

Spremljanje mednarodnih sistemov zvez kot domnevni poseg v komunikacijsko zasebnost posameznika v povezavi s teritorialnim principom varovanja te pravice

Primož Britovšek

Povzetek:

Namen prispevka:

Avtor v prispevku obravnava številna pravna in dejanska vprašanja v zvezi z ustavnostjo 21. člena ZSOVA, o čemer se tudi v javnosti, zlasti v zadnjem času, sprožajo številni dvomi. Gre za ureditev »spremljanja mednarodnih sistemov zvez«, ki ga pri svojem delu uporablja Slovenska obveščevalno-varnostna agencija in tudi Obveščevalno varnostna služba Ministrstva za obrambo. Avtor želi v zvezi s tem razjasniti različna stališča in pomisleke, ki se pojavljajo v zvezi z domnevnimi, nedovoljenimi posegi v komunikacijsko zasebnost, v povezavi s teritorialnim principom varovanja teh pravic.

Metodologija:

S primerjalno pravno metodo nemške ureditve neosredotočenega nadzora, po kateri se je pri sprejemanju ZSOVA zgledoval predlagatelj, kot tudi z metodo analize pravnih dokumentov v katerih svoja stališča, do opredeljenih pravnih vprašanj, izražajo priznani pravni strokovnjaki s področja ustavnega prava, avtor ob uporabi sklepanja iz splošnega na posamično, po t.i. deduktivni metodi, prihaja do določenih ugotovitev.

Ugotovitve:

»Spremljanje mednarodnih sistemov zvez« t.i. strateški oziroma neosredotočen nadzor bi bilo v prihodnje, zaradi razvoja številnih možnosti prikritega nadzora, s katerimi je mogoče poseči v zasebnost konkretnih posameznikov, potrebno ločiti na osredotočen in neosredotočen nadzor. S tem v zvezi tudi varstvo pravic posameznikov tako tistih, ki prebivajo na območju R Slovenije ali zunaj nje, z določitvijo ustreznih kriterijev dopustnosti posegov v zasebnost, oblikovanih ob smiselnem razumevanju ustavnih določb.

Omejitve:

Avtor se je v prispevku omejil na obravnavo določb, ki v ZSOVA urejajo področje »spremljanja mednarodnih sistemov zvez« in nadzorovanje ter snemanje telekomunikacij v R Sloveniji.

Izvirnost:

Pri svojih ugotovitvah avtor prihaja do zaključkov, da bi morebitna nova oziroma spremenjena, dopolnjena, normativna ureditev področja »spremljanja mednarodnih sistemov zvez« v ZSOVA, lahko ob povečanih nadzornih mehanizmih ponudila možnost razširitve uporabe takšne oblike nadzora tudi v R Sloveniji.

Ključne besede: spremljanje mednarodnih sistemov zvez, neosredotočen nadzor, osredotočen nadzor, komunikacijska zasebnost, razumno pričakovanje zasebnosti, teritorialni princip

1 UVODNA BESEDA

V zadnjem času lahko v javnosti zasledimo številna pravna in dejanska vprašanja v zvezi z dopustnostjo posegov oziroma omejevanjem pravice do komunikacijske zasebnosti posameznika. Najpogosteje v tej zvezi zasledimo termin »spremljanje mednarodnih sistemov zvez«, ukrep, katerega v zvezi s svojim delom uporablja Slovenska obveščevalno-varnostna agencija, kot tudi Obveščevalno varnostna služba Ministrstva za obrambo. Nenazadnje je tudi Ustavno sodišče RS s sklepom št. U-I-216/07-8 z dne 4.10.2007 odločalo o zahtevi za oceno ustavnosti prvega odstavka 21. člena Zakona o Slovenski obveščevalno-varnostni agenciji, ki v normativnem smislu ureja »spremljanje mednarodnih sistemov zvez«, začeti na pobudo predsednika Vrhovnega sodišča, da je izpodbijana določba v neskladju z drugim odstavkom 37. člena Ustave RS. V tej zvezi je tudi Informacijska pooblaščenka na Ustavno sodišče RS naslovila zahtevo za oceno ustavnosti prvega, drugega in tretjega odstavka 21. člena ZSOVA, ki ureja »spremljanje mednarodnih sistemov zvez«.

Ker gre za pomembna pravna in dejanska vprašanja v zvezi z izvajanjem »spremljanja mednarodnih sistemov zvez« pri čemer se domnevno posega v komunikacijsko zasebnost posameznika bom poskusil v nadaljevanju predstaviti določene poglede in dileme v zvezi z uporabo tega ukrepa.

2 STRATEŠKI OBVEŠČEVALNI NADZOR

Ali lahko trdimo, da gre pri izvajanju ukrepa »spremljanje mednarodnih sistemov zvez« za strateški nadzor? Odgovor na to vprašanje je povezan s številnimi pomisleki in izraža dileme, saj gre v praksi še vedno za pravno neopredeljeno definicijo pojma »spremljanje mednarodnih sistemov zvez«. Nikjer ni definirano kaj takšno spremljanje zajema. Dodatno zmedo pa povzroča prav tako nedefiniran pojem »mednarodni sistem zvez«, ki ne določa: kje se nadzor izvaja oziroma kje je mesto telekomunikacijskega priključka in mesto priklopa.

»Spremljanje mednarodnih sistemov zvez« ureja 21. člen ZSOVA v zvezi z 2. in 20. členom. Opredeljuje ga kot posebno obliko pridobivanja podatkov iz tujine pomembnih za zagotavljanje varnostnih, političnih in gospodarskih interesov države ali o organizacijah, skupinah in osebah, ki s svojo dejavnostjo iz tujine ali v povezavi s tujino ogrožajo ali bi lahko ogrozile nacionalno varnost države in njeno ustavno ureditev, ob upoštevanju, da ne gre za določljiv priključek ali posameznika na območju R Slovenije. Njegovo uporabo dovoljuje direktor Agencije z odredbo v kateri določi način, obseg in trajanje izvajanja ukrepa. Nadalje ga opredeljuje kot zadevo in se ne nanaša na konkretnega posameznika.

Na podlagi slednjega lahko torej upravičeno sklepamo, da gre pri »spremljanju mednarodnih sistemov zvez« za strateški nadzor telekomunikacij, kar lahko opišemo kot preventivno in proaktivno zajemanje podatkov v tujini ali iz tujine, kjer še ni lociran konkreten posameznik. Gre torej za neke vrste preventivno zajemanje določene vrste komunikacij ob vključevanju mednarodnega elementa z namenom iskanja relevantnih informacij s pomočjo uporabe informacijske tehnologije, preko nabora t. i. iskalnih parametrov, ki hkrati ne smejo vsebovati identifikacijskih znakov z namenom zajemanja komunikacij z določljivega komunikacijskega priključka ali za določljivega posameznika v R Sloveniji. Biti morajo v skladu z zadevo, zaradi katere je bila odredjena ta posebna oblika pridobivanja podatkov.

Kot izhaja iz razvida zakonodajnega procesa se je zakonodajalec pri takšni ureditvi »spremljanja mednarodnih sistemov zvez« v ZSOVA zgledoval po nemški ureditvi v zvezi z

delom in pooblastili Zvezne obveščevalne službe BND¹, ki jo je uredil nov zakon o omejitvi tajnosti pisem, pošte in telekomunikacij.

Zvezna obveščevalna služba sme na podlagi takšne ureditve poseči v mednarodne brezžične sisteme zvez zaradi zbiranja informacij, ki imajo zunanjepolitični in varnostni pomen, kot tudi v nekaterih drugih izjemnih primerih, ki jih ureja zakon. Gre za t.i. strateški nadzor, za zajemanje komunikacij in iskanje relevantnih informacij, pri čemer je služba omejena na uporabo takšnih iskalnih orodij oziroma nabor iskalnih parametrov, ki onemogočajo poseg v določljiv komunikacijski priključek na območju ZRN ali v tujini, kadar bi lahko bil njegov zakoniti uporabnik ali lastnik državljan ali pravna oseba ZRN. Ukrep mora utemeljiti razloge zaradi katerih je bil odrejen. Zakon² določa tudi časovno omejenost ukrepa in ravnanje s pridobljenimi osebnimi podatki ter tudi pristojnosti v zvezi z odrejanjem takšnega ukrepa, ki je zaupano od predsednika vlade pooblaščenemu ministrstvu. (Vuksanović, 2007)

Kot lahko torej vidimo predstavlja »Spremljanje mednarodnih sistemov zvez« posebno obliko pridobivanja podatkov, ki pa se po vsebinski plati razlikuje od podobnega, globljega posega v komunikacijsko zasebnost, kot ga določa in ureja 23. in 24. člen ZSOVA. V tem primeru gre za nadzorovanje in snemanje nacionalnih komunikacij ob upoštevanju posebnih kriterijev, kot jih ureja ZSOVA.

Nadzorovanje in snemanje nacionalnih komunikacij dovoli na predlog direktorja agencije s pisno odredbo, za vsak primer posebej, predsednik Vrhovnega sodišča R Slovenije, pri čemer mora biti podana »velika verjetnost«³, da obstaja nevarnost za varnost države. Zakon namesto točno določenih kaznivih dejanj, katerih domnevno izvrševanje, ob upoštevanju drugih z ustavo določenih kriterijev, bi upravičevalo takšen poseg, določa opise dejanj, v katerih je mogoče najti elemente kaznivosti zoper varnost R Slovenije ter človečnost in mednarodno pravo. Utemeljiti mora pričakovanje, da se v zvezi s prepovedano dejavnostjo uporablja ali se bo uporabljalo določeno telekomunikacijsko sredstvo, podatkov pa ni mogoče pridobiti drugače oziroma bi takšno pridobivanje na drug način lahko ogrozilo življenje in zdravje ljudi. Zakon v nadaljevanju določa tudi vsebino predloga in odredbe, trajanje ukrepa in njegovo prenehanje. Določa ravnanje s pridobljenimi podatki, kot tudi opisuje okoliščine v katerih primerih je posameznika potrebno seznaniti z izvršenim ukrepom.

S takšno ureditvijo ZSOVA je prišlo do ločitve posegov v komunikacijsko zasebnost nacionalnih, slovenskih, komunikacijskih priključkov oziroma komunikacijskih priključkov na ozemlju R Slovenije in mednarodnih komunikacij. Razloge za to pa je iskati v temeljni dilemi kdo je pristojen za odrejanje nadzora tujih telekomunikacij.

Predlagatelj je pri oblikovanju zakona izhajal iz teze, da morajo obveščevalno-varnostni organi, za razliko od organov kazenskega pregona imeti (večjo) pravico delovati proaktivno. Zaradi česar morajo imeti načelno možnost posega v komunikacijsko zasebnost oseb, za katere še ne obstaja predhoden, specifičen, artikuliran in na konkretna dejstva oprt sum, da predstavljajo grožnjo za varnost države. (Poročevalec DZ, 2. branje, 29.1.1999)

¹ Bundesnachrichtendienst

² (Gesetz zur Neuregelung von Beschränkungen des Brief, Post und Fernmeldgeheimnisses)

³ Pri opredeljevanju stopnje suma lahko govorimo o verjetnosti ali o gotovosti. »Velika verjetnost« je po pravnem standardu skoraj izenačena z gotovostjo (s konkretnimi podatki o nedovoljeni dejavnosti mora agencija že razpolagati), ki pa je ni mogoče potrditi drugače, kot z dovoljenimi posegi v varstvo komunikacijske zasebnosti. Ta pravni standard je določen edino v ZSOVA, zato je primerjava primerna.

3 POSEG V KOMUNIKACIJSKO ZASEBNOST

Pravico posameznika do komunikacijske zasebnosti predstavlja v prvi vrsti varstvo posameznikovega interesa, da se nihče⁴ ne seznani z vsebino sporočila, ki ga posameznik posreduje preko kateregakoli sredstva, ki omogoča izmenjavo oziroma posredovanje informacij na daljavo, kot tudi interes posameznika, da ima nadzor, komu, v kakšnem obsegu, na kakšen način in pod kakšnimi pogoji bo posredoval določeno sporočilo⁵. (Klemenčič v Šturm ur., 2002)

Kot enega izmed ključnih kriterijev, ki ga je potrebno uporabiti pri ocenjevanju dopustnosti posegov v komunikacijsko zasebnost v primerih, ki niso že v naprej urejeni z zakoni in ga je pri svojih odločitvah prvo uporabilo Vrhovno sodišče ZDA je utemeljitev na konceptu »razumnega pričakovanja zasebnosti« (reasonable expectation of privacy). Pri tem je potrebno tehtati dva elementa in sicer: pričakovanje zasebnosti in upravičenost pričakovanja. (Klemenčič v Šturm ur., 2002)

Gre za primere, kadar se posameznik nahaja v prostoru, kjer lahko upravičeno pričakuje, da bo sam oziroma kadar posameznik pri posredovanju svojega sporočila razumno upravičeno pričakuje, da bo njegova komunikacija nenadzorovana. Izjave, ki jih posameznik vede⁶ izpostavi tretjim osebam, ne glede na to kje jih je izpostavil, zasebni prostor ali javni kraj, niso predmet ustavnega varstva. (Klemenčič, 2002)

V tem pogledu, ne glede na kraj izjavljanja, predstavlja predmet varstva le to, kar poskuša posameznik ohraniti za zasebno, po konceptu »razumnega pričakovanja«⁷. Tudi v primeru uporabe splošno dostopnega komunikacijskega sredstva za oddajo sporočila, ki ga posameznik nameni nedoločljivi skupini prejemnikov ter se s takšno uporabo komunikacijskega sredstva in prenosom sporočila strinja, ne more govoriti o »razumnem pričakovanju«. Posameznik se v takšnih okoliščinah odpoveduje pravici do varstva svoje zasebnosti, saj mora upoštevati, da se njegove izjave lahko snemajo, shranijo, prepišejo, razmnožijo in obdelajo⁸. Pri tem pa je teritorialna ali lastninska koncepcija komunikacijskega sredstva v večji meri neuporabna. Varstvo komunikacijske zasebnosti izhaja iz potrebe po varovanju zaupnosti razmerij in ne iz vrste, statusa ali lastništva uporabljenega občila⁹, saj sporočanje ni vedno omejeno na določen prostor, temveč najpogosteje predstavlja komunikacijo na daljavo in s tem uporabo komunikacijskih sredstev, na katerih posameznik, ki jih uporablja, praviloma nima lastninske pravice¹⁰.

Koncept »razumnega pričakovanja zasebnosti«, je kasneje prevzela tudi judikatura ESČP (primer Halford v. Združeno kraljestvo, 25.6.1997) in tudi slovensko Ustavno sodišče (OdlUS VI, 158). (Klemenčič v Šturm ur., 2002)

⁴ S tem pojmom je mišljena tako država ali nepovabljeni tretji.

⁵ Gre torej za svobodno in nenadzorovano komunikacijo ter s tem varovanje zaupnosti razmerij v katere stopa posameznik pri sporočanju.

⁶ Poudarek je na zavedanju.

⁷ V skladu s splošnimi stališči družbe bi bilo neupravičeno pričakovati, da bi lahko bili pogovori na prostem zavarovani pred prestrežanjem tretjih.

⁸ Upoštevati pa je potrebno varstvo morebitnih avtorskih pravic.

⁹ Besedo občila je potrebno razlagati v najširšem pomenu besede, ki poleg pisem obsega tudi druge načine in sredstva za sporazumevanje (telefon, telefaks, elektronska pošta, SMS sporočila preko mobilnih telefonov, druge oblike komunikacij preko računalniških oziroma telekomunikacijskih omrežij).

¹⁰ V sodbi ESČP Halford v. Združeno kraljestvo, je zavzelo stališče, da ima posameznik pravico do zasebnosti tudi na delovnem mestu in pri uporabi službenih komunikacijskih sredstev.

Varstvo komunikacijske zasebnosti predstavlja v nadaljevanju celoten komunikacijski krog oziroma tudi podatke, povezane z njo in ne zgolj vsebine komunikacije. Gre za podatke, ki se samodejno tvorijo oziroma so potrebni za posredovanje informacij predvsem zaradi tehnično zahtevnih postopkov uporabe modernih oblik komuniciranja, kot so: podatki o registriranih odhodnih in dohodnih klicih, vključno s podatki o lastnikih oziroma uporabnikih telekomunikacij sredstev, podatki o vzpostavitvi in trajanju zveze ter klicanih telefonskih številkah. Govorimo o t.i. prometnih podatkih¹¹. Takšno stališče je zavzelo ESČP v primeru *Malone v. Združeno kraljestvo* (2.8.1984, A 82)¹² glede registriranja klicanih telefonskih števil. Zapisalo je, da posnetki zapisov vsebujejo podatke, ki so integralni del telefonskih komunikacij, katerih prepustitev policiji brez pristanka naročnika oziroma brez sodne odredbe bi pomenilo poseganje v zagotovljene pravice. K takšnemu mnenju pa se je pridružilo tudi Vrhovno sodišče RS, ki je v načelnem pravnem mnenju zavzelo stališče, da predmet varstva 37. člena Ustave ne predstavlja sama vsebina komunikacije temveč tudi vsi podatki, ki so integralni del te komunikacije. (Klemenčič v Šturm ur., 2002)

V nadaljevanju je potrebno omeniti, da poseg v pravico do komunikacijske zasebnosti predstavlja že samo dejstvo, da je nekdo brez ustavnih in zakonskih omejitev prestregel komunikacijo in se seznanil z njeno vsebino. Pri tem pa je nepomembno ali je bilo prestreženo sporočilo kasneje tudi uporabljeno v kakršnikoli namen, (primer *Kopp v. Švica* (25.3.1998, Reports 1998-II). (Klemenčič v Šturm ur., 2002)

Povzamemo lahko, da je pri posegu v komunikacijsko zasebnost treba določiti, kdaj lahko posameznik pri uporabi določenega komunikacijskega sredstva za prenos določenega sporočila, razumno upravičeno pričakuje določeno stopnjo zasebnosti ter v katerih primerih je to pričakovanje manjše oziroma ni prisotno¹³, ne glede na to s kakšnim komunikacijskim sredstvom (telefonsko omrežje, računalniško omrežje...) se komunikacija izvaja in kdo je lastnik teh sredstev.

Vendar pa pravica do komunikacijske zasebnosti ni absolutna, kar je ESČP v primeru *Klass in drugi v. Nemčija* (6.9.1978, A 28) tudi zapisalo in sicer da je: »Tajen nadzor (tele) komunikacij dejstvo, ki ga sodišče, čeprav z obžalovanjem, v današnjih časih moderne družbe smatra kot nujno potreben element zagotavljanja nacionalne varnosti«. (Klemenčič v Šturm ur., 2002)

Dopustnost posegov v komunikacijsko zasebnost ureja 2. odstavek 8. člena EKČP, ki dopušča širše pogoje, kot jih opredeljuje Ustava v drugem odstavku 37. člena, saj komunikacijsko zasebnost obravnava skupaj s splošnim varstvom zasebnosti. Bistvena razlika med njima s primerjalnoppravnega vidika pa je v zahtevi po sodni odločbi. Večina tujih ustav in mednarodni pravni akti namreč ne zahtevajo sodne odločbe za vsak poseg v zasebnost posameznika, kot jo določa slovenska Ustava. Ob tem pa se nam zastavlja vprašanje ali »spremljanje mednarodnih sistemov zvez«, kot ga ureja ZSOVA predstavlja poseg v komunikacijsko zasebnost, katerega dopustnost je potrebno razlagati izključno ob upoštevanju vseh kriterijev dopustnosti¹⁴, kot jih ureja drugi odstavek 37. člena Ustave RS.

»Spremljanje mednarodnih sistemov zvez«, kot ga ureja 21. člen ZSOVA v povezavi z 2. in 20. členom, lahko razlagamo kot posebno obliko pridobivanja podatkov, ki ga izvaja Agencija na

¹¹ Zakon o elektronskih komunikacijah opredeljuje podatke o prometu kot kakršnekoli podatke, ki se obdelujejo zaradi prenosa komunikacij v elektronskem komunikacijskem omrežju ali zaradi njegovega obračunavanja.

¹² V njem je ESČP obseg varstva komunikacijske zasebnosti razširilo tudi na dejstva in okoliščine povezane s komunikacijo.

¹³ Pomemben je koncept »razumnega pričakovanja zasebnosti«.

¹⁴ Pri čemer je mišljena tudi odredba sodišča.

območju zunaj državnega ozemlja R Slovenije¹⁵, ukrep pa se ne nanaša na konkretnega posameznika¹⁶, temveč gre za zadevo¹⁷.

Na podlagi takšne ureditve oziroma opredelitve »spremljanja mednarodnih sistemov zvez«, lahko upravičeno sklepamo, da gre za t.i. strateški nadzor. Pri tem pa se nam zastavlja novo vprašanje. Ali je lahko takšna ureditev izvajanja strateškega nadzora telekomunikacij sploh ustavno dopustna, predvsem, ko je objekt varstva obstoj države in njenega ustavnega reda ter s tem povezana temeljna varnost njenih državljanov, ob upoštevanju, da gre pri izvajanju strateškega nadzora v širšem pomenu za izvrševanje ukrepa v preventivne namene¹⁸, ko (še) niso podani razlogi za konkreten sum, da nekdo ogroža varnost države in njeno ustavno ureditev¹⁹?

O takšni ureditvi »spremljanja mednarodnih sistemov zvez« v ZSOVA je v svojem interpretativnem Sklepu št. U-I-216/07-8 z dne 4.10.2007 zavzelo stališče in podalo razlago tudi Ustavno sodišče. »Spremljanje mednarodnih sistemov zvez«, je opredelilo kot ukrep, ki predstavlja del obveščevalne dejavnosti Agencije in se lahko nanaša le na območje zunaj državnega območja Republike Slovenije. Ustavno sodišče RS je v sklepu poudarilo, da: »Šele če bi pri spremljanju mednarodnih sistemov zvez lahko prišlo do položaja oziroma možnosti, da bi se to nanašalo tudi na državno območje Republike Slovenije ali na konkretno določeno osebo na tem območju, bi bila glede na drugi odstavek 37. člena Ustave potrebna odredba sodišča, ki jo je treba izdati v primerih, določenih v 24. členu ZSOVA.« (Sklep št. U-I-216/07-8 z dne 4.10.2007, točka 12., str. 3)

To pa ni edini primer, ko je Ustavno sodišče odločalo o ukrepih, ki posegajo v pravico do komunikacijske zasebnosti. V tej zvezi naj omenim odločbo št. U-I-25/95 z dne 27.11.1997 in odločbo št. U-I-158/95 z dne 2.4.1998, s katerima je Ustavno sodišče podrobneje opredelilo pogoje dopustnosti posegov v komunikacijsko zasebnost. Ustavno sodišče je z odločbo št. U-I-25/95 z enoletnim odložnim rokom razveljavilo 150. do 156. člen ZKP in z odločbo št. U-I-158/95 s šestmesečnim odložnim rokom delno razveljavilo 11. in 19. a člen ZNZ, ki so urejali uporabo prikritih preiskovalnih ukrepov. Ravno na podlagi teh odločb pa je kasneje predlagatelj ZSOVA utemeljeval ureditev področja posebnih oblik pridobivanja podatkov, kot ga poznamo danes.

Pravico do strateškega nadzora si pridržujejo številne tuje obveščevalno-varnostne službe v Evropi in širše. Tudi ESČP je že razsojalo o skladnosti strateškega nadzora z določili 8. in 13. člena EKČP, pri čemer pa ni ugotovilo neskladnosti takšne oblike nadzora. Ob tem je potrebno omeniti, da se praviloma v teh državah za poseg v komunikacijsko zasebnost ne zahteva z ustavo predpisana sodna odredba. ESČP pa pušča državam široko manevrsko polje pri določanju upravičenosti in nujnosti takšnih posegov.

¹⁵ Prvi odstavek 2. člena, ki govori da: »Agencija pridobiva in vrednoti podatke ter posreduje informacije: - iz tujine, pomembne za zagotavljanje varnostnih, političnih in gospodarskih interesov države; - o organizacijah, skupinah in osebah, ki s svojo dejavnostjo iz tujine ali v povezavi s tujino ogrožajo ali bi lahko ogrozile nacionalno varnost države in njeno ustavno ureditev.

¹⁶ Tretji odstavek 21. člena govori: »Spremljanje mednarodnih sistemov zvez se ne sme nanašati na določljiv priključek telekomunikacijskega sredstva ali na določenega uporabnika tega priključka na območju Republike Slovenije«.

¹⁷ Drugi odstavek 21. člena govori: »Odredba o spremljanju mednarodnih sistemov zvez mora vsebovati podatke o zadevi, na katero se posebna oblika pridobivanja podatkov nanaša, način, obseg in trajanje«.

¹⁸ Gre za preventivno/proaktivno zajemanje podatkov v tujini ali iz tujine, kjer še ni lociran konkreten posameznik.

¹⁹ Ali lahko takšen poseg utemeljimo samo na podlagi razlogov, da gre za določeno stopnjo suma ogrožanja nacionalne varnosti?

4 TERITORIALNI PRINCIP VAROVANJA PRAVICE DO KOMUNIKACIJSKE ZASEBNOSTI

Izhajajoč iz prvega odstavka 5. člena Ustave RS, država na svojem ozemlju varuje človekove pravice in temeljne svoboščine. Zadostnost sklicevanja na to določbo pri obravnavi »spremljanja mednarodnih sistemov zvez«²⁰ pa odpira številna pravna, kot tudi dejanska vprašanja. V zvezi s tem je potrebno omeniti, da celotno zadevo še dodatno zaplete nejasnost pojma »mednarodni sistem zvez« in s tem kje se nadzor izvaja.

S podobnimi vprašanji se je v Sklepu št. Pp 2/2007 z dne 12.11.2007 ukvarjal tudi predsednik Vrhovnega sodišča RS. Menil je, da se ukrep »spremljanja mednarodnih sistemov zvez« izvaja v t.i. kiberprostoru, ki pa nima lastnosti prostora v fizikalnem ali geografskem smislu ter da bi ga bilo mogoče v pravnem smislu locirati ob določitvi z navezavo nekaterih drugih okoliščin, kot je lokacija kjer se nahajajo osebe in naprave s katerimi se ukrep izvaja in ne z lokacijo elektronskega priključka oziroma priključka, ki omogoča nastanek podatka, njegov prenos oziroma komunikacijo. Ob tem bi bilo mogoče utemeljiti, da se ukrep izvaja v R Sloveniji. Vendar pa predsednik Vrhovnega sodišča opozarja, da je pri odrejanju ukrepa nadzorovanja in snemanja telekomunikacij v R Sloveniji, na podlagi 24. člena ZSOVA, kot kraj izvajanja ukrepa štel vedno kraj, kjer se konkreten telekomunikacijski priključek nahaja²¹. (Sklep predsednika VS RS, št. Pp 2/2007 z dne 12.11.2007)

»Spremljanje mednarodnih sistemov zvez«, kot ga ureja ZSOVA sicer v tretjem odstavku 21. člena na določen način locira telekomunikacijski priključek²², na podlagi katerega bi bilo mogoče, ob upoštevanju kriterijev za določitev kraja izvajanja ukrepa 24. člena ZSOVA, kot ga razume predsednik Vrhovnega sodišča, določiti lokacijo izvajanja ukrepa, ki bi lahko v tem primeru predstavljalo območje izven R Slovenije.

Z vidika teritorialnega principa varovanja pravic do komunikacijske zasebnosti pa menim, da je kljub določenim pogledom in merilom za določanje lokacije izvajanja nadzora, kot ga uporablja predsednik Vrhovnega sodišča, za odrejanje ukrepov po 24. členu ZSOVA, pri »spremljanju mednarodnih sistemov zvez« zaradi tehnične zahtevnosti, nemogoče presojati izključno na podlagi takšne določitve kraja izvajanja nadzora (tujina), brez upoštevanja dejstva, da se nadzor domnevno fizično izvaja na območju R Slovenije.

Ob tako zapletenih vprašanjih, ki se pojavljajo pri »spremljanju mednarodnih sistemov zvez«, je dejstvo, da gre za poseg, ki ga z vidika pristojnosti in veljavnosti ne omejuje zgolj Ustava RS. Menim, da je za reševanje vprašanja varstva človekovih pravic in temeljnih svoboščin pomembno upoštevati razmerje med nacionalnim in mednarodnim pravom.

Država²³ pri tem izhaja iz pojma pozitivnih obveznosti, ki izhaja iz sodne prakse ESČP, torej EKČP. Pozitivna obveznost državo zavezuje k minimumu aktivnega ravnanja, kar pomeni, da ne zadošča, če se država zgolj pasivno vzdrži določenih kršitev temveč gre za omejevanje države pri negativnem poseganju v pravice in temeljne svoboščine. Pri tem pa se država ne sme omejiti zgolj na ozemlje R Slovenije, saj iz nobene določbe Ustave ne izhaja, da se varovanje človekovih pravic oziroma poseganje v njih ustavi na državnih mejah Slovenije. Ustavne določbe, da država na svojem ozemlju varuje človekove pravice in temeljne svoboščine, ni mogoče razumeti, da je ne glede na ustavne omejitve in omejitve iz EKČP

²⁰ Ali »spremljanje mednarodnih sistemov zvez« z vidika varstva komunikacijske zasebnosti omejuje zgolj Ustava RS?

²¹ Gre za priključke slovenskih operaterjev.

²² Telekomunikacijski priključek se ne sme nanašati na določljivi priključek telekomunikacijskega sredstva ali na določenega uporabnika tega priključka na območju R Slovenije.

²³ Pri tem je mišljena sodna, zakonodajna in izvršilna oblast.

dovoljeno posegati s svojega ozemlja v pravice oseb, ki na njem ne prebivajo. (Ločeno mnenje sodnika dr. Cirila Ribičiča v zadevi št. U-I-216/07)

Tudi ohlapnejši standardi, ki določajo kriterije za posege v komunikacijsko zasebnost tujcev, namigujejo na pomisleke, da so pravice državljanov RS strožje varovane²⁴, čeprav je mogoče nevtravno dikcijo prvega odstavka 37. člena²⁵ Ustave razumeti, da so tudi tujci na enak način upravičeni do varstva komunikacijske zasebnosti, ob smiselnem upoštevanju 13. člena Ustave²⁶.

Ustava R Slovenije naj ne bi dopuščala razlikovanja med državljani RS in tujci, kot izhaja tudi iz judikature ESČP. Razlikovanje lahko izhaja le na podlagi stvarnega in razumskega upravičenja²⁷. Tako utemeljevanja zgolj nedefiniranih legitimnih ciljev varstva države ne zdržijo. Upravičenje pa bi lahko v teh primerih utemeljevali s povečano nevarnostjo delovanja tujih državnih organov, političnih ali verskih skupin, ki ogroža ali bi lahko ogrozili nacionalno varnost. (Vuksanović, 2007)

Zanimivo vprašanje v zvezi s teritorialnim dojemanjem pristojnosti se pojavi tudi v zvezi z zunajozemeljskimi dejavniki države, ki jih v posameznih primerih predstavljajo nekateri tuji državni organi, diplomatskih predstavništev, komunikacije tujih vojaških in obveščevalnih služb²⁸. Ali bi bilo mogoče v teh primerih zaključiti, kljub temu da gre za državno območje R Slovenije, da je ob upoštevanju, da gre za povečano nevarnost ogrožanja varnosti države (utemeljeni razlogi za sum), izvajanje nadzora »spremljanje mednarodnih sistemov zvez« t.i. strateškega nadzora, upravičeno? Razmišljanje o takšnem upravičenju dodatno podkrepljuje odsotnost pogoja »razumnega pričakovanja zasebnosti«, ki pri izmenjavi teh informacij ni podan.

Pri »spremljanju mednarodnih sistemov zvez«, kot lahko vidimo, gre za zelo kompleksna in zapletena vprašanja, ki sprožajo številne pomisleke. Kljub temu pa menim, da je potrebno ureditev t.i. strateškega nadzora v ZSOVA razumevati diferencirano. Upoštevati je potrebno zgodovinski vidik nastajanja oziroma ureditve te posebne oblike v ZSOVA, saj so takrat obstajale drugačne dejanske in tehnične rešitve. Nedvomno je hiter razvoj informacijske tehnologije prinesel neslutene možnosti tako izmenjave podatkov kot tudi prikritega nadzora ter s tem nevarnosti, ki posamezniku in njegovi zasebnosti preti s strani države. Tako je na primer sodnik Vrhovnega sodišča ZDA, Louis Brandeis že leta 1928 v enem izmed prvih primerov telefonskega prisluškovanja na svetu zapisal, da se napredek znanosti ne bo ustavil pri (prisluškovanju telefona) in da bo nekega dne razvoj znanosti državi omogočil reproduciranje papirjev, ne da bi jih dejansko fizično vzela iz obdolženčevega predala ter bo tako lahko sodišču razkrila najbolj intimne informacije iz njegove zasebnosti... (Klemenčič v Šturm ur., 2002)

Glede takšnih pomislekov menim, da je povsem na mestu razmišljanje ustavnega sodnika dr. Cirila Ribičiča, ki se je v ločenem mnenju k sklepu št. U-I-216/07-8 z dne 4.10.2007, zavzel, da je edina ustavnoskladna razlaga določbe, ki v ZSOVA ureja »spremljanja mednarodnih sistemov zvez« tista, ki na podlagi takšnega ukrepa onemogoča posege v pisemsko tajnost

²⁴ Posegi v komunikacijsko zasebnost telekomunikacij v R Sloveniji, imajo po 24. členu višji standard varnosti.

²⁵ Zagotovljena je tajnost pisem in drugih občil. Uporabljen besedni znak »zagotovljena je...«, uporablja Ustava za univerzalne pravice.

²⁶ V primerih, ko tujec na območju R Slovenije uporablja tuje komunikacijsko sredstvo, ki je pod nadzorom izvajanja ukrepa »spremljanja mednarodnih sistemov zvez«, upravičuje tak pomislek.

²⁷ Gre za utemeljene razloge za sum.

²⁸ Kot tudi letala, ladje...

kateregakoli posameznika, tako tistega, ki prebiva v Sloveniji, kot tistega, ki prebiva zunaj nje. (Ločeno mnenje sodnika dr. Cirila Ribičiča v zadevi št. U-I-216/07)

V nasprotnem primeru, kadar »spremljanje mednarodnih sistemov zvez« posega v zasebnost konkretnega kateregakoli posameznika pa bi bilo potrebno razmišljati o ureditvi takšnih posegov v skladu s kriteriji dopustnosti, kot jih ureja Ustava.

5 POMANJKLJIVOSTI VELJAVNE NORMATIVNE UREDITVE

Dejstvo je, da je Ustavno sodišče R Slovenije je v sklepu št. U-I-216/07-8 z dne 4.10.2007, načeloma pustilo odprto možnost drugačnega obravnavanja posegov v pravico do komunikacijske zasebnosti v primerih, kadar ne gre za ozemlje R Slovenije²⁹.

Tako ZSOVA ureja »spremljanje mednarodnih sistemov zvez« kot posebno obliko pridobivanja podatkov iz tujine ali v povezavi s tujino, pri čemer ne gre za poseg v določljiv telekomunikacijski priključek oziroma posameznika, temveč za poseg v nedoločen krog oziroma komunikacijski sistem (zadevo). Govorimo lahko o t.i. strateškem oziroma neosredotočenem nadzoru.

Dejstvo, da se je predlagatelj oziroma zakonodajalec odločil za takšen način urejanja nadzora mednarodnih komunikacij v ZSOVA povzroča določene pomisleke. Možnost strateškega nadzora tujih telekomunikacij se poslužujejo tudi druge številne države, pravno urejanje tega področja pa je pogosto, tudi namenoma zaradi pomislekov, da posegajo na nedovoljen način v suverenost drugih držav ter da kršijo mednarodno pravo, neurejeno. Težko si namreč predstavljamo kaj bi se zgodilo, če bi sodišče izdalo odredbo za »spremljanje mednarodnih sistemov zvez«, kar bi lahko pomenilo, da je sodišče v tuji državi dovolilo izvrševanja kaznivega dejanja vohunstva³⁰.

Bistven problem trenutne normativne ureditve predstavlja nedefiniranost pojma »spremljanje mednarodnih sistemov zvez«, ki bi ga v nadaljevanju bilo potrebno razdeliti na del neosredotočenega nadzora t.i. strateškega nadzora in drugi del, ki bi predstavljal osredotočeni nadzor (konkreten posameznik ali skupine).

Za izvajanje nadzora bi bilo potrebno jasneje in določneje definirati namen izvajanja nadzora, kot ga trenutno določa 2. člen ZSOVA³¹. Določba je najverjetneje podnormirana in premalo konkretizirana oziroma določna po teži diferenciranih varnostnih, političnih in gospodarskih interesov in kot takšna ne nudi zadostne pravne določnosti. Nujno bi bilo potrebno določiti tudi ravnanja v primeru neutemeljenega poseganja v komunikacijsko zasebnost³².

Za izvajanje nadzora bi bilo potrebno navesti razloge, ki bi omogočali preizkus nujnosti in subsidiarnosti takšnega ukrepa za varnost države iz česar bi izhajalo, da bi bilo drugačno pridobivanje podatkov nevarno in bistveno oteženo. Gre za upoštevanje načela sorazmernosti, ki je izvedeno iz načela pravne države. V tej zvezi bi bilo potrebno predvideti možnosti

²⁹ V zvezi s tem je v 12. točki navedlo, da v kolikor bi pri spremljanju mednarodnih sistemov zvez lahko prišlo do položaja oziroma možnosti, da bi se to nanašalo tudi na državno območje R Slovenije ali na konkretno določeno osebo na tem območju, bi bila glede na drugi odstavek 37. člena Ustave potrebna odredba sodišča.

³⁰ Čeprav bi se odredba izvrševala na slovenskem ozemlju pa bi posledice nastale v tujini.

³¹ ...za zagotavljanje varnostnih, političnih in gospodarskih interesov države....

³² Določiti bi bilo potrebno varnostne mehanizme, ki bodo preprečevali poseganja v področja poslovnih in drugih skrivnosti, ki niso zakonsko definirana.

omejitve posega le na primere, v katerih bi bil tak poseg v razumnem sorazmerju s ciljem. Določiti bi bilo potrebno način izvajanja ukrepa.

Naslednja pomanjkljivost je, da zdajšnja ureditev ne določa najdaljšega dopustnega obsega trajanja ukrepa, ki bi se lahko razlikoval glede na okoliščine izvajanja nadzora. Prav tako bi bilo potrebno določiti razloge in okoliščine za prenehanje izvajanja ukrepa kot tudi postopek ravnanja s pridobljenimi podatki³³. Nova ureditev določbe bi morala prav tako vsebovati pogojno možnost obveščanja nadzorovanca.

Pri urejanju vprašanja »spremljanja mednarodnih sistemov zvez« bi bilo potrebno razmišljati tudi o razširitvi oziroma dopolnitvi pristojnosti in nalog, ki so v zvezi z izvajanjem nadzora posebnih oblik pridobivanja podatkov zaupane parlamentarni komisiji za nadzor varnostnih in obveščevalnih služb. Gre za nadzor s sodno odločbo odrejenih ukrepov, kot tudi nadzor nad odreditvijo in uporabo nadzorovanih ukrepov, ki se ne odredajo s sodno odredbo. V tej zvezi in ob upoštevanju dejstva, da se je predlagatelj pri normiranju ZSOVA zgledoval po nemški ureditvi, bi bilo smiselno razmisliti o možnostih razširitve pooblastil parlamentarne komisije, kot jo pozna nemška ureditev³⁴. V tem delu mislim zlasti na pristojnost komisije, ki ji omogoča možnost predhodnega odločanju o dopustnosti dovoljenih posegov.

V primeru ločitve »spremljanja mednarodnih sistemov zvez« na področje neosredotočenega in osredotočenega nadzora, bi bilo potrebno za posege v zasebnost kateregakoli³⁵ konkretnega posameznika tako tistega, ki prebiva na območju R Slovenije ali zunaj nje, smiselno razmišljati o načinu ureditve izvajanja nadzora ob upoštevanju kriterijev, kot jih določa drugi odstavek 37. člena Ustave. Odločba sodišča na podlagi katere je mogoč poseg v zasebnost, je po stališču Ustavnega sodišča zavzeta zahteva, ki temelji na načelu pravne države, po katerem mora biti vmešavanje izvršilne oblasti v pravice posameznika podvrženo učinkoviti kontroli, ki naj bi bila zaupana predvsem sodišču³⁶. Zahteva po sodni odločbi vključuje tudi jamstva, ki jih zagotavlja pravica do enakega varstva pravic v postopku pred sodišči, pravica do sodnega varstva, pravica do pritožbe ali drugega pravnega sredstva ter pravica do pravnih jamstev. (Klemenčič v Šturm ur., 2002)

Pri oblikovanju tega vprašanja bi bilo smiselno upoštevati razumno interpretacijo 37. člena Ustave, pri čemer ne bi bil odločilen kriterij ozemlje oziroma državljanstvo (konkretnega) posameznika, temveč diferenciranje globine posega v komunikacijsko zasebnost.

V tem delu bi prav gotovo bilo smiselno razmišljati tudi o ureditvi vprašanj, ki se pojavljajo v zvezi z izvajanjem »spremljanja mednarodnih sistemov zvez« komunikacij tujih državnih organov, ne glede na njihovo teritorialnost. Vprašanja sem se že dotaknil v poglavju 4. Teritorialni princip varovanja pravice do komunikacijske zasebnosti. Gre za možnost uporabe izvajanja »spremljanja mednarodnih sistemov zvez« telekomunikacijskih priključkov na območju R Slovenije, ki pripadajo tujim državnim organom (diplomatska predstavništva, pripadniki tujih vojaških ali obveščevalnih služb) ob razlogih povečane nevarnosti, da obstaja nevarnost za varnost države.

Možnost razširitve izvajanja »spremljanja mednarodnih sistemov zvez« v omenjenem segmentu, bi na področju dela varnostnih in obveščevalnih služb prinesel določen napredek in omogočil večjo konkurenčnost služb pri izvajanju svojega poslanstva. Obveščevalna doktrina

³³ Tako uporabnimi, kot tudi neuporabnimi podatki.

³⁴ Gre za t.i. skupino G-10.

³⁵ Nanaša se tako na tujce kot tudi na državljane RS.

³⁶ Zaradi preprečevanja (zmanjševanja) zlorab.

se na področju protiobveščevalnega dela zelo pogosto srečuje z zlorabami imunitet diplomatskih predstavnikov za namene delovanja agentov tujih obveščevalno varnostnih struktur. V takšnih in podobnih primerih je Agencija z vidika uporabe posebnih oblik pridobivanja podatkov, konkretno uporabe 24. člena ZSOVA, na podlagi katere je mogoče nadzorovanje in snemanje nacionalnih telekomunikacijskih sistemov, prikrajšana, saj uslužbenke diplomatskih predstavništev (domnevne agente tujih služb) pred posegi v njihovo zasebnost zaradi diplomatske imunitete, ščiti dunajska konvencija. V praksi pa sodišče odredbe za izvajanje nadzora ne more izdati.

6 SKLEP

»Spremljanje mednarodnih sistemov zvez« predstavlja v veljavni normativni ureditvi ZSOVA obliko preventivnega in proaktivnega zajemanja podatkov v tujini ali iz tujine. Gre za t.i. strateški oziroma neopredeljeni nadzor³⁷. Takšno ugotovitev je v svojem sklepu št. U-I-216/07-8 z dne 4.10.2007 podalo tudi Ustavno sodišče.

Nedvomno bo v prihodnje zaradi hitrega razvoja informacijske tehnologije, ki ponuja številne možnosti prenosa podatkov in s tem tudi prikritega nadzora, potrebno zakonsko urejanje »spremljanja mednarodnih sistemov zvez« dopolniti oziroma spremeniti. Z razvojem informacijske dobe se je povečala nevarnost, ki preti posameznikom pred vdori v zasebnost. Kot takšno nevarnost lahko razumemo tudi »spremljanje mednarodnih sistemov zvez«, ki ga za pridobivanje podatkov iz tujine uporablja Slovenska obveščevalno-varnostna agencija.

Jasno je, da z vidika posegov v komunikacijsko zasebnost, predstavlja izvajanje nadzora »spremljanja mednarodnih sistemov zvez«, ob odsotnosti pogoja »razumnega pričakovanja«, kršitev teh pravic. Trenutna ureditev ZSOVA, ki jo je potrebno razumevati, da na podlagi »spremljanja mednarodnih sistemov zvez« ni mogoče posegati v zasebnost kateregakoli posameznika, bodisi na območju R Slovenije ali zunaj nje, in da se nanaša na »zadevo«, je pogojno sprejemljiva, vendar kot takšna povzroča številne pomisleke in dileme³⁸.

Zaradi takšnega razvoja informacijske tehnologije, ki dopušča tudi možnosti nadzora konkretnega posameznika, ne gre za »zadevo«, bi bilo potrebno razmisliti o razlikovanju med neosredotočenim in osredotočenim nadzorom. S tem v zvezi se pojavlja tudi razmišljanje ali za odrejanje takšnega, osredotočenega, nadzora zadostuje odredba izvršilne oblasti ali pa je v skladu s pogoji dopustnosti posegov v zasebnost potrebno upoštevati določila Ustave. Mnenja so različna. Tudi ustavne določbe, ki v prvem odstavku 5. člena določa, da država na svojem ozemlju varuje človekove pravice in temeljne svoboščine, ne moremo razumeti kot zadostne za urejanje tako občutljivega vprašanja, kot je zasebnost posameznika.

Menim, da bi bilo potrebno pravico do varstva zasebnosti razumevati širše ob smiselni in širši interpretaciji 37. člena Ustave, ki bi temeljila na globini posega v zasebnost.

Vprašanja v zvezi z dopolnitvami oziroma spremembami normativnega urejanja »spremljanja mednarodnih sistemov zvez« v ZSOVA pa ponujajo tudi priložnost, ki se kaže v tehtanju možnosti za razširitev uporabe nadzora v primerih tujih državnih organov ne glede na njihovo teritorialnost, s čimer bi povečali konkurenčnost Slovenske obveščevalno-varnostne agencije

³⁷ Nadzor, ki se nanaša na zadevo.

³⁸ Morda je bila takrat takšna ureditev v ZSOVA, zaradi drugačnih dejanskih in tehničnih izhodišč oziroma rešitev, zadostna.

in s tem prispevali k skrbi za nacionalno varnost. Vendar pa takšna ureditev ne sme biti v škodo doseženim in uveljavljenim človekovim pravicam in temeljnim svoboščinam.

Morda pa bo ustrezno rešitev že v kratkem nakazalo Ustavno sodišče, če bo ponovno »vrženo rokavico« s strani informacijske pooblaščenke pobralo in o zahtevi vsebinsko odločilo.

7 LITERATURA IN PRAVNI VIRI

- Evropska konvencija o varstvu človekovih pravic in temeljnih svoboščin. (1994). Uradni list RS, št. 33/1994. Mednarodne pogodbe, št. 7/1994.
- Klemenčič, G. et al. (2002). Vaše pravice v policijskih postopkih. Ljubljana, Založba Pasadena.
- Ločeno mnenje sodnika dr. Cirila Ribičiča v zadevi št. U-I-216/07 z dne 12.10.2007.
- Odločba Ustavnega sodišča RS, št. U-I-25/95 z dne 27.11.1997. (1998). Uradni list RS, št. 5/1998.
- Odločba Ustavnega sodišča RS, št. U-I-158/95 z dne 2.4.1998. (1998). Uradni list RS, št. 31/1998.
- Sklep Ustavnega sodišča RS, št. U-I-216/07-8 z dne 4.10.2007.
- Sklep predsednika VS RS, št. Pp 2/2007 z dne 12.11.2007.
- Šturm, L. urednik. (2002). Komentar ustave Republike Slovenije. Ljubljana, Fakulteta za podiplomske državne in evropske študije.
- Ustava Republike Slovenije. Uradni list RS, št. 33/1991, 42/1997, 66/2000, 24/2003, 69/2004, 68/2006.
- Vuksanović, I. (2007). Nekateri aktualni problemi komunikacijske zasebnosti. Pravna praksa, št. 33, 22 - 31.
- Zakon o Slovenski obveščevalno-varnostni agenciji. (2006). Uradni list RS, št. 81/2006.
- Zakon o obrambi. (2004). Uradni list RS, št. 103/2004.
- Zakon o parlamentarnem nadzoru obveščevalnih in varnostnih služb. (2007). Uradni list RS, št. 93/2007.
- Zakon o elektronskih komunikacijah. (2007). Uradni list RS, št. 13/2007.