UDK: 621.39:351.86(497.11)
656.8

Stručni rad
Rad je primljen/ Received:14.10.2021;
Korigovan/revised: 11.12.2021.
Prihvaćen/ Accepted: 20.02.2022.

BEZBEDNOSNI ASPEKTI TELEKOMUNIKACIONOG I POŠTANSKOG SAOBRAĆAJA U REPUBLICI SRBIJI

Ratomir Antonović[1]
Fakultetu za pravo, bezbednost i menadžment
"Konstantin Veliki", Niš,
Univerziteta Union Nikola Tesla Beograd
Anđela Marčetić[2]
Poljoprivredni fakultet Univerziteta u Beogradu
JEL: *G24, G32*

Sažetak: *Pitanje bezbednosti je aktuelno u svim sferama života. Tajnost lične telefonske, elektronske i drugih vidova komunikacije svakom savremenom čoveku danas predstavljaju imperativ. O svakom licu se naviše može saznati prodiranjem u njegovu intimnu sferu, do koje se najefikasnije stiže kroz njegovu komunikaciju sa drugim licima. Takođe, uvek je pitanje tajnosti telekomunikacionog i poštanskog saobraćaja bilo značajno, i to kako za korisnike ovih usluga, tako i za državu i pravni poredak, koji se stavljao u funkciju zaštite tajnosti telekomunikacionog i poštanskog saobraćaja. U radu autor predstavlja pozitivnu legislativu i zakonska rešenja u oblasti zaštite tajnosti telekomunikacionog i poštanskog saobraćaja, kao i zabeležene vidove njihove zloupotrebe u praksi. Takođe, poseban osvrt se daje na dozvoljene oblike presretanja telekomunikacionog i poštanskog saobraćaja u cilju zaštite viših interesa.*

Ključne reči: *pošiljka, telefon, internet, elektronska pošta, zaštita, presretanje*

Uvod

Nepovredivost tajnosti pisama i drugih sredstava komuniciranja je ustavna kategorija u Republici Srbiji. Član 41. Ustava Sr-

[1] antonovicr@gmail.com, https://oricid.org/0000-0001-9134-6346
[2] andjea marcetic13@gmail.com; https://oricid.org/0000-0001-5133-4623

bije[3] jamči svakom građaninu Republike Srbije pravo na nepovredivost tajnosti pisama i drugih sredstava komuniciranja, osim u slučajevima kad za to postoji validna odluka suda u cilju vođenja krivičnog postupka ili zaštite bezbednosti Republike Srbije. Taj postupak narušavanja nepovredivosti tajnosti pisama i drugih sredstava komuniciranja se mora odvijati u skladu sa zakonom i u precizno utvrđenom vremenskom okviru.

Ovakvim stavom, ustavopisac u Srbiji je zaštitio jedno od ličnih prava građana koje svakom garantuje pravo na privatnost. Međutim, iako načelno štiti ljudska i građanska prava, pozitivni Ustav Srbije u sebi nije u celosti reprodukovao sve garancije iz člana 8. Evropske konvencije o ljudskim pravima.[4]

Sledstveno ovakvoj ustavnoj garanciji, zaštita nepovredivosti tajnosti pisama i drugih sredstava komuniciranja je predmet regulisanja zakonskih akata u Republici Srbiji. Tako, Krivični zakonik Republike Srbije[5] u Glavi XIV „Krivična dela protiv sloboda i prava čoveka i građanina“, u članu 142. predviđa krivično delo povrede tajnosti pisama i drugih pošiljki. Biće ovog krivičnog dela se sastoji u neovlašćenom otvaranju tuđeg pisma, telegrama ili bilo kog zatvorenog pismena ili pošiljke i time se povredi tajnost istog. Takođe, ovo krivično delo vrši i ono lice koje neovlašćeno zadrži ili prikrije, uništi ili pismo preda nekom drugom licu ili ko povredi tajnost elektronske pošiljke, kao i nekog

[3] “Službeni glasnik RS“ broj 98/2006.

[4] Koju je ratifikovala Državna zajednica SCG 2003. godine donošenjem Zakona o ratifikaciji evropske Konvencije o ljudskim pravima i osnovnim slobodama, izmenjene u skladu sa protokolom broj 11 protokola uz Konvenciju o zaštiti ljudskih prava i osnovnih sloboda, protokola broj 4 uz Konvenciju za zaštitu ljudskih prava i sloboda kojima se obezbeđuju izvesna prava i slobode u koje nisu uključeni u Konvenciju i prvi protokol uz nju, protokola broj 6 uz Konvenciju o zaštiti ljudskih prava i osnovnih sloboda o ukidanju smrtne kazne, protokola broj 7 uz Konvenciju o zaštiti ljudskih prava i osnovnih sloboda, protokola broj 12 uz Konvencije o zaštiti ljudskih prava i osnovnih sloboda i protokola broj 13 uz Konvenciju o zaštiti ljudskih prava i osnovnih sloboda o ukidanju smrtne kazne u svim okolnostima („Službeni list SCG“ broj 9/2003, 5/2005, 7/2005 i „Službeni glasnik RS – Međunarodni ugovori“ broj 12/2010 i 10/2015).

[5] “Službeni glasnik RS“ broj 85/2005, 88/2005, 107/2005, 72/2009, 111/2009, 121/2012, 104/2013, 108/2014, 94/2016 i 35/2019.

drugog sredstva komunikacije. I samo saopštavanje sadržine tuđeg pisma ili telegrama ili sadržine elektronske pošte je način izvršenja ovog krivičnog dela. Posebno je predviđen stav u navedenom članu Zakonika koji se odnosi na službeno lice u vršenju službene dužnosti. Predviđene sankcije za izvršene oblike ovog krivičnog dela se kreću u rasponu od šest meseci do tri godine kazne zatvora, alternativno sa novčanim kaznama, čiju visinu zakonodavac nije definisao.

Zakon o poštanskim uslugama[6] definiše načelo nepovredivosti tajnosti pisama i drugih sredstava opštenja kao jedno od osnovnih načela rada poštanske službe u Republici Srbiji. Ovo načelo se realizuje tako što se od poštanskih operatora očekuje da prilikom prijema pisama strogo vode računa da ne povrede njihovu tajnost. Do narušavanja tajnosti dolazi ukoliko operator pismeno uruči neovlašćenom licu, ukoliko na neovlašćen način dođe do saznavanja sadržine poštanske pošiljke ili ga neovlašćeno zadrži. Takođe, ukoliko nekom neovlašćenom licu saopšti sadržaj pošiljke ili da informaciju o njenom primaocu ili pošiljaocu, operator je narušio tajnost pošiljke.

Samo pakovanje poštanske pošiljke mora biti takvo da čuva njenu tajnost. Pakovanje pošiljaka je predmet zakonskih akata, kao i Pravilnika o opštim uslovima za obavljanje poštanskih usluga[7] koji nalažu da se pošiljka mora tako upakovati da niko ne može neovlašćeno da se upozna sa njenim sadržajem.

Kad se govori o nepovredivosti tajnosti sredstava komunikacije, tu se svakako misli i na telekomunikacioni saobraćaj, kao i elektronske vidove komunikacije, putem interneta i elektronske pošte, koji danas postaju sve zastupljeniji.

Nadzor i presretanje telekomunikacionog saobraćaja

Iako Ustav i svi pozitivni zakoni u Republici Srbiji jasno stoje na stanovištu da je zagarantovana tajnost lične komunikacije, bilo pisane, bilo verbalne, u praksi ipak postoje slučajevi legalnog nadzora i presretanja telekomunikacionog saobraćaja. Reč je o vrlo delikatnom postupku koji je na granici između zakonitog prikup-ljanja operativnih informacija od opšteg značaja i grubog naruša-vanja ljudskih i

[6] „Službeni glasnik RS“ broj 77/2019.
[7] “Službeni glasnik RS“ broj 24/2010 i 58/2010.

građanskih prava i sloboda. Upravo zato, čitav postupak nadzora i presretanja mora biti preduzet strogo po pravima definisanim zakonom i podzakonskim aktima. Ne sme se ostaviti ni malo prostora na osnovu kog bi se moglo sumnjati u legalnost prime-ne ove mere, kao ni prostor za potencijalne zloupotrebe informacija do kojih se došlo kroz nadzor i presretanje telekomunikacionog sao-braćaja. Takođe, ovde se otvara uvek aktuelno pitanje pretežnosti javnog u odnosu na privatni interes i pravo i pretežnosti zaštitnog ob-jekta javne odnosno privatne sfere.

Nadzor i presretanje telekomunikacionog saobraćaja se u narodu naziva prisluškivanje telefona. Smatra se posebnom metodom uz pomoć koje nadležni državni organi tajno prikuplja podatke u krivičnom postupku za ona krivična dela koja mogu narušiti nacionalnu bezbednost. Posebnost ove metode se ogleda prevashodno u činjenici da je na prvi pogled u koliziji sa Ustavom Republike Srbije, kao najvišim pravnim aktom države. Međutim, i sam ustavopisac je predvideo kad i pod kojim okolnostima se zajamčena ljudska prava mogu derogirati, te se od organa koji ovu metodu primenjuju zahteva samo strogo poštovanje propisane forme postupka.

Nadzor i presretanje se odnosi na sve vidove komunikacije: praćenje pisama i pošiljaka, telefonskih razgovora, SMS poruka, govornih i video poruka, kao i elektronske pošte. Prisluškivanje telefonskih razgovora može ići simultano, u periodu trajanja telefonskog razgovora ili isti može biti sniman, pa naknadno slušan. Tom prilikom se vrši obavezna identifikacija učesnika u razgovoru, primaoca i pošiljaoca poziva, kao i poruka.

Da postupak nadzora i praćenja telekomunikacionog saobraćaja ne bi dobio karakter nedozvoljene radnje, mora se ispoštovati zakonom definisana procedura. Demokratska i otvorena društva su vrlo osetljiva na ovakve pojave, pa je zato postupak nadzora i praćenja strogo formalizovan. Za početak, pravo da sprovode ove mere imaju samo policijski i vojnobezbednosni organi, unutar kojih ove radnje sprovodi specijalizovan i uzan krug zaposlenih. U okviru organa unutrašnjih poslova u Republici Srbiji, ovi poslovi su povereni Službi za specijalne istražne metode pri Upravi kriminalističke policije, koja jedino može da sprovodi posebne dokazne radnje upotrebom specijalnih istražnih tehnika u cilju obezbeđenja dokaza i rasvetljavanja krivičnih dela. Kad se govori o vojnobezbednosnim orga-

nima, ove specijalne istražne metode vodi Vojna policija, odnosno Kriminalističko-istražna grupa (Živanović, 2018, 290-292).

Predmet ovakve opservacije može biti lice za koje se osnovano sumnja da je izvršilo ili planira da izvrši teško krivično delo iz nadležnosti tužilaštava za organizovani kriminal, ratne zločine i visokotehnološkog kriminala.[8] Potom, kod sumnje da je izvršilo ili planira da izvrši krivično delo kojim bi narušilo ustavni poredak Republike Srbije, kao i krivična dela teškog ubistva, razbojništva, otmice, dečje pornografije ili svojim radnjama i aktivnosti nastoji da osujeti rasvetljavanje ovih teških krivičnih dela.

Dakle, da bi se obezbedila zakonitost ove metode, neophodno je da se ona sprovodi u cilju zaštite najvažnijih vrednosti, kao što su nacionalna bezbednost, ustavni poredak, ljudski životi i tome slično. Ukoliko to nije slučaj, ne bi postojalo opravdanje za primenu metode nadzora i praćenja telekomunikacionog saobraćaja i drugih vidova komunikacije.[9]

Sudska odluka o presretanju i nadzoru saobraćaja

Da bi postupak nadzora i presretanja telekomunikacionog saobraćaja bio legalan i ispunjavao sve zakonom propisane elemente, za primenu ove metode mora postojati sudska odluka. Sud je jedini nadležan za donošenje odluke o primeni ove mere, međutim sudskoj odluci mora prethoditi jasno definisan predlog javnog tužioca ili nadležnih policijskih organa. Upravo ova uslovljenost na relaciji zahtev – odluka daju celom postupku dodatnu legitimnost, jer sam postupak nadzora i presretanja ne može biti rezultat proizvoljnosti ili greške jednog organa. Nema sudske odluke bez zahteva tužilaštva ili poli-

[8] U korpusu navedenih tužilaštava konkretno se ubrajaju sledeća krivična dela: trgovina narkoticima, oružjem i ljudima; zloupotreba službenog položaja; primanje i davanje mita; falsifikovanje novca, pranje novca; trgovina uticajem; oružana pobuna; terorizam i finansiranje terorizma; zločin u vreme oružanih sukoba; računarska prevara i sabotaža; neovlašćen pristup zaštićenom računarskom programu i slična.

[9] Minimalna zatvorska kazna predviđena KZ Republike Srbije je četiri godine da bi se metoda nadzora i praćenja komunikacije mogla sprovoditi. Za dela za koja je zaprećena kazna zatvora u vremenskom trajanju kraćem od četiri godine, primena ove metode nije dopuštena.

cije, niti se ova metoda može realizovati ako za nju ne postoji izričita sudska odluka.

U zavisnosti od vrste postupka, definisano je ko može biti zvanični predlagač sudu za donošenje odluke o realizaciji ove mere. Ta-ko, u krivičnim postupcima mere nadzora i presretanja može zahtevati jedino javni tužilac, a odluku donosi sudija za prethodni postupak.

U slučajevima kad je neophodno lišavanje slobode osumnjičenog lica, predlog dostavlja direktor policije, a odluku donosi predsednik Vrhovnog kasacionog suda. U postupcima zaštite nacionalne bezbednosti, predlog se upućuje od strane direktora BIA ili VBA, dok odluku donosi predsednik Višeg suda ili sudija posebnog odeljenja tog suda.

Sadržina predloga o nadzoru i presretanju telekomunikacionog saobraćaja je strogo formalna. Predlog mora biti jasno i precizno definisan, obrazložen i potkrepljen činjenicama. Stoga, predlog neophodno u sebi mora sadržati identifikacione podatke o licu nad kojim se sprovodi mera nadzora i presretanja telekomunikacionog saobraćaja, navođenje osnova sumnje zbog kog se predlaže sprovođenje ove mere, broj telefona, podatke o elektronskoj i drugoj pošti koje lice za kog se mera predlaže koristi, mora se dati informacija kako će se sam postupak prisluškivanja obaviti u praksi, kao i vremenski okvir u kom će se mera sprovoditi.

Rok u kom sud mora da odluči po predlogu je različit u zavisnosti od toga ko je predlagač. Kad predlog potiče od direktora policije i VBA, odluka mora biti donesena u roku od 24 časa od trenutka dostavljanja predloga, dok je taj rok 48 sati kad predlog potpisuje direktor BIA. Rokovi su promptni jer okolnosti samog slučaja često zahtevaju hitnost u postupanju i ne dopuštaju velika čekanja i odlaganja. Sa druge strane, iako bi po pravilu trebalo sačekati zvaničnu odluku suda, u izuzetno hitnim situacijama se sa primenom mere nadzora i presretanja telekomunikacionog saobraćaja može otpočeti i pre formalnog odobrenja suda, uz naknadno pribavljanje sudske odluke. Podrazumeva se da bi ovakve situacije trebalo da budu vanredne i da se primenjuju samo onda kad je to neophodno usled hitnosti same mere i njene realizacije. Međutim, osnovano se može postaviti pitanje da li se postojanje ove mogućnosti može javiti kao potencijalni mehanizam zloupotrebe, te ko ceni hitnost i neophodnost primene mere u odnosu na određeno lice i da li se ovim zapravo

pokušava minimizovati značaj i uloga suda kao korektivnog faktora postupka legalnosti procesne radnje prisluškivanja. Rokovi od 24, odnosno 48 časova nisu dugački, te se postavlja pitanje šta može biti toliko urgentno da ne može da sačeka protek i ovako kratkih i efikasnih rokova.

Upravo zbog osnovanosti navedenih primedbi, od direktora policije, koji nalaže primenu ove mere bez zvanične sudske odluke se zahteva da usmenim putem o tome izvesti sud i postupajućeg sudiju, koji sa merom i njenom primenom mora biti upoznat i saglasan. Time se obezbeđuje minimum uključenosti suda u proces prisluškivanja lica i bez zvanične odluke, uz ostavljanje mogućnosti da, ukoliko odluka bude negativna zbog nedovoljne obrazloženosti ili osnovanosti predloga, se postupak prisluškivanja istog trenutka obustavi. Podaci do kojih se došlo do trenutka obustave moraju biti izbrisani i ne smeju biti korišćeni u daljem postupku.

Postupak nadzora i presretanja saobraćaja

U ovom delu izlaganja, autor se neće baviti tehničkim i tehnološkim metodama realizacije postupka nadzora i presretanja svih vidova saobraćaja, već normativnim postupkom, definisanim pravnim aktima.

Na samom početku postupka nadzora i presretanja, nadležni organ je dužan da utvrdi sve vidove i kanale komunikacije koje koristi opservirano lice. Svi telefonski brojevi, elektronska i obična pošta moraju biti obuhvaćeni predlogom za praćenje i presretanje. Oni kanali komunikacije koji predlogom nisu obuhvaćeni, ne mogu biti predmet praćenja i presretanja, odnosno, oni za koje se sazna naknadno mogu biti podvrgnuti ovom postupku, ali uz prethodno podnesen predlog za širenje sredstava komunikacije koje će biti predmet postupka i dobijanja naknadne, ili dopunske odluke suda. Rok za donošenje dopunske odluke je 48 sati od trenutka dostavljanja predloga nadležnom sudu (Pejić, 2019, 28-30).

Vremenski okvir za trajanje ove mere je eksplicitan i ne može da traje duže od jedne kalendarske godine, dakle 12 meseci. Svakako, ako je za nadzorom i presretanjem saobraćaja prestala potreba ranije, usled obezbeđenja dovoljnog broja dokaza i ukoliko je otklonjena

opasnost po nacionalnu bezbednost, sa primenom ove mere će se prestati ranije.

Svrha nadzora i presretanja telekomunikacionog saobraćaja je pribavljanje dokaznog materijala protiv lica čiji saobraćaj je nadziran i presretan. Da bi pribavljeni dokazni materijal bio upotrebljiv, uslov je da se do njega došlo zakonitim putem. O legalnosti ove mere je već bilo reči, a u globalu, zakonitost se utvrđuje na osnovu poštovanja forme, počev od postupka predlaganja, odobravanja i same realizacije mere. Ukoliko se dokaže da je mera sprovedena nezakonito, bez poštovanja forme i zakonom propisane procedure ili da je mera sprovođena u druge, a ne svrhe za koje se prikazuje, dokazni materijal se ne može uzeti u razmatranje niti može biti korišćen protiv okrivljenog.

Prilikom postupka primene mere nadzora i presretanja telekomunikacionog, kao i drugih vidova saobraćaja, može doći do saznavanja činjenica koje se ne odnose samo na opservirano lice i potencijalno krivično delo za koje se ono tereti. Te novootkrivene činjenice se mogu ticati samo teških krivičnih dela za koja se odobrava primena ove mere, dok saznanja koja se odnose na ona krivična dela za koja se ne može dopustiti primena nadzora i presretanja, ne mogu biti uzeta u razmatranje i operativni rad.

Pored novih krivičnih dela, primenom mere nadzora i presretanja se može proširiti krug osumnjičenih potencijalnih počinilaca krivičnih dela. Pretežno se kod ovih krivičnih dela radi o teškim delima koja se izvršavaju u saizvršilaštvu ili od strane organizovane kriminalne grupe, te se kroz nadzor i presretanje komunikacije lako može doći do ostalih članova grupe i saizvršilaca.

Dokazni materijal do kojeg se došlo primenom ove mere se strogo čuva i prezentuje samo ukoliko dođe do pokretanja krivičnog postupka. Ukoliko se postupak ne pokrene, dokazi do kojih se došlo primenom mere nadzora i presretanja se uništavaju u roku od šest meseci od trenutka njihovog nastanka. To je ujedno i rok u kom se javni tužilac mora izjasniti da li je zainteresovan za ovaj dokazni materijal. U slučaju njegovog neizjašnjenja ili negativnog izjašnjenja, ovaj dokazni materijal se uništava, a o tome rešenje donosi nadležni sud (Ilik i dr. 2020, 52).

Materijali do kojih se došlo radnjom nadzora i presretanja koji imaju karakter dokaza protiv okrivljenog postaju sastavni deo sudskog

spisa krivičnog predmeta. Rokovi čuvanja ovih spisa su uređeni Sudskim poslovnikom[10], koji u svom članu 241. definiše rokove čuvanja, u zavisnosti od vrste samog predmeta. Tako na primer, spisi predmeta u stvarno-pravnim predmetima, stečajnim predmetima i krivičnim predmetima sa izrečenom kaznom zatvora u trajanju dužem od deset godina se čuvaju trideset godina. U krivično-pravnim predmetima u kojima je izrečena kazna zatvora u vremenskom trajanju do deset godina, spisi se čuvaju dvadeset godina. U krivično-pravnim predmetima u kojima je izrečena kazna zatvora do tri godine, spisi se čuvaju pet godina. U slučaju obustave krivičnog postupka, spisi predmeta se čuvaju dve godine. Spisi koji se odnose na platne naloge se čuvaju pet godina, kao i spisi u izvršnim postupcima i spisi iz drugostepenih postupaka. Spisi upravnih predmeta se čuvaju do deset godina.

Iz navedene odredbe sledi koliko će se dokazni materijal prikupljen primenom mere nadzora i presretanja telekomunikacionog saobraćaja dugo čuvati i biti dostupni nadležnim organima. Svi predmeti se čuvaju u sudskim arhivama, koje su obično u sastavu sudskih pisarnica. Sa druge strane, organi policije imaju pravo da trajno čuvaju podatke do kojih su došli tokom istražnog postupka. Za stručnu javnost je nepoznanica koliko dugo se čuvaju podaci do kojih su došli BIA i VBA usled nedovoljne transparentnosti podzakonskih akata ovih službi. Svakako da se upravo u tome otvara polje sumnje šta se radi sa ovim delikatnim podacima, koliko se bezbedno oni čuvaju i u kom vremenskom periodu. Tajnost postupaka u radu ovih službi je razumljiva ako se u obzir uzme značaj njihovog rada za nacionalnu bezbednost i sigurnost države i građana. Međutim, podatak o sudbini dokaznog materijala koji se obezbedio u istražnom postupku ne bi bio od takvog značaja i karaktera da bi ugrozio rad ovih službi, ali bi u velikoj meri otklonio sumnju koja za sad opravdano postoji na strani stručne i laičke javnosti u Srbiji (Ninčić, 2014, 89-102).

Podaci dobijeni putem mere nadzora i presretanja telefonske komunikacije se čuvaju tonski i u transkriptu. Čuvaju se kao tajna u posebnim sigurnosnim omotima, dok materijali koji se odnose na najteža krivična dela čuvaju u posebnim prostorijama i njima mogu

[10] "Službeni glasnik RS" broj 110/2009, 70/2011, 19/2012, 89/2013, 96/2015, 104/2015, 113/2015, 39/2016, 56/2016, 77/2016, 16/2018, 78/2018, 43/2019 i 93/2019.

pristupiti samo ovlašćena lica. Podaci koji su javno saopšteni u krivičnom postupku gube karakter tajnosti, ali se lični podaci koji se odnose na određena lica i dalje čuvaju kao tajna. Cirkulacija i razmena ovih informacije je jedino dopuštena između nadležnih državnih organa, kao i inostranih organa koji rade na suzbijanju organizovanog kriminala i terorizma na međunarodnom nivou.

Mere nadzora

Kao što je već naglašeno, u procesu primene mere nadzora i presretanja telekomunikacionog saobraćaja, uloga suda je od posebne važnosti. Osim što za njenu primenu mora postojati sudska odluka, na sudovima je i nadzor nad njenom primenom. Pored sudskih organa, pravo na nadzor imaju i nezavisne institucije poput Zaštitnika građana, Poverenika za informacije od javnog značaja, ali i Narodne skupštine kao najviše predstavničke zakonodavne vlasti. Kada se govori o internoj kontroli, tada ove mere sprovode organi unutrašnje kontrole pri Ministarstvu unutrašnjih poslova, koji postupaju kao korektivni faktor unutar sistema unutrašnjih poslova.

O realizaciji mere presretanja komunikacionih kanala se isključivo vodi pisana evidencija, koja predstavlja strogo čuvanu poslovnu tajnu. Ta pisana evidencija sadrži zahtev tužilaštva za primenu mere nadzora i presretanja saobraćaja, kao i odobrenje suda za primenu ove mere. Evidencija ima svoj broj pod kojim se vodi, datum dostave predloga, ime predlagača i sudije koji je doneo pozitivno rešenja, vrsta krivičnog dela za koje se primena mere traži, sudski nalog, nalog za produženje ili prekid mere, datum dostave izveštaja i sadržaja o sprovedenoj meri, rešenje o uništenju i datum kad je uništenje ovog materijala realizovano.

U ovom procesu značajno mesto zauzimaju telefonski i internet provajderi, koji obezbeđuju da se podatak o prisluškivanju sačuva u sistemu kao neizbrisiv trag. To se čini u cilju obezbeđenja mogućnosti uporedbe sa drugim evidencijama koje se vode kod ovlašćenih lica za realizaciju ove mere, kao i sudskih nadležnih organa.

Uloga suda kao korektivnog faktora u primeni ove mere je najvažnija. Kao što je više puta istaknuto, primena ove mere je direktno uslovljena dobijanjem sudske saglasnosti u vidu odluke o primeni ove mere. Bez sudske odluke nije moguće sprovoditi presretanje tele-

komunikacionog saobraćaja. Osim toga, sud ima pravo da nadzire primenu mere uz pravo da na dnevnom nivou od nadležnog organa koji presretanje obavlja zahteva izveštaje o samom postupku. Takođe, na sudu je najvažniji zadatak – ocena validnosti podataka prikupljenih ovom metodom. Uz ocenu, sud raspolaže relevantnim podacima koji se odnose na to ko je i po čijem nalogu sprovodio postupak nadzora i presretanja saobraćaja, raspolaže snimcima i pošiljkama kao i informacije u kom vremenskom periodu se nad opserviranim licem mera nadzora sprovodila. Ukoliko je bio širi krug nadziranih lica, daje se njihov spisak, kao i primena svih tehničkih metoda korišćenih tom prilikom. Uvidom u sve navedeno, sud daje konačnu ocenu svrsishodnosti, ali i validnosti materijala do kog se došlo primenom ove metode. Ukoliko je došlo do bitnih proceduralnih grešaka koje bi mogle da dovedu u pitanje zakonitost celog postupka, sudija je dužan da naredi uništavanje dokaza koji su na takav način pribavljeni. U takvim situacijama, sud obavezno mora pokrenuti pitanje odgovornosti onih koji nisu poštovali procedure i zbog čije greške je ceo postupak bio nelegalan i time doveo do ugrožavanja prava prisluškivanog lica.

Pored suda, čija uloga je u ovom postupku dominantna, Zaštitnik građana takođe može postupati u funkciji nadzora po prijavi građana (Reljanović, 2017, 271). Njegov zadatak je zaštita ljudskih i građanskih prava, te njegovo postupanje mora ići u tom pravcu. Zaštitnik u postupku nadzora mora dobiti sve značajne informacije, kao i državne tajne. Njegov nadzor se može vršiti kako po okončanju primene mere, tako i u vreme njenog trajanja. U slučaju da Zaštitnik konstatuje postojanje određenih nepravilnosti, o tome mora izvestiti organ uz izricanje preporuke za otklanjanje nepravilnosti. Rok za otklanjanje propusta je dva meseca od trenutka dostavljanja obaveštenja Zaštitnika. O otklonjenim nepravilnostima, nadležni organ je dužan da izvesti Zaštitnika. U onim situacijama kad se nepravilnost ne otkloni i odbija se saradnja sa Zaštitnikom, on može izreći i javnu opomenu i dati predlog za razrešenje direktora policije, BIA i VBA uz pokretanje disciplinskog postupka protiv zaposlenih koji su prisluškivanje vršili. Ukoliko se naknadno utvrdi da je u njihovom postupanju bilo elemenata krivičnog dela, može se protiv zaposlenih pokrenuti i krivični postupak.

Poverenik za informacije od javnog značaja ima kontrolnu funkciju, koja se ogleda u proveri zaštite ličnih podataka procesiranih

lica, kao i trećih lica do čijih podataka su došli u postupku prisluškivanja. Poverenik se stara o fizičkom obezbeđenju podataka o licima, proverava da li se do njih može doći neovlašćenim pristupom, kontroliše način njihove obrade u smislu da se koriste samo u onoj meri koja je najneophodnija, da se ne koriste u druge svrhe za koje ne postoji odobrenje, kao i da se podaci ne čuvaju duže od zakonom propisanog roka.

Poverenik ima posredničku ulogu između građana i organa koji prisluškivanje sprovode. Lice koje sumnja da se njegov telekomunikacioni saobraćaj prati, može se obratiti Povereniku za informacije od javnog značaja, koji od nadležnih organa može zahtevati tu vrstu informacije da mu dostavi. Međutim, s obzirom na tajnost postupka prisluškivanja i njegov karakter, Poverenik ne sme opserviranom licu podatak da li se njegov saobraćaj presreće da učini dostupnim, jer se time obesmišljava čitav postupak. Ta informacija se može licu saopštiti jedino ukoliko Poverenik ustanovi da se ceo postupak sprovodio nezakonito.

Kod nezakonitog primenjivanja ove mere, Poverenik za informacije od javnog značaja može da nadležnom organu izrekne opomenu i da zahteva da se lica čija su prava narušena o tome izvesti. On može izreći zabranu daljeg prisluškivanja, da zahteva brisanje podataka do kojih se nelegalno došlo, kao i da zabrani dalju distribuciju tih podataka, što u zemlji, što van nje. Nadležni organ, kao i službeno lice koje je prekoračilo svoja ovlašćenja mogu biti i novčano kažnjeni.[11]

Nadzornu funkciju u odnosu na primenu mere nadzora i presretanja telekomunikacionog saobraćaja ima i Narodna skupština Republike Srbije. Ovaj organ državne vlasti nadzor vrši preko svog stalnog Odbora za odbranu i unutrašnje poslove, kao i Odbora za kontrolu službi bezbednosti. Ovim odborima su organi unutrašnjih poslova dužni da dostavljaju redovne izveštaje, kao i izveštaje o prisluškivanjima, koji mogu i posebno biti zahtevani. Uloga članova ovih odbora nije da direktno impliciraju u postupku primene mere, već da se bave eventualnim sistemskim greškama i izradi boljih propisa koji bi regulisali ovu materiju. Kod krupnijih propusta u radu i primeni

[11] Kazna za nadležni organ se kreće u rasponu od 50 hiljada do dva miliona dinara, a za odgovorno lice od 5 do 20 hiljada dinara.

mere, Narodna skupština raspolaže mogućnošću formiranja anketnih odbora koji bi podrobno istraživali sve propuste i utvrđivali odgovornost nadležnih.

Privatnost elektronske pošte

U periodu sve intenzivnijeg razvoja visokotehnološkog kriminala, teško je govoriti o sigurnosti elektronske pošte. Neovlašćeni upadi u meiling liste, slanje neovlašćene elektronske pošte i prodor u istu, postali su svakodnevica. Na meti sajber kriminala se nalaze ne samo pojedinci i fizička lica, već i ozbiljne kompanije, ali i čitave države. Cilj ovog prodiranja u elektronsku poštu je sticanje lične imovinske koristi zloupotrebom važnih podataka, potom određene ucene, kao i destabilizacija bezbednosti mnogih velikih državnih sistema. Dakle, lepeza interesa, kao i samih napadača u svetu savremene elektronske komunikacije je vrlo široka i uključuje u sebi kako pojedinačne napadače, poznate pod nazivom hakeri, tako i čitave organizacije koje uglavnom imaju karakter terorističkih organizacija ili organizovanih kriminalnih grupa (Tobias i dr. 2012, 89-90).

Sposobnost savremene tehnologije i mogućnosti njene zloupotrebe nastaju sve intenzivnije zbog umrežavanja tehnologije i stvaranja moćne internet mreže. Grupe koje rade na presretanju elektronske komunikacije postaju sve rasprostranjenije i drskije u svom radu, te organizovano vrše kompjuterske diverzije na visokoprofesionalnom i tehnološki visokom nivou. Opseg njihovog delovanja je izrazito širok i nije vezan za geografska i nacionalna ograničenja, već se posredstvom interneta omogućuje da se radnja sajber krivičnog dela vrši u jednoj, a posledica te radnje da nastupa u drugoj državi. Neretko se ne radi o dve različite države, već i o dva različita kontinenta.

Radnje koje se mogu uspešno realizovati zloupotrebom savremene tehnologije su raznovrsne i mogu biti oličene u upadu u kompjuterske mreže, industrijskoj špijunaži, softverskoj pirateriji, dečjoj pornografiji, napadu na elektronsku poštu, otkrivanju lozinki, nedozvoljenom upadu u memoriju tuđeg računara, krađu podataka i tome slično. Među najopasnije oblike sajber kriminala se ubrajaju sabotaža, špijunaža, terorizam, ratovanje i hakovanje.

Sa aspekta same bezbednosti elektronske pošte, od posebnog značaja je sajber špijunaža. Suština špijunaže se ogleda u otkrivanju strogo čuvanih tajni, njihovom odavanju i predaji neovlašćenim licima, a sami strogo čuvani podaci mogu biti policijskog, vojnog, političkog, ekonomskog ili nekog drugog karaktera od vitalne važnosti za funkcionisanje države. Sajber špijunaža je relativno nov oblik izvršavanja radnje ovog dela i koristi se uz pomoć internet mreže, kao i specijalnih programa, koji imaju karakter virusa koji se ilegalno ubacuju u programe velikih kompjuterskih sistema.[12]

Podaci na meti sajber špijuna su podaci od vitalne važnosti za funkcionisanje država, velikih sistema, kompanija, vojske i policije, političkih organizacija, ali i pojedinaca koji su, iz nekog razloga interesantni sajber špijunima. Iz dosadašnje prakse, kroz špijuniranje elektronske pošte, dolazilo se uglavnom do ovih osetljivih podataka, kao što su poslovni planovi, pregovarački planovi, poslovni ugovori, ali i lični podaci koji su potom bili najčešće zloupotrebljavani.

Svi oblici neovlašćenog i nasilnog pristupa kompjuterskim sistemima se nazivaju hakovanjem, koje je zapravo preduslov za bilo koju drugu nedozvoljenu radnju iz oblasti sajber kriminala (Spalević i dr. 2013, 888-889). Hakovanjem se narušava kompjuterski sistem, uklanjaju potencijalni mehanizmi zaštite[13] i neovlašćeno se pristupa informacijama koje su pohranjene u tuđem računaru i bazi podataka. Hakovanje se može vršiti na velikim sistemskim računarima velikih državnih ili privatnih sistema, a može se vršiti i u odnosu na personalne računare individualnih korisnika. Hakeri vrlo precizno i brižljivo planiraju svoje akcije, bez prava i na najmanju grešku. Njihov rad karakteriše navalentan pristup štićenim računarskim sistemima, uz prisustvo nasilnih metoda otklanjanja zaštitnih lozinki i drugih zaštitnih mehanizama. Takođe, njihov rad karakteriše upad u tuđ računarski sistem, zloupotreba i operisanje sa tuđim bazama podataka i značajnim informacijama (Čisar, 2017, 37).

Ono što značajno otežava suzbijanje hakerstva u savremenim uslovima jeste velika fizička udaljenost hakera i objekta njihovog napada. Hakerstvo se može odvijati i na nekoliko hiljada kilometara

[12] To su programi poput: RAT; Keyloger, trojanski konj i tome slično.

[13] Provaljivanjem zaštitnih lozinki na primer ili uklanjanjem određenih zaštitnih barijera.

udaljenosti, jer fizičko prisustvo nije potrebno da bi se ušlo u štićene baze podataka. Takođe, hakerski napad u sticaju sadrži elemente više krivičnih dela, kao što su špijunaža, prevare, pronevere, kompjuterske sabotaže, oštećenje tuđeg računara i tome slično (Antonović i dr. 2019, 292-293). Hakeri mogu biti kako usamljeni pojedinci, koji rade svoj posao individualno, a mogu biti i deo organizovane kriminalne grupe koja se bavi isključivo hakerstvom i sajber kriminalom (Ugren, 2012, 10-11).

Prodor u tuđe kompjuterske baze podataka se vrši uvek sa određenom namerom, koja je pretežno lukrativne prirode. Ako se prodor vrši radi nekog višeg političkog ili vojnog interesa, kao i radi narušavanja bezbednosti određene države, onda se javlja tzv. sajber terorizam. Sajber terorizam poput ostalih oblika terorizma, ima za cilj sejanje straha i nesigurnosti, samo se kod ovog oblika terorizma ne može govoriti o strahu za ljudski život, ali se može govoriti o vrlo opravdanom strahu za bezbednost nacije, naročito u eri apsolutne digitalizacije i kompjuterizacije, kad svaki sistem funkcioniše uz pomoć savremenih kompjuterskih programa.

Sajber terorizam se može realizovati zloupotrebom interneta, u cilju plasiranja i propagiranja određene terorističke ideologije, pridobijanja što većeg broja pristalica, ali i finansijera. Savremena kompjuterska tehnologija pripadnicima terorističke grupacije značajno olakšava u preciznom planiranju terorističkih napada i njihovoj realizaciji. Kao najopasniji oblik zloupotrebe računara, javlja se neovlašćeni pristup strogo čuvanim državnim tajnama, što u realnom životu može izazvati posledice neslućenih razmera.

Ovde takođe treba napomenuti da u sajber svetu mogu da se vode čitavi virtuelni ratovi, sa vojnim kompjuterskim sistemima, sistemima državne uprave, sistemima za kontrolu vazdušnog i železničkog saobraćaja, komunalnim sistemima i ostalim vitalnim sistemima kao metama napada. Ratovanje se može voditi i kroz plasiranje netačnih informacija, polutačnih informacija i iznošenje informacija koje za cilj imaju da u narodu stvore osećaj straha, nesigurnosti i panike.

Kad se govori o prodoru u elektronsku poštu, kao i druge oblike elektronske komunikacije, tad se akcenat stavlja na sajber prevare, kod kojih se određeno lice dovodi u određeno stanje zab-lude, sa ciljem da se od njega dobiju značajne informacije, koje potom mogu biti

zloupotrebljene. Dovođenje u stanje zablude se vrši kroz lažno predstavljanje, iznošenje netačnih činjenica i podataka, zloupotreba nečije samilosti ili teškog psihološkog stanja, usamlje-nosti, nedovoljne mentalne zrelosti ili pak potrebe za upoznavanjem srodne duše.

Zaključak

Pitanje bezbednosti i zaštite ljudskih i građanskih prava predstavljaju supstancijalna pitanja od vitalnog značaja u periodu savremene komunikacije i telefonskog i poštanskog saobraćaja. Tema rada je usklađenost interesa ličnih prava pojedinca u odnosu na pretežne interese zaštite nacionalne bezbednosti i ustavnog poretka Republike Srbije.

Daje se prikaz najpre ustavnih i zakonskih garantija po pitanju zaštite tajnosti lične komunikacije, kako verbalne, tako i pisane. Međutim, daje se i prikaz mogućnosti ograničavanja ovih ustavnih garantija i zakonskih odredbi u strogo zakonom predviđenim okolnostima i uz strogo poštovanje formalnih procedura. Kao što je i u radu navedeno, rigorozan je postupak presretanja i nadzora telekomunikacionog saobraćaja fizičkih lica, kao i postupak obrade i korišćenja podataka do kojih se primenom ovih metoda došlo.

Iako je svako presretanje i nadzor telekomunikacionog saobraćaja, strogo formalno gledano, vrsta kršenja osnovnih ljudskih prava, jasno je da za time postoji nedvosmislena potreba i ujedno opravdanje. Velika opasnost koja se primenom mera nadzora i presretanja javlja jesu potencijalne zloupotrebe do kojih uvek može doći. Zato su potrebni strogi mehanizmi nadzora nad primenom ovih mera kako bi se svaki, i najblaži oblik zloupotreba u samom početku sasekao. Odgovornost u slučajevima zloupotrebe nije samo na organu koji je meru realizovao, već i na pojedincu, koji je u ime i za račun organa postupao, kao i na njegovom neposredno nadređenom koji je njegov rad morao nadzirati. Takođe, oštećeni građanin uvek ima pravo na krivičnu i materijalnu zaštitu i obeštećenje.

Sa druge strane, pored ovlašćenog nadzora i presretanja lanca komunikacije, javlja se i neovlašćeno prodiranje u strogo čuvane i zaštićene baze podataka, naročito u periodu digitalne ere, kad savremena tehnika dopušta mogućnosti koje ranije nisu bile dostupne.

Konkretno, misli se na sajber kriminal i pripadnike tzv. hakerskih bandi, koje neovlašćeno prodiru u čuvane baze podataka, ali ujedno narušavaju privatnost i fizičkim licima, prodorom u njihove personalne računare, elektronsku poštu, društvene mreže i ostale vidove komunikacije.

Dok je kod legalnog, od strane suda dopuštenog nadzora i presretanja komunikacije, cilj pribavljanje dokaznog materijala, kod nelegalnog je cilj sticanje lične koristi ili narušavanje vitalnih društvenih vrednosti, kao što su red, mir, ekonomska sigurnost, bezbednost građana, ustavni poredak i tome slično.

Ono što se nameće kao generalni zaključak je da je u eri savremene tehnologije mnogo teže sačuvati privatnost od različitih oblika i vidova njenog narušavanja. Za početak, treba krenuti od rasprostranjenih mogućnosti tonskog i vizuelnog snimanja upotrebom pametnih mobilnih telefona, dostupnih svakome. Potom, da su svi veći gradovi pokriveni sistemom video nadzora, koji snimaju sve značajnije saobraćajnice, ulice, parkove, trgove i druga mesta na kojima se okuplja veći broj ljudi. Takođe, internet mreža daje mogućnost plasmana velikog broja sadržaja, koji uključuju lične podatke, fotografije i druge značajne informacije o određenim licima, često i bez njihovog znanja i saglasnosti, što može da dovede do ozbiljnog narušavanja privatnosti tih lica.

Dakle, tajnost telekomunikacionog, poštanskog i drugih vidova saobraćaja se može narušavati legalnim i ilegalnim putem. U prvom slučaju se to čini radi zaštite viših interesa, a u drugom radi sticanja lične koristi i nekog drugog nezakonitog cilja.

Literatura i izvori

1. Antonović, R; Bejatović, G. (2019) "Ličnost izvršilaca visokotehnoloških krivičnih dela", *Pravo i digitalne tehnologije,* Pravnički dani prof. dr Slavko Carić, Privredna akademija, Novi Sad.
2. Čisar, P. (2017) „Opšti aspekti aplikativne IT bezbednosti", *NBP časopis Policijske akademije,* god. 22, broj 2.
3. Ilik, G; Tilovska-Kechegi, E; Gjorhoski, N. (2020) "Constitutinalization of the individual liberty as a human right in the US Political System", International Scientific Conference "Towards a

Better Future: Human Rights, Organized Crime and Digital Society", Faculty of Law - Kicevo, University "St. Climent Ohridski".
4. Krivični zakonik RS ("Službeni glasnik RS" broj 85/2005, 88/2005, 107/2005, 72/2009, 111/2009, 121/2012, 104/2013, 108/2014, 94/2016 i 35/2019).
5. Ninčić, Ž. (2014) „Nadzor komunikacija kao mera procesne prinude, *Bezbjednost - Policija - Građani*, godina 10, broj 1-2, Banjaluka.
6. Pejić, J. (2019) *Moja prava u slučaju (ne)zakonitog prisluškivanja,* Komitet pravnika za ljudska prava YUCOM, Beogradski centar za bezbednosnu politiku, Beograd.
7. Reljanović, M. (2017) "Zaštitnik građana (ombudsman) u pravnom sistemu Republike Srbije: normativni i praktični detalji", *Ombudsmani za ljudska prava u BiH: bilans jednog neuspjeha,* Sarajevo.
8. Spalević, Ž; Banović, B; Vrhovšek, M. (2013) *Cyber crime in states of Western Balcan,* TTM, Sarajevo, BiH.
9. Tobias, K; Berman, L. (2012) *Privacy : management, legal issues, and security aspects,* Nova Science Publishers, New York.
10. Ugren, V. (2012) *Cyber criminal,* Univerzitet Singidunum, Departman za postdiplomske studije i međunarodnu saradnju, Beograd.
11. Ustav Republike Srbije („Službeni glasnik RS" broj 89/2006).
12. Zakon o poštaniskim uslugama („Službeni glasnik RS" broj 77/2019)
13. Živanović, K. (2018) „Posebna dokazna radnja tajnog nadzora komunikacije", *NBP časopis Policijske akademije,* god. 23, br. 3.

SECURITY ASPECTS OF TELECOMMUNICATIONS AND POSTAL TRAFFIC IN THE REPUBLIC OF SERBIA

Abstract: *The issue of security is topical in all spheres of life. The secrecy of personal telephone, electronic and other forms of communication is an imperative for every modern man today. The most can be learned about each person by penetrating his intimate sphere, which is most effectively*

reached through his communication with other persons. Also, the issue of secrecy of telecommunication and postal traffic has always been important, both for the users of these services, and for the state and the legal order, which was put in the function of protecting the secrecy of telecommunication and postal traffic .In this paper, the author presents positive legislation and legal solutions in the field of protection of secrecy of telecommunications and postal traffic, as well as the recorded types of their abuse in practice. Also, special attention is given to the permitted forms of interception of telecommunication and postal traffic in order to protect higher interests.

Keywords: *shipment, telephone, internet, e-mail, protection, interception.*

Kako citirati ovaj članak/how to cite this article:

Antonović R., Marčetić A., (2021) Bezbednosni aspekti telekomunikacionog i poštanskog saobraćaja u Republici Srbiji. *Horizonti menadžmenta*. II(1), 183-201.