PRAVO NA PRIVATNOST I POSEBNE MERE TAJNOG PRIKUPLJANJA PODATAKA U REPUBLICI SRBIJI

Sanela Veljković[26], Milica Ćurčić[27], Marina Dabetić[28]

doi: 10.59864/Oditor62403SV

Pregledni rad
UDK: 342.721(497.11)
343.985

Apstrakt

Pravo na privatnost predstavlja jedno od osnovnih ljudskih prava pojedinca u demokratskom društvu. Na međunarodnom i regionalnom planu postoje brojni instrumenti koji garantuju pravo na privatnost. Države su dužne da obezbede nesmetano uživanje ovog prava svom stanovništvu. Danas, jedan od najvećih izazova po pravo na privatnost jesu posebne mere tajnog prikupljanja podataka koje stoje na raspolaganju određenim akterima bezbednosno-obaveštajnog sistema i drugim državnim akterima prilikom obavljanja poslova iz njihove nadležnosti. Treba imati u vidu da pravo na privatnost nije apsolutno, te da se zakonom propisuje na koji način ono može biti ograničeno. U Republici Srbiji, derogacija prava na privatnost jeste predmet pojedinih zakona, a posebno onih kojima se reguliše način funkcionisanja bezbednosno-obaveštajnog sistema. Stoga, u radu se analizira normativni okvir koji reguliše posebne mere tajnog prikupljanja podataka koje stoje na raspolaganju različitim akterima bezbednosno-obaveštajnog sistema. Ujedno, predmet analize predstavljaće i normativne odredbe kojima je regulisana kontrola posebnih mera tajnog prikupljanja podataka. Rad teži da ispita negativan uticaj primene posebnih mera na pravo na privatnost, kao i mogućnost unapređenja trenutnog normativnog okvira koji postoji u Republici Srbiji.

Ključne reči: *pravo na privatnost, posebne mere tajnog prikupljanja podataka, bezbednosno-obaveštajni sistem, kontrola*

---

[26] Sanela Veljković, istraživač pripravnik, Institut za nuklearne nauke „Vinča“- Institut od nacionalnog značaja za Republiku Srbiju, Univerzitet u Beogradu, email: sanela.veljkovic@vin.bg.ac.rs ORCID 0009-0003-3650-290X

[27] dr Milica Ćurčić, istraživač saradnik, Institut za nuklearne nauke „Vinča“- Institut od nacionalnog značaja za Republiku Srbiju, Univerzitet u Beogradu, email: milica.curcic@vin.bg.ac.rs ORCID 0000-0002-4326-4036

[28] Marina Dabetić, istraživač saradnik, Institut za nuklearne nauke „Vinča“- Institut od nacionalnog značaja za Republiku Srbiju, Univerzitet u Beogradu, email: fmarina@vin.bg.ac.rs ORCID 0000-0003-0903-0110

Rad je nastao u okviru naučno-istraživačke delatnosti Instituta za nuklearne nauke „Vinča” – Instituta od nacionalnog značaja za Republiku Srbiju, finansiranog od strane Ministarstva nauke, tehnološkog razvoja i inovacija, broj granta 451-03-47/2023-01/200017.

***JEL**: K22, K29.*

Uvod

Uživanje prava na privatnost neophodno je obezbediti pojedincima u demokratskom društvu. Država treba da ima adekvatan normativni okvir koji obezbeđuje uživanje prava na privatnost i koji je smislen i jasan svakom građaninu. Ujedno, država treba da obezbedi i adekvatne institucionalne mehanizme putem kojih pojedinci mogu da se obrate relevantnim institucijama ukoliko smatraju da je njihovo pravo na privatnost na bilo koji način ugroženo. Pravo na privatnost, iako je jedno od fundamentalnih ljudskih prava, nije apsolutno. Moguće je ograničiti uživanje ovog prava pojedincima u određenim situacijama koje bi trebalo biti jasno definisane zakonskim odredbama. Najveći izazov za uživanje prava na privatnost predstavljaju posebne mere tajnog prikupljanja podataka koje različiti državni akteri koriste prilikom vršenja svojih nadležnosti. Kako akteri mogu biti različiti, isto tako su drugačiji i nazivi ovih postupaka i mera u zakonskim rešenjima. Predmet analize jeste normativni okvir koji reguliše primenu posebnih mera tajnog prikupljanja podataka bezbednosno-obaveštajnog sistema Republike Srbije. Međutim, Zakonom o Bezbednosno-informativnoj agenciji i Zakonom o Vojnobezbednosnoj i Vojnoobaveštajnoj agenciji ne iscrpljuje se lista postupaka i mera koje pomenuti državni akteri imaju na raspolaganju, te je neophodno dotaći se i Zakonika o krivičnom postupku. Prošlih godina, određene odredbe i delovi trenutnog normativnog okvira Republike Srbije pretrpeli su pojedine modifikacije u cilju njihovog usaglašavanja sa Ustavom. Rad teži da ispita mogućnost unapređenja normativnog okvira kojim se reguliše režim posebnih mera tajnog prikupljanja podataka. Stoga, prvi deo rada posvećen je pravu na privatnost. Drugi deo rada bavi se konkretnim merama tajnog prikupljanja podataka koje akteri bezbednosno-obaveštajnog sistema imaju na raspolaganju. Treći deo rada posvećen je kontroli primene posebnih mera tajnog prikupljanja podataka, a posebno sudskoj kontroli. U četvrtom delu, izloženi su mogući problemi koji se javljaju na relaciji pravo na privatnost – posebne mere tajnog prikupljanja podataka pri čemu rad teži da identifikuje nedostatke koji postoje u trenutnim zakonskim odredbama. Na samom kraju, pored zaključka, biće ponuđen spisak literature i zakona koji su korišćeni za izradu rada.

Pravo na privatnost

Jedno od temeljnih ljudskih prava predstavlja pravo na privatnost. Pravo na privatnost ne odnosi se na jedno konkretno pravo, već obuhvata širok spektar prava i to „pravo na poštovanje privatnog i porodičnog života, pravo na poštovanje nepovredivosti doma, pravo na poštovanje nepovredivosti prepiske, kao i pravo na poštovanje nepovredivosti časti i ugleda“ (Dimitrijević i sar., 2007, str. 203). Na međunarodnom i regionalnom planu, Univerzalna deklaracija o

ljudskim pravima iz 1948. godine, Pakt o građanskim i političkim pravima iz 1966. godine, kao i Evropska konvencija o ljudskim pravima iz 1950. godine, garantuju pravo na privatnost. Na osnovu člana 8 stava 1 Evropske konvencije o ljudskim pravima: „Svako ima pravo na poštovanje svog privatnog i porodičnog života, doma i prepiske“ (European Convention for the Protection of Human Rights and Fundamental Freedoms, 1950). Stavom 2 regulisano je da se: „javne vlasti neće mešati u vršenje ovog prava sem ako to nije u skladu sa zakonom i neophodno u demokratskom društvu u interesu nacionalne bezbednosti, javne bezbednosti ili ekonomske dobrobiti zemlje, radi sprečavanja nereda ili kriminala, zaštite zdravlja ili morala, ili radi zaštite prava i sloboda drugih“ (European Convention on Human Rights, 1950). Iako se na osnovu sadržaja stava 2 čini da su situacije u kojima je moguće ograničiti pravo na privatnost brojne, ipak u praksi države ne mogu tako lako ograničiti pravo na privatnost svojim građanima.

Razmatrajući slučajeve koji se odnose na povredu člana 8. Evropske konvencije o ljudskim pravima, Evropski sud za ljudska prava je u godinama koje usledile ustanovio određene standarde u vezi prava na privatnost. Oni se mogu sumirati na sledeći način: „1) slučajevi mešanja u pravo na privatnost moraju biti zakonom regulisani dovoljno jasno da bi bili predvidivi; 2) takvi slučajevi treba da se urede restriktivno i da budu prevashodno vezani za teška krivična dela i pretnje po bezbednost; 3) procedura za primenu mera propisuje se zakonom, a o primeni mera treba da odlučuje sud ili drugi organ na osnovu postojanja osnova sumnje; 4) početak i trajanje mere određuje se u odluci suda ili drugog organa, koji i nadziru primenu mere; 5) postupak za zaštitu građana treba da bude propisan zakonom i da obuhvati mogućnost sudske zaštite, a građanin obavešten o meri na svoj zahtev kada to bude moguće; i 6) zakon treba da predvidi sankcije za kršenje pravila o primeni takvih mera“ (Milosavljević, 2015, str. 25). Značaj Evropskog suda za ljudska prava ogleda se upravo u mogućnosti da pojedinac može da se obrati sudu i tuži sopstvenu državu ukoliko smatra da mu je neko od prava zagarantovanih Evropskom konvencijom o ljudskim pravima uskraćeno ili povređeno.

Pravo na privatnost ne reguliše se samo na međunarodnom i regionalnom planu, već je i predmet ustavnog i zakonskog okvira država. Upravo iz razloga što pravo na privatnost štiti sledeće interese: „a) čovekove interese autonomije odlučivanja u intimnim stvarima; b) interes pojedinca da se zaštiti od otkrivanja ličnih okolnosti; c) interes pojedinca da se obezbedi od neosnovane prismotre od strane vlasti“ (Dimitrijević, 2011, str. 203). Zaštita poslednjeg interesa predstavlja jedan od danas najčešćih problema na relaciji država – pojedinac. Stoga, može se zaključiti da „država ima dvostruku obavezu: negativnu – da se uzdrži od mešanja u privatnost i pozitivnu – da pruži zaštitu privatnosti pojedinca i obezbedi pravni okvir i zaštitu od napada drugih pojedinaca“ (Dimitrijević i sar., 2007, str. 203). Ustav Republike Srbije, iako ne sadrži konkretnu odredbu o pravu na privatnost, članom 40. garantuje nepovredivost stana, članom 41. tajnost pisama i drugih sredstava opštenja i članom 42. zaštitu podataka o ličnosti. Ujedno, treba imati u

vidu da se Ustavni sud u svojoj odluci 3238/1 iz 2012. godine izjasnio da pravo na privatnost predstavlja sastavni deo ustavnog prava i potpada pod član 23. Ustava, odnosno pod pravo na dostojanstvo i slobodan razvoj ličnosti (Beogradski centar za ljudska prava, 2023, str. 94).

Neizostavni deo prava na privatnost predstavlja i pravo na zaštitu podataka o ličnosti. U Republici Srbiji donet je zakon 2008. godine čime su Povereniku za informacije od javnog značaja pridodata zaduženja i u oblasti zaštite podataka o ličnosti. Međutim, zbog brojnih nedostataka starog zakonskog rešenja, nov zakon je donet tokom 2018. godine. Podatak o ličnosti predstavlja „svaki podatak koji se odnosi na fizičko lice čiji je identitet određen ili odrediv, neposredno ili posredno, posebno na osnovu oznake identiteta, kao što je ime i identifikacioni broj, podataka o lokaciji, identifikatora u elektronskim komunikacionim mrežama ili jednog, odnosno više obeležja njegovog fizičkog, genetskog, metalnog, ekonomskog, kulturnog i društvenog identiteta“ (Zakon o zaštiti podataka o ličnosti, 2018). Pravo na zaštitu podataka o ličnosti i pravo na privatnost mogu biti ozbiljno ugroženi posebnim merama tajnog prikupljanja podataka koje bezbednosno-obaveštajni sistem ima na raspolaganju prilikom obavljanja svojih nadležnosti. Najčešći vidovi mešanja u privatnost građana jesu tajni nadzor i prikupljanje podataka o pojedincima, njihovo čuvanje i objavljivanje (Ignjatović, 2015, str. 10). Iz tog razloga, neophodan je adekvatan normativni okvir koji propisuje posebne mere, način njihovog vršenja, a posebno njihove kontrole. U narednom delu rada predstavljene su zakonske odredbe koje se odnose na posebne mere tajnog prikupljanja podataka Bezbednosno-informativne agencije, Vojnobezbednosne i Vojnoobaveštajne agencije.

Posebne mere tajnog prikupljanja podataka

Posebni postupci i mere predstavljaju „specijalna ovlašćenja bezbednosnih organa i organa krivičnog gonjenja za tajno prikupljanje podataka kojima se izuzetno, na određeno vreme i bez znanja građana, a na osnovu odluke suda i pod uslovima propisanim zakonom, odstupa od pojedinih ustavom zajemčenih individualnih prava“ (Milosavljević, 2015, str. 11). Postoje dve grupe posebnih mera za tajno prikupljanje podataka. Prva grupa obuhvata mere koje ne narušavaju znatno ljudska prava i slobode pojedinca, dok u drugu grupu spadaju mere kojima se privremeno i bez znanja pojedinca narušavaju njegova ljudska prava i slobode, a posebno njegovo pravo na privatnost (Milosavljević, 2008). Posebni postupci i mere ne stoje na raspolaganju samo akterima bezbednosno-obaveštajnog sistema, već i drugim državnim organima poput policije, te je neophodno napraviti distinkciju među njima. Na osnovu cilja prikupljanja podataka, svi posebni postupci i mere se dele u dve grupe: 1) posebni postupci i mere čiji je cilj vođenje krivičnog postupka koje bliže uređuje Zakonik o krivičnom postupku i Zakon o policiji; 2) posebni postupci i mere čiji je cilj preventivno delovanje radi zaštite nacionalne bezbednosti koje bliže uređuju zakoni o bezbednosno-obaveštajnom

sistemu (Milosavljević, 2007, str. 59-60). Iako se za posebne postupke i mere koriste različiti termini u različitim zakonskim rešenjima, posebni postupci i mere koje stoje na raspolaganju organima bezbednosno-obaveštajnog sistema nisu predmet samo Zakona o Bezbednosno-informativnoj agenciji i Zakona o Vojnobezbednosnoj i Vojnoobaveštajnoj agenciji, već i Zakonika o krivičnom postupku.

Na osnovu Zakonika o krivičnom postupku, Bezbednosno-informativna agencija i Vojnobezbednosna agencija mogu primenjivati posebne dokazne radnje. Posebne dokazne radnje se primenjuju prema licu za koje postoji osnov sumnje da je učinilo krivično delo ili se priprema za njegovo izvršenje, a to se ne može na drugačiji način otkriti, sprečiti ili dokazati ili bi to izazvalo nesrazmerne teškoće ili veliku opasnosti (Zakonik o krivičnom postupku, 2011, član 161). Zakonik propisuje krivična dela za koja se mogu primeniti posebne dokazne radnje, način postupanja sa prikupljenim materijalom, mogućnost slučajnog nalaza, kao i tajnost podataka. Kao posebne dokazne radnje, Zakonik navodi tajni nadzor komunikacije, tajno praćenje i snimanje, simultane poslove, računarsko pretraživanje podataka, kontrolisanu isporuku i prikrivenog islednika. Pored policije, Bezbednosna-informativna agencija i Vojnobezbednosna agencija mogu sprovoditi tajni nadzor komunikacije, tajno praćenje i snimanje, simultane poslove, kao i računarsko pretraživanje podataka. Na osnovu teksta Zakonika, kontrolisanu isporuku sprovodi policija, kao i drugi državni organi koje odredi javni tužilac čime ova odredba ostavlja prostor i za aktere bezbednosno-obaveštajnog sistema. Prikriveni islednik može biti ovlašćeno lice policije, Bezbednosno-informativne agencije, kao i Vojnobezbednosne agencije. Zakonik o krivičnom postupku bliže uređuje svaku od posebnih dokaznih radnji odnosno uslove za sprovođenje, instancu koja donosi naredbu, tok sprovođenja, mogućnost proširenja, kao i potrebu dostavljanja izveštaja i prikupljenih materijala.

Zakonom o Bezbednosno-informativnoj agenciji bliže se uređuje način rada, organizacija, kontrola i druga pitanja vezana za Bezbednosno-informativnu agenciju. Agencija može da primenjuje operativne metode, mere i radnje, kao i odgovarajuća operativno-tehnička sredstva prilikom obavljanja poslova iz svoje nadležnosti (Zakon o Bezbednosno-obaveštajnoj agenciji, 2002, član 9). Posebne mere koje Bezbednosno-informativna agencija ima na raspolaganju su: tajni nadzor i snimanje komunikacije bez obzira na oblik i tehnička sredstva preko kojih se obavlja ili nadzor elektronske ili druge adrese; tajni nadzor i snimanje komunikacije na javnim mestima i mestima kojima je pristup ograničen ili u prostorijama; statistički elektronski nadzor komunikacije i informacionih sistema u cilju pribavljanja podataka o komunikaciji ili lokaciji korišćene mobilne terminalne opreme; računarsko pretraživanje već obrađenih ličnih i drugih podataka i njihovo upoređivanje sa podacima koji su prikupljeni primenom drugih posebnih mera (Zakon o Bezbednosno-informativnoj agenciji, 2002, član 13). Posebne mere se primenjuju kada postoji osnov sumnje da određeno lice, grupa ili

organizacija priprema ili preduzima radnje usmerene protiv bezbednosti države, a to se ne bi moglo na drugačiji način sprečiti ili dokazati ili bi izazvalo nesrazmerne teškoće ili veliku opasnost (Zakon o Bezbednosno-informativnoj agenciji, 2002, član 14). Kada se odlučuje o primeni posebnih mera posebno se razmatra da li bi isti rezultat mogao da se postigne na način kojim se manje ograničavaju ljudska prava, u obimu koji je neophodan da se svrha ograničavanja zadovolji u demokratskom društvu (Zakon o Bezbednosno-informativnoj agenciji, 2002, član 14). Direktor Bezbednosno-informativne agencije podnosi predlog o kome odlučuje predsednik Višeg suda u Beogradu, odnosno sudija kog on odredi među sudijama koji su raspoređeni u Posebno odeljenje koje postupa u predmetima teških krivičnih dela, pri čemu je odluku neophodno doneti u roku od 48 sati. Posebna mera može trajati tri meseca, a može se produžiti najviše tri puta po tri meseca. Na osnovu člana 15b, Bezbednosno-informativna agencija ima mogućnost proširenja primene posebnih mera.

Posebni postupci i mere za tajno prikupljanje podataka koje Vojnobezbednosna agencija ima na raspolaganju jesu: operativni prodor u organizacije, grupe i institucije; tajno pribavljanje i otkup dokumenata i predmeta; tajni uvid u evidencije podataka; tajno praćenje i nadzor lica na otvorenom prostoru i javnim mestima uz korišćenje tehničkih sredstava; tajni elektronski nadzor telekomunikacija i informacionih sistema radi prikupljanja zadržanih podataka o telekomunikacionom saobraćaju, bez uvida u njihov sadržaj; tajno snimanje i dokumentovanje razgovora na otvorenom i u zatvorenom prostoru uz korišćenje tehničkih sredstava; tajni nadzor sadržine pisama i drugih sredstava komuniciranja, uključujući i tajni elektronski nadzor sadržaja telekomunikacija i informacionih sistema; tajni nadzor i snimanje unutrašnjosti objekata, zatvorenih prostora i predmeta (Zakon o Vojnobezbednosnoj i Vojnoobaveštajnoj agenciji, 2009, član 12). O primeni prve četiri mere odlučuje direktor agencije ili lice koje on ovlasti i one se primenjuju dok postoje razlozi za njihovu primenu. O primeni pete mere odlučuje nadležni Viši sud u roku od 8 sati. O primeni šeste, sedme i osme mere odlučuje Vrhovni kasacioni sud u roku od 24 sata. Trajanje primene ostalih mera je šest meseci uz mogućnost produženja još šest. Posebni postupci i mere za tajno prikupljanje podataka koje Vojnoobaveštajna agencija ima na raspolaganju su: tajna saradnja radi prikupljanja podataka; tajno pribavljanje i otkup dokumenata i predmeta; operativni prodor u organizacije, institucije i grupe; preduzimanje mera na prikrivanju identiteta i svojine; osnivanje pravnih lica; prikriveno korišćenje imovine i usluga uz naknadu; korišćenje posebnih dokumenata i sredstava kojima se štiti agencija, njeni pripadnici, prostorije i sredstva. (Zakon o Vojnobezbednosnoj i Vojnoobaeštajnoj agenciji, 2009, član 27). Navedeni postupci i mere se preduzimaju na osnovu odluke direktora agencije ili lica koje on ovlasti.

Kontrola primene posebnih mera

Svrha kontrole bezbednosno-obaveštajnog sistema jeste u utvrđivanju da li bezbednosno-obaveštajni sistem postupa u skladu sa zakonom, poštujući zagarantovana ljudska prava uz obezbeđivanje najveće moguće efikasnosti sistema (Born, 2007, p. 163). Kontrolori bezbednosno-obaveštajnog sistema su brojni. Prevashodno, kontrolu vrše tri grane vlasti. Iako bezbednosno-obaveštajni sistem predstavlja deo izvršne vlasti, Vlada je jedna od instanci kontrole. Kontrola koju sprovodi Narodna skupština ispoljava se u više vidova pri čemu je rad Odbora za kontrolu službi bezbednosti najznačajniji. Sudska kontrola se ogleda u odobravanju primene posebnih mera za tajno prikupljanje podataka. Ujedno, kontrolu sprovode i nezavisne državne institucije od kojih su najznačajnije Zaštitnik građana, Poverenik za informacije od javnog značaja i zaštitu podataka o ličnosti i Državna revizorska institucija. Kontrolnu funkciju mogu vršiti i civilno društvo, javnost i mediji. Štaviše, u okviru samih bezbednosno-obaveštajnih službi postoje i tela koju su zadužena za unutrašnju kontrolu koja su zapravo „prva brana od nezakonitog i nepravilnog postupanja službi bezbednosti“ (Petrović, 2020v, str. 63).

Postoje dva cilja zbog kojih akteri bezbednosno-obaveštajnog sistema mogu koristiti posebne mere za tajno prikupljanje podataka kojima se zadiru u ljudska prava i slobode. Prvi je otkrivanje, istraživanje i dokumentovanje teških krivičnih dela, a drugi je preventivno delovanje (Petrović, 2020b, str. 21). Na prve se primenjuje Zakonik o krivičnom postupku kojim sudovi imaju mnogo veću kontrolnu funkciju, a na druge Zakon o BIA i Zakon o VBA i VOA prilikom čega se uloga suda svodi samo na davanje saglasnosti (Petrović, 2020b, str. 68). Na osnovu Zakonika o krivičnom postupku, sud donosi odluku o tome da li su ispunjeni uslovi za primenu određene posebne dokazne radnje. Prilikom njenog sprovođenja, akter koji je sprovodi mora da dostavlja dnevne izveštaje zajedno sa materijalom koji je prikupljen. Ujedno, nakon okončanja primene posebne dokazne radnje, akter koji je sprovodio posebnu dokaznu radnju mora da dostavi i poseban izveštaj, kao i sav prikupljeni materijal. Sa druge strane, prema Zakonu o Bezbednosno-informativnoj agenciji i Zakonu o Vojnobezbednosnoj i Vojnoobaveštajnoj agenciji, prikupljeni podaci primenom neke od posebnih mera predstavljaju tajne podatke. Stoga, sudska kontrola prema Zakoniku o krivičnom postupku obuhvata sve tri faze kontrole odnosno pre, tokom i nakon okončanja mera i time je sveobuhvatnija u odnosu na sudsku kontrolu koju predviđaju zakoni o bezbednosno-obaveštajnim službama jer je svode samo na prvu fazu (Petrović, 2015, str. 39).

Trenutni normativni okvir koji reguliše primenu posebnih mera za tajno prikupljanje podataka u Republici Srbiji proteklih godina pretrpeo je određene modifikacije (Milošević i Putnik, 2017). Tokom 2013. godine, Ustavni sud se bavio odredbama Zakona o elektronskim komunikacijama na osnovu kojih su operateri bili u obavezi da dostavljaju podatke o elektronskim komunikacijama u skladu sa zakonima kojima se uređuje krivični postupak, rad bezbednosno-

obaveštajnog sistema i policije (Odluka Ustavnog suda RS, br. predmeta IUz-1245/2010). S obzirom da su Ustavom propisana određena ograničenja tajnosti pisama i drugih sredstava opštenja, ta ograničenja ne mogu biti predmet različitih zakonskih rešenja. Ustavni sud je zaključio da ovakve odredbe nisu u skladu sa Ustavom, čime su one kasnije izmenjene. Tokom kasnijih godina, određene odredbe Zakona o Bezbednosno-informativnoj agenciji i Zakona o Vojnobezbednosnoj i Vojnoobaveštajnoj agenciji bile su predmet razmatranja Ustavnog suda. Pozivajući se na i u ovom slučaju na tajnost pisama i drugih sredstava opštenja odnosno pravo koje je zagarantovano samim Ustavom, Ustavni sud je odlučio da nije moguće da direktor vojne agencije određuje primenu posebne mere tajnog elektronskog nadzora bez odobrenja sudske instance (Odluka Ustavnog suda RS, IUz -1218/2010). Rezultat ovakve odluke Ustavnog suda bila je kasnija modifikacija zakonske odredbe u pravcu da na predlog direktora Vojnobezbednosne agencije tajni elektronski nadzor odobrava viši sud. Kako bi se zaštitila ljudska i manjinska prava, modifikovani su i članovi 13., 14. i 15. Zakona o Bezbednosno informativnoj agenciji. Ranije odredbe ovog zakona nisu predviđale kriterijume na osnovu kojih bi se odredilo lice prema kome se primenjuju posebne mere, nije navedeno šta sve mogu podrazumevati posebne mere i na šta se one odnose, čime je zakon nejasan i nedovoljno precizan, te je podložan proizvoljnom tumačenju (Odluka Ustavnog suda PS, br. predmeta IUz-252/2002). Iako je došlo do modifikacije ovih članova i njihovog preciziranja, određene odredbe Zakona o Bezbednosno-informativnoj agenciji su i danas predmet kritika. Dosadašnje zakonske modifikacije izvršene su kako bi se zaštitilo pravo na privatnost građana prilikom primene posebnih mera tajnog prikupljanja podataka. Međutim, neophodno je analizirati da li je pravo na privatnost na adekvatni način zagarantovano postojećim normativnim okvirom. U narednom delu rada predstavljeni su mogući problemi u vezi sa primenom posebnih mera, kao i potreba izmene pojedinih zakonskih rešenja.

Mogući problemi u vezi primene posebnih mera

U Republici Srbiji, pravo na privatnost je zagarantovano Ustavom. I drugi pravni akti na posredan ili neposredan način teže da zaštite pravo na privatnost građana. Krivičnim zakonikom Republike Srbije predviđene su kazne za narušavanje nepovredivosti stana (član 139), protivzakonito pretresanje (član 140), povreda tajnosti pisma i drugih pošiljki (član 142), neovlašćeno prisluškivanje i snimanje (član 143), neovlašćeno fotografisanje (član 144), neovlašćeno prikupljanje ličnih podataka (član 146). Posebne mere tajnog prikupljanja podataka koje stoje na raspolaganju akterima bezbednosno-obaveštajnog sistema ozbiljno mogu da ugroze pravo na privatnost. Stoga, neophodno je razmisliti o načinu unapređenja trenutnog normativnog okvira kojima se reguliše način primene posebnih mera za tajno prikupljanje podataka. Problematične su odredbe zakona na osnovu kojih Bezbednosno-informativna agencija, Vojnobezbednosna agencija i policija mogu

da prošire primenu mera i na druga lica i sredstva komunikacije, jer kako bi pravo na privatnost zaista bilo zagarantovano neophodno je da se mere primenjuju prema tačno određenom licu i prema tačno određenim sredstvima komunikacije (Bećirović, 2017, str. 168). Navedeno „negativno utiče na buduće slučajeve tajnog nadzora komunikacije, jer se ne razvijaju mehanizmi za kritičko i objektivno razlikovanje nepotrebnog primenjivanja posebnih dokaznih radnji, čemu bi i te kako doprinelo učešće lica o čijoj privatnosti je reč u celoj proceduri“ (Kovačević, 2014, str. 178).

Zakon o Bezbednosno-informativnoj agenciji čini se da na nedovoljno jasan način definiše operativne metode, mere, radnje i operativno-tehnička sredstva koje Bezbednosno-informativna agencija može primeniti prilikom obavljanja poslova (Petrović, 2020v, str. 118). Ujedno, neophodno je detaljno definisati šta sve može podrazumevati „osnov sumnje“, prema kome, u kojim slučajevima i za koje pretnje se primenjuju posebne mere i uvesti obavezu da se obaveste lica koja su bila na merama, omogućiti im uvid u prikupljene podatke i regulisati način njihovog uništenja (Maričić i Živković, 2022, str. 6-7). U uporednoj perspektivi sa Zakonom koji reguliše rad vojnih agencija, Zakon o Bezbednosno-informativnoj agenciji je dosta kraći te se stiče utisak da u njemu postoji dosta pravnih praznina. Primena posebnih mera za tajno prikupljanje podataka zaista ozbiljno može da ugrozi privatnost građana jer u ove mere spadaju svi „oni načini prikupljanja podataka koji omogućavaju da se bez znanja osoba, grupa i/ili organizacija koji su predmet istrage prikupljaju podaci o njima“ (Petrović, 2020b, str. 23). Na osnovu zakona kojima se reguliše rad bezbednosno-obaveštajnog sistema, svi prikupljeni podaci primenom posebnih mera predstavljaju tajne podatke čime se zapravo „ograničava i pravo građanina na pravni lek“ (Bećirović, 2017, str. 170). Neophodno je zakonom urediti veću sudsku kontrolnu funkciju kako je to regulisano Zakonikom o krivičnom postupku. Posebne mere potrebno je dodatno regulisati na način da se u zakonodavstvu predvide kazne za njihovu nezakonitu i nepravilnu primenu i predvidi vremenski rok nakon čijeg isteka bi pojedinac bio obavešten da je bio predmet posebnih mera (Petrović, 2020v, str. 57-58). Ujedno, neophodno je definisati i šta se dešava sa prikupljenim materijalom.

Tajni nadzor predstavlja „nadgledanje i snimanje pojedinca, upotrebu skrivenih prislušnih uređaja i presretanje komunikacija“ (Ignjatović, 2015, str. 10). Kada je u pitanju nadzor i presretanje komunikacije u Republici Srbiji, čini se da Bezbednosno-informativna agencija ima primat u odnosu na vojne agencije i policiju. Stoga, neophodno je ustanoviti monitoring centar koji bi bio nezavistan od bezbednosno-obaveštajnih službi i to iz sledećih razloga: podaci o primeni mera službi bezbednosti bi se nalazili na jednom mestu; bezbednosno-obaveštajne službe bi imale ravnopravne mogućnosti čime bi se izbegla situacija u kojoj jedna služba ima primat i uvid u mere drugih bezbednosno-obaveštajnih službi i policije (Petrović, 2020v, str. 55). Primarna nadležnost nezavisnog monitoring centar bila bi tajni nadzor komunikacija i on bi delovao kao nezavisni posrednik između

sudova i službi bezbednosti (Petrović, 2020a, str. 5). Trenutni problemi kada je u pitanju tajni nadzor jesu sledeći: „nadziranje bez odluke suda i drugih osoba sa kojima je osoba koja je predmet mera u kontaktu; za presretanje komunikacije moguće je izbeći telekomunikacione operatere ako se za to koriste mobilni uređaji; mogućnost angažovanja privatnih aktera u ove svrhe; postavljanje na ove pozicije ljudi odanih partiji kako bi se mogli nadzirati kritičari vlasti“ (Petrović, 2020b, str. 51-52). Buduće zakonske modifikacije bi trebalo da obuhvate uvođenje obaveze o neprestanom vođenju evidencije o tajnom nadzoru komunikacija od strane bezbednosno-obaveštajnih službi, policije, sudova i drugih državnih institucija (Petrović, 2020a, str. 8). Kao određeni nedostaci trenutnog normativnog okvira koji postoji u Republici Srbiji mogu se navesti i: postojanje drugih ovlašćenja koja nisu obuhvaćena popisima posebnih postupaka i mera, složenost pravnog okvira, nedoslednost u određivanju posebnih postupaka i mera, razlike u postupcima za sudsko odobravanje, nedovoljna uređenost mehanizama za nadzor (Milosavljević, 2015, str. 28-30). Može se zaključiti da u Republici Srbiji postoji još prostora za preciznije uređenje primene posebnih mera za tajno prikupljanje podataka. Rezultat takvih eventualnih budućih zakonskih modifikacija bio bi čvršća zaštita prava na privatnost građana.

Tajni nadzor komunikacija podrazumeva „kako mere kojima se ostvaruje uvid u sadržaj komunikacija, tako i mere kojima se prikupljaju podaci o komunikaciji bez uvida u sam sadržaj (tzv. zadržani podaci)“ (Petrović i Đokić, 2017, str. 12). Zadržani podaci, na osnovu Zakona o elektronskim komunikacijama, jesu informacije o izvoru i odredištu komunikacije, vreme početka, trajanja i završetka komunikacije, vrsti komunikacije, terminalnoj opremi korisnika i njegovoj lokaciji“ (Zakon o elektronskim komunikacijama, 2010, član 129). Bezbednosno-informativna agencija i Vojnobezbednosna agencija mogu se obratiti operatoru kako bi pristupile zadržanim podacima. Obe strane su u obavezi da vode evidenciju o zahtevima za pristup zadržanim podacima u toku jedne kalendarske godine i da dostavljaju Povereniku za informacije od javnog značaja i zaštitu podataka o ličnosti evidenciju koja mora da sadrži broj upućenih zahteva, broj ispunjenih zahteva i vreme koje je proteklo od dana kad su podaci zadržani do dana kad je pristup podacima zatražen (Zakon o elektronskim komunikacijama, 2010, član 130a). Međutim, kada su u pitanju zadržani podaci problem se ispoljava u činjenici da osoba neće biti obaveštena da li je neka od bezbednosno-obaveštajnih službi pristupila zadržanim podacima (Pejić, 2014, str. 13). Neophodno je obezbediti pravo na privatnost pojedincima, a posebne postupke i mere posmatrati kao „kompromis između potrebe da se u konkretnoj situaciji zaštiti javni interes i opšteg pravila da državni organi u svakoj situaciji imaju obavezu da poštuju ljudska prava i slobode“ (Mirković, 2017, str. 90). U tom pravcu, adekvatan normativni okvir je prvi korak na tom putu.

Zaključak

Primena posebnih mera tajnog prikupljanja podataka uređena je normativnim okvirom Republike Srbije. Usled brojnih pravnih praznina i mogućnosti zloupotrebe, evidentno je da postoji još prostora za uređenje njihove primene kako bi se adekvatno zaštitilo pravo na privatnost građana Republike Srbije. Posebne mere tajnog prikupljanja podataka koje stoje na raspolaganju Bezbednosno-informativnoj agenciji i Vojnobezbednosnoj agenciji uređene su zakonima kojima se reguliše rad bezbednosno-obaveštajnog sistema, kao i Zakonikom o krivičnom postupku. Ovim zakonima neophodne su određene buduće modifikacije pri čemu zakonodavac može da se ugleda na odredbe Zakonika o krivičnom postupku. Prema Zakonu o Bezbednosno informativnoj agenciji i Zakonu o Vojnobezbednosnoj i Vojnoobaveštajnoj agenciji, sudska instanca koja odobrava primenu posebnih mera razlikuje se od slučaja do slučaja. Nejasno je zašto u slučaju Bezbednosno-informativne agencije primenu posebnih mera odobrava Viši sud u Beogradu, a u slučaju primene posebnih mera Vojnobezbednosne agencije nadležni Viši sud ili Vrhovni kasacioni sud. Ujedno, funkcija suda je svedena na odobravanje primene posebnih mera tajnog prikupljanja podataka. Stoga, neophodno je proširiti kontrolnu funkciju sudstva na period trajanja primene posebnih mera, kao i period nakon okončanja njihove primene kao što je to regulisano Zakonikom o krivičnom postupku. Podaci koji su prikupljeni primenom posebnih mera ne treba da predstavljaju tajne podatke, već je neophodno uvesti odredbu po kojoj bi bezbednosno-obaveštajne službe u određenim situacijama i nakon adekvatnog protoka vremena obavestile pojedinca koji je bio predmet mera. Zakonik o krivičnom postupku reguliše način postupanja sa informacijama koje su prikupljene primenom posebnih dokaznih radnji i ostavlja mogućnost da sudija za prethodni postupak obavesti lice prema kome je posebna dokazna radnja sprovedena. Izostanak takvih odredaba u trenutnim zakonima kojima se reguliše rad bezbednosno-obaveštajnog sistema navode na zaključak da pravo na privatnost svakog pojedinca može biti ugroženo. I pored dosadašnjih modifikacija zakonskih odredaba, neophodna je njihova buduća izmena kako primena posebnih mera tajnog prikupljanja podataka ne bi mogla da povredi pravo na privatnost građana Republike Srbije. Dodatno uređenje primene posebnih mera tajnog prikupljanja podataka bi pozitivno uticalo i na poverenje građana prema bezbednosno-obaveštajnom sistemu.

Literatura

1. Bećirović, E. (2017). Posebne dokazne radnje sa posebnim fokusom na tajni nadzor komunikacija. Pravne teme 5(10), 145-175.

2. Born H. (2007). Parliamentary and External Oversight of the Intelligence Services. In: Democratic Control of Intelligence Services (pp. 163-177). Routledge.
3. Beogradski centar za ljudska prava. (2023). Ljudska prava u Srbiji 2022. dostupno na web sajtu: https://www.bgcentar.org.rs/wp-content/uploads/2023/03/2023-04-24-Ljudska-prava-u-Srbiji-2022-web.pdf.
4. Dimitrijević, V., Popović, Papić, T., i Petrović, V. (2007). Međunarodno pravo ljudskih prava. Beograd: Dosije i Beogradski centar za ljudska prava.
5. Dimitrijević, P. (2011). Pravna regulacija elektronske komunikacije i pravo na privatnost. Zbornik radova Pravnog fakulteta Univerziteta u Istočnom Sarajevu, 199-211.
6. Zakon o Bezbednosno-informativnoj agenciji, Službeni glasnik RS, br. 42/2002, 111/2009, 65/2014 – odluka US, 66/2014, 36/2018.
7. Zakon o Vojnobezbednosnoj i Vojnoobaveštajnoj agenciji, Službeni glasnik RS, br. 88/2009, 55/2012 – odluka US i 17/2013.
8. Zakon o elektronskim komunikacijama, Službeni glasnik RS, br. 44/2010, 60/2013 – odluka US, 62/2014, 95/2018 – dr. zakon i 35/2023 – dr. zakon.
9. Zakon o zaštiti podataka o ličnosti, Službeni glasnik RS, br.87/2018.
10. Zakonik o krivičnom postupku, Službeni glasnik RS, br. 72/2011, 101/2011, 121/2012, 32/2013, 45/2013, 55/2014, 35/2019, 27/2021 – odluka US i 62/2021 – odluka US.
11. Ignjatović, D. (2015). Mere presretanja komunikacije i zadržavanja podataka iz perspektive Strazbura i propisa i prakse u Republici Srbiji. Beograd: Beogradski centar za bezbednosnu politiku.
12. Kovačević, M. (2014). Tajni nadzor komunikacije – usklađenost sa praksom Evropskog suda za ljudska prava. Anali Pravnog fakulteta u Beogradu, 62(2), 164-179.
13. Krivični zakonik, Službeni glasnik RS, br. 85/2005, 88/2005 - ispr., 107/2005 - ispr., 72/2009, 111/2009, 121/2012, 104/2013, 108/2014, 94/2016 i 35/2019.
14. Maričić, J. i Živković, D. (2022). Izlazak iz mraka: Primena posebnih mera Bezbednosno-informativne agencije u Srbiji. Beograd: Beogradski centar za bezbednosnu politiku.
15. Milosavljević, B. (2008). Ovlašćenje policije i drugih državnih organa za tajno prikupljanje podataka – domaći propisi i evropski standardi. U: Demokratski nadzor nad primenom posebnih ovlašćenja (str. 59-75). Beograd: Centar za civilno vojne odnose.
16. Milosavljević, B. (2015). Pravni okvir i praksa primene posebnih postupaka i mera za tajno prikupljanje podataka u Republici Srbiji. Beograd: Beogradski centar za bezbednosnu politiku.
17. Milošević, M., i Putnik, N. (2017). Sajber bezbednost i zaštita od visokotehnološkog kriminala u Republici Srbiji – strateški i pravni okvir. Kultura polisa, 33, 177-191.

18. Mirković, V. (2017). Sudska kontrola specijalnih istražnih mera službi bezbednosti u Republici Srbiji. NPB – Žurnal za kriminalistiku i pravo, 22(3), 89-105.
19. Odluka Ustavnog suda RS, IUz – 1218/2010, od 19.04.2012. godine, objavljena u Službenom glasniku RS, br. 88/09.
20. Odluka Ustavnog suda RS, IUz – 252/2002, od 26.12.2013. godine, objavljena u Službenom glasniku RS, br. 65/2014.
21. Pejić, J. (2014). Ko nas prisluškuje? – Kako funkcioniše presretanje elektronskih komunikacija i pristup zadržanim elektronskim podacima u Srbiji?. Beograd: Beogradski centar za bezbednosnu politiku.
22. Petrović, P. (2015). Posebne mere tajnog prikupljanja podataka: nadzor za vodič. Beograd: Beogradski centar za bezbednosnu politiku.
23. Petrović, P. (2020a). Ključne tačke reforme službi bezbednosti: iskustvo Srbije, Severne Makedonije i Crne Gore. Beograd: Beogradski centar za bezbednosnu politiku.
24. Petrović, P. (2020b). Anatomija zarobljavanja bezbednosno-obaveštajnog sektora u Srbiji. Beograd: Beogradski centar za bezbednosnu politiku.
25. Petrović, P. (2020v). Reforma službi bezbednosti u Srbiji 2000-2017. Doktorski rad. Beograd: Fakultet političkih nauka.
26. Petrović, P. i Đokić, K. (2017). Crne tačke reforme službi bezbednosti u Srbiji. Beograd: Beogradski centar za bezbednosnu politiku.
27. Ustav Republike Srbije, Službeni glasnik RS, br. 98/2006 i 115/2021.
28. Council of Europe, European Convention for the Protection of Human Rights and Fundamental Freedoms, 1950.

Datum prijema (Date received): 03.06.2024.
Datum prihvatanja (Date accepted): 17.07.2024.

THE RIGHT TO PRIVACY AND SPECIAL MEASURES OF SECRET DATA COLLECTION IN THE REPUBLIC OF SERBIA

Sanela Veljković[29], Milica Ćurčić[30], Marina Dabetić[31]

Abstract

The right to privacy represents one of the fundamental human rights of individuals in a democratic society. There are numerous international and regional instruments that guarantee the right to privacy. States are obligated to ensure unhindered enjoyment of this right to their population. Today, one of the greatest challenges of the right to privacy is special measures of secret data collection available to certain actors within the security-intelligence system and other state actors in the performance of their duties within their jurisdiction. It should be noted that the right to privacy is not absolute, and the law specifies how it can be limited. In the Republic of Serbia, derogation of the right to privacy is the subject of certain laws, especially those regulating the functioning of the security-intelligence system. Therefore, the paper analyzes the normative framework regulating special measures of secret data collection available to various actors within the security-intelligence system. Additionally, the analysis will encompass the normative provisions regulating the control of special measures of secret data collection. The paper aims to examine the negative impact of the implementation of special measures on the right to privacy, as well as the possibility of improving the current normative framework existing in the Republic of Serbia.

Keywords: *right to privacy, special measures of secret data collection, security-intelligence system, control*

[29] Sanela Veljković, Research Intern, Institute for Nuclear Sciences "Vinča" - Institute of National Importance for the Republic of Serbia, University of Belgrade, email: sanela.veljkovic@vin.bg.ac.rs ORCID 0009-0003-3650-290X

[30] dr Milica Ćurčić, Research Associate, Institute for Nuclear Sciences "Vinča" - Institute of National Importance for the Republic of Serbia, University of Belgrade, email: milica.curcic@vin.bg.ac.rs ORCID 0000-0002-4326-4036

[31] Marina Dabetić, Research Associate, Institute for Nuclear Sciences "Vinča" - Institute of National Importance for the Republic of Serbia, University of Belgrade, email: fmarina@vin.bg.ac.rs ORCID 0000-0003-0903-0110

The work was created within the framework of the scientific and research activities of the Institute for Nuclear Sciences "Vinča" - Institute of National Importance for the Republic of Serbia, funded by the Ministry of Science, Technological Development and Innovation, grant number 451-03-47/2023-01/200017.

Introduction

Enjoyment of the right to privacy must be ensured for individuals in a democratic society. The state should have an adequate normative framework that ensures the enjoyment of the right to privacy and that is meaningful and clear to every citizen. At the same time, the state should also provide adequate institutional mechanisms through which individuals can address relevant institutions if they believe that their right to privacy has been violated in any way. The right to privacy, although one of the fundamental human rights, is not absolute. It is possible to limit the enjoyment of this right to individuals in certain situations that should be clearly defined by legal provisions. The greatest challenge to the enjoyment of the right to privacy is represented by special measures of secret data collection that various state actors use when exercising their powers. Since the actors can be different, the names of these procedures and measures in legal solutions are also different. The subject of the analysis is the normative framework that regulates the application of special measures of secret data collection of the security and intelligence system of the Republic of Serbia. However, the Law on the Security and Information Agency and the Law on the Military Security and Military Intelligence Agency do not exhaust the list of procedures and measures that the aforementioned state actors have at their disposal, and it is therefore necessary to touch upon the Criminal Procedure Code. In recent years, certain provisions and parts of the current normative framework of the Republic of Serbia have undergone certain modifications in order to bring them into line with the Constitution. The paper seeks to examine the possibility of improving the normative framework regulating the regime of special measures of secret data collection. Therefore, the first part of the paper is dedicated to the right to privacy. The second part of the paper deals with specific measures of secret data collection that the actors of the security and intelligence system have at their disposal. The third part of the paper is dedicated to the control of the application of special measures of secret data collection, and in particular to judicial control. In the fourth part, possible problems that arise in the relationship between the right to privacy and special measures of secret data collection are presented, whereby the paper seeks to identify shortcomings that exist in the current legal provisions. At the very end, in addition to the conclusion, a list of literature and laws used in the preparation of the paper will be offered.

Right to privacy

One of the fundamental human rights is the right to privacy. The right to privacy does not refer to one specific right, but encompasses a wide range of rights, namely “the right to respect for private and family life, the right to respect for the inviolability of the home, the right to respect for the inviolability of

correspondence, and the right to respect for honour and reputation" (Dimitrijević et al., 2007, p. 203). At the international and regional level, the Universal Declaration of Human Rights from 1948, the Covenant on Civil and Political Rights from 1966, and the European Convention on Human Rights from 1950, guarantee the right to privacy. According to Article 8, paragraph 1 of the European Convention on Human Rights: "Everyone has the right to respect for his private and family life, his home and his correspondence" (European Convention for the Protection of Human Rights and Fundamental Freedoms, 1950). Paragraph 2 provides that: "a public authority shall not interfere with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others" (European Convention on Human Rights, 1950). Although the content of paragraph 2 suggests that the situations in which it is possible to restrict the right to privacy are numerous, in practice states cannot so easily restrict the right to privacy of their citizens.

In considering cases concerning violations of Article 8 of the European Convention on Human Rights, the European Court of Human Rights has established certain standards in the years that followed regarding the right to privacy. They can be summarized as follows: "1) cases of interference with the right to privacy must be regulated by law with sufficient clarity to be foreseeable; 2) such cases should be regulated restrictively and primarily relate to serious crimes and threats to security; 3) the procedure for applying measures is prescribed by law, and the application of measures should be decided by a court or other authority based on the existence of grounds for suspicion; 4) the beginning and duration of the measure is determined in a decision of a court or other authority, which also supervises the application of the measure; 5) the procedure for the protection of citizens should be prescribed by law and include the possibility of judicial protection, and the citizen should be informed of the measure upon his/her request when possible; and 6) the law should provide for sanctions for violating the rules on the application of such measures" (Milosavljević, 2015, p. 25). The importance of the European Court of Human Rights is reflected precisely in the possibility that an individual can turn to the court and sue his/her own state if he/she believes that any of the rights guaranteed by the European Convention on Human Rights have been denied or violated.

The right to privacy is not only regulated at the international and regional level, but is also subject to the constitutional and legal framework of states. Precisely because the right to privacy protects the following interests: "a) human interests in decision-making autonomy in intimate matters; b) the individual's interest in being protected from the disclosure of personal circumstances; c) the individual's interest in being protected from unfounded surveillance by the authorities"

(Dimitrijević, 2011, p. 203). The protection of the latter interest represents one of the most common problems in the state-individual relationship today. Therefore, it can be concluded that "the state has a double obligation: negative – to refrain from interfering with privacy and positive – to provide protection for the privacy of the individual and provide a legal framework and protection from attacks by other individuals" (Dimitrijević et al., 2007, p. 203). The Constitution of the Republic of Serbia, although it does not contain a specific provision on the right to privacy, guarantees inviolability of the home in Article 40, secrecy of letters and other means of communication in Article 41, and protection of personal data in Article 42. At the same time, it should be borne in mind that the Constitutional Court, in its decision 3238/1 from 2012, stated that the right to privacy is an integral part of constitutional law and falls under Article 23 of the Constitution, i.e. the right to dignity and free development of the personality (Belgrade Center for Human Rights, 2023, p. 94).

An indispensable part of the right to privacy is also the right to the protection of personal data. In the Republic of Serbia, a law was passed in 2008, which added responsibilities to the Commissioner for Information of Public Importance in the field of personal data protection. However, due to numerous shortcomings of the old legal solution, a new law was passed in 2018. Personal data is "any data relating to a natural person whose identity is determined or determinable, directly or indirectly, in particular on the basis of an identity marker, such as a name and identification number, location data, identifiers in electronic communications networks or one or more features of his or her physical, genetic, metal, economic, cultural and social identity" (Act on the Protection of Personal Data, 2018). The right to the protection of personal data and the right to privacy can be seriously threatened by special measures of secret data collection that the security and intelligence system has at its disposal when exercising its powers. The most common forms of interference with the privacy of citizens are secret surveillance and collection of data on individuals, their storage and publication (Ignjatović, 2015, p. 10). For this reason, an adequate normative framework is necessary that prescribes special measures, the manner of their implementation, and especially their control. The following part of the paper presents legal provisions relating to special measures of secret data collection by the Security and Information Agency, the Military Security Agency and the Military Intelligence Agency.

Special measures for secret data collection

Special procedures and measures represent "special authorizations of security and criminal prosecution authorities for secret data collection that exceptionally, for a certain period of time and without the knowledge of citizens, and based on a court decision and under the conditions prescribed by law, deviate from certain constitutionally guaranteed individual rights" (Milosavljević, 2015, p. 11). There are two groups of special measures for secret data collection. The first group

includes measures that do not significantly violate the human rights and freedoms of an individual, while the second group includes measures that temporarily and without the knowledge of an individual violate his or her human rights and freedoms, especially his or her right to privacy (Milosavljević, 2008). Special procedures and measures are not available only to actors in the security and intelligence system, but also to other state bodies such as the police, and it is necessary to make a distinction between them. Based on the purpose of data collection, all special procedures and measures are divided into two groups: 1) special procedures and measures aimed at conducting criminal proceedings, which are more closely regulated by the Criminal Procedure Code and the Police Act; 2) special procedures and measures aimed at preventive action to protect national security, which are regulated in more detail by the laws on the security and intelligence system (Milosavljević, 2007, pp. 59-60). Although different terms are used for special procedures and measures in different legal solutions, special procedures and measures available to the security and intelligence system authorities are not only subject to the Law on the Security and Intelligence Agency and the Law on the Military Security and Military Intelligence Agency, but also to the Criminal Procedure Code.

Based on the Criminal Procedure Code, the Security and Intelligence Agency and the Military Security Agency may apply special evidentiary measures. Special evidentiary measures are applied to a person for whom there is a basis for suspicion that he has committed a criminal offense or is preparing to commit it, and this cannot be detected, prevented or proven in any other way or would cause disproportionate difficulties or great danger (Criminal Procedure Code, 2011, Article 161). The Code prescribes the criminal offences for which special evidentiary actions may be applied, the manner of handling the collected material, the possibility of accidental discovery, and the confidentiality of data. As special evidentiary actions, the Code lists secret surveillance of communications, secret monitoring and recording, simultaneous operations, computer search of data, controlled delivery, and an undercover investigator. In addition to the police, the Security and Information Agency and the Military Security Agency may conduct secret surveillance of communications, secret monitoring and recording, simultaneous operations, and computer search of data. Based on the text of the Code, controlled delivery is conducted by the police, as well as other state bodies designated by the public prosecutor, which leaves room for actors of the security and intelligence system. An undercover investigator may be an authorized person of the police, the Security and Information Agency, and the Military Security Agency. The Code of Criminal Procedure regulates in more detail each of the special evidentiary actions, i.e. the conditions for implementation, the instance issuing the order, the course of implementation, the possibility of expansion, and the need to submit reports and collected materials.

The Law on the Security and Intelligence Agency regulates in more detail the manner of work, organization, control and other issues related to the Security and Intelligence Agency. The Agency may apply operational methods, measures and actions, as well as appropriate operational and technical means when performing tasks within its jurisdiction (Law on the Security and Intelligence Agency, 2002, Article 9). Special measures available to the Security and Intelligence Agency are: secret surveillance and recording of communications regardless of the form and technical means through which surveillance is carried out or of electronic or other addresses; secret surveillance and recording of communications in public places and places with restricted access or on premises; statistical electronic surveillance of communications and information systems in order to obtain data on communications or the location of mobile terminal equipment used; computer search of already processed personal and other data and their comparison with data collected through the application of other special measures (Law on the Security and Intelligence Agency, 2002, Article 13). Special measures are applied when there is a reasonable suspicion that a certain person, group or organization is preparing or undertaking actions directed against the security of the state, which could not be prevented or proven in any other way or would cause disproportionate difficulties or great danger (Law on the Security and Information Agency, 2002, Article 14). When deciding on the application of special measures, special consideration is given to whether the same result could be achieved in a manner that is less restrictive of human rights, to the extent necessary to satisfy the purpose of the restriction in a democratic society (Law on the Security and Information Agency, 2002, Article 14). The Director of the Security and Information Agency submits a proposal, which is decided by the President of the High Court in Belgrade, or a judge designated by him from among the judges assigned to the Special Department that deals with serious criminal cases, and the decision must be made within 48 hours. A special measure may last three months, and may be extended a maximum of three times for three months. Pursuant to Article 15b, the Security and Intelligence Agency has the possibility of expanding the application of special measures.

The special procedures and measures for secret data collection that the Military Security Agency has at its disposal are: operational penetration into organizations, groups and institutions; secret acquisition and purchase of documents and objects; secret inspection of data records; secret monitoring and surveillance of persons in open spaces and public places using technical means; secret electronic surveillance of telecommunications and information systems in order to collect retained data on telecommunications traffic, without insight into their content; secret recording and documentation of conversations in open and closed spaces using technical means; secret surveillance of the content of letters and other means of communication, including secret electronic surveillance of the content of telecommunications and information systems; secret surveillance and recording

of the interior of buildings, closed spaces and objects (Law on the Military Security and Military Intelligence Agency, 2009, Article 12). The application of the first four measures is decided by the director of the agency or a person authorized by him and they are applied as long as there are reasons for their application. The competent High Court shall decide on the application of the fifth measure within 8 hours. The Supreme Court of Cassation shall decide on the application of the sixth, seventh and eighth measures within 24 hours. The duration of the application of the other measures is six months with the possibility of an extension of another six months. The special procedures and measures for covert data collection that the Military Intelligence Agency has at its disposal are: covert cooperation for the purpose of collecting data; covert acquisition and purchase of documents and objects; operational penetration into organizations, institutions and groups; taking measures to conceal identity and property; establishing legal entities; covert use of property and services for a fee; use of special documents and means to protect the agency, its members, premises and assets. (Law on the Military Security and Military Intelligence Agency, 2009, Article 27). The above-mentioned procedures and measures are undertaken on the basis of a decision by the director of the agency or a person authorized by him.

Control of the implementation of special measures

The purpose of control of the security and intelligence system is to determine whether the security and intelligence system acts in accordance with the law, respecting guaranteed human rights while ensuring the greatest possible efficiency of the system (Born, 2007, p. 163). There are numerous controllers of the security and intelligence system. Control is primarily exercised by three branches of government. Although the security and intelligence system is part of the executive branch, the Government is one of the control instances. Control exercised by the National Assembly is manifested in several forms, with the work of the Committee for the Control of Security Services being the most significant. Judicial control is reflected in the approval of the implementation of special measures for secret data collection. At the same time, control is also exercised by independent state institutions, the most significant of which are the Protector of Citizens, the Commissioner for Information of Public Importance and Personal Data Protection, and the State Audit Institution. The control function can also be exercised by civil society, the public, and the media. Moreover, within the security and intelligence services themselves, there are also bodies responsible for internal control, which are actually “the first line of defense against illegal and improper conduct by security services” (Petrović, 2020v, p. 63).

There are two goals for which actors in the security and intelligence system may use special measures for the secret collection of data that infringe on human rights and freedoms. The first is the detection, investigation and documentation of serious crimes, and the second is preventive action (Petrović, 2020b, p. 21). The

former is governed by the Criminal Procedure Code, in which courts have a much greater control function, and the latter by the Law on the BIA and the Law on the VBA and VOA, in which the role of the court is reduced only to granting consent (Petrović, 2020b, p. 68). Based on the Criminal Procedure Code, the court makes a decision on whether the conditions for the application of certain special evidentiary measures have been met. During its implementation, the actor conducting it must submit daily reports together with the material collected. At the same time, after the completion of the application of the special evidentiary action, the actor who conducted the special evidentiary action must submit a special report, as well as all the collected material. On the other hand, according to the Law on the Security and Information Agency and the Law on the Military Security and Military Intelligence Agency, the data collected by applying some of the special measures constitute secret data. Therefore, judicial control under the Criminal Procedure Code includes all three phases of control, i.e. before, during and after the completion of the measures, and is therefore more comprehensive than the judicial control provided for by the laws on security and intelligence services, as it is limited to only the first phase (Petrović, 2015, p. 39).

The current normative framework regulating the application of special measures for secret data collection in the Republic of Serbia has undergone certain modifications in recent years (Milošević and Putnik, 2017). In 2013, the Constitutional Court dealt with the provisions of the Law on Electronic Communications, based on which operators were obliged to submit data on electronic communications in accordance with the laws regulating criminal procedure, the work of the security and intelligence system and the police (Decision of the Constitutional Court of the RS, case no. IUz-1245/2010). Given that the Constitution prescribes certain restrictions on the confidentiality of letters and other means of communication, these restrictions cannot be subject to different legal solutions. The Constitutional Court concluded that such provisions are not in accordance with the Constitution, which is why they were later amended. In subsequent years, certain provisions of the Law on the Security and Information Agency and the Law on the Military Security and Military Intelligence Agency were subject to consideration by the Constitutional Court. Referring to the confidentiality of letters and other means of communication, and in this case to the right guaranteed by the Constitution itself, the Constitutional Court decided that it is not possible for the director of a military agency to order the application of a special measure of secret electronic surveillance without the approval of a court instance (Decision of the Constitutional Court of the Republic of Serbia, IUz -1218/2010). The result of this decision of the Constitutional Court was a later modification of the legal provision in the direction that, upon the proposal of the director of the Military Security Agency, secret electronic surveillance is approved by a higher court. In order to protect human and minority rights, Articles 13, 14 and 15 of the Law on the Security and Information Agency

were also modified. The previous provisions of this law did not provide for criteria on the basis of which a person to whom special measures are applied would be determined, it was not stated what special measures could entail and what they relate to, which makes the law unclear and insufficiently precise, and subject to arbitrary interpretation (Decision of the Constitutional Court of the RS, case no. IUz-252/2002). Although these articles have been modified and clarified, certain provisions of the Law on the Security and Information Agency are still subject to criticism today. The legal modifications made so far were made in order to protect the right to privacy of citizens when applying special measures of secret data collection. However, it is necessary to analyze whether the right to privacy is adequately guaranteed by the existing normative framework. The following part of the paper presents possible problems related to the application of special measures, as well as the need to amend certain legal solutions.

Possible problems related to the implementation of special measures

In the Republic of Serbia, the right to privacy is guaranteed by the Constitution. Other legal acts also seek to protect the right to privacy of citizens, either directly or indirectly. The Criminal Code of the Republic of Serbia provides for penalties for violating the inviolability of a dwelling (Article 139), unlawful search (Article 140), violation of the confidentiality of letters and other mail (Article 142), unauthorized eavesdropping and recording (Article 143), unauthorized photography (Article 144), and unauthorized collection of personal data (Article 146). Special measures of covert data collection available to actors of the security and intelligence system can seriously jeopardize the right to privacy. Therefore, it is necessary to consider how to improve the current normative framework regulating the application of special measures for covert data collection. The provisions of the law on the basis of which the Security and Information Agency, the Military Security Agency and the police can extend the application of measures to other persons and means of communication are problematic, because in order for the right to privacy to be truly guaranteed, it is necessary for the measures to be applied to a precisely defined person and to precisely defined means of communication (Bećirović, 2017, p. 168). The above “negatively affects future cases of secret surveillance of communication, because mechanisms for critical and objective distinction of unnecessary application of special evidentiary actions are not developed, which would be greatly contributed to by the participation of the person whose privacy is at stake in the entire procedure” (Kovačević, 2014, p. 178).

The Law on the Security and Information Agency seems to define in a sufficiently clear manner the operational methods, measures, actions and operational-technical means that the Security and Information Agency can apply when performing its tasks (Petrović, 2020v, p. 118). At the same time, it is necessary to define in detail what "grounds for suspicion" may entail, according to whom, in which cases and

for which threats special measures are applied, and to introduce an obligation to notify persons who were subject to the measures, provide them with access to the collected data and regulate the method of their destruction (Maričić and Živković, 2022, pp. 6-7). In a comparative perspective with the Law regulating the work of military agencies, the Law on the Security and Information Agency is much shorter and one gets the impression that there are many legal gaps in it. The application of special measures for secret data collection can indeed seriously threaten the privacy of citizens, because these measures include all "those methods of data collection that allow data to be collected about persons, groups and/or organizations that are the subject of the investigation without their knowledge" (Petrović, 2020b, p. 23). Based on the laws regulating the operation of the security and intelligence system, all data collected through the application of special measures are classified data, which actually "limits the citizen's right to legal remedy" (Bećirović, 2017, p. 170). It is necessary to regulate by law a greater judicial control function as regulated by the Criminal Procedure Code. Special measures need to be further regulated in such a way that the legislation provides for penalties for their illegal and improper application and provides for a time limit after the expiry of which the individual would be informed that he or she was subject to special measures (Petrović, 2020v, pp. 57-58). At the same time, it is necessary to define what happens to the collected material.

Secret surveillance is "the monitoring and recording of an individual, the use of hidden listening devices and the interception of communications" (Ignjatović, 2015, p. 10). When it comes to surveillance and interception of communications in the Republic of Serbia, it seems that the Security and Information Agency has primacy over military agencies and the police. Therefore, it is necessary to establish a monitoring center that would be independent of the security and intelligence services for the following reasons: data on the implementation of security services measures would be located in one place; security and intelligence services would have equal opportunities, which would avoid a situation in which one service has primacy and insight into the measures of other security and intelligence services and the police (Petrović, 2020v, p. 55). The primary responsibility of an independent monitoring center would be secret surveillance of communications and it would act as an independent mediator between the courts and security services (Petrović, 2020a, p. 5). Current problems with secret surveillance include: "surveillance without a court order and of other persons with whom the person subject to the measures is in contact; it is possible to avoid telecommunications operators for interception of communications if mobile devices are used for this purpose; the possibility of engaging private actors for these purposes; the appointment of people loyal to the party in these positions in order to monitor critics of the government" (Petrović, 2020b, pp. 51-52). Future legal modifications should include the introduction of an obligation to continuously keep records of secret surveillance of communications by security

and intelligence services, police, courts and other state institutions (Petrović, 2020a, p. 8). Some of the shortcomings of the current normative framework in the Republic of Serbia include: the existence of other powers that are not included in the lists of special procedures and measures, the complexity of the legal framework, inconsistency in determining special procedures and measures, differences in procedures for court approval, insufficient regulation of supervision mechanisms (Milosavljević, 2015, pp. 28-30). It can be concluded that there is still room for more precise regulation of the application of special measures for secret data collection in the Republic of Serbia. The result of such possible future legal modifications would be stronger protection of the right to privacy of citizens.

Secret surveillance of communications includes "both measures that provide insight into the content of communications, and measures that collect data about communications without insight into the content itself (so-called retained data)" (Petrović and Đokić, 2017, p. 12). Retained data, according to the Law on Electronic Communications, is information about the source and destination of communication, the time of the beginning, duration and end of communication, the type of communication, the user's terminal equipment and its location" (Law on Electronic Communications, 2010, Article 129). The Security and Information Agency and the Military Security Agency may contact the operator to access the retained data. Both parties are obliged to keep records of requests for access to retained data during one calendar year and to submit to the Commissioner for Information of Public Importance and Personal Data Protection a record that must contain the number of requests made, the number of fulfilled requests and the time that has elapsed from the date the data was retained to the date access to the data was requested (Law on Electronic Communications, 2010, Article 130a). However, when it comes to retained data, the problem is manifested in the fact that a person will not be informed whether any of the security and intelligence services have accessed the retained data (Pejić, 2014, p. 13). It is necessary to ensure the right to privacy for individuals, and to view special procedures and measures as a "compromise between the need to protect the public interest in a specific situation and the general rule that state authorities have an obligation to respect human rights and freedoms in every situation" (Mirković, 2017, p. 90). In this regard, an adequate normative framework is the first step on that path.

Conclusion

The application of special measures of secret data collection is regulated by the normative framework of the Republic of Serbia. Due to numerous legal gaps and possibilities of abuse, it is evident that there is still room for regulating their application in order to adequately protect the right to privacy of citizens of the Republic of Serbia. Special measures of secret data collection available to the Security Intelligence Agency and the Military Security Agency are regulated by

the laws regulating the work of the security intelligence system, as well as by the Criminal Procedure Code. These laws require certain future modifications, whereby the legislator can take as an example the provisions of the Criminal Procedure Code. According to the Law on the Security Intelligence Agency and the Law on the Military Security and Military Intelligence Agency, the court instance that approves the application of special measures differs from case to case. It is unclear why in the case of the Security Intelligence Agency the application of special measures is approved by the High Court in Belgrade, and in the case of the application of special measures by the Military Security Agency, the competent High Court or the Supreme Court of Cassation. At the same time, the function of the court is reduced to approving the application of special measures of secret data collection. Therefore, it is necessary to expand the control function of the judiciary to the period of application of special measures, as well as the period after their completion, as regulated by the Criminal Procedure Code. Data collected through the application of special measures should not represent secret data, but it is necessary to introduce a provision according to which the security and intelligence services would, in certain situations and after an adequate period of time, inform the individual who was the subject of the measures. The Criminal Procedure Code regulates the manner of handling information collected through the application of special evidentiary measures and leaves the possibility for the pre-trial judge to inform the person against whom the special evidentiary measure was carried out. The absence of such provisions in the current laws regulating the operation of the security and intelligence system leads to the conclusion that the right to privacy of each individual may be threatened. Despite the modifications of the legal provisions to date, their future amendment is necessary so that the application of special measures of secret data collection could not violate the right to privacy of citizens of the Republic of Serbia. Additional regulation of the implementation of special measures for secret data collection would also have a positive impact on citizens' trust in the security and intelligence system.

References

1. Bećirović, E. (2017). Posebne dokazne radnje sa posebnim fokusom na tajni nadzor komunikacija. Pravne teme 5(10), 145-175.
2. Born H. (2007). Parliamentary and External Oversight of the Intelligence Services. In: Democratic Control of Intelligence Services, 163-177.
3. Belgrade Center for Human Rights. (2023). Human Rights in Serbia 2022. https://www.bgcentar.org.rs/wp-content/uploads/2023/03/2023-04-24-Ljudska-prava-u-Srbiji-2022-web.pdf.
4. Dimitrijević, V., Popović, Papić, T. & Petrović, V. (2007). Međunarodno pravo ljudskih prava. Beograd: Dosije i Beogradski centar za ljudska prava.

5. Dimitrijević, P. (2011). Pravna regulacija elektronske komunikacije i pravo na privatnost. Zbornik radova Pravnog fakulteta Univerziteta u Istočnom Sarajevu, 199-211.
6. Law on Security and Information Agency, Official Gazette of the Republic of Serbia, No. 42/2002, 111/2009, 65/2014 – decision of the Constitutional Court, 66/2014, 36/2018.
7. Law on Military Security and Military Intelligence Agency, Official Gazette of the Republic of Serbia, No. 88/2009, 55/2012 – decision of the Constitutional Court and 17/2013.
8. Law on Electronic Communications, Official Gazette of the Republic of Serbia, No. 44/2010, 60/2013 – decision of the Constitutional Court, 62/2014, 95/2018 – other law and 35/2023 – other law.
9. Law on the Protection of Personal Data, Official Gazette of the Republic of Serbia, No. 87/2018.
10. Criminal Procedure Code, Official Gazette of the Republic of Serbia, No. 72/2011, 101/2011, 121/2012, 32/2013, 45/2013, 55/2014, 35/2019, 27/2021 – decision of the Constitutional Court and 62/2021 – decision of the Constitutional Court.
11. Ignjatović, D. (2015). Mere presretanja komunikacije i zadržavanja podataka iz perspektive Strazbura i propisa i prakse u Republici Srbiji. Beograd: Beogradski centar za bezbednosnu politiku.
12. Kovačević, M. (2014). Tajni nadzor komunikacije – usklađenost sa praksom Evropskog suda za ljudska prava. Anali Pravnog fakulteta u Beogradu, 62(2), 164-179.
13. Criminal Code, Official Gazette of the Republic of Serbia, No. 85/2005, 88/2005 - corrigendum, 107/2005 - corrigendum, 72/2009, 111/2009, 121/2012, 104/2013, 108/2014, 94/2016 and 35/2019.
14. Maričić, J. i Živković, D. (2022). Izlazak iz mraka: Primena posebnih mera Bezbednosno-informativne agencije u Srbiji. Beograd: Beogradski centar za bezbednosnu politiku.
15. Milosavljević, B. (2008). Ovlašćenje policije i drugih državnih organa za tajno prikupljanje podataka – domaći propisi i evropski standardi. U: Demokratski nadzor nad primenom posebnih ovlašćenja, 59-75.
16. Milosavljević, B. (2015). Pravni okvir i praksa primene posebnih postupaka i mera za tajno prikupljanje podataka u Republici Srbiji. Beograd: Beogradski centar za bezbednosnu politiku.
17. Milošević, M. & Putnik, N. (2017). Sajber bezbednost i zaštita od visokotehnološkog kriminala u Republici Srbiji – strateški i pravni okvir. Kultura polisa, 33, 177-191.
18. Mirković, V. (2017). Sudska kontrola specijalnih istražnih mera službi bezbednosti u Republici Srbiji. NPB – Žurnal za kriminalistiku i pravo, 22(3), 89-105.

19. Decision of the Constitutional Court of the Republic of Serbia, IUz – 1218/2010, dated 19.04.2012., published in the Official Gazette of the Republic of Serbia, No. 88/09.
20. Decision of the Constitutional Court of the Republic of Serbia, IUz – 252/2002, dated 26.12.2013., published in the Official Gazette of the Republic of Serbia, No. 65/2014.
21. Pejić, J. (2014). Ko nas prisluškuje? – Kako funkcioniše presretanje elektronskih komunikacija i pristup zadržanim elektronskim podacima u Srbiji?. Beograd: Beogradski centar za bezbednosnu politiku.
22. Petrović, P. (2015). Posebne mere tajnog prikupljanja podataka: nadzor za vodič. Beograd: Beogradski centar za bezbednosnu politiku.
23. Petrović, P. (2020a). Ključne tačke reforme službi bezbednosti: iskustvo Srbije, Severne Makedonije i Crne Gore. Beograd: Beogradski centar za bezbednosnu politiku.
24. Petrović, P. (2020b). Anatomija zarobljavanja bezbednosno-obaveštajnog sektora u Srbiji. Beograd: Beogradski centar za bezbednosnu politiku.
25. Petrović, P. (2020v). Reforma službi bezbednosti u Srbiji 2000-2017. Doktorski rad. Beograd: Fakultet političkih nauka.
26. Petrović, P. i Đokić, K. (2017). Crne tačke reforme službi bezbednosti u Srbiji. Beograd: Beogradski centar za bezbednosnu politiku.
27. Constitution of the Republic of Serbia, Official Gazette of the RS, No. 98/2006 and 115/2021.
28. Council of Europe, European Convention for the Protection of Human Rights and Fundamental Freedoms, 1950.