UDK 343.14/.15 ; 342.738 ; 341.231.14(4)

*Nikola Paunović**

TAJNI NADZOR KOMUNIKACIJE KAO LEGITIMAN OSNOV ZA ODSTUPANJE OD PRAVA NA PRIVATNOST LIČNOSTI SA OSVRTOM NA PRAKSU EVROPSKOG SUDA ZA LJUDSKA PRAVA

Efikasna borba protiv teških oblika kriminala zahteva pod određenim uslovima primenu tajnog nadzora komunikacije kao posebne dokazne radnje čije sprovođenje dovodi u pitanje nepovredivost prava na privatnost ličnosti. Ipak, imajući u vidu da se nepovredivost ovog prava ne shvata u apsolutnom smislu, ni na nivou nacionalnog pravnog okvira, niti na evropskom planu oličenom u Evropskoj konvenciji o osnovnim pravima i slobodama, budući da je kao legitiman osnov za njegovo odstupanje normirana neophodnost vodjenja krivičnog postupka, u radu se polazi od osnovne prezumpcije da tajni nadzor komunikacije predstavlja legitiman osnov za odstupanje od prava na privatnost ličnosti. Stoga, autor u prvom delu rada posvećuje pažnju uslovima za sprovođenje tajnog nadzora komunikacije u nacionalnom krivičnoprocesnom okviru, sa osvrtom na sporna pitanja iz domaće sudske prakse, kojima je probuđena sumnja u njegovu validnost kao legitimnog osnova za odstupanje od prava na privatnost ličnosti. Štaviše, drugi deo rada bavi se razmatranjem sudske prakse Evropskog suda za ljudska prava u slučajevima koji se odnose na član 8 Evropske konvencije o osnovnim pravima i slobodama u kojima je dovedena u pitanje legitimnost odstupanja od prava na poštovanje privatnog i porodičnog života usled primene tajnog nadzora komunikacije pred nacionalnim organima vlasti. U zaključnim razmatranjima se ističe da primena tajnog nadzora komunikacije za potrebe vođenja krivičnog postupka, isključivo uz poštovanje principa nužnosti, proporcionalnosti i restriktivnosti, te zakonskih uslova za njegovo sprovođenje, ne dovodi do neosnovanog odstupanja od prava na privatnost.

Ključne reči: *Tajni nadzor komunikacije. – Posebna dokazna radnja. – Pravo na privatnost. – Evropski sud za ljudska prava.*

* Autor je pripravnik u Ministarstvu spoljnih poslova i doktorand Pravnog fakulteta Univerziteta u Beogradu, *dzoni925@gmail.com* (Republika Srbija)

1. UVODNA RAZMATRANJA

Pravo na poštovanje privatnosti prepoznato je u međunarodnom pravu ljudskih prava u Univerzalnoj deklaraciji o ljudskim pravima (u daljem tekstu: Deklaracija) usvojenoj 1948. godine kao jedno od osnovnih ljudskih prava. Naime, Deklaracija u članu 12 jemči da se niko ne sme izložiti proizvoljnom mešanju u privatni život, porodicu, stan ili prepisku, niti napadima na čast i ugled, te da svako ima pravo na zaštitu zakona protiv ovakvog mešanja ili napada.[1] Ubrzo nakon usvajanja Deklaracije na međunarodnom nivou, u Evropi je takođe potvrđeno postojanje ovog prava u Evropskoj konvenciji o zaštiti ljudskih prava i osnovnih sloboda (u daljem tekstu: EKLJP) usvojenoj 1950. godine.[2] EKLJP, u članu 8, normira pravo na poštovanje privatnog i porodičnog života zbog čega Evropski sud za ljudska prava postupajući po predstavkama podnosilaca odlučuje i o pitanju eventualnog zadiranja u to pravo. U tom smislu, pravo na poštovanje privatnosti se sastoji od opšte zabrane neovlašćenog mešanja u privatni ili porodični život pojedinca.[3] S druge strane, iako Ustav Republike Srbije ne jemči pravo na poštovanje privatnog i porodičnog života kao takvo, on ipak štiti u članu 41 tajnost pisama i drugih oblika komunikacije kao oblika prava na privatnost predviđajući takođe odstupanja od ovog prava ukoliko je to neophodno zbog vođenja krivičnog postupka odnosno zaštite bezbednosti, na način predviđen zakonom.[4] Iz navedenog proizilazi da je, u određenim slučajevima, kao što je potreba prikupljanja činjenica od značaja za vođenje krivičnog postupka, dozvoljeno odstupanje od prava na poštovanje porodičnog i privatnog života. U tom smislu, jedna od krivičnoprocesnih mera kojima se, za potrebe vođenja krivičnog postupka, odstupa od zajemčenog prava na privatnost jeste primena tajnog nadzora komunikacije kao posebne dokazne radnje. Stoga, treba

1 The Universal Declaration of Human Rights, *http://www.un.org/en/universal-declaration-human-rights/,* 11. avgust 2019.

2 European Convention on Human Rights, *https://www.echr.coe.int/Documents/Convention_ENG.pdf,* 12. avgust 2019. Republika Srbija je ratifikovala ovaj međunarodni ugovor. Zakon o potvrđivanju Evropske konvencija o zaštiti ljudskih prava i osnovnih sloboda, *Službeni glasniku RS – Međunarodni ugovori*, br. 12/2010.

3 Els De Busser, „Open Source Data and Criminal Investigations: Anything You Publish Can and Will Be Used Against You", *Groningen Journal of International Law*, 2/2014, 93.

4 Ustav Republike Srbije, *Službeni glasnik RS*, br. 98/2006.

istaći da odstupanje od prava na privatnost primenom tajnog nadzora komunikacije predstavlja legitimnu meru u procesu otkrivanja najtežih krivičnih dela, posebno onih koja je uobičajenim procesnim sredstvima nemoguće dokazati zbog složenosti izvršenih krivičnih dela, visokog nivoa konspirativnosti izvršilaca i kasnijeg mogućeg uticaja na redovan tok krivičnog postupka.[5]

S tim u vezi, dovedeći u vezi pravo na privatnost ličnosti u kontekst primene posebne dokazne radnje – tajni nadzor komunikacije, pojavljuje se dilema oko toga da li dati prednost javnom interesu oličenom u potrebi vođenja krivičnog postupka ili privatnom interesu pojedinaca oličenom u neophodnosti zaštite privatnosti. Ovo stoga što je postizanje ravnoteže između privatnosti i slobode, sa jedne strane, i bezbednosti, sa druge, jedan od ciljeva demokratskih društava.[6] To, međutim, nije nimalo lak zadatak jer se ta ravnoteža narušava stalnim redefinisanjem, usložnjavanjem i umnožavanjem bezbednosnih izazova, rizika i pretnji, uzrokovanim naglim i brzim razvojem tehnike i tehnologije. Otud službe bezbednosti i policije nastoje da preduprede ove pretnje proširivanjem svojih nadležnosti i ovlašćenja, čime neminovno sve više zadiru u privatnost ličnosti. To dovodi do zahteva da se uspostavi što šira zaštita prava na privatnosti. U ovom stalnom redefinisanju ravnoteže između zaštite privatnosti ličnosti i opšte bezbednosti veliku ulogu ima praksa Evropskog suda za ljudska prava kao i domaćih sudova koji su nadležni za odobravanje i kontrolu primenu tajnog nadzora komunikacije.[7] U tom pogledu treba ukazati da primena tajnog nadzora komunikacije kao posebne dokazne radnje ne sme biti previše široka, jer tada dolazi do izvesnog zadiranja u zagarantovano pravo na privatnost, ali ni previše uska, jer se tada gubi njegov efekat. Dakle, reč je o večitom vaganju između jačanja sloboda i prava pojedinaca, kojima se postavljaju granice represiji koju krivično pravo

5 Goran Matić, „Pitanje primene specijalnih istražnih tehnika od strane policije i službi bezbednosti", *Suprotstavljanje organizovanom kriminalu pravni okvir, međunarodni standardi i procedure*, (ur. D. Kolarić), Kriminalističko-policijska akademija, Beograd 2013, 189–190.

6 Vladan Mirković, „Sudska kontrola specijalnih istražnih mera službi bezbednosti u Republici Srbiji", *Žurnal za kriminalistiku i pravo*, 3/2017, 90.

7 Dušan Ignjatović, *Mere presretanja komunikacije i zadržavanja podataka iz perspektive Strazbura i propisa i prakse u Republici Srbiji*, Beogradski centar za bezbednosnu politiku, Beograd 2015, 5.

nužno sa sobom nosi i jačanja ovlašćenja države zarad efikasnije borbe protiv teških oblika kriminala, a na uštrb sloboda i prava pojedinaca.[8]

Stoga, polazeći od potrebe za uspostavljanjem ravnoteže između neophodnosti primene tajnog nadzora komunikacije, s jedne strane i zaštite privatnosti pojedinca, s druge strane u radu se nastoje preispitati uslovi za određivanje ove posebne dokazne radnje u nacionalnom pravnom okviru, sa ciljem analize slučajeva iz domaće sudske prakse u kojima je osporena njegova validnost kao legitimnog osnova za odstupanje od prava na privatnost ličnosti. Dodatno, razmatranjem relevatne sudske prakse Evropskog suda za ljudska prava u slučajevima koji se tiču primene člana 8 – zaštita prava na privatni i porodični život ELJKP, cilj rada jeste prepoznavanje situacija u kojima postoji legitimnost odstupanja od prava na poštovanje privatnog i porodičnog života usled primene tajnog nadzora komunikacije pred nacionalnim organima vlasti od onih u kojima to nije slučaj, budući da je došlo do povrede ovog prava.

2. *RATIO LEGIS* ODSTUPANJA OD PRAVA NA PRIVATNOST LIČNOSTI KAO POSLEDICA PRIMENE POSEBNE DOKAZNE RADNJE TAJNOG NADZORA KOMUNIKACIJE

Uopšteno govoreći, posebne dokazne radnje, u koje potpada i tajni nadzor komunikacije, se označavaju kao specijalne dokazne tehnike, odnosno specijalne istražne tehnike i predstavljaju načine prikupljanja dokaza koji su po svom karakteru atipični, te se primenjuju samo u odnosu na neka krivična dela, koja su s jedne strane, veoma teška, odnosno ozbiljna, kako u faktičkom pogledu s obzirom na posledice koje prouzrokuju u jednom opštem životnom smislu, tako i u krivičnopravnom pogledu, imajući u vidu zaprećenu kaznu, dok se s druge strane, takva dela zahvaljujući nekim njihovim fenomenološkim karakteristikama, te psihološkim i drugim osobinama učinilaca, veoma teško otkrivaju, razjašnjavaju i dokazuju korišćenjem uobičajenih,

8 Žarko Sinđelić, „Primena savremenih tehnologija prilikom realizacije posebnih i drugih dokaznih radnji u cilju sprečavanja i suzbijanja organizovanog kriminala", *Suprotstavljanje organizovanom kriminalu pravni okvir, međunarodni standardi i procedure* (ur. D. Kolarić), Kriminalističko-policijska akademija, Beograd 2013, 363.

odnosno redovnih dokaznih metoda.[9] To je i dovelo do potrebe da se u savremena krivičnoprocesna zakonodavstva uvedu tzv. specijalne istražne tehnike, a time i legitimni osnov za odstupanja od prava na privatnost ličnosti.[10] U svakom slučaju, ovakvo stanje stvari je s jedne strane razumljivo, s obzirom na to da efikasno i ekspeditivno vođenje krivičnog postupka ponekad iziskuje određeno ograničavanje prava osumnjičenih lica. No, s druge strane, ne treba gubiti iz vida osnovnu pretpostavku na kojoj celokupni krivični postupak počiva– pretpostavku nevinosti, koja nalaže da se licu čija krivica još nije dokazana prava i slobode ograničavaju samo ukoliko je to apsolutno neizbežno, pa i tada samo u najmanjoj mogućoj meri.[11]

Posebna dokazna radnja u vidu tajnog nadzora komunikacije predstavlja tradicionalno sredstvo rada službi bezbednosti ne samo u kontekstu preventivne, obaveštajne svrhe, već i radi vođenja krivičnog postupka. Osnovne karakteristike tajnog nadzora komunikacije kao posebne dokazne radnje jesu: tajnost, ograničeno (neophodno) odstupanje od zajemčenih prava i slobode čoveka i građanina, i dokazna neupotrebljivost rezultata tih radnji ako je u njegovoj primeni povređen zakon. Prema tome, u osnovnim karakteristikama tajnog nadzora komunikacije sadržana su ograničenja za njegovu primenu.[12] S tim u vezi, primena tajnog nadzora komunikacije je po pravilu nužno skopčana sa bitnim odstupanjima od Ustavom i međunarodnopravnim aktima garantovanih prava i ljudskih sloboda, a pre svega prava na privatnost, što i predstavlja razlog da samo sud u određenom funkcionalnom obliku može da odobri i nadzire njegovu primenu. Prema tome, posebna dokazna radnja tajnog nadzora komunikacije je nužno ekskluzivnog karaktera zbog čega ne dolazi u obzir njegova široka primena, jer bi to

9 Council of Europe, *The deployment of special investigative means*, Council of Europe, Office in Belgrade, Belgrade 2013, 12.

10 Milan Škulić, „Tajni audio i video nadzor kao posebna dokazna radnja u Zakoniku o krivičnom postupku", *Tužilačka reč*, 28/2015, 24. Vid. više o tome John Vervaele, „Special procedural measures and respect of human rights", *International Review of Penal Law,* 1/2009, 88.

11 Milica Kovačević, „Tajni nadzor komunikacije – usklađenost sa praksom Evropskog suda za ljudska prava", *Anali Pravnog fakulteta u Beogradu*, 2/2014, 165.

12 Goran Ilić, Marina Matić Bošković, *Posebne mere tajnog prikupljanja podataka u krivičnom postupku: pogled iz pravosuđa*, Beogradski centar za bezbednosnu politiku, Beograd 2015, 6.

s jedne strane, ne samo dovelo u pitanje njegov izuzetan karakter i učinilo ga manje efikasnom, već bi se tada, s druge strane, to svelo na neopravdano odstupanje od prava na privatnost ličnosti. Stoga je princip racionalne i celishodne primene ove posebne dokazne radnje od najvećeg značaja, jer tajni nadzor komunikacije, iako predstavlja moćno „oružje" u suzbijanju nekih uobičajenim dokaznim metodama teško dokazivih krivičnih dela (pre svega organizovanog kriminala), ako se preterano koristi, može da bude izrazito štetna po stabilnost pravnog sistema.[13] Iz tog razloga, primena ove posebne dokazne radnje treba da bude krajnje selektivna iz dva osnovna razloga. Prvo, treba uvek načelno biti oprezan kada su u pitanju radnje kojima se u bitnoj meri na Zakonikom o krivičnom postupku[14] (u daljem tekstu: ZKP) regulisan način odstupa od Ustavom garantovanih ljudskih prava, a pre svega prava na privatnost, dok s druge strane, da bi radnje tajnog nadzora komunikacije uopšte mogle da budu uspešne one nužno ne smeju biti masovne, jer bi tada njihova neekskluzivna i preterano široka primena, po logici stvari, dovela do toga da one budu neefikasne.[15]

3. USLOVI ZA PRIMENU TAJNOG NADZORA KOMUNIKACIJE U KRIVIČNOPROCESNOM ZAKONODAVSTVU REPUBLIKE SRBIJE

Imajući u vidu razmotrene osnovne karakteristike za određivanje tajnog nadzora komunikacije, opšti uslovi za određivanje ove posebne dokazne radnje definisani su ZKP-om (članovi 161–165) na krajnje *ultima ratio* način, koji ograničava njegovu primenu samo ako se na drugi način ne mogu prikupiti dokazi za krivično gonjenje ili bi njihovo prikupljanje bilo znatno otežano odnosno ako 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. Dodatno, prilikom odlučivanja o određivanju i trajanju tajnog nadzora

13 M. Škulić, „Specijalne istražne tehnike u funkciji suzbijanja organizovanog kriminaliteta", *Društveni aspekti organizovanog kriminala* (ur. A. Fatić, B. Banović), Institut za međunarodnu politiku i privredu, Beograd 2011, 224.

14 Zakonik o krivičnom postupku, *Službeni glasnik RS*, br. 72/2011, 101/2011, 121/2012, 32/2013, 45/2013 i 55/2014.

15 M. Škulić, „Posebne dokazne radnje u novom Zakoniku o krivičnom postupku", *Revija za bezbednost*, 7/2008, 23–24.

komunikacije organ postupka će posebno ceniti da li bi se isti rezultat mogao postići na način kojim se manje ograničavaju prava građana. Stoga, prilikom postavljanja opštih uslova za primenu posebnih dokaznih radnji, a time i tajnog nadzora komunikacije, zakonodavac je nastojao da zadovolji kriterijume supsidijarnosti i srazmernosti.[16] Dok supsidijarnost podrazumeva da primena posebnih dokaznih radnji dolazi u obzir samo ako se isti rezultat ne bi mogao postići na način kojim se manje ograničavaju prava građana, dotle se srazmernost odnosi na ocenu opravdanosti preduzimanja tajnog nadzora komunikacije s obzirom na stepen odstupanja od prava na privatnost i težinu krivičnog dela.[17] Ipak, treba istaći da je korišćenje posebne dokazne radnje tajni nadzor komunikacije radi vođenja krivičnog postupka u današnje vreme postalo nužno u borbi protiv savremenog kriminala. Naime, savremeni oblici kriminala postavljaju pred organe krivičnog gonjenja složene zadatke koji ne mogu biti uspešno izvršeni bez korišćenja savremenih tehničkih sredstava. S druge strane, korišćeni pod zakonom strogo utvrđenim uslovima, po odluci suda, ovi metodi prikupljanja dokaza za krivični postupak sami po sebi ne dovode u pitanje prava građana na poštovanje privatnosti.[18]

U tom smislu, ako su ispunjeni napred navedeni opšti uslovi za primenu posebnih dokaznih radnji, u skladu sa posebno normiranim uslovima (članovi 166–170 ZKP), na obrazloženi predlog javnog tužioca, sud može odrediti nadzor i snimanje komunikacije koja se obavlja putem telefona ili drugih tehničkih sredstava ili nadzor elektronske ili druge adrese osumnjičenog i zaplenu pisama i drugih pošiljki. Naredba o tajnom nadzoru komunikacije koju određuje sudija za prethodni postupak treba da sadrži raspoložive podatke o licu prema kojem se ova posebna dokazna radnja primenjuje, 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.[19] Kada je reč o trajanju

16 Goran P. Ilić, „Značaj posebnih dokaznih radnji u otkrivanju i dokazivanju koruptivnih krivičnih dela", *Hereticus*, 3–4/2013, 59–60.

17 Darko Marinković, *Suzbijanje organizovanog kriminala: specijalne istražne metode*, Prometej, Novi Sad 2010, 267.

18 Tihomir Vasiljević, Momčilo Grubač, *Komentar zakonika o krivičnom postupku*, Službeni glasnik, Beograd 2011, 1001.

19 Ž. Sinđelić, „Nedostaci posebnih dokaznih radnji tajnog nadzora komunikacije i tajno praćenje i snimanje u novom ZKP", *Tužilačka reč*, 28/2015, 86.

treba istaći da se sprovođenje nadzora prekida čim prestanu razlozi za njegovu primenu. Ipak, maksimalni rok za primenu ove posebne dokazne radnje određen je u dvostrukom smislu. Tako, za sva krivična dela u odnosu na koja se može odrediti tajni nadzor komunikacije, osim krivičnih dela za koja je posebnim zakonom određeno da postupa javno tužilaštvo posebne nadležnosti, ova posebna dokazna radnja može trajati tri meseca, s tim što se zbog neophodnosti daljeg prikupljanja dokaza može produžiti najviše za tri meseca.[20] U suprotnom, ako je reč o krivičnim delima za koja je posebnim zakonom određeno da postupa javno tužilaštvo posebne nadležnosti, tajni nadzor može se izuzetno produžiti još najviše dva puta u trajanju od po tri meseca.[21]

S druge strane, što se tiče načina sprovođenja tajnog nadzora komunikacije propisano je da ovu posebnu dokaznu radnju izvršava policija, Bezbednosno-informativna agencija ili Vojnobezbednosna agencija, tako što se sačinjavaju dnevni izveštaji koji se zajedno sa prikupljenim snimcima komunikacije, pismima i drugim pošiljkama koje su upućene osumnjičenom ili koje on šalje dostavljaju sudiji za prethodni postupak i javnom tužiocu na njihov zahtev.[22] Dodatno, u postupku sprovođenja tajnog nadzora komunikacije definisana je obaveza poštanskih, telegrafskih i drugih preduzeća, društva i lica registrovanih za prenošenje informacija da državnom organu koji izvršava ovu posebnu dokaznu radnju, omoguće sprovođenje nadzora i snimanja komunikacije i da, uz potvrdu prijema, predaju pisma i druge pošiljke.[23] Ipak, imajući u vidu da postoje realni izgledi da lice prema kojem se sprovodi tajni nadzor komunikacije promeni broj telefona ili adresu zakonom je regulisana i situacija proširenja primene tajnog nadzora komunikacije i na taj telefonski broj ili adresu, pod uslovom da se u toku sprovođenja ove posebne dokazne radnje dođe do saznanja da

20 Jelena Pejić, *Kako funkcioniše presretanje elektronskih komunikacija i pristup zadržanim elektronskim podacima u Srbiji?*, Beogradski centar za bezbednosnu politiku, Beograd 2014, 11.

21 M. Škulić, *Osnovne novine u krivičnom procesnom pravu Srbije: novi Zakonik o krivičnom postupku iz 2011. godine*, Beograd 2013, 54.

22 Gordana Nikolić, Miraš Tomović, „Tajni nadzor komunikacije – zakonska regulativa i neka sporna pitanja", *Evropske integracije: pravda, sloboda i bezbednost* (ur. Đ. Đorđević), Kriminalističko-policijska akademija fondacija „Hans Zajdel", Beograd 2016, 135.

23 M. Škulić, „Tajni audio i video nadzor – pravila novog Zakonika o krivičnom postupku Srbije iz 2011. godine i uporednopravna analiza", *Kaznena reakcija u Srbiji II deo*, (ur. Đ. Ignjatović), Pravni fakultet Univerziteta u Beogradu, 2012, 58.

osumnjičeni koristi drugi telefonski broj ili adresu. O ovome je državni organ koji sprovodi tajni nadzor komunikacije dužan da odmah obavestiti javnog tužioca koji će potom podneti predlog da se naknadno odobri proširenje tajnog nadzora komunikacije. O predlogu odlučuje sudija za prethodni postupak u roku od 48 časova od prijema predloga. Ako usvoji predlog, sudija za prethodni postupak će naknadno odobriti proširenje tajnog nadzora komunikacije, a ako odbije predlog, materijal koji je prikupljen se uništava.[24]

Nasuprot zakonskoj mogućnosti za proširenje primene tajnog nadzora komunikacije ako dođe do saznanja da osumnjičeni koristi drugi telefonski broj ili adresu, predviđena je i situacija kada se tokom preduzimanja ove posebne dokazne radnje prikupi materijal o krivičnom delu ili učiniocu koji nije bio obuhvaćen odlukom o određivanju tajnog nadzora komunikacije. Takav materijal se može koristiti u postupku samo ako se odnosi na krivična dela u odnosu na koja se primenjuju tajni nadzor komunikacije kao posebna dokazna radnja. U svakom slučaju, po završetku tajnog nadzora komunikacije organ koji izvršava ovu posebnu dokaznu radnju dostavlja sudiji za prethodni postupak snimke komunikacije, pisma i druge pošiljke i poseban izveštaj koji sadrži: vreme početka i završetka nadzora, podatke o službenom licu koje je nadzor sprovelo, opis tehničkih sredstava koja su primenjena, broj i raspoložive podatke o licima obuhvaćenim nadzorom i ocenu o svrsishodnosti i rezultatima primene nadzora.[25]

4. SPORNA PITANJA U VEZI SA PRIMENOM TAJNOG NADZORA KOMUNIKACIJE KAO LEGITIMNOG OSNOVA ZA ODSTUPANJE OD PRAVA NA PRIVATNOST U DOMAĆOJ SUDSKOJ PRAKSI

U cilju izbegavanja situacija u kojima dolazi do neosnovanog odstupanja od prava na privatnost ličnosti zarad primene tajnog nadzora komunikacije, svi organi koji učestvuju u predlaganju, odobravanju i nadziranju sprovođenja ove posebne dokazne radnje treba što detalj-

24 M. Škulić, *Krivično procesno pravo*, Pravni fakultet Univerziteta u Beogradu, Beograd 2014, 249.

25 M. Škulić, *Organizovani kriminalitet: pojam, pojavni oblici, krivična dela i krivični postupak*, Beograd 2015, 489.

nije da provere da li su ispunjeni svi prethodno analizirani uslovi za njegovo određivanje.[26] Ovo stoga što je posledica nezakonitog prikupljanja materijala nastalog primenom tajnog nadzora komunikacije neopravdano odstupanje od prava na privatnost ličnosti, a koje su stoga bez valjanog osnova stavljene pod ovu posebnu dokaznu radnju. Dodatno, nepoštovanje uslova za odobravanja tajnog nadzora komunikacije može dovesti i do toga da se prikupljeni rezultati ne mogu upotrebljati u krivičnom postupku, a što može ugroziti ishod celog slučaja pred sudom.[27] U vezi sa primenom tajnog nadzora komunikacije pojavljaju se različiti slučajevi u kojima se dovodi u pitanje validnost njihovog korišćenja kao legitimnog osnova za odstupanje od prava na privatnost. Upravo iz tog razloga u ovom radu ne mogu se obuhvatiti svi takvi slučajevi, ali ono što može, to je da se razmotre najčešća sporna pitanja u primeni tajnog nadzora komunikacije nastala u domaćoj sudskoj praksi u kontekstu upotrebe ove posebne dokazne radnje.

U tom smislu, u daljim redovima, nastojaće se da se odgovori na sledeća sporna pitanja: 1) da li postoji legitimno odstupanje od prava na privatnost, a time i zakonitost u pribavljanju dokaza prikupljenih putem tajnog nadzora komunikacije ukoliko javni tužilac izmeni pravnu kvalifikaciju krivičnog dela nakon sprovođenja ove posebne dokazne radnje u delo za koje nije dozvoljena primena tajnog nadzora komunikacije; 2) da li se u vezi sa legitimnim odstupanjem od prava na privatnost, može u krivičnom postupku koristiti dokazni materijal koji je prikupljen tajnim nadzorom komunikacije u slučaju koji se ticao krivičnog dela u odnosu na koje je dozvoljena primena ove posebne dokazne radnje, ukoliko je po njegovom okončanju izvršena pravna kvalifikacija u drugo krivično delo za koje je takođe moguća primena ove posebne dokazne radnje; 3) da li se u kontekstu legitimnog odstupanja od prava na privatnost, presuda može zasnovati na dokaznom materijalu koji je prikupljen pre datuma donošenja naredbe sudije za prethodni postupak o tajnom nadzoru komunikacije; 4) da li je za legitimno odstupanje od prava na privatnost, neophodno opredeliti precizan vremenski momenat do kada tačno traje posebna dokazna radnja tajni nadzor komunikacije, ili je dovoljno opredeliti početak njenog sprovođenja i dužinu trajanja; 5) da li postoji legitimno odstupanje od

26 D. Ignjatović, *op. cit.*, 16.

27 Petar Petrović et al., *Posebne mere tajnog prikupljanja podataka: vodič za nadzor*, Beogradski centar za bezbednosnu politiku, Beograd 2015, 17.

prava na privatnost, ukoliko je u naredbi o određivanju tajnog nadzora komunikacije označen samo IMEI broj mobilnog telefona osumnjičenog, bez označavanja telefonskog broja.

U kontekstu prvog spornog pitanja, da li postoji legitimno odstupanje od prava na privatnost, a time i zakonitost u pribavljanju dokaza putem tajnog nadzora komunikacije ukoliko javni tužilac izmeni pravnu kvalifikaciju krivičnog dela nakon sprovođenja ove posebne dokazne radnje u delo za koje nije dozvoljena primena tajnog nadzora komunikacije, bilo je reči u predmetu Kzz 1306/2017 u kome je branilac okrivljenog podneo zahtev za zaštitu zakonitosti zbog toga što u odnosu na okrivljenog ne samo da nije postojala naredba sudije za preduzimanje posebne dokazne radnje tajni nadzor komunikacije, već je njemu stavljeno na teret krivično delo u odnosu na koje se ne primenjuje ova posebna dokazna radnja. Vrhovni kasacioni sud je pošao od toga da iako u konkretnom slučaju okrivljeni nije bio obuhvaćen odlukom o određivanju tajnog nadzora komunikacije, u vreme donošenja naredbe o preduzimanju ove posebne dokazne radnje i za sve vreme trajanja iste njemu je bilo stavljeno na teret izvršenje krivičnog dela u odnosu na koje se primenjuje ova posebna dokazna radnja. Stoga je zauzeo mišljenje da se materijal koji je prikupljen u postupku primene mere tajnog nadzora komunikacije, u konkretnom slučaju, mogao koristiti kao dokaz u postupku, kao tzv. slučajni nalaz, zbog čega činjenica da je javni tužilac izmenio pravnu kvalifikaciju krivičnog dela tek nakon prestanka primene ove posebne dokazne radnje, tako što je umesto krivičnog dela iz člana 114 KZ za koje se primenjuje tajni nadzor komunikacije, stavio na teret izvršenje krivičnog dela iz člana 113 KZ u odnosu na koje se ne primenjuje ova posebna dokazna radnja, ostaje bez uticaja na zakonitost pribavljanja dokaza u odnosu na okrivljenog.[28]

S druge strane, u sudskoj praksi se postavilo pitanje da li se u vezi sa legitimnim odstupanjem od prava na privatnost, može u krivičnom postupku koristiti dokazni materijal koji je prikupljen tajnim nadzorom komunikacije u slučaju koji se ticao krivičnog dela u odnosu na koje je dozvoljena primena ove posebne dokazne radnje, ukoliko je po njegovom okončanju izvršena pravna kvalifikacija u drugo krivično delo za koje je takođe moguća primena ove posebne dokazne radnje. Upravo o ovom pitanju se odlučivalo po zahtevu za zaštitu

28 Presuda Vrhovnog kasacionog suda Kzz 1306/2017 od 19.12.2017. godine.

zakonitosti u predmeta Kzz 378/2014 u kome je branilac okrivljenog isticao da se prikupljeni dokazni materijal tajnim nadzorom komunikacije zbog postojanja osnova sumnje da je okrivljeni izvršio krivično delo primanje mita iz člana 367 KZ, nije mogao koristiti u predmetnom krivičnom postupku protiv okrivljenog koji je naknadno vođen zbog krivičnog dela trgovina uticajem iz člana 366 KZ. Vrhovni kasacioni sud je naveden zahtev branioca ocenio neosnovanim prihvatajući dokazni materijal pribavljen merom tajnog nadzora komunikacije okrivljenog, zbog postojanja osnova sumnje da je okrivljeni izvršio krivično delo primanje mita, a zbog kojeg dela je predmetni krivični postupak protiv okrivljenog i pokrenut i vođen, kao validan dokaz. Usled toga, okolnost da je tek pred završetak glavnog pretresa izmenjena optužnica okrivljenom, bez izmene činjeničnog opisa u pogledu preduzetih radnji izvršenja dela, kada mu je stavljeno na teret izvršenje krivičnog dela trgovina uticajem u odnosu na koje je takođe dozvoljena primena tajnog nadzora komunikacije, ostaje bez uticaja na zakonitost njegovog korišćenja u krivičnom postupku.[29]

Preostala tri pitanja se odnose na sporne elemente u vezi sa naredbom o sprovođenju tajnog nadzora komunikacije. Tako, jedno od spornih pitanja se odnosi na dilemu da li se u kontekstu legitimnog odstupanja od prava na privatnost, presuda može zasnovati na dokaznom materijalu koji je prikupljen pre datuma donošenja naredbe sudije za prethodni postupak o tajnom nadzoru komunikacije. Postavljeno pitanje bilo je predmet zahteva za zaštitu zakonitosti u predmetu Kzz 315/2019 u kome je branilac okrivljene isticao da se pobijana pravnosnažna presuda zasniva na transkriptima razgovora okrivljene sa drugim licima, a koji dokaz nije pribavljen u skladu sa zakonom, jer su neki od razgovora okrivljene sa drugim licima vođeni pre datuma donošenja naredbe sudije za prethodni postupak o tajnom nadzoru komunikacije okrivljene. Iznete navode iz zahteva za zaštitu zakonitosti branioca okrivljene Vrhovni kasacioni sud nije prihvatio kao osnovane, budući da je na osnovu raspoloživih spisa utvrdio da nižestepeni sud nije zasnovao pravnosnažnu presudu na transkriptima razgovora vođenim pre donošenja naredbe, već je sud u konkretnom slučaju u toku dokaznog postupka izvršio samo uvid u te transkripte i pobijanu pravnosnažnu presudu zasnovao samo na transkriptima snimljenih telefonskih razgovora i „sms“ porukama okrivljene ostvarenim nakon

29 Presuda Vrhovnog kasacionog suda Kzz 378/2014 od 20.5.2014 godine.

donošenja naredbe.[30] Stoga iz navedenog jasno proizilazi da transkripti i po načinu pribavljanja i po svojoj sadržini predstavljaju zakonit dokaz na kojem se presuda može zasnivati budući da su nastali kao rezultat zakonito sprovedene posebne dokazne radnje tajni nadzor komunikacije okrivljene sa drugim licima, a koja je izvršena na osnovu obrazložene naredbe sudije za prethodni postupak.[31]

Takođe, kao sporno u sudskoj praksi postavilo se pitanje da li je za legitimno odstupanje od prava na privatnost, neophodno opredeliti precizan vremenski momenat do kada tačno traje posebna dokazna radnja tajni nadzor komunikacije, ili je dovoljno opredeliti početak njenog sprovođenja i dužinu trajanja. O ovom pitanju bilo je reči u predmetu Kzz 431/18 pred Vrhovnim kasacionim sudom u kome je branilac okrivljenog isticao da je pobijanim pravosnažnim presudama učinjena bitna povreda odredaba krivičnog postupka, na taj način što su odluke suda zasnovane na dokazima na kojima se po odredbama ZKP ne mogu zasnivati, imajući u vidu da u naredbi nije na nesumnjiv način određeno njeno trajanje. Vrhovni kasacioni sud našao je neosnovanim zahtev za zaštitu zakonitosti uzimajući u obzir da u naredbama kojima se određuje tajni nadzor komunikacije, shodno odredbama člana 166 i 167 ZKP, nije neophodno opredeliti i do kada tačno traje ova mera, već je dovoljno opredeliti početak sprovođenja mere i dužinu trajanja, što je i bilo učinjeno u konkretnom slučaju. U tom smislu, u konkretnom slučaju sud je u naredbi naveo da ova mera počinje da teče od 25.12.2013. godine i da će trajati tri meseca, te da je ova naredba produžena naredbom od 19.3.2014. godine za još tri meseca, pri čemu je u ovoj naredbi navedeno i da mera ne može više biti produžena, te da počinje da teče od 25.3.2014. godine i da može najduže trajati do 25.6.2014. godine, zbog čega je zahtev za zaštitu zakonitosti branioca okrivljenog, u delu u kojem ističe da navedena naredba ne sadrži vreme trajanja i da je stoga nezakonita, ocenjen neosnovanim.[32]

Konačno, u pogledu spornih pitanja u vezi sa podacima koje naredba o sprovođenju tajnog nadzora komunikacije može da sadrži kao sporno u sudskoj praksi se pojavilo pitanje da li postoji legitimno odstupanje od prava na privatnost, ukoliko je u naredbi o određivanju

30 Željko Ninčić, „Nadzor komunikacija kao mera procesne prinude", *Bezbjednost – Policija – Građani*, 1–2/14, 94.

31 Presuda Vrhovnog kasacionog suda Kzz 315/2019 od 3.4.2019. godine.

32 Presuda Vrhovnog kasacionog suda Kzz 431/2018 od 18.4.2018. godine.

tajnog nadzora komunikacije označen samo IMEI broj mobilnog telefona osumnjičenog, bez označavanja telefonskog broja. [33] Ovim pitanjem se bavio Vrhovni kasacioni sud u predmetu Kzz 1306/2017 u kome je odbio kao neosnovan zahtev za zaštitu zakonitosti branioca okrivljenog podnet zbog bitne povrede odredaba krivičnog postupka iz člana 438, stav 2, tačka 1 ZKP u kome se isticalo da je pravnosnažna presuda zasnovana na dokazu na kome se, po odredbama ZKP ne može zasnivati, a kao nezakonit dokaz označen je dokaz proizašao iz tajnog nadzora komunikacije, zbog toga što je ova posebna dokazna radnja određena prema broju telefonskog aparata – IMEI broj, a ne prema telefonskom broju kako ZKP to nalaže. Ovo stoga što, po oceni Vrhovnog kasacionog suda, IMEI broj predstavlja jedinstveni broj dodeljen svakom mobilnom telefonu ponaosob i uvek je vidljiv prilikom praćenja telefonske komunikacije, te je, u smislu odredaba ZKP, podoban za identifikaciju telefonskog aparata.[34]

5. TAJNI NADZOR KOMUNIKACIJE I USLOVI ZA ODSTUPANJE OD PRAVA NA POŠTOVANJE PRIVATNOG I PORODIČNOG ŽIVOTA U PRAKSI EVROPSKOG SUDA ZA LJUDSKA PRAVA

Prema EKLJP, član 8, predviđeno je da svako ima pravo na poštovanje svog privatnog i porodičnog života, doma i prepiske, te da javna vlast ne sme da se meša u vršenje ovog prava, osim ako je takvo mešanje predviđeno zakonom i ako je to neophodna mera u demokratskom društvu u interesu nacionalne sigurnosti, javne sigurnosti, ekonomske dobrobiti zemlje, sprečavanja nereda ili sprečavanja zločina, zaštite zdravlja i morala ili zaštite prava i sloboda drugih.[35] U tom smislu, da bi se podnosilac predstavke pozvao na član 8 EKLJP, on mora dokazati da se njegova predstavka tiče jednog od četiri zaštićenih dobara sadržanih u ovom članu, a to su: privatni život, porodični život, dom i

33 International Mobile Equipment Identity – IMEI broj, predstavlja jedinstveni identitetski broj koji poseduje svaki mobilni telefon. Vesna Antonić, Dragan Mitrović, *Posebne istražne radnje*, Visoko sudsko i tužilačko vijeće BiH, Sarajevo 2012, 32.

34 Presuda Vrhovnog kasacionog suda Kzz 1306/2017 od 19.12.2017. godine.

35 Milica Kolaković-Bojović, „Posebna dokazna radnja tajni nadzor komunikacije i granice prava na privatnost", *Tužilačka reč*, 28/2015, 50.

prepiska.[36] Nakon što Evropski sud za ljudska prava utvrdi da podneta predstavka podleže primeni člana 8, on ispituje da li je došlo do nezakonitog odstupanja od prava na poštovanje privatnog i porodičnog života. Uslovi pod kojima nadležni organi vlasti država mogu odstupiti od ovog prava utvrđeni su u stavu 2 člana 8 EKLJP. Naime, potrebno je da zaštita interesa nacionalne sigurnosti, javne bezbednosti ili ekonomskog blagostanja zemlje, sprečavanja nereda ili kriminala, zaštite zdravlja ili morala ili zaštite prava i sloboda drugih u konkretnom slučaju ima prevagu u odnosu na pravo na poštovanje privatnog i porodičnog života. Pored toga, odstupanja od prava iz člana 8 EKLJP su dozvoljena ako su „u skladu sa zakonom" ili „propisana zakonom" kao i ako su „neophodna u demokratskom društvu" radi zaštite jednog od gore navedenih interesa.[37] U proceni ispunjenosti uslova „neophodnosti u demokratskom društvu", Evropski sud za ljudska prava mora često da odmerava interese podnosioca zahteva zaštićenih članom 8 EKLJP i interese treće strane zaštićene drugim odredbama EKLJP i njenih protokola.[38] Kada se dovede u vezi zaštita prava na privatnost, zajemčena članom 8 EKLJP, u kontekst primene mera tajnog nadzora komunikacije kao posebne dokazne radnje jasno proizilazi da je njeno sprovođenje dozvoljeno pod sledećim uslovima.[39] Prvo, primena tajnog nadzora komunikacije mora biti „u skladu sa nacionalnim zakonom". Drugo, sprovođenje ove posebne dokazne radnje mora biti „neophodno u demokratskom društvu". Konačno, potrebno je da u konkretnom slučaju zaštita nekog od propisanih „legitimnih interesa", kao što su nacionalna sigurnost, javna sigurnost, ekonomska dobrobit zemlje, sprečavanje nereda ili sprečavanje zločina, zaštita zdravlja i morala ili zaštita prava i sloboda drugih ima prevagu nad obavezom zaštite prava na privatnost pojedinca zbog čega postoji legitimno opravdavanje organa javne vlasti za odstupanje od prava na privatni i porodični život ličnosti.

36 European Court of Human Rights (a), *Annual report*, Council of Europe, Strasbourg 2018, 88.

37 Toon Moonen, „Special Investigation Techniques, Data Processing and Privacy Protection in the Jurisprudence of the European Court of Human Rights", *International law review online companion*, 9/2010, 105.

38 European Court of Human Rights (b), *Guide on Article 8 of the European Convention on Human Rights*, Council of Europe, Strasbourg 2018, 7.

39 Bart van der Sloot, „Privacy as Personality Right: Why the ECtHR's Focus on Ulterior Interests Might Prove Indispensable in the Age of „Big Data", *Utrecht Journal Of International And European Law*, 31/2015, 27.

U pogledu prvog uslova koji se odnosi na to da primena tajnog nadzora komunikacije mora biti „u skladu sa nacionalnim zakonom" Evropski sud za ljudska prava je u svojoj sudskoj praksi zauzeo stav da se to tumači na način da određivanje ove posebne dokazne radnje mora imati određenu osnovu u domaćem pravu i biti kompatibilno sa vladavinom prava. U tom smislu, nacionalni zakon mora ispuniti zahteve dostupnosti dotičnoj osobi i predvidljivosti u pogledu posledica njegovih normi koje se odnose na primenu tajnog nadzora komunikacije. Ipak, predvidljivost u kontekstu tajnog nadzora komunikacije ne može značiti da pojedinci treba da budu u stanju da predvide kada nadležni organi vlasti nameravaju da nadziru njihove komunikacije, te da u skladu sa tim adekvatno prilagode svoje ponašanje. Međutim, kako bi se izbeglo proizvoljno mešanje organa javne vlasti u pravo na privatni i porodični život, neophodno je nacionalnim zakonom propisati jasna i detaljna pravila o uslovima za legalno presretanje telefonskih i drugih razgovora ili komunikacija. Naime, nacionalni zakon mora biti dovoljno precizan pružajući građanima garantije u vezi sa okolnostima u kojima se može pribeći tajnom nadzoru komunikacije i pod kojim uslovima su organi javne vlasti ovlašćeni da pribegnu takvim tajnim merama. Pored toga, zakon mora navesti obim diskrecionog prava izvršnog organa i suda, kao i način njegovog vršenja na dovoljno precizan način da bi se pojedincu pružila adekvatna zaštita od proizvoljnog mešanja. U tom pogledu, nacionalni zakon koji reguliše mere tajnog nadzora komunikacije mora obezbediti sledeće minimalne mere zaštite protiv zloupotrebe organa vlasti: a) propisivanje kataloga krivičnih dela u pogledu kojih se mogu odrediti mere tajnog nazora komunikacije; b) odredbe o minimalnom i maksimalnom trajanju mere; c) postupak za ispitivanje, korišćenje i čuvanje dobijenih podataka; d) mere predostrožnosti koje treba preduzeti prilikom dostavljanja podataka drugim licima; e) okolnosti u kojima rezultati tajnog nadzora komunikacije mogu ili moraju biti izbrisani ili uništeni.[40] S druge strane, kada je reč o drugom i trećem uslovu, Evropski sud za ljudska prava je istakao da primena tajnog nadzora komunikacije mora da ima legitiman cilj i da bude neophodna u demokratskom društvu kako bi se taj cilj ostvario.[41] U tom smislu, nacionalne vlasti uživaju određenu slobodu pri-

40 Stjepan Gluščić, „Posebne dokazne radnje", *Policija i sigurnost*, 3/2012, 571.

41 Juliane Kokott, Christoph Sobotta, „The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR", *International*

likom procene ispunjenosti legitimnog cilja zaštite nacionalne sigurnosti primenom tajnog nadzora komunikacije. Međutim, ova sloboda nacionalnih vlasti podleže nadzoru Evropskog suda za ljudska prava koji mora biti uveren da postoje adekvatne i delotvorne garancije protiv zloupotreba nacionalnih organa vlasti. Procena Evropskog suda za ljudska prava po pitanju postojanja navedenih garancija zavisi od svih okolnosti konkretnog slučaja, kao što su priroda, obim i trajanje mere tajnog nadzora komunikacije, propisani uslovi za njegovo određivanje, nadležni organi za sprovođenje, izvršenje i nadzor kao i vrsta pravnih lekova predviđenih nacionalnim zakonom.[42]

Evropski sud za ljudska prava je cenio ispunjenost navedena tri uslova, primera radi, u slučaju *Faiza (Faiza) protiv Francuske* koji se ticao dozvoljenosti primene posebne dokazne radnje tajnog nadzora komunikacije prema podnosiocu predstavke u kontekstu istrage koja se sprovodila protiv njega zbog osnova sumnje da je izvršio krivično delo trgovine drogom. Podnosilac predstavke je tvrdio da je primena ove posebne dokazne radnje, i to sudski nalog izdat operateru mobilne telefonije za prikupljanje podataka o njegovim dolaznim i odlaznim pozivima, predstavljala zadiranje u njegovo pravo na poštovanje privatnog i porodičnog života iz člana 8 EKLJP.[43] Ispitujući ispunjenost navedena tri uslova pod kojim je dozvoljeno sprovoditi tajni nadzor komunikacije, Evropski sud za ljudska prava je zaključio da *nije došlo* do povrede člana 8 EKLJP u vezi sa nalogom suda koji je izdat operateru mobilne telefonije sa ciljem pribavljanja liste dolaznih i odlaznih poziva podnosioca predstavke. Prvo, ovo stoga što je Evropski sud za ljudska prava našao da iako je sudski nalog predstavljao slučaj odstupanja od prava na privatni i porodični život podnosioca predstavke, to je bilo *u skladu sa zakonom*, budući da je nalog bio usmeren na utvrđivanje istine u krivičnom postupku. Drugo, primena tajnog nadzora komunikacije je određena zbog postojanja osnova sumnje da je podnosilac predstavke izvršio krivično delo trgovine drogom zbog čega je bio ispunjen i uslov zaštite *legitimnih ciljeva sprečavanja izvršenja krivičnih dela i zaštite javnog zdravlja* koji imaju prevagu nad zaštitom prava na

Data Privacy Law, 4/2013, 224–225.

42 European Court of Human Rights (2018b), *op. cit.*, 92.

43 Gert Vermeulen, Eva Lievens, *Data Protection and Privacy under Pressure Transatlantic tensions, EU surveillance, and big data*, Maklu-Publishers, Antwerp 2017, 184–185.

privatnost u konkretnom slučaju. Konačno, Evropski sud za ljudska prava je smatrao da je ta posebna dokazna radnja bila *neophodna u demokratskom društvu* jer je imala za cilj da spreči i uđe u trag značajnim operacijima trgovine drogom.[44] S tim u vezi, Evropski sud za ljudska prava je u slučaju *Klas i drugi (Klass and others) protiv Nemačke,* u kome su se podnosioci predstavke žalili na neovlašćeno odstupanje od prava na privatnost i porodični život u pogledu nemačkog zakonodavstva prema kome su organi javne vlasti ovlašćeni da tajno nadziru njihovu telefonsku komunikaciju, zaključio da *nije došlo* do povrede člana 8 EKLJP, utvrdivši da je primena ove posebne dokazne radnje u izuzetnim slučajevima *neophodna u demokratskom društvu* u interesu zaštite nacionalne sigurnosti i sprečavanja nereda ili kriminala.[45]

S druge strane, Evropski sud za ljudska prava je u slučaju *Vis (Wisse) protiv Francuske* koji se odnosio na primenu tajnog nadzora komunikacije u prostorijama za posete pritvorenicima zaključio da je *došlo* do povrede člana 8 EKLJP, s obzirom na to da francuski zakon nije dovoljno jasno naznačio, kada i u kojoj meri organi javne vlasti mogu zadirati u privatni i porodični život pritvorenika odnosno nije precizno definisao obim i način vršenja diskrecionog ovlašćenja organa javne vlasti u toj sferi, zbog čega sprovođenje ove posebne dokazne radnje u konkretnom slučaju niti je bilo u skladu sa zakonom niti neophodno u demokratskom društvu budući da podnosioci predstavke nisu uživali minimalni stepen zaštite koji zahteva vladavina prava.[46] Ovo iz razloga što su sistematska snimanja razgovora u sobi za posete u svrhe koje nisu neophodne u cilju obezbeđenja reda u pritvorskoj jedinici lišavale te sobe njihove uloge onemogućavajući pritvorenicima održavanje određenog stepena privatnog i porodičnog života, uključujući i privatni razgovor sa svojim porodicama.[47] Takođe, i u slučaju *Dragojević protiv Hrvatske*, koji se odnosio na sprovođenje tajnog nadzora telefonskih razgovora prema podnosiocu predstavke, osumnjičenom za trgovinu

44 The ECHR case of Ben Faiza v. France, application no. 31446/12, Judgement of 8 February 2018.

45 The ECHR case of Klass and others v. Germany, application no. 5029/71, Judgement of 6 September 1978.

46 Council of Europe*, Case Law Of The European Court Of Human Rights Concerning The Protection Of Personal Data, Council of Europe, 2018, 105.*

47 The ECHR case of Wisse v. France, application no 71611/01, Judgement of 20 December 2005.

drogom, a u kome je imenovani smatrao da je istražni sudija propustio da postupi po postupku koji je propisan hrvatskim zakonom kako bi efikasno procenio da li je korišćenje tajnog nadzora komunikacije u njegovom slučaju bilo neophodno u demokratskom društvu, Evropski sud za ljudska prava je zaključio da je *došlo* do povrede člana 8 EKLJP. Ovo stoga što je utvrdio da hrvatski zakon nije pružio razumnu jasnost u pogledu diskrecionih ovlašćenja organa javne vlasti u određivanju mere tajnog nadzora komunikacija zbog čega nisu postojale dovoljne zaštitne mere protiv eventualnih zloupotreba.[48]

Konačno, a u pogledu prethodno istaknutog, Evropski sud za ljudska prava je u slučaju *Zakarov (Zakharov) protiv Rusije* koji se odnosio na ispitivanje uslova za dozvoljenost primene tajnog nadzora komunikacije putem mobilne telefonije našao da je *došlo* do povrede člana 8 EKLJP, utvrdivši da ruske zakonske odredbe koje regulišu nadzor komunikacija nisu obezbeđivale adekvatne i efikasne garancije protiv proizvoljnosti i zloupotreba koje su inherentne sistemu tajnog nadzora komunikacije.[49] Posebno, ovo zato što je Evropski sud za ljudska prava utvrdio da su postojali nedostaci u pravnom okviru po pitanju: okolnosti u kojima su organi javne vlasti u Rusiji ovlašćeni da pribegavaju merama tajnog nadzora komunikacije; trajanja takvih mera, posebno okolnosti pod kojima bi ih trebalo prekinuti; procedura za odobravanje nadzora komunikacije, odnosno čuvanja i uništavanja presretnutih podataka; kao i nadzora nad presretanjem komunikacija. Na kraju, prema mišljenju Evropskog suda za ljudska prava, efikasnost pravnih sredstava koja su bila na raspolaganju za osporavanje presretanja komunikacija bila je ugrožena činjenicom da su ona bila dostupna samo osobama koje su mogle da podnesu dokaze o presretanju, te da je pribavljanje takvog dokaza bilo nemoguće u odsustvu bilo kakvog sistema obaveštenja ili mogućnosti pristupa informacijama o presretanju.[50]

48 The ECHR case of Ante Dragojević v. Croatia, application no. 68955/11, Judgement of 15 January 2015.

49 European Court of Human Rights (2018b), *op. cit*., 98.

50 The ECHR case of Roman Zakharov v. Russia, application no. 47143/06, Judgement of 4 December 2015.

6. ZAKLJUČNA RAZMATRANJA

Pravo na poštovanje privatnosti zajemčeno je najznačajnijim međunarodnim i evropskim izvorima prava kao osnovno ljudsko pravo vezano za ličnu sferu pojedinaca. Ipak, kada je reč o navedenom pravu treba imati na umu da ono nije apsolutne prirode, zbog čega njegova primena ne važi u svim slučajevima. U tom smislu, kako u evropskim tako i u nacionalnim izvorima predviđena su odstupanja od apsolutnog uživanja navedenog prava, kao i uslovi pod kojima su ta odstupanja dozvoljena. Na evropskom planu odstupanja su dozvoljena ako je zadiranje u pravo na privatnost i privatni život predviđeno zakonom i ako je to neophodna mera u demokratskom društvu u interesu nacionalne ili javne sigurnosti, ekonomske dobrobiti zemlje, sprečavanja nereda ili sprečavanja zločina, zaštite zdravlja i morala ili zaštite prava i sloboda drugih odnosno ako se takvim ograničenjem poštuje suština temeljnih prava i sloboda, te ako ono predstavlja nužnu i srazmernu meru u demokratskom društvu s obzirom na potrebu sprečavanja, istrage, otkrivanja ili gonjenja za krivična dela ili izvršenja krivičnopravnih sankcija odnosno zaštitu od pretnji javnoj sigurnosti i njenom sprečavanju.

S druge strane, na nacionalnom planu odstupanja su dozvoljena samo na određeno vreme i na osnovu odluke suda, ako su neophodna radi vođenja krivičnog postupka ili zaštite bezbednosti Republike Srbije, na način predviđen zakonom. Međutim, kada je reč o uslovu da su odstupanja moguća samo ako su predviđena zakonom, treba konstatovati da navedeno ljudsko pravo može biti zakonom ograničeno samo ako prethodno ograničenje dopušta Ustav kao najviši pravni akt u zemlji i to pod tri uslova: a) u svrhe radi kojih Ustav to dopušta; b) u obimu neophodnom da se ustavna svrha ograničenja zadovolji u demokratskom društvu i c) bez zadiranja u suštinu zajemčenog prava. Dalje, kada je reč o uslovu da su odstupanja moguća samo na osnovu odluke suda, potrebno je istaći da su sudovi, pri ograničavanju prava na privatnost, dužni da vode računa o suštini prava koje se ograničava, važnosti svrhe ograničenja, prirodi i obimu ograničenja, odnosu ograničenja sa svrhom ograničenja i o tome da li postoji način da se svrha ograničenja postigne manjim ograničenjem prava. S tim u vezi, kada je reč o primeni u radu analizirane posebne dokazne radnje – tajni nadzor komunikacije – treba istaći da iako je njeno sprovođenje neophod-

no u slučajevima otkrivanja i dokazivanja teških oblika kriminala, ne postoji niti bezuslovnost niti apsolutnost u određivanju ove specijalne istražne radnje, već se ona koristi u predistražnom postupku samo pod restriktivnim uslovima. Iz navedenog proizilazi zaključak da prilikom odlučivanja o određivanju i trajanju tajnog nadzora komunikacije organ postupka treba posebno da ceni postojanje mogućnosti da se isti rezultat postigne na način kojim se manje ograničavaju prava građana.

Dakle, imajući u vidu navedeno, treba primetiti da iako je primena tajnog nadzora komunikacije legitimna posebna dokaznja radnja u otkrivanju određenih ozbiljnih krivičnih dela kojima se ne može ući u trag korišćenjem klasičnih dokaznih radnji iz analizirane prakse Evropskog suda za ljudska prava proizilazi da je za dozvoljenost njegovog korišćenja u krivičnom postupku potrebno da je nacionalnim zakonima država propisano postojanje određenih procesnih garancija u kontekstu utvrđivanja da li je odstupanje od navedenog zajemčenog prava bilo nužno zbog ostvarivanja interesa vođenja krivičnog postupka odnosno nacionalne bezbednosti kao i da li je bilo proporcionalno tim ciljevima. Konkretno, kada je reč o procesnim garancijama potrebnim za legalno korišćenje rezultata dobijenih primenom tajnog nadzora komunikacije kao posebne dokazne radnje u krivičnom postupku, nacionalnim zakonom treba da bude određena: a) kategorija lica prema kojima može biti određena; b) vrsta krivičnih dela za koje se može primeniti; c) kategorija minimalnog i maksimalnog trajanja; d) procedura za njeno sprovođenje koja mora biti poštovana; e) mere predostrožnosti koje se moraju preduzeti u smislu obezbeđivanja tajnosti prikupljenih podataka kao i f) procedura pod kojom se prikupljeni materijal mora uništiti.

Upoređujući usvojene standarde iz prakse Evropskog suda za ljudska prava pod kojima je dozvoljeno sprovođenje tajnog nadzora komunikacije sa uslovima u kojima je moguća njena primena u domaćem krivičnoprocesnom zakonodavstvu dolazi se do zaključka da postoji visok stepen usaglašenosti. Naime, uslovi za sprovođenje tajnog nadzora komunikacije su propisani na restriktivan način uzimajući u obzir potrebu balansiranja između neophodnosti primene ove posebne dokazne radnje u kontekstu otkrivanja teških krivičnih dela i nužnosti poštovanja prava na privatnost. U tom smislu, treba konstatovati da je našim zakonodavstvom propisan katalog krivičnih dela u odnosu na koja se mogu primeniti ova posebna dokazna radnja, a samim

tim i kategorija lica prema kojima može biti određena njena primena. Takođe, normiran je postupak za sprovođenje ove posebne dokazne radnje, prema kojem je određivanje, kontrola i nadzor nad njenom primenom u nadležnosti suda. Dodatno, propisan je minimalni i maksimalni vremenski period njenog trajanja, s tim da se sprovođenje ove posebne dokazne radnje prekida čim prestanu razlozi za njenu primenu. Konačno, predviđene su i posebne odredbe o postupanju sa prikupljenim materijalom i o tajnosti podataka.

S tim u vezi, treba dodati i to da je sudska praksa, tumačeći zakonske odredbe, zauzela stav da na shvatanje tajnog nadzora komunikacije kao legitimnog osnova za odstupanje od prava na privatnost ne utiče okolnost da li je javni tužilac izmenio pravnu kvalifikaciju krivičnog dela nakon sprovođenja ove posebne dokazne radnje u delo za koje nije dozvoljena ili je takođe dozvoljena primena tajnog nadzora komunikacije, s tim da se pravosnažna presuda može zasnovati isključivo na dokaznom materijalu koji je prikupljen posle datuma donošenja naredbe sudije za prethodni postupak o tajnom nadzoru komunikacije, pri čemu u naredbi nije neophodno opredeliti precizan vremenski momenat do kada tačno traje ova posebna dokazna radnja, već je dovoljno opredeliti početak njenog sprovođenja i dužinu trajanja. Konačno, sudska praksa je prihvatila stav da ne postoji legitimno odstupanje od prava na privatnost, ukoliko je u naredbi o određivanju tajnog nadzora komunikacije označen samo IMEI broj mobilnog telefona osumnjičenog, bez označavanja telefonskog broja. Ovi primeri iz sudske prakse su pokazali da iako u teoriji postoji načelna zabrinutost da se primenom tajnog nadzora komunikacije kao posebne dokazne radnje može neosnovano odstupati od prava na privatnost, to u praksi uopšte ne mora biti slučaj. Drugim rečima, u slučajevima kada sudovi primenjuju odredbe nacionalnih zakonodavstava kojima su propisani limitativni uslovi za sprovođenje ove posebne dokazne radnje, uzimajući u obzir princip *nužnosti* njene primene u smislu njene neophodnosti za vođenje krivičnog postupka odnosno za zaštitu nacionalne bezbednosti, te *proporcionalnosti* u smislu cilja koji se želi postići u demokratskom društvu njenim sprovođenjem kao i *restriktivnosti* u njenoj primeni u smislu da u konkretnom slučaju ne postoji drugi način putem koga bi se manje ograničavala prava građana, ne treba da postoji bojazan da će doći do neosnovanog odstupanja od prava na privatnost ličnosti.

Nikola Paunović
Assistant at the Ministry of Foreign Affairs
PhD Candidate at the University of Belgrade, Faculty of Law

COVERT INTERCEPTION OF COMMUNICATIONS AS LEGITIMATE BASIS FOR DEROGATION FROM THE RIGHT TO PRIVACY OF PERSONALITY WITH REFERENCE TO THE CASE-LAW OF EUROPEAN COURT OF HUMAN RIGHTS

Summary

An effective fight against serious forms of crime requires, under certain conditions, the conducting of covert interception of communications as a special investigative technique, whose application can jeopardize the right to privacy of personality. However, bearing in mind, that the inviolability of this right is not understood in absolute sense, neither at the level of the national legal framework, nor at the European level embodied in the European Convention on Fundamental Rights and Freedoms, since the necessity for conducting criminal proceedings is prescribed as a legitimate ground for its derogation, the paper starts from the basic presumption that covert interception of communications constitutes a legitimate ground for derogation from the right to privacy of personality. Therefore, the author in the first part of the paper pays attention to the conditions for conducting a covert interception of communications in the national criminal procedural framework, with reference to disputed issues from domestic case-law questioning its validity as a legitimate basis for derogation from the right to privacy of personality. Moreover, the second part deals with the analysis of the case-law of the European Court of Human Rights in cases relating to Article 8 of the European Convention on Fundamental Rights and Freedoms, in which the legitimacy of the derogation of the right to privacy is questioned due to the conducting of covert interception of communications before national authorities. In concluding remarks it is emphasized that the application of covert interception of communications for the purpose of conducting criminal proceedings,

solely in compliance with the principles of necessity, proportionality and restrictiveness, and the legal conditions for its implementation, does not lead to an unjustified derogation from the right to privacy of personality.

Key words: *Covert Interception of Communications. – Special investigative technique. – Right to privacy. – European Court of Human Rights.*