara, a naročito *nisu put u sistemima sa slabim demokratskim kapacitetima i vladavinom prava*.[163]

161 Zakon o medijima Crne Gore, „Službeni list Crne Gore", br. 82/20 od 6. avgusta 2020.

162 Novinar je dužan da na zahtev državnog tužioca, otkrije izvor informacija kada je to neophodno radi zaštite interesa nacionalne bezbednosti, teritorijalnog integriteta i zaštite zdravlja. Ostatak procedure podrazumijeva da će prilikom donošenja odluke o saslušanju novinara po zahtjevu tužioca, sud "posebno voditi računa o tome da li je utvrđena informacija u neposrednoj vezi sa konkretnim slučajem, da li se informacija može pribaviti iz drugih izvora", te da li interes za otkrivanje izvora preteže, u odnosu na zaštitu izvora informacije. Više o tome: Slavoljub Šćekić, Dok izvori utihnu, Vijesti (20.8.2020.), Dostupno na: https://www.vijesti.me/kolumne/457303/dok-izvori-utihnu#
Vidi isto: admin, Kako ćemo zaštiti izvore, Čitaj između redova (6.12.2022), Dostupno na: https://citajizmedjuredova.me/?p=3869

163 Na primeru Crne Gore medijski eksperti zaključuju „Još jednom se pokazuje, u stvari, da najgore što se može desiti jeste kada se hibridni režim pozove na rješenja demokratskog svijeta, čak ih i bukvalno prepiše, da bi dokinuo i malo preostale slobode medija.", što se može odnositi i na Srbiju. Ibid.

6. Preporuke

Preporuke treba čitati, razmatrati i primenjivati uzimajući u obzir sve prethodno ukazane prakse, standarde i jurisprudenciju Evropskog suda za ljudska prava. Preporuke ne pretenduju da ukažu na pojedinačna zakonska i institucionalna rešenja, već predstavljaju mapu (mogućeg) puta ka jačanju zakonske i institucionalne zaštite novinarskih izvora. Ipak, važno ih je razmatrati kao set prioriteta, gde je prvi i kontinuirani put jačanje medijskih sloboda i poverenja između građana i medija, a svaki sledeći korak vezan je za ispunjenost prethodnog koraka.

1. Mediji i novinari *kontinuirano* da rade na podizanju kapaciteta, unapređenju znanja i „digitalne higijene"

Imajući u vidu da je zaštita izvora jedan od ključnih privilegija, ali i obaveza novinara, potrebno je da oni konstantno rade na podizanju nivoa profesionalizacije i podizanju sopstvenih kapaciteta kako bi se bolje zaštitili i blagovremeno prepoznali potencijalne pretnje. Obuke treba da budu redovne, a mogle bi da obuhvate teme poput korišćenja bezbednih digitalnih alata, enkripcije, fizičke bezbednosti, prepoznavanja digitalnih etičkih standarda i zakonskih osnova o zaštiti izvora. Ova preporuka je ključna za očuvanje integriteta i otpornosti medija u sve zahtevnijem digitalnom i društvenom okruženju.

Kako bi se ojačalo poverenje u medije, kao i poverenje između medija i izvora, mreže podrške sa organizacijama civilnog društva, akademskom zajednicom i širom javnošću, kroz solidarnost, omogućavaju zajednički odgovor na pritiske, razmenu znanja i resursa, kao i „glasnije" insistiranje na poštovanju zakona i zagovaranje za slobodu medija i prava na informisanje. Jačanjem međusobnog poverenja i koordinacije, novinari i njihovi partneri mogu se efikasnije suprotstaviti pritiscima i stvoriti otporniji medij-

ski i javni prostor. Udruženi nastupi dovode do veće vidljivosti problema, a samim tim i do veće mobilizacije podrške u javnosti. Važno je da pojedinačni mediji ne ostaju sami i izolovani u svojim naporima za zaštitu prava.

Paralelno, od krucijalne važnosti je,

2. Sprovesti istrage u vezi sa digitalnim nadzorom nad novinarima i procenu zaštite novinarskih izvora

Sveobuhvatna zaštita izvora mora biti predmet razmatranja i multisektorske diskusije tek nakon sprovedene efikasne, adekvatne nezavisne istrage u cilju utvrđivanja postupanja institucija sistema u slučajevima digitalnog nadzora nad novinarima u prethodnom periodu. Ova nezavisna istraga ne isključuje, već treba da upotpuni istrage i sudske postupke koje treba da vode nadležni državni organi u skladu sa svojim zakonskim ovlašćenjima. Ove istrage moraju pokazati da li su organi postupali u skladu sa zakonom, sa posebnim osvrtom na opravdanost potencijalnih ograničenja slobode izražavanja novinara i zaštite izvora. Ukoliko nezavisna (pre svega u smislu oslobođena od političkog uticaja), efikasna istraga u razumnom roku ukaže da je došlo do ugrožavanja novinara i njihovih izvora na pravno nedozvoljeni način, odgovorna lica moraju biti adekvatno sankcionisana u sudskom postupku. Samo nakon dubinske istrage biće moguće utvrditi „slabe karike sistema" na koje treba posebno obratiti pažnju tokom potencijalnih izmena zakonskog okvira koji treba da osigura veći nivo zaštite izvora, a naročito od digitalnog nadzora.

Novinari koji su bili meta digitalnog nadzora moraju imati mogućnost pristupa pravdi, koja podrazumeva pružanje informacija o pravno-tehničkim detaljima svakog pojedinačnog slučaja. Novinari moraju razumeti doseg ograničenja svojih prava, a to znači da razumeju prirodu prikupljenih podataka, imaju uvid u to koje su im institucije pristupale i u kom periodu, kao i mogućnost da zahtevaju brisanja tih podataka. Na tako objavljenim podacima, potrebno je sprovesti ex-post analize, dok se ne utvrde

manjkavosti, slabosti i nejasnoće kako u radu institucija sistema, tako i u smislu zakonskih rešenja. Analize treba da otvore i bolna pitanja političkog uticaja na rad institucija i da dublje proniknu u razloge društvenog i institucionalnog pozicioniranja novinarstva kao profesije koja se, kao što je analiza pokazala, mora kontrolisati umesto osnaživati, a u cilju jačanja demokratskih kapaciteta.

Nakon sprovedene istrage, sledeći korak bi bio kreiranje fonda podrške novinarima, medijima urednicima, medijskim radnicima, organizacijama koje su pružale podršku ovim licima, kao i porodicama novinara i medijskih radnika.[164]

3. Zaštita novinarskih izvora iz Zakona o javnom informisanju i medijima ne treba da bude predmet izmena u datim političkim okolnostima

Trenutne političke, društvene i institucionalne tenzije nisu odgovarajući trenutak za promene medijskog zakonodavstva, a po najmanje senzitivne norme kao što je zaštita novinarskih izvora. Preduslov za bilo kakvu izmenu propisa iz ove oblasti je sprovođenje sveobuhvatne istrage, kao što je navedeno, u okolnostima društvene stabilnosti, poštovanja vladavine prava, podele vlasti i nezavisnosti medijskog sektora uz osiguran multisektorski i interdisciplinarni pristup koji posebnu pažnju posvećuje i daje glas medijskoj zajednici i ekspertizi.

164 Što je i u skladu sa članom 4, EMFA, vidi više: Jan Erik Kermer, Član 4. Evropskog akta o slobodi medija: propuštena prilika? Procena nedostataka u zaštiti novinarskih izvora, Centar za pluralizam i slobodu medija, Dostupno na: https://cmpf.eui.eu/article-4-of-the-european-media-freedom-act-a-missed-opportunity, str.198

4. Obezbediti zaštitu novinarskih izvora kroz druge zakonske propise

U pogledu drugih zakonskih propisa i praksi potrebno je da „povezani" zakonski propisi uvedu poseban režim u odnosu na zaštitu novinarskih izvora. Bez ulaženja u detalje, ZKP treba da oslobodi novinare dužnosti svedočenja ukoliko postoji mogućnost otkrivanja izvora. Pored toga, pretres redakcije i novinarskih domova potrebno je detaljnije definisati kako bi se ograničila ovlašćenja policije, a na način na koji se garantuje zaštita izvora. Još važnije je da se prakse oduzimanja uređaja, pristupa podacima, komunikaciji i drugi oblici nadzora nad novinarima u budućim zakonskim izmenama ZEK, Zakona o unutrašnjim poslovima, ZBIA, ZKP, ZVOA – regulišu tako da onemogućavaju zaobilaženje zaštite izvora, a kroz predviđanje uslova i standarda koji se odnose na zaštitu izvora generalno. Zakonsko rešenje Belgije može biti dobra baza za razmišljanje, dodatno pojačana navedenim standardima.

ZKP i ZBIA, kada se za to steknu uslovi, treba proširiti kroz uvođenje zabrane primene određenih radnji i mera, kao što je recimo korišćenje intruzivnog špijunskog softvera. Izuzeci od ostalih oblika digitalnog nadzora moraju biti usko tumačeni u skladu sa standardima Evropskog suda za ljudska prava; kroz uvođenje obaveze procene svrsishodnosti, neophodnosti i uticaja na ograničenje prava tokom i nakon trajanja mera nadzora, sa posebnim uputstvima za postupanje u cilju pristupa tačno onim podacima koji su potrebni za vođenje istrage kroz proces filtriranja, a uz asistenciju suda. Ukoliko ne dođe do pokretanja postupka, novinar o čijim podacima je reč *mora* (umesto sada predviđenog *može* u članu 163. ZKP-a) biti obavešten da su podaci uništeni uz podnošenje dokaza o uništenim podacima.

Zbog veoma kompleksnog konteksta digitalnog nadzora nad novinarima u Srbiji, neophodno je, kada se za to steknu uslovi, kreirati i nezavisno telo sastavljeno od eksperata iz različitih oblasti, koji će vršiti kontrolu i korekciju i ukazivati na propuste u radu institucija sistema koji sprovode digitalni nadzor. Novinarima, takođe, treba da bude omogućena i naknada

štete u slučajevima kršenja prava na zaštitu izvora, a podaci prikupljeni na ovaj način ne smeju se koristiti u sudskim postupcima kao dokaz.

5. Harmonizacija sa članom 4. Akta o medijskim slobodama (EMFA) mora biti odložena dok se ne ispune prethodno navedene preporuke

Imajući u vidu opisane problematične prakse nadzora i korišćenje špijunskog softvera, posebno je važno potpuno onemogućiti korišćenje špijunskog softvera. Slično je navedeno i u Rezoluciji Komiteta za zaštitu ljudskih prava (UN HRC), koji u svojim preporukama predlaže uvođenje moratorijuma na sisteme za presretanje i biometrijske sisteme, ukoliko ne postoje odgovarajući mehanizmi zaštite.[165] Zabrana će osigurati ne samo da se podrobno ispitaju svi prethodni slučajevi, nego će posebno informisati proces usaglašavanja sa EMFA. Član 4. predstavlja samo minimum pravne zaštite, a zemlje članice, a naročito zemlje kandidati treba da osiguraju onaj nivo zaštite koji štiti medijske slobode na demokratski način.

6. Ojačati ulogu suda u procesu odlučivanja o zahtevu za sprovođenje posebnih dokaznih radnji i mera digitalnog nadzora

Imajući u vidu važnost suda u procesu odlučivanja u sprovođenju posebnih dokaznih radnji i posebnih dokaznih mera za pristup podacima i presretanje komunikacije, u budućnosti treba razmotriti mogućnost da sudski organi imaju pojačanu kontrolnu funkciju u procesu. Potrebno je posebno odrediti sve ključne elemente koje sud posebno uzima u obzir u cilju zaštite izvora, kao što je precizno definisan obim pristupa, ispitivanje ispunjenosti uslova za sprovođenje mere, postupanje sa podacima koji mogu da otkriju izvore, a nisu nužni za konkretan slučaj, ispitivanje

165 UN HRC 68/1169, Zaštite privatnosti u digitalnoj eri, Izveštaj., 12. septembar - 7. oktobar 2022. para. 56 (g)

zakonitosti nadzora tokom trajanja mere. Sud ili drugi nezavisni organ treba da ima mogućnost da organu koji je podneo zahtev dozvoli (samo) pristup podacima koji su isključivo potrebni za otkrivanje počinioca i okolnosti krivičnog dela. Na ovaj način, ograničava se mogućnost masovnog pristupa podacima, a kroz proces minimizacije podataka štiti se sloboda izražavanja i pravo na privatnost novinara.

Pored toga, treba razmotriti dvostepeni sistem: prvi nivo bi mogao da predviđa da samo visoko pozicionirani službenici mogu zahtevati pretres redakcije i doma, kao i mere digitalnog nadzora nad novinarima. Sam zahtev mora sadržati detaljno objašnjenje ispunjenosti svih uslova za ograničenje prava, uključujući i navođenje dokaza. Zahtev na prvom nivou ispituje sudija, a nakon sprovedene radnje, sudija na drugom nivou ispituje zakonitost ove mere, uključujući i određivanje opsega podataka kojima se omogućuje pristup.

7. Transparentne javne nabavke i kontrolni mehanizmi

Javne nabavke, specifikacije opreme, ugovori kao i druga dokumenta u vezi sa opremom za nadzor moraju biti javno dostupni u registrima. Nabavka i korišćenje sistema nadzora mora biti predmet javne rasprave, stručnih analiza o uticaju na ljudska prava, efikasnosti i dostupnosti institucionalnih mehanizama za zaštitu od intruzivnog dejstva ovih sistema, sa posebnim akcentom na medijske i novinarske slobode. Korišćenje ovih mera mora biti praćeno, odobreno i kontrolisano od strane mehanizama nadzora (engl. overisight) koji imaju demokratsku i korektivnu kontrolu.

Država mora da osigura strožiju regulaciju korišćenja, razvoja, transfera i drugih radnji. S obzirom na trenutne okolnosti, a posebno imajući u vidu prethodne prakse digitalnog nadzora, uvođenje hitnog moratorijuma na uvoz, razvoj i korišćenje ovih tehnologija je prvi korak ka kreiranju okruženja za ponovnu izgradnju poverenja između novinara, izvora i institucija sistema. To je neophodno i za društveno konfigurisanje novinarstva kao

profesije rada u javnom interesu, baš kao što i institucije sistema moraju samo služiti istom. Takođe, potrebno je preispitati izmene i dopune zakonskih normi koje potencijalno mogu dodatno ugroziti zaštitu novinarskih izvora. Država mora posvetiti više pažnje ovom pitanju prilikom izrade i usvajanja propisa, kako se ne bi narušio standard zaštite izvora niti otvorio prostor za zloupotrebe. Obezbeđivanje čvrstih i jasnih zakonskih garancija zaštite novinarskih izvora predstavlja ključni element slobode medija i jedno od osnovnih merila vladavine prava.