Vošnjakova 1, p.p. 78, SI-1000 Ljubljana
Telefon: + 386 (0) 1 230 97 30
Faks: + 386 (0) 1 230 97 78
www.ip-rs.si

Številka:
Datum:

USTAVNO SODIŠČE REPUBLIKE SLOVENIJE
Beethovnova 10

1000 Ljubljana

Informacijski pooblaščenec na podlagi 23a. člena Zakona o Ustavnem sodišču (Ur. l. RS, št. 64/2007 - UPB, ZUstS) vlaga v zvezi z zadevo inšpekcijskega nadzora pod št. 0612-18/2008

ZAHTEVO ZA OCENO USTAVNOSTI

- prvega, drugega in tretjega odstavka 21. čl. Zakona o Slovenski obveščevalno-varnostni agenciji (Ur. l. RS, št. 23/99 ter spremembe, ZSOVA):

(1) Spremljanje mednarodnih sistemov zvez ter tajni nakup dokumentov in predmetov dovoljuje direktor agencije s pisno odredbo.

(2) Odredba o spremljanju mednarodnih sistemov zvez mora vsebovati podatke o zadevi, na katero se posebna oblika pridobivanja podatkov nanaša, način, obseg in trajanje.

(3) Spremljanje mednarodnih sistemov zvez se ne sme nanašati na določljiv priključek telekomunikacijskega sredstva ali na določenega uporabnika tega priključka na območju Republike Slovenije.

*** * ***

O b r a z l o ž i t e v :

I. Povezanost s postopkom Informacijskega pooblaščenca

Kot izhaja iz priloženega spisa št. 0612-18/2008, je Informacijski pooblaščenec po uradni dolžnosti začel inšpekcijski postopek nad izvajanjem določb Zakona o varstvu osebnih podatkov (Uradni list RS, št. 94/07 - UPB1, ZVOP-1) in vseh drugih predpisov, ki urejajo varstvo osebnih podatkov v skladu z 2. čl. Zakona o Informacijskem

pooblaščencu (Uradni list RS, št. 113/05 in 51/07 – ZUstS-A; ZInfP) pri Slovenski obveščevalno-varnostni agenciji (v nadaljevanju SOVA). V okviru nadzora je bila pregledana dokumentacija povezana s pristojnostmi Informacijskega pooblaščenca, zlasti so bile pregledane vsebine zbirk osebnih podatkov, ki nastajajo na podlagi aktivnosti, ki jih izvaja SOVA.

V okviru inšpekcijskega ogleda je bilo ugotovljeno, da SOVA izvaja 21. čl. ZSOVA tako, da vse prisluhe posname, v tem okviru pa je zabeležen čas komunikacije, njena dolžina in obe telefonski številki. Ta zbirka oziroma posnetek postane del razvida, ki se vodi na podlagi 13. in 14. čl. ZSOVA, šele, ko pristojna oseba naredi dobeseden zapis-transkript (včasih pa kratek povzetek, če je večina informacij irelevantnih). Ko pristojna oseba naredi transkript oz. povzetek v Wordovem urejevalniku, ga prenese v razvid.

Pri inšpekcijskem nadzoru je bila pri vpogledu v razvid, ki se vodi na podlagi 13. in 14. čl. ZSOVA, naključno izbrana ena zadeva, opravljena na podlagi 21. čl. ZSOVA. Pri pregledu zbranih podatkov pri SOVA je bilo ugotovljeno, da je naključno izbrani dokument vseboval ime in priimek in telefonsko številko nadzirane osebe. Izbrani dokument je imel ustrezno pravno podlago v odredbi predstojnika, ki je prisluh odobril na podlagi izpodbijanega 21. člena ZSOVA (1. odstavek).

II. Neskladnost izpodbijane določbe z 2., 15. in 38. čl. Ustave

Vlagatelj zahteve ugotavlja, da 21. čl. ZSOVA omogoča zbiranje osebnih podatkov. Na podlagi 21. čl. ZSOVA se namreč zbirajo in obdelujeta osebno ime in telefonska številka nadzirane osebe, ki skupaj z barvo glasu tvorijo osebne podatke v smislu 6. čl. ZVOP-1. ZVOP-1 v 1. in 5. tč. 6. čl. kot osebni podatek določa katerikoli podatek, ki se nanaša na posameznika, ne glede na obliko, v kateri je izražen, kot zbirko osebnih podatkov pa vsak strukturiran niz podatkov, ki vsebuje vsaj en osebni podatek, ki je dostopen na podlagi meril, ki omogočajo uporabo ali združevanje podatkov, ne glede na to, ali je niz centraliziran, decentraliziran ali razpršen na funkcionalni ali geografski podlagi; strukturiran niz podatkov je niz podatkov, ki je organiziran na takšen način, da določi ali omogoči določljivost posameznika. Glede na obe opredelitvi in upoštevaje vsebino zbranih osebnih podatkov na podlagi 21. čl. ZSOVA je mogoče ugotoviti, da se ob tem obdelujejo podatki takšne kvalitete, da je omogočena določljivost posameznika in da jih je mogoče organizirati tako, da je v razvidu omogočeno iskanje po posameznih osebnih podatkih.

Pri izvajanju 21. čl. ZSOVA gre za obliko nadzora, ki je imanentno povezana z delovanjem obveščevalnih služb, in sicer za t.i. *strateški nadzor telekomunikacij*, kjer naj ob začetku izvajanja nadzora ne bi šlo za nadzor nad določeno osebo ali priključkom, temveč naj bi šlo za zajemanje množice oziroma vnaprej neopredeljenega števila komunikacij, vendar zgolj preko sistema mednarodnih zvez, torej sistema, ko ne gre za:

- določljiv priključek oziroma
- določljivega uporabnika priključka na ozemlju RS.

Obrnjeno se torej lahko 21. čl. ZSOVA nanaša na primere, ko gre za:

- nedoločen ali nedoločljiv priključek,
- nedoločljivega uporabnika priključka na ozemlju RS,
- določljivega uporabnika priključka izven ozemlja RS,
- določenega uporabnika priključka izven ozemlja RS.

V inšpekcijskem nadzoru je bilo ugotovljeno, da SOVA izvaja nadzor na podlagi izpodbijanega člena (tudi) tako, da predstojnik odobri nadzor nad konkretno telefonsko številko.

Določbe, ki varujejo človekovo osebno dostojanstvo, osebnostne pravice, zasebnost in varnost (od 34. do 38. čl. Ustave RS) imajo posebno mesto med človekovimi pravicami in temeljnimi svoboščinami, predvsem pa vsem prepovedujejo - na prvem mestu državi, pa tudi posameznikom - poseganje v naštete pravice (OdlUS VI, 158, U-I-25/95, Ur. l. RS 5/98). Test sorazmernosti pomeni prepoved prekomernih posegov in ustrezno tehtanje, ali so ukrepi, določeni v zakonu, skladni z njegovim namenom. Zato mora biti vsak ukrep države utemeljen s ciljem in to tako, da v najmanjši možni meri vpliva na položaj prizadetih subjektov oziroma na njihove pravice in interese. Ukrepi morajo biti sicer primerni za dosego zakonodajalčevih ciljev, potrebni za njihovo implementacijo glede na objektivne interese državljanov, in nikakor ne smejo biti izven vsakega razumnega razmerja do družbene vrednosti teh ciljev. Zakonodajalec lahko poseže v ustavno varovane položaje posameznikov, a le, če je s tem uresničil neki drugi ustavno dopusten cilj, pri čemer mora biti ta ukrep neogibno potreben za dosego tega cilja, izbrano sredstvo za dosego cilja pa tako, da cilja ni mogoče doseči na način, ki bi manj posegel v ustavno varovane položaje, poseg (obseg prizadetosti varovane dobrine) pa v sorazmerju z vrednostjo zastavljenih zakonodajnih ciljev.

Tudi posegi v varstvo osebnih podatkov iz 38. čl. Ustave RS so po ustaljeni presoji Ustavnega sodišča dopustni, vendar le, če so v skladu z načelom sorazmernosti. To pomeni, da mora biti omejitev potrebna in nujna za dosego zasledovanega ustavno legitimnega cilja (javna korist ali varstvo pravic drugih) ter v sorazmerju s pomembnostjo tega cilja (3. odst. 15. čl.). Dopustna je potemtakem le v tistem obsegu, ki še prestane t.i. strogi test sorazmernosti.

Nekaterim človekovim pravicam je imanentno, da ena pravica ovira drugo oziroma, da jo omejuje. V vsakem primeru tka dveh ustavnih pravic pa je potrebno spoštovati načelo praktične konkordance, tako da je določeno področje varovanja dopustno omejiti samo, kadar to terjajo pravice drugih in v primerih, ki jih določa ustava (3. odst. 15. čl. Ustave RS). Obseg varovanja vsake pravice se zato lahko zmanjša le v tistem obsegu, ki je nujno potreben za uveljavljanje druge pravice. To pomeni, da so omejitve in posegi v človekove pravice v določenih primerih ustavno dopustni, in sicer takrat, kadar to zahtevajo pravice drugih in v primerih, ki jih določa ustava Dopustnost omejitev oziroma posegov v človekove pravice se presoja s testom sorazmernosti, ki izhaja iz 2. čl. Ustave RS, ki določa, da je Republika Slovenija pravna država. Iz načela pravne

države izhaja tudi, da mora zakonodajalec določno in nedvoumno urediti pooblastilo organa, ki posega v človekove pravice in temeljne svoboščine.

Prepoved čezmernih posegov države oziroma načelo sorazmernosti je prav z odločitvami Ustavnega sodišča dobilo ustavni rang splošnega ustavnega načela, ki zavezuje vse državne organe, torej tudi zakonodajalca. Človekove pravice namreč zakonodajalca vežejo tudi v vseh tistih primerih, kjer mu sicer ustava izrecno dopušča možnost zakonskega urejanja in s tem tudi omejevanja posameznih ustavno varovanih pravic in svoboščin. Poleg zahteve, da so takšne omejitve dopustne samo z zakonom in da morajo biti že v samem zakonu podani bistveni kriteriji (jasna določitev vsebine, namena in obsega urejanja) za nadaljnje delovanje, mora biti v samem zakonu spoštovano tudi načelo sorazmernosti. S to zahtevo, ki izvira iz načela pravne države, se postavlja omejitev zakonodajalčevim omejitvam človekovih pravic in temeljnih svoboščin in vzpostavlja kvalificirana povezava med zakonodajalčevim motivom in namenom, ki ga zasleduje, ter sredstvi in pravno normativnimi rešitvami, ki jih v tam namen uporabi (več Komentar Ustave RS, urednik Lovro Šturm, Fakulteta za podiplomske državne in evropske študije, Ljubljana, 2002).

Kot je zapisalo Ustavno sodišče RS v odločbi št. 165-09-4/2002 (Ur. l. RS, št. 22/2002), informacijska tehnologija ne prinaša le bistvenih olajšav pri obdelavi podatkov in informacij, temveč se z njenim razširjanjem na vsa področja družbenega življenja povečuje tudi tveganje, da posameznik nima več možnosti sam odločati o tem, kdaj, kako in v kakšnem obsegu bodo informacije o njem posredovane drugim. Da bi preprečili to nevarnost, Ustava v 38. čl.:
1.) prepoveduje uporabo osebnih podatkov v nasprotju z namenom njihovega zbiranja,
2.) zbiranje, obdelovanje, namen uporabe, nadzor in varstvo tajnosti osebnih podatkov določa za predmet zakonskega urejanja in
3.) vsakomur daje pravico, da se seznani z zbranimi osebnimi podatki, ki se nanj nanašajo, za primer zlorabe pa tudi pravico do sodnega varstva.

Poglavitno zapoved iz 38. čl. Ustave RS, da mora biti v temeljih urejanje varstva osebnih podatkov pridržano zakonodajni veji oblasti, tj. zakonodajalcu in s tem urejanju z zakonom, je treba povezati z načelom iz 2. čl. Ustave RS, ki določa, da je Republika Slovenija pravna država. Iz načela pravne države med drugim izhaja tudi, da mora zakonodajalec določno in nedvoumno urediti pooblastilo organa, ki posega v človekove pravice in temeljne svoboščine. Iz tega načela se izpeljuje predvsem zahteva po določeni kvaliteti zakona, ki se mora odražati v njegovi jasnosti in določnosti. Preko takšne kvalitete se odpravlja pravna negotovost kot nasprotje pravne varnosti in s tem pravne države.

Kot izhaja že iz odločbe Ustavnega sodišča U-I-229/03, II. odst. 38. člena Ustave med drugim določa, da mora biti v zakonu določen namen uporabe osebnih podatkov. V zakonu določen namen obdelave osebnih podatkov pa ne sme biti določen ohlapno ali preširoko. Da mora biti namen obdelave osebnih podatkov v zakonu določen eksplicitno, je presodilo tudi Ustavno sodišče, in sicer (opomba št. 3 k odločbi št. U-I-

298/04 z dne 27. 10. 2005, Uradni list RS, št. 100/05 o presoji Zakona o plačilnem prometu, ZPlaP), da načel v zakonu po oceni Ustavnega sodišča ni mogoče šteti za opredelitev namena uporabe, kot to zahteva 38. člen Ustave RS.

Pravico do varstva osebnih podatkov zagotavlja tudi Evropska konvencija o človekovih pravicah (v nadaljevanju EKČP) v 8. čl. V skladu z razumevanjem te pravice, iz te pravice izhaja negativna dolžnost države, da se vzdrži poseganja v zasebnost in da posamezniku zagotavlja varstvo pred samovoljo javnih oblasti. Pravica do zasebnosti je pravica do lastnega življenja in vključuje svobodo posameznika pred neutemeljenimi posegi države v njegovo zasebno sfero (*right to be let alone*). V sodbi *Malone proti Združenemu kraljestvu* (št. 8691/79, 2.8.1984), je Evropsko sodišče za človekove pravice (v nadaljevanju ESČP) obravnavalo predvsem vprašanje določenosti z zakonom in vsebino zahteve »v skladu z zakonom«. ESČP je ocenilo, da zakonodaja ne določa dovolj jasno, kdaj in kako so dovoljeni ukrepi prisluškovanja, ki tudi pomeni obdelavo osebnih podatkov. Ker obdelave osebnih podatkov oziroma prisluškovanja ni uredil zakon, takšno pravno stanje pomeni kršitev 8. čl. EKČP. Iz tega sledi, da bi morali biti osebni podatki v vsakem primeru konkretizirani v takšni meri, da se ne bi mogel pojaviti noben dvom v obseg posega v informacijsko zasebnost, kar vključuje tud zahtevo, da mora biti v zakonu določno in v skladu z načelom sorazmernosti določen tudi namen obdelave. Brez zakonsko določenega namena obdelave se namreč ne morejo z gotovostjo določiti vrste in števila osebnih podatkov, ki so v skladu z zakonom lahko obdelovani, zlasti pa se v okviru pravnega reda RS ne more zadostiti ustavni zahtevi iz prvega odstavka 38. čl. Ustave RS, da je prepovedana uporaba osebnih podatkov v nasprotju z namenom njihovega zbiranja.

Izpodbijana določba ne določa ustrezno namena zbiranja oziroma obdelave osebnih podatkov, saj ji primanjkuje takšna stopnja določnosti in jasnosti, ki bi še zagotavljala pravno varnost. Določeno je namreč, da sme direktor SOVE s pisno odredbo dovoliti spremljanje mednarodnih sistemov zvez za namen opravljanja nalog SOVE. Naloge SOVE, s tem pa tudi namen zbiranja osebnih podatkov, je zato mogoče iskati zgolj v prvem odstavku 2. čl. ZSOVA, po katerem 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.

Namen zbiranja osebnih podatkov po 21. čl. ZSOVA je opredeljen tako na široko, da po oceni vlagatelja zahteve ne prestane testa sorazmernosti. Kot je poudarilo Ustavno sodišče RS v odločbi št. U-I-152/03 z dne 23.3.2006, morajo biti v primerih posegov v človekove pravice, izvedenih v preventivne namene, med katere sodi tudi strateški nadzor telekomunikacij po 21. čl. ZSOVA, pooblastila države še bolj omejena kot sicer. To pomeni, da bi morala zakonska norma v tem primeru zlasti zadostiti zahtevi po *lex*

certa. V njej ne bi smelo biti nejasnosti, dvoumnosti ali pomensko ohlapnih besed, saj se v nasprotnem primeru na stežaj odpira vrata samovolji in arbitrarni uporabi zakona, ki je pri posegih v temeljne človekove pravice najstrožje prepovedana. Predvsem se morajo določno in natančno urediti vsakršni posegi v človekove pravice. Izpodbijana določba pa je nasprotno tem zahtevam pomensko ohlapna in dopušča poseg v pravico do varstva osebnih podatkov že iz pomensko odprtih razlogov, kot so zagotavljanje varnostnih, političnih in gospodarskih interesov države.

Prav tako pa v celoti opisana ureditev ni v skladu z načelom pravne države. Iz teh zahtev sicer izhaja, da mora biti vsakršno zbiranje osebnih podatkov potrebno, legitimno, primerno in nujno, torej v skladu z načelom sorazmernosti, izpodbijana določba pa takšnim kriterijem ne ustreza. Na način, določen v izpodbijani določbi, posameznik postaja »objekt informacije«, kar je v neskladju z 38. čl. Ustave. Omogočeno je namreč zbiranje in obdelovanje osebnih podatkov za namene, ki ustrezajo nalogam SOVE, pri čemer je po oceni vlagatelja zahteve očitno podano dramatično veliko nesorazmerje med posegom v pravico do varstva osebnih podatkov in zasledovanimi cilji – zagotavljanju varnostnih, političnih in gospodarskih interesov.

V nasprotnem primeru, če bi se zgolj zaradi zakonske podlage za obdelavo osebnih podatkov, dovolilo kakršnokoli oziroma nesorazmerno zbiranje osebnih podatkov, bi imela država povsem proste roke. To je v nasprotju z načelom, da mora biti vsak poseg, to je obseg prizadetosti varovane dobrine, v vrednostnem sorazmerju z vrednostjo zastavljenih zakonodajnih ciljev. Težo legitimnih posegov zakonodajalca je potrebno zmanjšati do mere, ki še zagotavlja doseganje postavljenih ciljev in tako vzpostaviti razumno ravnovesje med vrednostjo teh ciljev in težo posegov.

III. Neskladnost izpodbijane določbe s 37. čl. Ustave RS

Ukrep iz spornega člena ZSOVA predstavlja posebno obliko pridobivanja podatkov - v tujini ali iz tujine - za strateški nadzor telekomunikacij z namenom pridobivanja informacij in podatkov, 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. Ukrep se naj po zakonu ne bi nanašal na določljivega posameznika ali določljiv priključek (čeprav iz ugotovitve ob inšpekcijskem nadzoru vlagatelja izhaja nasprotno). Ukrep odreja direktor SOVA, pri čemer ukrep zakonsko časovno ni omejen. Pri tem je potrebno poudariti, da se ukrep izvaja na ozemlju Slovenije, s strani uradnih oseb Republike Slovenije in na komunikacijah, ki "fizično" potekajo preko Slovenije. Razlika ukrepa mednarodnega spremljanja sistemov zvez po 21. členu ZSOVA od v 24. členu ZSOVA neprimerljivo strožje in določneje reguliranega ukrepa nadzora komunikacij je primarno v tem, da gre pri slednjem za spremljanje komunikacij v domačem komunikacijskem omrežju.

Slovenska Ustava sicer zagotavlja varstvo zasebnosti v več določbah, vendar so različne pojavne oblike zasebnosti ločene zgolj zato, ker ustava zagotavlja specifične

pogoje za posege v posamezne vidike zasebnosti (več Klemenčič, G.: Komentar 37. člena, v: Šturm, L. (ur.): Komentar Ustave RS, Fakulteta za podiplomske državne in evropske študije, Ljubljana, 2002).

Na tem mestu vlagatelj zahteve opozarja na dvojno varstvo podatkov o osebnem imenu, telefonski številki in zapisu pogovora. Na to je opozorilo že Ustavno sodišče RS v odločbi št. U-I-25/95 z dne 27.11.1997; dvojno varstvo pomeni, da so na ta način zbrani podatki varovani ne le na podlagi 38. čl. Ustave RS, temveč tudi na podlagi 37. čl. Ustave RS. Sama vsebina pogovora oziroma posnetka, posredovanega preko kateregakoli komunikacijskega sredstva (na primer telefona), pa primarno ni varovana kot informacijska (38. čl. Ustave RS), temveč kot komunikacijska zasebnost (37. čl. Ustave RS).

Pravica do komunikacijske zasebnosti obsega tajnost vseh vrst občil in s tem varuje tajnost komunikacije, ki je posredovana s katerimkoli komunikacijskim sredstvom. Namen tega varstva je v preprečevanju, da bi se kdorkoli seznanil z vsebino posredovanega poročila. Prav tako pa ta pravica zagotavlja svobodo komuniciranja, ki se izraža kot svobodna odločitev posameznika o tem, komu in kako bo določeno sporočilo posredovano, iz česar izhajajo prepovedi nesorazmernih poseganj v posameznikovo odločitev, kako, kdaj in s kom bo komuniciral.

Ustavno sodišče RS se je v preteklosti že večkrat srečalo s pooblastili državnih varnostnih in obveščevalno-varnostnih organov, ki posegajo v (komunikacijsko) zasebnost (U-I-25/95, U-I-158/95, Up-412/03-21, U-I-383/98, in U-I-152/03). Glavne poudarke naštetih odločb je pri sprevku *Nekateri aktualni problemi komunikacijske zasebnosti, Nadzor telekomunikacij* (Pravna praksa, 26/33; glej tudi Teršek, A: *Ustavnopravna analiza razmerja med 35. in 37/2. členom Ustave RS*, Pravna praksa, l. 2003/10) strnil Igor Vuksanović:

1. zakon, ki dovoljuje posege, mora biti posebej jasen in določen in delovanje državnih organov na njegovi podlagi mora biti predvidljivo. Urejati mora nadzor nad uporabo ukrepov ter pravna sredstva zoper zlorabo. V zakonu morajo biti opredeljene kategorije ljudi, ki jim je možno prisluškovati, vrsta in stopnja suma, ki je potrebna za začetek izvajanja ukrepa, natančno morajo biti določena kazniva dejanja, trajanje prisluškovanja, predpisan mora biti postopek, po katerem se ravna s povzetki pogovorov, določene morajo biti okoliščine in pogoji za njihovo uničenje ter urejeni kontrolni mehanizmi;

2. "nujnost" posega je treba razumeti v smislu splošnega ustavnega načela sorazmernosti, vključno s potrebo po tehtanju med težo posega in vrednostjo s posegom zavarovane dobrine, kar se kaže pri ustreznem določanju stopnje in vrste suma, ki zadošča za poseg, pa tudi pri določanju kaznivih dejanj, v zvezi s katerimi je poseg mogoč;

3. določno je treba v zakonu opredeliti, kdaj je poseg nujen, ker dokazov ni mogoče pridobiti na drug način ali je to nesorazmerno težko;

4. med različno intenzivnimi posegi je treba vzpostaviti diferenciacijo;

5. odredba sodišča mora vsebovati utemeljitev, zakaj je v konkretnem primeru ukrep nujno potreben, in mora splošno gledano izvajanje ukrepa omejiti na nujno potrebno mero.

Po 2. odst. 37. čl. Ustave RS lahko samo zakon predpiše, da se na podlagi odločbe sodišča za določen čas ne upošteva varstvo tajnosti pisem in drugih občil in nedotakljivost človekove zasebnosti, če je to nujno za uvedbo ali potek kazenskega postopka ali za varnost države. Po tej ustavni določbi morajo biti izpolnjeni štirje osnovni pogoji za omejitev te pravice:

1. poseg v pravico mora biti vnaprej abstraktno določen v zakonu,
2. poseg v to pravico mora biti časovno omejen,
3. konkreten poseg v to pravico je dopusten, če je dovoljen z odločbo, izdano s strani sodne veje oblasti,
4. omejitev je dopustna, če je to nujno za uvedbo ali potek kazenskega postopka ali za varnost države.

K spoštovanju te pravice so nedvomno zavezani najmanj vsi organi, ki delujejo na območju jurisdikcije Republike Slovenije, in tudi vsi tisti, katerih dejanja bi imela posledice na območju Republike Slovenije.

Enako kot pravica do varstva osebnih podatkov, sta tajnost pisem in drugih občil ter svoboda komuniciranja, prav tako zajeti v 8. čl. EKČP. Obširno prakso v zvezi z razumevanjem pravice do komunikacijske zasebnosti je prav tako razvilo ESČP, zato vlagatelj zahteve na tem mestu omenja samo nekatere za to zadevo najpomembnejše poudarke iz njegove sodne prakse:

- »Besedna zveza »v skladu z zakonom« v smislu 2. odst. 8. čl. kot temeljna zahteva, da ima ukrep podlago v domačem zakonu, nanaša pa se tudi na kvaliteto spornega predpisa, ki mora biti v skladu z vladavino prava in dostopen prizadeti osebi, ta pa mora biti zmožna predvideti njegove posledice zanjo. Druga zahteva, ki izvira iz besedne zveze »v skladu z zakonom«, v pričujočem primeru ne predstavlja težave. Tega pa ne moremo trditi za tretjo zahtevo po predvidljivosti predpisa. (…) Nikjer na primer niso definirane skupine oseb, za katere je moč sodno odrediti prisluškovanje telefona, niti narava prestopkov, ki upravičujejo tovrstno odredbo. (…) Podobno nedoločeni so postopki za izdelavo poročil, ki vsebujejo prestrežene pogovore …« (*Huvig proti Franciji*, št. 11105/84, 24. 4. 1990).
- »Za poseg v pravico do komunikacijske zasebnosti gre že, ko je komunikacija prestrežena in se je tretji seznanil z vsebino posredovanega poročila« (*Kopp proti Švici*, št. 23224/94, 25. 3. 1998).

Tudi zahteve ESČP v zvezi z vsebino komunikacijske zasebnosti obširno obravnava Igor Vuksanović, ki obenem poudarja, da je vprašanje dopustnosti strateškega nadzora telekomunikacij obravnavalo ESČP v zadevi *Weber in Saravia proti Nemčiji* (št. 54934/00, 29. 6. 2006), kjer je kot očitno neutemeljeno zavrnilo zahtevo za obravnavo kršitve konvencijskih pravic (8., 10. in 13. člen). Kot eden od temeljnih elementov presoje pri presoji testov sorazmernosti je bilo v tem primeru upoštevano, da je tak

ukrep v nemškem pravu dopusten le zaradi odvrnitve nekaterih temeljnih nevarnosti za državno varnost in da je presojana nemška ureditev vsebovala natančne varovalke v zvezi z odrejanjem in izvajanjem spornega ukrepa in tudi v zvezi z ravnanjem v zvezi s tako pridobljenimi podatki.

Kot je bilo ugotovljeno, lahko izvajanje 21. čl. ZSOVA vodi do zbiranja osebnih podatkov in do posega v tajnost komunikacij določljivega posameznika izven območja Republike Slovenije. Pri tem je treba upoštevati, da lahko gre v tem primeru tako za državljana RS kot tudi za tujca, ki uporabljata telekomunikacijske storitve na priključku izven območja Republike Slovenije. To lahko pomeni, da sta temeljni človekovi pravici do komunikacijske in informacijske zasebnosti neenako uporabljani za državljane RS in tujce pri komunikacijah izven ozemlja RS, saj imajo državljani po 24. členu ZSOVA višji standard varnosti, zagotovljen tako, da se za prisluhe potrebuje odredbo sodišča, za tujce pri mednarodnih komunikacijah pa se prisluh lahko odredi zgolj na podlagi odredbe predstojnika SOVA. Neenako sta pravici spoštovani tudi glede na nadzor nad telekomunikacijami na ozemlju RS in izven ozemlja za državljane RS, saj pri mednarodnih prisluhih tudi za državljana RS zadostuje zgolj odredba predstojnika SOVA.

Ob tem navajamo ločeno pritrdilno mnenje sodnika Ustavnega sodišča dr. Cirila Ribičiča (pritrdilno ločeno mnenje v zadevi št. U-I-216/07, ki se mu je pridružila sodnica dr. Mirjam Škrk):

»Necivilizirano bi bilo obravnavati ljudi, ki živijo izven njenega ozemlja kot brezpravne osebke, ki ne uživajo nobenih človekovih pravic in svoboščin. Še bolj to velja za vsakogar, ki prebiva v drugi državi članici Sveta Evrope ali v drugi državi članici Evropske Unije. Prebivalcev držav, ki skupaj s Slovenijo sestavljajo navedeni mednarodni organizaciji, ni več mogoče obravnavati kot "navadnih" tujcev, saj pripadajo skupnostim držav, ki si skupaj s Slovenijo prizadevata za skupne vrednote.«

Sodnik dr. Ribičič je dodal še, da je bilo z vidika obravnavane zadeve (zahteva predsednika Vrhovnega sodišča) pomembno, da Ustava dovoljuje posege v tajnost pisem in drugih občil zaradi varnosti države, vendar samo začasno in samo na podlagi odločbe sodišča. Po mnenju sodnika Ribičiča je določbe 21. člena Zakona o slovenski obveščevalno-varnostni agenciji mogoče in treba razlagati tako, da ne dovoljuje posegov v pisemsko tajnost konkretnih posameznikov v drugih državah. Tretji odstavek 21. člena namreč govori o tem, da se spremljanje mednarodnega sistema zvez "ne sme nanašati na določljiv priključek telekomunikacijskega sredstva ali na določenega uporabnika tega priključka na območju Republike Slovenije". Meni, da je edina ustavnoskladna razlaga te določbe tista, ki na podlagi spremljanja mednarodnega sistema zvez onemogoča posege v pisemsko tajnost katerega koli posameznika; tako tistega, ki prebiva v Sloveniji, kot tistega, ki prebiva zunaj nje! Besedilo "na območju Republike Slovenije" je treba namreč razlagati restriktivno, torej tako, da se nanaša le na določenega uporabnika in ne tudi na določljiv priključek telekomunikacijskega sredstva (pri katerem omejitev, da se nanaša na območje Republike Slovenije, ni izrecno določena). Takšna razlaga 21. člena, ki bi jo podalo Ustavno sodišče v interpretativni odločbi ali v okviru sklepa o zavrženju, bi preprečila, da bi lahko država

posegala v človekove pravice in svoboščine prebivalcev drugih držav tudi brez odločbe sodišča.

Ob tem še enkrat poudarjamo, da SOVA prisluhe mednarodnih zvez izvaja na konkretne telefonske številke.

Zato vlagatelj zahteve tudi ocenjuje, da izpodbijana določba 21. čl. ZSOVA ni v skladu s 37. čl. Ustave RS, in sicer iz naslednjih poglavitnih razlogov:

- poseg v pravico do komunikacijske zasebnosti v zakonu ni vnaprej določen tako, da bi omogočal jasne in preverljive razmere, okoliščine in razloge, pod katerimi bi bil ta poseg dopusten;
- niso navedene tiste diferencirane okoliščine, ki bi varnost države podrobneje specificirale;
- ni določeno, v kakšnih razmerah in na kakšen način se ta poseg lahko opravi;
- iz te določbe ne izhaja zahteva po potrebnih časovnih omejitvah tega posega, ki bi se lahko razlikovali glede na različnost okoliščin;
- za posege v pravico določljivega posameznika (državljana RS ali tujca), četudi se nahaja oz. uporablja priključek izven območja Republike Slovenije, se v očitnem nasprotju s 37. čl. Ustave RS ne zahteva predhodnega dovoljenja v obliki sodne odločbe;
- ni navedenih razlogov, ki bi omogočali preizkus, ali je bil poseg dopusten, ker je bil nujen, potreben in primeren za varnost države.

Vlagatelj ocenjuje, da izpodbijana določba 21. čl. ZSOVA predpisuje in omogoča način posega v komunikacijsko zasebnost v nasprotju s temeljnimi pogoji, ki jih za tak poseg zahteva 37. člen Ustave. Nadalje je določba 21. člena ZSOVA izrazito podnormirana in v nasprotju z zahtevo po sorazmernosti in pravni določnosti, kot temeljnima prvinama pravne države, in s tem krši 2. člen Ustave: poseg v pravico do komunikacijske zasebnosti v izpodbijani določbi zaradi svoje nejasnosti in podnormiranosti ni vnaprej določen tako, da omogoča predvidljivost situacij, v katerih je poseg dopusten in v kakšnem obsegu; trajanje ukrepa ni časovno omejeno; ena temeljnih ustavnih pravic - pravica do zasebnosti - se v nasprotju z načelom sorazmernosti podreja sicer legitimnemu, a splošnemu in nižjemu cilju: ”zagotavljanju ..., političnih in gospodarskih interesov države”; ni navedenih razlogov, ki bi omogočali preizkus, ali je izvedba ukrepa dopustna, glede na njegovo nujnost, potrebnost in primernost za varnost države; nedoločnost in premajhna vsebinska diferenciacija ukrepov iz 21. in 24. člena ZSOVA odpira možnost, da se na podlagi arbitrarne presoje organa izvršilne veje oblasti, pod zelo različnimi pogoji vsebinsko zelo podobno posega v ustavno varovano pravico do zasebnosti. Nazadnje je 21. člen ZSOVA tudi v nasprotju s pravico do pravnega varstva po 25. členu Ustave, saj njegova ureditev onemogoča učinkovit pravni nadzor ter ustrezna in učinkovita sredstva zoper zlorabo ukrepa, ki ga regulira - ureditev izključuje predhodno, *de facto* pa tudi naknadno sodno varstvo: ukrep odreja direktor Agencije; izvaja se brez vednosti osebe, v katere zasebnost ukrep neposredno ali posredno posega; zakon ne zahteva niti naknadnega obveščanja posameznika o izvedenem ukrepu.

Vlagatelj zahteve opozarja tudi, da v ZSOVA ni opredeljen termin »spremljanje mednarodnih sistemov zvez«, kar zaradi nejasnosti in nedoločnosti predstavlja kršitev načela pravne države.

Ob nedavnih dogodkih, ki so vzbudili tudi zanimanje javnih občil, so se z vprašanjem ustavne skladnosti izpodbijane določbe ukvarjali tudi pravniki, od tega poglobljeno in s primerjalnopravnim prikazom Igor Vuksanović, v zgoraj navedenem članku.

Ustavno sodišče RS je v odločbi št. U-I-152/03 z dne 23. marca 2006 poudarilo, da morajo biti v primerih posegov v človekove pravice, izvedenih v preventivne namene, pooblastila države še bolj omejena kot sicer, pri običajnem testu sorazmernosti, kot izhaja iz 2. čl. Ustave RS. Ne glede na verjetno potrebnost in dopustnost določene omejene in nadzorovane oblike strateškega nadzora telekomunikacij, pa bo potrebno razrešiti vprašanje, na kakšen način bi bil strateški nadzor na telekomunikacijah urejen na ustavno dopusten način in kako bi združeval potrebo po pridobitvi sodne odločbe pri nadzoru nad določljivimi posamezniki, nad eksplicitno določenimi dejavnostmi ali aktivnostmi, ki neposredno in huje ogrožajo varnost države.

Podoben pristop je ubralo tudi Ustavno sodišče Zvezne republike Nemčije v dne 27. 2. 2008 izdani odločbi št. 1 BvR 370/07 in 1 BvR 595/07, v kateri je presojalo ustavnost nemškega zakona, ki je določal skrivni oz. tajen dostop do informacijskih sistemov preko t. i. trojanskih konjev (t.i. on-line preiskava). Presodilo je namreč, da je v neskladju z ustavo ureditev, ki obveščevalni službi omogoča neposreden in brez vnaprej znanih pravil dostop do informacijskih sistemov (računalnikov), posledično pa preko različnih informacijskih ukrepov, tudi kopiranje celotnih diskov ter celo nadzor oz. krmiljenje posameznikovega informacijskega sistema. Po tej odločbi je zakon, ki je omogočal tajno infiltracijo v posameznikov informacijski sistem, zaradi nedoločnosti, saj ni določal potrebe po vnaprejšnji konkretni nevarnosti in pravne dobrine, zaradi katere bi bil poseg v zasebnost primeren, potreben in nujen, v nasprotju z načelom sorazmernosti. Nemško Zvezno ustavno sodišče je poudarilo, da gre za hud poseg v komunikacijsko zasebnost, ki je ustavno dopusten le, če je v skladu z načeli pravne države, predvsem načelom sorazmernosti in če so v zakonu predvideni zadostni zakonski ukrepi, ki preprečujejo poseg v popolnoma zaščiteno jedro oziroma bistvo posameznikove zasebnosti.

Sodba je v celoti dosegljiva na spletni strani:

http://www.bverfg.de/entscheidungen/rs20080227_1bvr037007.html

Na tem mestu se dodatno zastavlja tudi vprašanje, ali Ustava RS dovoljuje različne standarde posega v pravico do komunikacijske zasebnosti pri izvajanju strateškega nadzora telekomunikacij oziroma pri izvajanju takšnega nadzora telekomunikacij, ki vodi v poseg v pravico do komunikacijske zasebnosti določljivega posameznika na območju Republike Slovenije (to vprašanje naj bi bilo sicer urejeno v 24. čl. ZSOVA), oziroma določljivega (ne)državljana Republike Slovenije izven njenega ozemlja (21. čl. ZSOVA).

Pri pritrdilnem odgovoru na to vprašanje bo moralo Ustavno sodišče osvetliti tudi razlike med standardi, ki bi bile ustavnopravno skladne.

Pri tem je potrebno posebej poudariti, da Ustava RS za posege v komunikacijsko zasebnost predpisuje strožje pogoje kot EKČP. Celo več - Ustava RS je ena redkih v evropskem prostoru, ki za vse (!) posege v komunikacijsko zasebnost izrecno zahteva predhodno sodno odredbo. V tej luči je brez vrednosti morebiten argument, da mnoge evropske države (ne pa vse!) za posege v zasebnost s strani obveščevalno-varnostnih služb (za razliko od ukrepov s strani organov odkrivanja in pregona) pogosto ne zahtevajo sodne odredbe. Primerjaj odločbo US RS, št. U-I-25/95: "Dejstvo, da govori Ustava o odločbi sodišča, samo na podlagi katere je poseg v zasebnost dovoljen, pomeni po že zavzetem stališču Ustavnega sodišča, da se zahteva odločanje o posegu s strani sodne (in ne izvršilne!) veje oblasti. Tudi ta določba temelji na načelu pravne države, po katerem mora biti vmešavanje izvršilne oblasti v pravice posameznika podvrženo učinkoviti kontroli, ki naj bi bila zaupana predvsem sodišču."

V luči zgoraj zapisanega je prvo vprašanje, ali pomeni ukrep, kot je urejen v 21. členu ZSOVA, poseg v komunikacijsko zasebnost. Odgovor na to vprašanje po mnenju vlagatelja ne more biti sporen. Ukrep vodi do zbiranja podatkov o elektronskih (npr. telefonskih in internetnih) komunikacijah posameznikov, ki so - kot je bilo ugotovljeno - vnaprej ali *ex post* (z naknadno analizo podatkov) določeni ali vsaj določljivi. Kot je bilo ugotovljeno pri inšpekcijskem pregledu, je zmotno morebitno sklepanje, na katerega lahko napeljuje termin "spremljanje mednarodnih sistemov zvez", da gre za zajemanje velikega snopa komunikacij, ki ga na podlagi določenih filtrov (npr. ključnih besed) nepersonificirano obdeluje računalnik z namenom iskanja določenih vzorcev, trendov, nepersonificiranih informacij ter da je za konkreten "prisluh" vedno uporabljen 24. člen ZSOVA. 21. člen ZSOVA v praksi vodi do zbiranja osebnih podatkov in do "prisluhov" konkretnim osebam, pri čemer ej ključna razlika od klasičnega "policijskega prisluškovanja" ali nadzora po 24. členu ZSOVA v tem, da tak nadzor primarno ni osredotočen na osebo, ampak na vsebino komunikacije oziroma na komunikacijsko sredstvo in da Agencijo primarno zanima pridobljen podatek in zgolj sekundarno oseba, ki komunicira. Poseg v pravico do komunikacijske zasebnosti nastane že s samim dejstvom, da je nekdo izven ustavnih in zakonskih omejitev prestregel komunikacijo in se seznanil z njeno vsebino (glej Kopp proti. Švici). Pri tem je nepomembno, ali je bilo prestreženo sporočilo pozneje uporabljeno v kakršenkoli namen (npr. ali so bili izsledki prisluškovanja uporabljeni v poznejšem kazenskem postopku in ali je osebo prizadela kakršnakoli druga sankcija).

S tem v zvezi je potrebno ponoviti ustaljeno ustavnosodno doktrino pojmovanja pravice do zasebnosti tako v ZDA (Katz proti US), Evropi (Halford proti Združenemu kraljestvu, 25. 6. 1997) kot Sloveniji (Odl US VI, 158, U-I-25/95). Po doktrini utemeljenega pričakovanja zasebnosti, pravo (Ustava) primarno ne ščiti prostorov, lastnine ali lastnikov, temveč posameznike, ki v določenem trenutku, v določenem prostoru ali pri določenem ravnanju (upravičeno) pričakujejo svojo zasebnost (glej več Klemenčič, G.: Komentar 37. člena, v: Šturm, L. (ur.): Komentar Ustave RS, Fakulteta za podiplomske državne in evropske študije, Ljubljana, 2002; Zupančič, B.M. in drugi: Ustavno kazensko procesno pravo, 3. izdaja, Založba Pasadena, Ljubljana 2000). Povedano v kontekstu 21. člena ZSOVA: ustava ščiti ljudi in njihovo zasebnost in ne telefonskih priključkov! Zato ni pomembno, ali gre za mednarodno zvezo, za "zadevo" ..., če za njo stoji določljiv (pa čeprav naknadno) posameznik, ki naj bi užival bodisi jamstva slovenske

ustave, bodisi jamstva EKČP. Analogno bi nas po logiki *in absurdum* pojmovanje, da "neosredotočen" poseg v zasebnost ne spada pod jamstva Ustave, privedlo do situacije, ko bi npr.varnostni organi lahko izvajali hišne preiskave brez odločb sodišča mimo strogih jamstev 36. člena, dokler bi zgolj iskali določene predmete in informacije, imetnik stanovanja pa jih ne bi zanimal. Ali kot je v pritrdilnem ločenem mnenju k zadevi OdlUS VI, 158, U-I-25/95 zapisal takratni ustavni sodnik dr. Boštjan M. Zupanič: "Vprašanje pa ne more biti -- že zaradi varstva zaupanja v pravo --, ali Ustava varuje le zasebnost kot tako, oziroma ali varuje tudi pričakovanje zasebnosti. Jasno je in je skoraj tavtologija, če rečemo, da je namen objektivnega ustavnega varstva zasebnosti, da daje podlago -- ker kaj pa je zasebnost drugega kot pričakovanje? -- za subjektivno pričakovanje zasebnosti. K bistvu vsake pravice (tudi lastninske in vseh drugih) sodi pravna garancija, da bo na pravni normi utemeljeno pričakovanje tudi udejanjeno."

Nenazadnje je celo predlagatelj zakona ob sprejemu ZSOVA med obrazložitvami posredno priznal, da ukrep pomeni poseg v komunikacijsko zasebnost: "Zakonodajalec je izhajal iz teze, da morajo imeti obveščevalni organi, za razliko od organov kazenskega pregona (večjo) pravico delovati proaktivno; zaradi tega morajo imeti načelno možnost posega v komunikacijsko zasebnost ljudi, 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. januar 1999).

Če ne more biti sporno, da ukrep iz 21. člena ZSOVA posega v komunikacijsko zasebnost (najmanj v delu, ki se nanaša na komunikacije *ex ante* ali *ex post* določljive osebe), je ključno vprašanje, ali gre za poseg, ki ga z vidika veljavnosti in pristojnosti omejuje Ustava RS. Tudi če sprejmemo izrazito restriktivno razlago, omejeno na ozek teritorialen princip pristojnosti, ki jo je Ustavno sodišče RS nakazalo v sklepu št. U-I-216/07 (ker gre za sklep, v katerem ni meritorno odločalo o zadevi, vlagatelj meni, da tako stališče US v kontekstu celotne ocene 21. člena ZSOVA in precendenčno zavezujoče oziroma dokončno), ko je zavrnilo ustavno presojo ZSOVA, vloženo s strani predsednika Vrhovnega sodišča, je vlagatelj še vedno mnenja, da ima uporaba spornega člena ZSOVA za posledico kršitev 37. člena Ustave.

Na tovrsten problem opozarja tudi Franc Testen, predsednik Vrhovnega sodišča: "Glede na to, da se izvajanje ukrepov v primeru elektronskih komunikacij odvija v ti. kiberprostoru, ki nima lastnosti prostora v fizikalnem, geografskem smislu, bi se lahko sicer zastavilo vprašanje, ali ni mogoče lokacije, ki v pravnem smislu določa, kje se ukrep izvaja, določiti tudi z navezavo na druge okoliščine – na primer na kraj, kjer se nahajajo osebe oziroma naprave, s katerimi se ukrep izvaja - in ne nujno na to, na katerem krajevnem območju se nahaja elektronski priključek, žična zveza ali druga fizična naprava, ki omogoča nastanek podatka, njegov prenos oziroma komunikacijo. V tem primeru bi lahko utemeljili, da se tudi navedeni ukrep izvaja v Sloveniji. Vendar je predsednik Vrhovnega sodišča izhajal iz utečene prakse pri obsedanjem izvajanju določbe 24. člena ZSOVA, ki je kot kraj, kjer se opravlja nadzorovanje in snemanje telekomunikacij, vedno štel kraj, kjer se nahaja konkreten telekomunikacijski priključek: za potrebe 24. člena ZSOVA torej telefonski, elektronski in drugi priključki slovenskih operaterjev. Da je na ta način mogoče določiti lokacijo telefonskega priključka, nenazadnje izhaja tudi iz tretjega odstavka 21. člena ZSOVA, ki ne locira dejavnosti (izvajanje ukrepa – ki v določenem smislu »plava« v kiberprostoru), ampak priključek sam (ki se nahaja na določenem prostoru v fizičnem smislu)." (Sklep predsednika VS RS, Pp 2/2007 z dne 12.11.2007)

Kot je bilo ugotovljeno, se nadzor po 21. čl. ZSOVA fizično izvaja na ozemlju RS, zaradi tehnične zahtevnosti (npr. pri mobilni telefoniji, elektronski pošti, vse bolj pogosti telefoniji preko interneta – VoIP, internetnih povezavah), pa je pri mednarodnih zvezah težko ločiti primere, ko komunikacija izvira iz ozemlja Slovenije, se končuje na ozemlju Slovenije, ko oseba (slovenski ali tuji državljan) na ozemlju Slovenije uporablja tuje komunikacijsko sredstvo, ali ko je v komunikacij, ki zgolj "poteka" preko ozemlja Slovenije, vključen slovenski državljan (kot naslovnik ali sprejemnik). Že iz tega vidika gre vsaj v določenih primerih - tudi po teritorialnem principu - za poseg v 37. člen Ustave.

Vsakršen tajni nadzor komunikacij po 21. člen ZSOVA nadalje torej vselej po sami naravi trči v pravico do zasebnosti tretjih oseb, s katerimi nadzorovana oseba komunicira, oziroma oseb, ki uporabljajo določeno komunikacijsko sredstvo. V luči sporne določbe ZSOVA lahko govorimo o več kot zgolj hipotetični možnosti verižne proliferacije oseb, ki bodo prizadete v svoji zasebnosti (glej npr. odločitev ESČP v primeru Klass in nemško ureditev ali ameriško ureditev "strateškega nadzora", ki se poskuša temu v čim večji meri izogniti).

Kot je bilo ugotovljeno, lahko izvajanje 21. čl. ZSOVA vodi do zbiranja osebnih podatkov in do posega v tajnost komunikacij določljivega posameznika izven območja Republike Slovenije. Pri tem je treba upoštevati, da lahko gre v tem primeru tako za državljana RS kot tudi za tujca, ki uporabljata telekomunikacijske storitve na priključku izven območja Republike Slovenije. To lahko pomeni, da sta temeljni človekovi pravici do komunikacijske in informacijske zasebnosti neenako uporabljani za državljane RS in tujce pri komunikacijah izven ozemlja RS, saj imajo državljani po 24. členu ZSOVA višji standard varnosti, zagotovljen tako, da se za prisluhe potrebuje odredbo sodišča, za tujce pri mednarodnih komunikacijah pa se prisluh lahko odredi zgolj na podlagi odredbe predstojnika SOVA. Neenako sta pravici spoštovani tudi glede na nadzor nad telekomunikacijami na ozemlju RS in izven ozemlja za državljane RS, saj pri mednarodnih prisluhih tudi za državljana RS zadostuje zgolj odredba predstojnika SOVA.

Po mnenju vlagatelja je zgolj teritorialna omejitev dosega jamstev komunikacijske zasebnosti - v luči nekaterih ostalih veljavnih predpisov - v nasprotju z 2. členom ustave. Širši vidik pravne države namreč zahteva tudi pravno varnost, ki jo med drugim zagotavlja sistemska skladnost in preglednost pravnih norm. Tako npr. Zakon o elektronskih komunikacijah, ki na zakonski ravni udejanja varstvo tajnosti elektronskih komunikacij in z njimi povezanimi osebnimi podatki, v ničemer ne razlikuje med tajnostjo "domačih" in "mednarodnih komunikacij". Še pomembneje pa se zdi vlagatelju opozoriti, da skladno z določbami Kazenskega zakonika (členi 120 - 126) Slovenija svojo represivno oblast skladno s t.i. personalitetnim načelom širi na vsa kazniva dejanja (ob pogoju dvojne kaznivosti), ki jih slovenski državljani storijo v tujini, in na tujce, ki v tujini storijo kaznivo dejanje zoper slovenske državljane ali slovensko državo. Absurdno bi bilo, da bi Ustava RS dovoljevala, da država na eni strani širi svojo represivno oblast na ravnanje svojih državljanov - in v nekaterih primerih tudi tujih državljanov - izven svojih meja, hkrati pa tem istim osebam izven svojih meja ne bi zagotavlja temeljnih varstev pred neupravičenimi posegi v zasebnost s strani državnih organov te iste države.

Četudi bi sprejeli ozko stališče teritorialnega principa, Slovenijo zavezuje vsaj 8. člen EKČP. Ta določene posege v komunikacijsko zasebnost dovoljuje tudi brez sodne odredbe, vendar še vedno zahteva zakonsko ureditev, ki je določna, predvidljiva, nujna v demokratični družbi in sorazmerna.

Vprašanje, ali gre v primeru 21. člena ZSOVA za regulativo, ki v nasprotju z Ustavo omogoča posege v zasebnosti, je navsezadnje ključno povezano tudi z določnostjo in vsebino izpodbijane oblike posebnega pridobivanja podatkov. Kot je zapisalo US v odločbi št. U-I-383/98, je ocena, ali določeni ukrepi državnih organov posegajo v ustavno varovano zasebnost, odvisna od vsebine posameznega ukrepa oziroma od pristojnosti državnega organa pri njihovem izvajanju. Tudi - in v prvi vrsti - s tega vidika je ureditev 21. člena ZSOVA v nasprotju z Ustavo RS.
Na koncu Ustavno sodišče vlagatelj še obvešča, da na enak ustavnopravni problem naletimo tudi pri Zakonu o obrambi, kjer se 4. odstavek 32. čl. Zakona o obrambi (Ur. l. RS, št. 82/94 ter spremembe, ZObr) glasi:

(4) Elektronsko spremljanje mednarodnih sistemov zvez, pomembnih za obrambne interese države, opravljajo za obveščevalno varnostno službo ministrstva in druge potrebe, enote za elektronsko bojevanje Slovenske vojske.

Povsem enaki argumenti za neskladnost z Ustavo RS po oceni vlagatelja veljajo torej tudi za določbo 32. čl. Zakona o obrambi, ki v drugem in tretjem odstavku opredeljuje »obveščevalne, protiobveščevalne in varnostne naloge«, ki jih opravlja obveščevalno varnostna služba Ministrstva za obrambo, v spornem četrtem odstavku pa nedopustno širi spremljanje mednarodnih sistemov zvez za vnaprej nedoločene namene.

Izpodbijana določba je po oceni vlagatelja zahteve v neskladju 2., 15., 37. in 38. čl. Ustave, zato Informacijski pooblaščenec

p r e d l a g a,

da Ustavno sodišče RS oceni njeno ustavnost, ugotovi neskladnost z Ustavo ter naloži Državnemu zboru RS odpravo tega neskladja v razumnem roku.

Hkrati tudi predlagamo, da Ustavno sodišče zadevo obravnava prednostno.

Informacijski pooblaščenec:
Nataša Pirc Musar,
informacijska pooblaščenka