REPUBLIKA SLOVENIJA
INFORMACIJSKI POOBLAŠČENEC
Zaloška 59, 1000 Ljubljana, Slovenija
T: 01 230 9730
F: 01 230 9778
gp.ip@ip-rs.si
www.ip-rs.si

Številka: 050-1/2017/1

Datum: 22.6.2017

USTAVNO SODIŠČE REPUBLIKE SLOVENIJE

Beethovnova 10

1000 Ljubljana

Informacijski pooblaščenec na podlagi 22. člena v zvezi s šesto alinejo prvega odstavka 23a. člena Zakona o Ustavnem sodišču (Ur. l. RS, št. 64/2007 - UPB, ZUstS) vlaga v zvezi z zadevo inšpekcijskega nadzora pod št. 0612-81/2013 na Ustavno sodišče RS (v nadaljevanju US RS)

ZAHTEVO ZA OCENO USTAVNOSTI

prvega in tretjega odstavka 21. člena Zakona o Slovenski obveščevalno-varnostni agenciji (Ur. l. RS, št. 81/2006-UPB2; ZSOVA) zaradi neskladja z 2., 15., 37. in 38. členom Ustave Republike Slovenije (Ur. l. RS, št. 33/91-I, 42/97 – UZS68, 66/00 – UZ80, 24/03 – UZ3a, 47, 68, 69/04 – UZ14, 69/04 – UZ43, 69/04 – UZ50, 68/06 – UZ121,140,143, 47/13 – UZ148, 47/13 – UZ90,97,99 in 75/16 – UZ70a; URS)

ZSOVA določa: »*21. člen*
(1) Spremljanje mednarodnih sistemov zvez ter tajni nakup dokumentov in predmetov dovoljuje direktor agencije s pisno odredbo.
…
(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. Obstoj procesnih predpostavk

Informacijski pooblaščenec je v skladu z drugo alinejo prvega odstavka drugega člena Zakona o Informacijskem pooblaščencu (Ur. l. RS, št. 113/05 in 51/07 – ZUstS-A; ZInfP) v okviru načrtovanih inšpekcijskih ogledov pri upravljavcih javnega sektorja po uradni dolžnosti v letu 2013 začel postopek inšpekcijskega nadzora št. 0612-81/2013 nad izvajanjem določb Zakona o varstvu osebnih podatkov (Ur. l. RS, št. 94/07 – uradno prečiščeno besedilo; ZVOP-1) in drugih predpisov, ki urejajo varstvo ali obdelavo osebnih podatkov oziroma iznos osebnih podatkov iz Republike Slovenije pri Slovenski obveščevalno-varnostni agenciji (v nadaljevanju SOVA). Namen postopka inšpekcijskega nadzora je bil preveriti, ali obdelava osebnih podatkov pri spremljanju mednarodnih sistemov zvez – ki zajema med drugim nedvomno tudi zbiranje in obdelavo osebnih podatkov, kar je Ustavno sodišče RS že ugotovilo[1], enako pa ugotavlja tudi Informacijski pooblaščenec v okviru predmetnega postopka inšpekcijskega nadzora – kot jo urejajo določbe ZSOVA, poteka skladno z določbami ZVOP-1 in

[1] V točki 9 sklepa št. U-I-45/08-21, z dne 8. 1. 2009 (OdlUS XIII, 3) in v točki 7 U-I-216/07-8, z dne 4. 10. 2007 (Ur. l. RS, št. 99/2007 in OdlUS XVI, 75).

drugih predpisov, ki urejajo varstvo osebnih podatkov. Državni nadzorniki za varstvo osebnih podatkov so v ta namen opravili več ogledov na sedežu zavezanca ter pridobili odgovore zavezanca na pozive za podajo pisnih pojasnil in dokumentacije. Večina dokumentov je zaradi varovanja tajnih podatkov označena s stopnjami tajnosti. Državni nadzornik za varstvo osebnih podatkov je na podlagi ugotovljenega dejanskega stanja, kot je podrobno opisano v zapisnikih in ostalih dokumentih zadeve št. 0612-81/2013, povzel svoje ugotovitve v dokumentu, ki vsebuje s strani zavezanca označene tajne podatke, zato je označen s stopnjo zaupnosti TAJNO in se hrani pri zavezancu.[2]

V okviru tega postopka in upoštevajoč nedavno sodno prakso Ustavnega sodišča[3] ter Evropskega sodišča za človekove pravice (v nadaljevanju ESČP)[4] je državni nadzornik za varstvo osebnih podatkov pri izvrševanju svojih pristojnosti naletel na zakonske določbe (prvega in tretjega odstavka 21. člena ZSOVA), ki mu zaradi domnevnega neskladja z Ustavo preprečujejo učinkovito zagotovitev varstva informacijske zasebnosti. Nastal je pravni položaj, ko predlagatelj ne more nadaljevati, zakonito izpeljati in zaključiti postopka inšpekcijskega nadzora, preden ta dvom, ki ga lahko naslovi edino Ustavno sodišče, ni razčiščen.

Konkretno se je po mnenju predlagatelja **pojavilo vprašanje ustavnosti in zakonitosti:**

1. **prvega odstavka 21. člena ZSOVA v delu**, ki se nanaša na pooblastilo SOVA za **»spremljanje mednarodnih sistemov zvez« zgolj na podlagi odredbe direktorja SOVA** brez odredbe sodišča ter
2. **tretjega odstavka 21. člena ZSOVA v delu**, ki se nanaša na pravno **neopredeljeno pooblastilo SOVA za »spremljanje mednarodnih sistemov zvez« pod vsebinsko nejasnim pogojem**, da ne sme iti za spremljanje določljivega priključka telekomunikacijskega sredstva ali določenega uporabnika tega priključka na območju Republike Slovenije, iz katerega zgolj na podlagi ZSOVA in drugih predpisov **ni mogoče razbrati, katere osebne podatke, lahko na tej podlagi SOVA zakonito zbira in kako dolgo jih lahko hrani.**

Ustavno sodišče v 8. točki sklepa št. U-I-45/08-21, z dne 8. 1. 2009 (OdlUS XIII, 3), v katerem je odločalo o zahtevi Informacijskega pooblaščenca v zvezi z 21. členom ZSOVA pojasnjuje, da »… kadar predlagateljica pri izvrševanju svojih pristojnosti ugotovi, da so izpolnjeni pogoji za odreditev ukrepov, ki jih določa ZVOP-1, jih mora kot pristojni državni organ tudi odrediti. Inšpekcijski ukrepi, ki so ji na voljo v 54. členu ZVOP-1, ji omogočajo, da zaščiti domnevno ogrožene človekove pravice oseb, ki jim je SOVA prisluškovala. Kadar pa predlagateljica pri izvrševanju svojih pristojnosti naleti na zakonske določbe, ki ji zaradi domnevnega neskladja z Ustavo preprečujejo učinkovito zagotovitev varstva informacijske zasebnost (38. člen Ustave), lahko vloži zahtevo za oceno ustavnosti. Samo v tem primeru je Informacijska pooblaščenka upravičena oseba za vložitev zahteve iz šeste alineje prvega odstavka 23.a člena ZUstS.«

Podobno izhaja iz odločbe USRS v zvezi z zahtevo za oceno ustavnosti in zakonitosti Zakona o dostopu do informacij javnega značaja (Ur. l. RS, št. 51/06 – uradno prečiščeno besedilo, 117/06 – ZDavP-2, 23/14, 50/14, 19/15 – odl. US in 102/15)[5], da mora biti za obstoj procesne legitimacije za vložitev zahteve po 23.a členu ZUstS v zvezi z vprašanjem dvoma o ustavnosti ali zakonitosti v zvezi s postopkom, ki ga pooblaščeni predlagatelj vodi, podan položaj, ko predlagatelj »ne more nadaljevati postopka nadzora, preden ni ta dvom razčiščen«.

54. člen ZVOP-1 določa, da ima nadzornik, ki pri opravljanju inšpekcijskega nadzora ugotovi kršitev tega zakona ali drugega zakona ali predpisa, ki ureja varstvo osebnih podatkov, pravico takoj:

---

[2] Vsebinsko povzemanje teh dokumentov na način, da bi bili razkriti tajni podatki, za namen vložitve te zahteve ni potrebno, zato predmetna zahteva ni označena z nobeno od stopenj tajnosti.

[3] Odločba št. U-I-246/14-20 z dne 24. 3. 2017, v kateri je USRS ugotovilo neskladnost prvega odstavka 154. člena Zakona o kazenskem postopku (Ur. l. RS, št. 32/12 – uradno prečiščeno besedilo, 47/13, 87/14, 8/16 – odl. US, 64/16 – odl. US in 65/16 – odl. US) z URS, kolikor določa, da podatke, sporočila, posnetke ali dokazila, pridobljene z uporabo prikritih preiskovalnih ukrepov, hrani sodišče, dokler se hrani kazenski spis.

[4] Zadeva Roman Zakharov proti Rusiji, z dne 4. 12. 2015, v kateri je ESČP ugotovilo kršitev 8. člena Konvencije o varstvu človekovih pravic in temeljnih svoboščin (Uradni list RS, št. 33/94, MP, št. 7/94).

[5] U-I-201/14-14 in U-I-202/14-13, z dne 19. 2. 2015, Uradni list RS, št. 72/2014 in Uradni list RS, št. 19/2015.

1. odrediti, da se nepravilnosti ali pomanjkljivosti, ki jih ugotovi, odpravijo na način in v roku, ki ga sam določi;
2. odrediti prepoved obdelave osebnih podatkov osebam javnega ali zasebnega sektorja, ki niso zagotovile ali ne izvajajo ukrepov in postopkov za zavarovanje osebnih podatkov;
3. odrediti prepoved obdelave osebnih podatkov ter anonimiziranje, blokiranje, brisanje ali uničenje osebnih podatkov, kadar ugotovi, da se osebni podatki obdelujejo v nasprotju z določbami zakona;
4. odrediti prepoved iznosa osebnih podatkov v tretjo državo ali njihovega posredovanja tujim uporabnikom osebnih podatkov, če se iznašajo ali posredujejo v nasprotju z določbami zakona ali obvezujoče mednarodne pogodbe;
5. odrediti druge ukrepe, določene z zakonom, ki ureja inšpekcijski nadzor, ter zakonom, ki ureja splošni upravni postopek.

Potrebni predpogoj za odreditev ukrepov nadzornika je torej, d*a »nadzornik pri opravljanju inšpekcijskega nadzora ugotovi kršitev tega zakona ali drugega zakona ali predpisa, ki ureja varstvo osebnih podatkov*«. Iz ugotovitev državnega nadzornika za varstvo osebnih podatkov v predmetnem postopku inšpekcijskega nadzora pa je razvidno, da niso izpolnjeni pogoji za odreditev ukrepov, ki jih določa ZVOP-1. Inšpekcijski ukrepi, ki so Informacijskemu pooblaščencu na voljo v 54. členu ZVOP-1, namreč upoštevajoč domnevno z Ustavo neskladne določbe prvega in tretjega odstavka 21. člena ZSOVA, ne omogočajo, da bi lahko zaščitil ogrožene človekove pravice oseb, ki jim je SOVA prisluškovala.

Informacijski pooblaščenec na podlagi opravljenih procesnih dejanj v zgoraj navedenem inšpekcijskem postopku pri SOVA ocenjuje, da so pogoji za vložitev zahteve s strani predlagatelja, ki jih je v svoji dosedanji sodni praksi oblikovalo USRS (med drugim v zgoraj citiranih odločitvah US RS), izpolnjeni. Zahteva Informacijskega pooblaščenca zato, kot podrobneje pojasnjujemo v nadaljevanju, po mnenju predlagatelja izpolnjuje procesne predpostavke glede izpodbijanih določb ZSOVA, ki se nanašajo na spremljanje mednarodnih sistemov zvez.

i. Obstoj procesnih predpostavk za vložitev zahteve za oceno ustavnosti prvega odstavka 21. člena ZSOVA

21. člen ZSOVA v prvem odstavku določa, da spremljanje mednarodnih sistemov zvez dovoljuje direktor SOVA s pisno odredbo. Odredba mora v skladu z drugim odstavkom vsebovati podatke o zadevi, na katero se posebna oblika pridobivanja osebnih podatkov nanaša, način, obseg in trajanje. 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.

Ustava sicer zagotavlja varstvo zasebnosti v več določbah, vendar so različne pojavne oblike zasebnosti ločene zgolj zato, ker URS zagotavlja specifične pogoje za posege v posamezne vidike zasebnosti[6]. Na tem mestu predlagatelj zahteve opozarja na dvojno varstvo podatkov t.i. prometnih podatkov (v konkretnem primeru predvsem podatkov o osebnem imenu, telefonskih številkah, času komunikacije) in zapisu pogovora. Na to je opozorilo že Ustavno sodišče v odločbi št. U-I-25/95 z dne 27.11.1997 (Ur. l. RS, št. 5/98 in OdlUS VI, 158), ko je opredelilo dvojno varstvo pravic do zasebnosti. V tem konkretnem primeru to pomeni, da so na ta način zbrani podatki varovani ne le na podlagi 38. člena URS, temveč tudi na podlagi 37. člena URS. Sama vsebina pogovora oziroma posnetka, posredovanega preko kateregakoli komunikacijskega sredstva (na primer telefona), pa primarno ni varovana kot informacijska (38. člena URS), temveč kot komunikacijska zasebnost (37. člen URS).

[6] Več o tem Klemenčič, G.: Komentar 37. člena, v: Šturm, L. (ur.): Komentar Ustave RS, Fakulteta za podiplomske državne in evropske študije, Ljubljana, 2002.

Pravica do komunikacijske zasebnosti namreč 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 sporočila. 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.

Glede na navedeno se je državni nadzornik v konkretnem inšpekcijskem postopku soočil s stanjem, v katerem za zagotovitev pravice do varstva osebnih podatkov, kot dela pravice do komunikacijske zasebnosti, nima na voljo učinkovitih inšpekcijskih ukrepov: spremljanje mednarodnih zvez namreč poteka na podlagi odredb, ki pa jih - skladno z ZSOVA - izdaja direktor ZSOVA in ne sodišče, kar sicer zahteva za posege v komunikacijsko zasebnost drugi odstavka 37. člena Ustave. Direktor ZSOVA tako pri odrejanju ukrepov, s katerimi se posega v komunikacijsko in informacijsko zasebnost posameznikov, ni podvržen nobenemu predhodnemu sodnemu nadzoru.

V primerih ko so torej odredbe direktorja vsebinsko ustrezne glede na zahteve drugega odstavka 21. člena ZSOVA in skladne s pogoji iz tretjega odstavka 21. člena ZSOVA (se ne nanašajo na spremljanje določljivega priključka telekomunikacijskega sredstva ali določenega uporabnika tega priključka na območju Republike Slovenije), nadzornik ne more odrediti inšpekcijskih ukrepov, saj v skladu z ZSOVA ne gre za nezakonitosti, četudi se postavlja dvom o ustavni skladnosti navedenih določb.

Kot je bilo ugotovljeno, lahko izvajanje 21. člena 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 je za prisluhe zahtevana odredba sodišča, za tujce pri mednarodnih komunikacijah pa se prisluh lahko odredi (že) zgolj na podlagi odredbe direktorja 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 direktorja SOVA.

Po drugem odstavku 37. člena Ustave 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. Zakon, ki daje podlago za zbiranje osebnih podatkov, pa ne upošteva navedenih pogojev iz drugega odstavka 37. člena Ustave. Posledično so zbiranje osebnih podatkov (in druge oblike posegov v komunikacijsko zasebnost) zakoniti, predvsem pa z vidika pristojnosti vlagatelja ni podlage za izrek inšpekcijskih ukrepov. Vsekakor pa se zato poraja utemeljen dvom v ustavnost zakona, ki dopušča takšno zbiranje osebnih podatkov. Če pojasnimo s konkretnim primerom – zoper odredbo direktorja SOVA za spremljanje mednarodnih sistemov zvez z nadzorom komunikacije konkretne telefonske številke, ki se npr. nanaša na mednarodne zveze slovenskih državljanov, ko so v tujini in ki ustreza pogojem iz drugega odstavka 21. člena ZSOVA (ter se ne nanaša na spremljanje določljivega priključka telekomunikacijskega sredstva ali določenega uporabnika tega priključka na območju Republike Slovenije), državni nadzornik ne more odrediti ukrepov iz 54. člena ZVOP-1, saj je odredba

formalno zakonita. Obstaja pa utemeljen dvom, ali je zakonska podlaga, ki omogoča takšno odredbo skladna z drugim odstavkom 37. člena Ustave. O tem pa lahko, tudi v skladu z odločitvami Ustavnega sodišča[7], presoja zgolj slednje.

Informacijski pooblaščenec prav tako ni pristojen za presojo sorazmernosti in ustavne skladnosti konkretnih posegov v varstvo osebnih podatkov in komunikacijsko zasebnost na podlagi posameznih odredb preko morebitnega 'samoomejevalnega' ravnanja direktorja SOVA, s ciljem naknadnega zagotavljanja preprečevanja prekomernih posegov v zasebnost na način, da bi se zgolj 'delno' izvajala zakonsko naložena pooblastila. Za vstop predlagatelja v posamičen pravni postopek in za njegovo neposredno poseganje v vodenje takega postopka zaradi zagotavljanja ustavnoskladne in zakonite obdelave osebnih podatkov namreč ni zakonske podlage niti v določbah, ki urejajo pristojnosti predlagatelja, niti v določbah zakonov, ki ureja jo postopke odločanja o posamičnih pravnih zadevah. Če bi obstoječa ureditev predlagatelju tako pooblastilo dajala, bi to bilo po mnenju Ustavnega sodišča pri odločanju v deloma sorodnem primeru, neskladno z Ustavo.[8] Zato vlagatelj tudi na ta način ne more zagotoviti zakonitosti obdelave osebnih podatkov in odrediti ukrepov iz 54. člen ZVOP-1, ker bi sicer posegal v pristojnosti drugega organa.

ii. Obstoj procesnih predpostavk za vložitev zahteve za oceno ustavnosti za tretji odstavek 21. člena ZSOVA

Tretji odstavek 21. člena ZSOVA določa podrobneje obseg dopustnega posega v varstvo osebnih podatkov in komunikacijsko zasebnost s spremljanjem mednarodnih sistemov zvez, s tem ko določa, da **se spremljanje mednarodnih sistemov zvez ne sme nanašati na določljiv priključek telekomunikacijskega sredstva ali na določenega uporabnika tega priključka na območju Republike Slovenije.** Ugotovitve predmetnega inšpekcijskega nadzora kažejo, da na podlagi besedila tretjega odstavka 21. člena ZSOVA ni mogoče ugotoviti, katere osebne podatke lahko SOVA zakonito zbira na tej podlagi, saj ni mogoče z gotovostjo za vsak posamezen primer opredeliti, kateri osebni podatki izpolnjujejo pogoje, ki jih za zakonito spremljanje mednarodnih sistemov zvez zahteva tretji odstavek 21. člen ZSOVA.

Pogoj za dopustnost spremljanja mednarodnih zvez sta torej obstoj odredbe direktorja SOVA, ki vsebuje elemente (opredeljene v drugem odstavku 21. člena ZSOVA, t.j. podatke o zadevi, na katero se posebna oblika pridobivanja podatkov nanaša, način, obseg in trajanje) ter vsebinska zahteva, da se to ne sme nanašati na določljiv priključek telekomunikacijskega sredstva ali na določenega uporabnika tega priključka na območju Republike Slovenije. ZSOVA ne določa nobenih drugih omejitev ali pogojev.

Pri izvajanju 21. člena 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. člen ZSOVA nanaša na primere, ko gre za:

- nedoločen ali nedoločljiv priključek,
- nedoločljivega uporabnika priključka na ozemlju RS,

---

[7] Tako Ustavno sodišče v 8. točki sklepa št. U-I-45/08-21, z dne 8. 1. 2009 (OdlUS XIII, 3): »Kadar pa predlagateljica pri izvrševanju svojih pristojnosti naleti na zakonske določbe, ki ji zaradi domnevnega neskladja z Ustavo preprečujejo učinkovito zagotovitev varstva informacijske zasebnost (38. člen Ustave), lahko vloži zahtevo za oceno ustavnosti. Samo v tem primeru je Informacijska pooblaščenka upravičena oseba za vložitev zahteve iz šeste alineje prvega odstavka 23.a člena ZUstS.«

[8] Tako v primerljivi situaciji tudi Ustavno sodišče v točki 10 sklepa št. U-I-92/12-13 (Ur. l. RS, št. 89/2013).

- določljivega uporabnika priključka izven ozemlja RS,
- določenega uporabnika priključka izven ozemlja RS.

ZSOVA ne vsebuje definicije pravnega termina »*spremljanje mednarodnih sistemov zvez*«, niti te definicije ne vsebuje noben drug predpis. **Na podlagi navedenih pravnih norm in ugotovitev inšpekcijskega nadzora je mogoče razumeti, da glede na popolno vsebinsko odprtost pod pojem mednarodni sistemi zvez lahko sodijo vse oblike komunikacij, ki jih omogočajo elektronski (in drugi) komunikacijski sistemi in oprema in imajo element mednarodnosti.** Opredelitev elementa mednarodnosti kot pogoja za dopustnost zbiranja osebnih podatkov (najmanj podatka o številki in ali imenu in priimku priključka elektronskih ali drugih komunikacij, ki potekajo preko mednarodnih sistemov zvez in so predmet nadzora) pa je glede na naravo tehnologij elektronskih komunikacij, ki so danes na voljo, mogoče iskati bodisi v smislu lokacije najmanj enega od udeležencev komunikacije, priključka (npr. telefona, modema) ali drugega dela komunikacijske opreme (npr. bazne postaje) izven ozemlja RS bodisi sodelovanje najmanj enega udeleženca komunikacij, ki ni slovenski državljan, bodisi sodelovanje ponudnika elektronskih komunikacij, ki ima (glavni) sedež izven Republike Slovenije v konkretni komunikacijski zvezi. Drugačne definicije tudi ni mogoče jasno in enoznačno opredeliti na podlagi jezikovne, logične ali namenske razlage zakona.

Nadalje upoštevajoč dejansko naravo elektronskih in drugih komunikacijskih sistemov in opreme in ugotovitve inšpekcijskega nadzora, ki so na voljo, po mnenju predlagatelja **v praksi ni mogoče na ustavno skladen način dosledno in v vseh primerih zadostiti zahtevi tretjega odstavka 21. člena ZSOVA, da se spremljanje mednarodnih sistemov zvez ne sme nanašati na določljiv priključek telekomunikacijskega sredstva ali na določenega uporabnika tega priključka na območju Republike Slovenije.** Iz odločitve USRS v zadevi ZSOVA[9] pa izhaja, da se lahko spremljanje mednarodnih sistemov zvez, kot del obveščevalne dejavnosti, nanaša le na območje zunaj državnega območja Republike Slovenije.

Upoštevajoč navedeno in ugotovitve inšpekcijskega nadzora, predlagatelj ugotavlja, da v predmetnem inšpekcijskem primeru ne drži ugotovitev US RS ob predhodni obravnavi zahteve za oceno ustavnosti 21. člena ZSOVA, ko je US RS poudarilo, da ob takšni z URS skladni razlagi izpodbijane določbe (določbe 1., 2. in 3. odstavka 21. člena ZSOVA) Informacijskemu pooblaščencu ne morejo preprečiti, da izpolni svojo zakonsko nalogo nadzora nad pravilnim (torej tudi z URS skladnim) izvajanjem predpisov, ki urejajo obdelavo, varstvo ali iznos osebnih podatkov v tujino[10].

Nasprotno, Informacijski pooblaščenec na podlagi ugotovitev v okviru navedenega inšpekcijskega postopka ugotavlja, da v predmetni zadevi ni mogoče sprejeti zaključka, kdaj so kršene določbe tretjega odstavka 21. člena ZSOVA. Sklepanje po nasprotnem razlogovanju (*argumentum a contrario*), ki pa ne more biti zakonit način za zapolnjevanje pravne praznine ali nejasnosti zakonske določbe, še toliko bolj v primeru poseganja organov pregona in varnostnih služb v temeljne človekove pravice, bi pomenilo, da so vsakršne oblike obdelave osebnih podatkov z mednarodnim elementom dopustne brez omejitev, če:

a) obstaja za to pisna odredba direktorja SOVA in

---

[9] Točki 11: »… Ob upoštevanju že navedenih določb Ustave je mogoče njeno vsebino razlagati le v povezavi z vsebino drugega in tretjega odstavka tega člena ter v konkretnem primeru prvega odstavka 2. člena ZSOVA. Izpodbijano določbo je zato treba najprej razlagati tako, da se spremljanje mednarodnih sistemov zvez kot del obveščevalne dejavnosti agencije lahko nanaša le na območje zunaj državnega območja Republike Slovenije. V prid takšni razlagi govorijo namreč prvi odstavek 2. člena ter drugi in zlasti tretji odstavek 21. člena ZSOVA. Poleg slednjega iz drugega odstavka 21. člena ZSOVA jasno izhaja, da gre za zadevo in ne za konkretnega posameznika. Tretji odstavek 21. člena ZSOVA še dodatno izrecno določa, da se spremljanje mednarodnih sistemov zvez ne sme nanašati na določljiv priključek telekomunikacijskega sredstva ali na določenega uporabnika tega priključka na območju Republike Slovenije.« in točke 12: »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.« sklepa USRS U-I-216/07-8, z dne 4. 10. 2007 (Ur. l. RS, št. 99/2007 in OdlUS XVI, 75).

[10] Tako USRS v točki 9 sklepa št. U-I-45/08-21, z dne 8. 1. 2009 (OdlUS XIII, 3).

b) bodisi gre za prestrezanje komunikacij, ki ne potekajo čez območje RS, bodisi gre za prestrezanje komunikacij, ki potekajo čez ozemlje RS, a se prestrezanje ne nanaša na določljiv priključek telekomunikacijskega sredstva ali na določenega uporabnika tega priključka na območju Republike Slovenije.

Pojem spremljanje mednarodnih zvez je namreč tako širok, da bi dejansko lahko pomenil vse možne oblike prestrezanja elektronskih ali drugih komunikacij s kakršnimkoli mednarodnim elementom ob navedenih pogojih. Druga možnost pa bi bil zaključek, da nobeno spremljanje mednarodnih sistemov zvez ni dovoljeno, saj dejansko tehnično ni izvedljivo na v celoti ustavno skladen in predvidljiv (že v osnovi popolnoma brez prestrezanja komunikacije določljivih priključkov telekomunikacijskih sredstev ali določenih uporabnikov teh priključkov na območju Republike Slovenije) način zgolj s spremljanjem nedoločljivih priključkov in nedoločenih uporabnikov na območju RS in vseh zunaj območja Republike Slovenije. Takega predpisa zaradi nedoločnosti tudi ni mogoče nadzorovati, saj zaradi nejasnosti določb državni nadzornik ne more odrediti ukrepov iz 54. člen ZVOP-1 brez poseganja v pristojnosti drugega organa[11].

Iz ugotovitev inšpekcijskega nadzor ob takšnem sklepanju tako lahko izhaja zgolj, da državni nadzornik za varstvo osebnih podatkov ugotovi obstoj odredbe direktorja SOVA za vsak posamezen primer spremljanja mednarodnih sistemov zvez, ki se lahko dejansko nanaša na kakršnekoli oblike prestrezanja elektronskih ali drugih komunikacij s kakršnimkoli mednarodnim elementom. Ne more pa odrediti inšpekcijskih ukrepov zoper dejanja, ki niso skladna z zahtevami ZSOVA, četudi bi šlo v posamezni odredbi dejansko zgolj za neomejen popis katerihkoli dejanj spremljanja mednarodnih zvez.

Iz navedenega izhaja, da formalno v skladu z ustavno sodno prakso niso izpolnjeni pogoji za odreditev ukrepov, ki jih določa ZVOP-1. Inšpekcijski ukrepi, ki so Informacijskemu pooblaščencu na voljo v 54. členu ZVOP-1, namreč ne omogočajo, da bi lahko zaščitil ogrožene človekove pravice oseb, ki jim je SOVA prisluškovala, saj so izpodbijane določbe ZSOVA v določanju dopustnih oblik zbiranja in obdelave osebnih podatkov nejasne do te mere, da ni mogoče na vnaprej predvidljiv način presoditi, kdaj gre za zakonito in kdaj za nezakonito zbiranje osebnih podatkov.

II. Neskladnost določbe prvega odstavka 21. člena ZSOVA s 37. členom Ustave RS

Ustavno sodišče RS se je v preteklosti tudi sicer 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).[12] Po 2. odst. 37. člena USRS lahko samo zakon predpiše,

[11] Kot ugotavlja USRS v sklepu št. U-I-92/12-13 (Ur. l. RS, št. 89/2013) namreč »za vstop predlagatelja (op. IP) v posamični pravni postopek in za njegovo neposredno poseganje v vodenje takega postopka zaradi zagotavljanja ustavno skladne in zakonite obdelave osebnih podatkov ni zakonske podlage niti v določbah, ki urejajo pristojnosti predlagatelja niti v določbah zakonov, ki urejajo postopke odločanja o posamičnih pravnih zadevah.« »Uporaba takih pristojnosti (op. prepoved nadaljnje obdelave osebnih podatkov oziroma njihovo uničenje) ne more biti dopustna proti drugemu državnemu organu, ki vodi upravni ali drug postopek, za katerega je pristojen na podlagi zakona.«

[12] Glavne poudarke naštetih odločb je prispevku 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

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, pri čemer morajo biti izpolnjeni navedeni štirje osnovni pogoji za omejitev te pravice.

Ob tem dodatno navajamo ločeno pritrdilno mnenje sodnika Ustavnega sodišča dr. Cirila Ribičiča (v zadevi št. U-I-216/07, z dne 4. 10. 2007, (Ur. l. RS, št. 99/2007 in OdlUS XVI, 75) ki se mu je pridružila sodnica dr. Mirjam Škrk), ki gre v tolmačenju zahtevanega obsega subjektov, na katere se varstvo nanaša, celo dlje: »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.« Sodnik dr. Ribičič je dodal še, da je bilo z vidika obravnavane zadeve (zahteva za oceno ustavnosti prvega odstavka 21. člena ZSOVA v tem primeru podana s strani 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 ZSOVA mogoče in treba razlagati tako, da ne dovoljujejo posegov v pisemsko tajnost konkretnih posameznikov v drugih državah. Meni, da je edina ustavnoskladna razlaga te določbe tista, ki na podlagi spremljanja mednarodnih sistemov 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. Iz ugotovitev inšpekcijskega postopka v predmetni zadevi Informacijskega pooblaščenca pa izhaja, da SOVA prisluhe mednarodnih zvez izvaja na konkretne telefonske številke.

Varstvo t.i. prometnih podatkov o komunikaciji (npr. podatkov o osebnem imenu, telefonski številki in času komunikacije) ter vsebina zapisa pogovora, je, kot je pojasnjeno zgoraj, dejansko dvojno[13]. Dvojno varstvo v tem primeru pomeni, da so na ta način zbrani podatki varovani ne le na podlagi 38. člena URS, temveč tudi na podlagi 37. člena URS. Do zbiranja osebnih podatkov namreč v tem primeru dejansko ne more priti brez posega v komunikacijsko zasebnost. **Če naj se torej zagotovi zakonito zbiranje osebnih podatkov, mora biti zakonit, in ustavno skladen najprej poseg v komunikacijo zasebnost, ki je omogočil samo zbiranje osebnih podatkov**. Torej, kot pojasnjeno zgoraj, v skladu s pogoji iz drugega odstavka 37. člena URS. 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.

Spremljanje mednarodnih sistemov zvez inherentno pomeni obdelavo osebnih podatkov o prometu elektronskih komunikacij, katerih varstvo zagotavljata tako 37. kot 38. člen URS. Pri razlagi določbe 37. člena URS se Informacijski pooblaščenec opira predvsem tudi na odločitev US RS številka Up-106/05, z dne 2. 10. 2008[14], v kateri je US RS (ponovno) presodilo, da poseg v svobodo komuniciranja ni dovoljen brez predhodnega dovoljenja sodišča. V razsodbi je US RS zapisalo, da na področje

---

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.

[13] Kot je opozorilo že US RS v zgoraj omenjeni odločbi št. U-I-25/95 z dne 27.11.1997, Ur. l. RS, št. 5/98 in OdlUS VI, 158.

[14] Ur. l. RS, št. 100/2008 in OdlUS XVII, 84.

komunikacijske zasebnosti sodijo v prvi vrsti podatki, ki se nanašajo na vsebino sporočila. Glede prisluškovanja in snemanja telefonskih pogovorov je US RS že zavzelo stališče, da morajo biti za njegovo dopustnost podane predpostavke iz drugega odstavka 37. člena Ustave[15]. Ustavno sodišče je v nadaljevanju izpostavilo, da je v teoriji zastopano stališče, da **ni varovana zgolj vsebina komunikacije, temveč tudi okoliščine in dejstva, povezana s komunikacijo**. Med te okoliščine in dejstva prav gotovo sodijo podatki o tem, kdo je komuniciral, kdaj in s kom, morda pa tudi druge okoliščine, kot je npr. vrsta uporabljene komunikacije[16]. V Dopolnitvi komentarja Ustave Republike Slovenije je tako zapisano, cit.: »varstva komunikacijske zasebnosti glede na ustaljeno domačo in tujo ustavnosodno prakso ni mogoče zožiti na samo vsebino sporočanja, ampak ista pravica varuje tudi podatke o tem, na kakšen način je komunikacija potekala, kdo jo je vzpostavil, s kom je bila vzpostavljena, od kod je bila vzpostavljena in ali je sploh potekala.«

V zvezi s tem gre ESČP v sodbi Zakharov proti Rusiji, z dne 4. 12. 2015 s svojimi ugotovitvami še korak dlje glede zahtevanega obsega varstva, saj se opredeli, da nacionalna zakonodaja ne omogoča učinkovitega pravnega sredstva osebi, ki sumi, da se zoper njo izvaja prikrito prestrezanje komunikacij. **Sam obstoj zakonodaje, ki tak poseg omogoča, naj bi torej že predstavljal poseg v pravico do zasebnosti po 8. členu Konvencije o varstvu človekovih pravic in temeljnih svoboščin** (Uradni list RS, št. 33/94, MP, št. 7/94 – v nadaljevanju EKČP). Za ESČP je bilo v tej zadevi pomembno, ali za sistem prikritega nadzora z namenom zaščite nacionalne varnosti, kot je opredeljen v ruski zakonodaji, obstajajo primerne in učinkovite varovalke zoper zlorabo tega sistema. ESČP se je v predmetni zadevi pri oceni ali postopki dopuščanja tajnega nadzora niso odrejeni samovoljno, nezakonito ali brez ustrezne in primerne obravnave osredotočilo predvsem na naslednja vprašanja:

1. kateri organ je pristojen za odreditev nadzora,
2. kakšen je obseg nadzora teh postopkov in
3. vsebine pooblastil za prestrezanje komunikacij.

Vse navedeno je relevantno tudi v primeru pooblastil za spremljanje mednarodnih sistemov zvez na podlagi 21. člena ZSOVA s strani SOVA.[17] Pri tem je ESČP postavilo rigorozne standarde za dopustnost množičnega nadzora telekomunikacij za obveščevalske namene. Zahteve ESČP bi lahko strnili v naslednje točke[18]:

1) Zakonodaja države mora zamejiti prisluškovalne aktivnosti tako, da ne bo mogoč »strateški nadzor« komunikacij (vseh relevantnih telefonskih številk oz. priključkov v neki zadevi), ampak da se bo ciljalo na individualizirane osebe oz. telefonske priključke.
2) Prisluškovanje se lahko začne šele po zunanji odobritvi, ki mora biti vsebinska in ne zgolj formalna, in mora temeljiti vsaj na navedbi razlogov, zakaj je prisluškovanje določeni osebi oz. številki pomembno in primerno v posamični zadevi. »Interne« odobritve s strani direktorja varnostno-obveščevalne agencije, pravosodnega ministra, notranjega ministra, idr. ne zadostujejo, ker so vse del izvršne veje oblasti in s tem nezdružljivo povezane z obveščevalnimi agencijami[19].
3) Neposredni nadzor telekomunikacijskih vodov s strani obveščevalcev ne zagotavlja ustreznih in učinkovitih varovalk zoper zlorabe.

Zaključek ESČP v zvezi s tem je bil, da ruska zakonodaja o prestrezanju komunikacij ne zagotavlja primernih in učinkovitih varovalk zoper arbitrarnost in zoper tveganje za zlorabe, ki so imanentne

[15] Glej odločbo USRS št. U-I-25/95 z dne 27. 11. 1997, Ur. l. RS, št. 5/98 in OdlUS VI, 158.
[16] Več v: Komentar Ustave Republike Slovenije: Dopolnitev komentarja-A. Avtorji Matej Avbelj et al. urednik Lovro Šturm. Ljubljana: Fakulteta za državne in evropske študije 2011, str. 523.
[17] Povzeto po točki 257 sodbe v zadevi Roman Zakharov proti Rusiji, z dne 4. 12. 2015.
[18] Povzeto v točkah 302 in 303 sodbe v zadevi Roman Zakharov proti Rusiji, z dne 4. 12. 2015.
[19] Glej tudi sodbo ESČP Szabó and Vissy proti Madžarski, št. 37138/14 z dne 21. 1. 2016.

vsakemu sistemu prikritega nadzora. ESČP je posebej izpostavilo pomanjkljivosti ruske ureditve: okoliščine, v katerih se lahko odredi prikrit nadzor, trajanje takih ukrepov, okoliščine, v katerih je ukrepe treba prenehati izvajati, postopek odreditve prestrezanja komunikacij ter shranjevanje in uničevanje pridobljenih podatkov in nadzor nad prestrezanjem komunikacij.[20]

Spremljanje mednarodnih zvez s strani ZSOVA je tako »strateško«, nanaša pa se tehnično tudi na posamezne osebe ali organizacije. Strateški nadzor se nanaša na »zadeve«, tj. posamezne grožnje za slovensko nacionalno varnost oz. druge varnostne, politične in gospodarske interese države Slovenije (naloge SOVE, 2. člen[21]). Odločitev, komu se bo dejansko prisluškovalo in v kakšnem obsegu, ter sama odobritev je skladno z določbami prvega odstavka 21. člena ZSOVA **zgolj in samo v rokah direktorja agencije**, ki s pisno odredbo, v kateri na splošno navede »način, obseg in trajanje prisluhov« kot to od njega terja drugi odstavek 21. člena ZSOVA, odredi spremljanje mednarodnih sistemov zvez brez sodne odobritve. **Odločitev, komu se bo prisluškovalo in v kakšnem obsegu se sprejme brez vednosti ali odločitve sodišča, kar sicer zahteva 2. odstavek 37. člena Ustave RS.** Posledično Informacijski pooblaščenec ocenjuje, da določbe prvega odstavka 21. člena ZSOVA niso skladne s standardi, ki jih je v sodbi Zakharov postavilo ESČP, z dne 4. 12. 2015, kakor tudi ne z določbami 2. odstavka 37. člena Ustave RS.

Izpodbijane določbe prvega odstavka 21. člena ZSOVA so po oceni predlagatelja v neskladju z drugim odstavkom 37. člena Ustave, ker:

1. v očitnem nasprotju z drugim odstavkom 37. člena US RS za poseg v pravico do informacijske in komunikacijske zasebnosti (določljivih in nedoločljivih posameznikov - državljanov RS ali tujcev, če se oseba nahaja oz. uporablja priključek izven območja Republike Slovenije) s strani državnega organa z ukrepom spremljanja mednarodnih sistemov zvez ni zahtevano predhodno dovoljenje v obliki sodne odločbe;
2. ni navedenih razlogov, ki bi omogočali preizkus, ali je bil poseg dopusten, ker je bil nujen, potreben in primeren za varnost države.

III. Neskladnost določbe tretjega odstavka 21. člena ZSOVA z 2., 15., 37. in 38. členom Ustave RS

Iz ustaljene ustavnosodne presoje izhaja, da se v prvem odstavku 38. člena Ustave kot poseben vidik zasebnosti zagotavlja varstvo osebnih podatkov. Namen varstva osebnih podatkov je zagotoviti spoštovanje posebnega vidika človekove zasebnosti – t. i. informacijsko zasebnost. S tem ko URS to pravico posebej ureja, ji daje posebno mesto in pomen v siceršnjem varstvu zasebnosti posameznika. Posebno mesto ima tudi na ravni Evropske unije. Listina Evropske unije o temeljnih pravicah (UL C 326, 26. 10. 2012 – v nadaljevanju Listina)[22] je pravico do varstva osebnih podatkov v 8. členu tudi deklaratorno povzdignila med temeljne človekove pravice. Po ustaljeni ustavnosodni presoji pomeni vsako zbiranje in obdelovanje osebnih podatkov poseg v pravico do varstva zasebnosti oziroma v pravico posameznika, da obdrži informacije o sebi, ker noče, da bi bili z njimi seznanjeni drugi. Temeljna vrednostna podstat te pravice je spoznanje, da ima posameznik pravico zadržati informacije o sebi zase in da je v izhodišču on tisti, ki odloča, koliko informacij o sebi bo razkril in komu.[23] Vendar pravica do informacijske zasebnosti ni neomejena, ni absolutna. Zato mora posameznik sprejeti omejitve informacijske zasebnosti oziroma dopustiti posege vanjo v prevladujočem splošnem interesu

[20] Povzeto v točkah 302 in 303 sodbe v zadevi Roman Zakharov proti Rusiji, z dne 4. 12. 2015.
[21] Tako izhaja že iz predloga Informacijskega pooblaščenca za oceno ustavnosti iz leta 2008.
[22] Glej drugi stavek 29. točke sodbe v združenih zadevah C-293/12 in C-594/12.
[23] Glej točko 12 obrazložitve odločbe Ustavnega sodišča št. U-I-98/11 z dne 26. 9. 2012 (Uradni list RS, št. 79/12).

in ob izpolnjevanju ustavno določenih pogojev. Poseg je dopusten pod pogoji iz tretjega odstavka 15. člena in 2. člena Ustave.[24]

Ustava zakonodajalcu s tem izrecno nalaga, da mora vsako materijo posega v zasebnost ne le zakonsko urediti, ampak da mora to urediti določno in nedvoumno. Izključena mora biti vsaka možnost arbitrarnega odločanja državnega organa. Kot je Ustavno sodišče že večkrat poudarilo v svojih odločbah, je določnost zakona (*lex certa*) praprvina pravne države (2. člen Ustave) in bi veljala kot imperativni ustavni postulat celo, če v Ustavi sploh ne bi bila izrecno omenjena.[25] Načelo jasnosti in določnosti predpisov zahteva, da je iz predpisa mogoče nedvoumno ugotoviti vsebino in namen norme.

Po mnenju predlagatelja ZSOVA v delu, ki določa zakonsko pooblastilo SOVA za spremljanje mednarodnih sistemov zvez, ne zadosti tem načelom. Pojem »spremljanje mednarodnih sistemov zvez« je namreč nedefiniran[26] in ne določa, kje se nadzor izvaja oziroma kje je mesto telekomunikacijskega priključka in mesto priklopa. Prav tako ne pojasni, ali je zakonsko dopustno nadzorovati vse mednarodne zveze, do katerih ima lahko dostop SOVA, ali je npr. zakonsko dopustno prestrezati vse komunikacije na komunikacijskih vodih, ki potekajo čez Slovenijo, dokler gre za komunikacije tujih državljanov. Edina vsebinska in pravna zamejitev posega spremljanja mednarodnih sistemov zvez (ki pravno ni neopredeljen pojem) je namreč, da se to ne sme nanašati na določljiv priključek telekomunikacijskega sredstva ali na določenega uporabnika tega priključka na območju Republike Slovenije. Glede na naravo stvari ta zahteva v praksi ni vedno povsem dosledno izvršljiva na ustavno skladen način – to je brez vsaj zajema v določenih primerih tudi komunikacij določljivih priključkov telekomunikacijskih sredstev ali določenih uporabnikov teh priključkov na območju Republike Slovenije. Drugače povedano iz besedila predpisa ni mogoče nedvoumno ugotoviti vsebine in namena norme ter posledično pogojev zakonite obdelave osebnih podatkov. Npr. mobilni telefon, ki sprejme telefonski klic iz tujine, preko ene od baznih postaj mobilnih operaterjev, ki se nahaja na območju Republike Slovenije je v istem trenutku, če gre za naročnika določljiv uporabnik na območju Republike Slovenije. Pojmu določljiv v primeru mobilnih telefonov glede na zbirke podatkov, ki jih operaterji hranijo, namreč ne zadostijo edino tisti mobilni telefoni, ki uporabljajo povezavo preko predplačniških paketov, če so anonimni, pa tudi tu je njihova dejanska anonimnost relativna. Posledično je stopnja spoštovanja ene od temeljnih pravic odvisna zgolj od proste presoje SOVA in njene izvedbe predpisa, kar z vidika predvidljivosti posegov v ustavno varovane pravice in 2. člena URS ni sprejemljivo.

Kot je US RS odločilo v odločbi št. U-I-246/14-20 z dne 24. 3. 2017 (Ur. l. RS, št. 16/2017) v zvezi s primerljivimi posegi v pravice do zasebnosti v zvezi s hrambo podatkov, sporočil, posnetkov ali dokazil pridobljenih z uporabo prikritih preiskovalnih ukrepov (v nadaljevanju PPU), je v primeru teh ukrepov velikega pomena tudi dejstvo, da izpodbijane določbe spadajo na področje obdelave osebnih podatkov osumljencev in drugih oseb, proti katerim so bili uporabljeni PPU. PPU (primerljivo kot posegi v zasebnost s strani SOVA) po svoji naravi izjemno intenzivno posegajo na področje, ki ga varujejo različni vidiki človekove pravice do zasebnosti (35., 36., 37. in 38. člen URS). Zato je za vsa vprašanja v zvezi s PPU podana ustavna zahteva poudarjene jasnosti, razumljivosti, določnosti, nedvoumnosti in predvidljivosti ustreznih zakonskih določb. To ne velja samo za pravne podlage za izvajanje PPU v ožjem smislu (torej za vdiranje v sfero zasebnosti s pridobivanjem in beleženjem različnih podatkov), pač pa tudi za predpise, ki urejajo nadaljnjo obdelavo ustreznih izsledkov, npr. hrambo, uporabo, posredovanje med različnimi upravičenci itd.

---

[24] Glej točko 16 odločbe US RS št. U-I-65/13-19 z dne 4. 7. 2014 (Uradni list RS, št. 54/2014 in OdlUS XX, 27).
[25] Glej točko 42 odločbe USRS št. U-I-25/95 z dne 27. 11. 1997, Ur. l. RS, št. 5/98 in OdlUS VI, 158.
[26] BRITOVŠEK, Primož, 2008, Spremljanje mednarodnih sistemov zvez kot domnevni poseg v komunikacijsko zasebnost posameznika v povezavi s teritorialnim principom varovanja te pravice. V : [na spletu]. 2008. [Dostopano 13 junij 2017]. Pridobljeno od: https://dk.um.si/IzpisGradiva.php?lang=slv&id=30078

US RS je prav tako že v odločbi št. U-I-25/95 z dne 27. 11. 1997 (Uradni list RS, št. 5/98, in OdlUS VI, 158), ko je presojalo tedanjo ureditev PPU (»posebne operativne metode in sredstva«), sprejelo stališče o potrebi po zakonski določnosti (*lex certa*) primerov, v katerih je dopusten poseg v zasebnost tako, da so sodišču in pred tem že državnemu tožilcu dane jasne meje pri presoji, v katerih primerih je pogoj izpolnjen. Med drugim je poudarilo, da mora biti **»določenost v zakonu« kot ustavni pogoj za poseg v zasebnost zagotovljena z natančno in predvidljivo ureditvijo uporabe ukrepa**.

Po mnenju Informacijskega pooblaščenca vse navedeno glede na občutljivost posegov pri spremljanju mednarodnih sistemov zvez še toliko bolj velja za te posege, katerih subjekti so teoretično lahko vsi posamezniki, niti ne nujno osumljenci. Predlagatelj namreč poudarja, da narava posega v obdelavo osebnih podatkov s strani SOVA prav tako predstavlja izjemno intenziven poseg na področje različnih vidikov človekove pravice do zasebnosti, ki je ustavno varovana pravica, zato bi ti standardi najmanj v enaki meri kot za PPU morali veljati za vse vrste tajnega pridobivanja podatkov kot ga ureja V. poglavje ZSOVA, torej tudi za spremljanje mednarodnih sistemov zvez.

Pravico do komunikacijske zasebnosti in s tem povezane obdelave osebnih podatkov opredeljuje tudi 8. člen EKČP. V zvezi s tem je ESČP konec leta 2015 glede državnega nadziranja elektronskih komunikacij s strani varnostno-obveščevalnih služb[27] odločilo, da **pomeni neustrezna zakonska ureditev prestrezanja komunikacij, ki ne določa ustreznih varovalk pred zlorabami in samovoljnosti, konkretno z omogočanjem avtomatske hrambe očitno nepomembnih podatkov ter odsotnostjo dovolj določne zakonske ureditve hrambe ter uničenja izsledkov po koncu kazenskega postopka kršitev 8. člena EKČP**.[28]

V zvezi s tem pa gre poudariti tudi, da je Ustavno sodišče v odločbi št. U-I-65/13-19 z dne 4. 7. 2014 (Uradni list RS, št. 54/2014 in OdlUS XX, 27) odločilo, da pomeni hramba t.i. prometnih podatkov (to so podatki vseh komunikacij pri telefoniji v fiksnem omrežju, mobilni telefoniji, pri dostopu do interneta, internetne elektronske pošte in internetne telefonije, ki kažejo na posamezna dejstva, okoliščine, relacije, dinamike in vzorce življenja posameznika[29]) v nesorazmernem obsegu (v konkretnem primeru obvezna 14- oz. 8-mesečna hramba določenih prometnih podatkov) glede na ustaljeno ustavnosodno presojo in tudi prakso Sodišča Evropske unije poseg v pravico do varstva osebnih podatkov, ki jo zagotavljajo 38. člen Ustave, 8. člen Listine in tudi 8. člen EKČP[30] v konkretnem primeru[31].

ESČP že **sam obstoj zakonodaje, ki dopušča možnost tajnega prestrezanja komunikacij preko mobilnih telefonov in predstavlja tveganje, da bi se posameznik nekoč lahko znašel kot predmet prestrezanja, prepozna za kršitev 8. člena EKČP**, ne glede na to, da pritožnik v obravnavanem primeru še ni bil predmet konkretnega posega v zasebnost.[32] Po mnenju sodišča predstavlja zakonodaja, ki vzpostavlja sistem tajnega nadzora, v skladu s katerim bi lahko bila tarča prestrezanja komunikacij po mobilnem telefonu katerakoli oseba, ki uporablja mobilni telefon ruskih operaterjev, že sama po sebi poseg v pravice vseh uporabnikov mobilnih telefonov, četudi niso bili dejansko tarča prestrezanja.[33]

---

[27] Zadeva Roman Zakharov proti Rusiji, z dne 4. 12. 2015.
[28] Povzeto po točki 255 sodbe v zadevi Roman Zakharov proti Rusiji, z dne 4. 12. 2015, točka .
[29] V konkretnem primeru za namene, kot jih predvideva izpodbijana ureditev Zakona o elektronskih komunikacijah.
[30] Glej predvsem sodbe ESČP v zadevah *Leander proti Švedski* z dne 26. 3. 1987*, Amann proti Švici* z dne 16. 2. 2000*, Kopp proti Švici* z dne 25. 3. 1998.
[31] Glej sodbo v združenih zadevah *Volker und Markus Schecke GbR in Hartmut Eifert proti zvezni deželi Hessen*, C-92/09 in C-93/09, z dne 9. 11. 2010.
[32] Povzeto po točki 163 sodbe v zadevi Roman Zakharov proti Rusiji, z dne 4. 12. 2015.
[33] Povzeto po točki 175 sodbe v zadevi Roman Zakharov proti Rusiji, z dne 4. 12. 2015.

V zvezi s tem ESČP[34] razlaga 8. člen EKČP tako, da posebej izpostavlja, da **mora biti pravo (*in accordance with the law*), ki ureja skrivni nadzor, dostopno in predvidljivo ter zlasti dovolj jasno, da lahko državljani vedo, pod katerimi pogoji in v kakšnih okoliščinah se lahko pooblaščeni državni organi zatečejo k temu tajnemu in tveganemu vmešavanju v pravico do spoštovanja zasebnega življenja in dopisovanja.** Zaradi tveganja zlorab, lastnega vsakemu sistemu tajnega nadzora, morajo ti ukrepi temeljiti na posebej natančnem pravu. Obstoj jasnih in podrobnih pravil na tem področju je ključnega pomena, še posebno, ker se stalno veča sofisticiranost nadzorne tehnologije. Predlagatelj opozarja, da bi to še posebej moralo veljati za tajno pridobivanje podatkov preko spremljanja mednarodnih sistemov zvez, ki ob odsotnosti jasne definicije pojma lahko dejansko pomeni stalen nadzor vseh elektronskih ali drugih komunikacijskih sistemov in opreme z mednarodnim elementom.

ESČP v sodbi[35] vztraja pri tem, da **morajo določene minimalne varovalke biti jasno določene v zakonu** (*statute law*); med njimi so tudi **postopek za pregledovanje, uporabo in hrambo z nadzorom pridobljenih podatkov, previdnostni ukrepi pri sporočanju podatkov nadaljnjim prejemnikom ter okoliščine, v katerih se gradivo lahko uniči ali se mora uničiti**. EKČP v fazi, ko je tajni nadzor že končan, zahteva natančno ureditev postopkov za ohranitev integritete in zaupnosti pridobljenih izsledkov kakor tudi postopkov za njihovo končno uničenje. Sklep, da se ne dopusti pritožba, ki je temeljila na očitkih proti »strateškemu nadzoru« telekomunikacij v Zvezni republiki Nemčiji, je senat ESČP sprejel (tudi) na podlagi zaključka, da je upoštevna zakonodaja jasno, podrobno in razdelano urejala postopke za analizo, uporabo in tudi za uničevanje pridobljenih podatkov, po periodičnem preverjanju, če so še potrebni, in da so bile postavljene ustrezne omejitve in varovalke v zvezi z izročanjem podatkov drugim organom. Nasprotno, s sodbo v zadevi Roman Zakharov proti Rusiji z dne 4. 12. 2015 je ESČP ugotovilo kršitev 8. člena EKČP zaradi splošne neustreznosti jamstev ruske ureditve prestrezanja komunikacij proti zlorabam in arbitrarnosti.

Pojmovna odprtost pravne norme, ki ne vsebuje nedvoumne zakonske opredelitve osnovnega pojma, ki ne zamejuje obsega nadzora in poseganja v zasebnost na način, ki je v praksi predvidljivo izvedljiv v skladu z URS in, ki ne določa postopkov za analizo, uporabo in tudi ne opredeljuje roka hrambe oz. meril za ugotovitev roka uničevanja pridobljenih podatkov, po periodičnem preverjanju, če so še potrebni, in s tem posameznikom ne dopušča gotovosti in predvidljivosti dopustnih oblik nadzora po oceni predlagatelja ni skladna z 2., 15., 37. in 38. členom URS kot tudi ne z 8. členom EKČP. Primerljive zaključke je namreč sprejelo ESČP v sodbi Roman Zakharov proti Rusiji, z dne 4. 12. 2015, s katero je ugotovilo kršitev 8. člena EKČP.

Izpodbijane določbe tretjega odstavka 21. člena ZSOVA so iz navedenih razlogov po oceni predlagatelja v neskladju z 2., 15., 37. in 38. členom Ustave, ker:

1. poseg v pravico do informacijske in komunikacijske zasebnosti z ukrepom spremljanja mednarodnih sistemov zvez v zakonu ni vnaprej določen tako, da bi omogočal jasne in preverljive pogoje, okoliščine in razloge, pod katerimi je ta poseg (in s tem tudi zbiranje in obdelava osebnih podatkov) dopusten in zakonit;
2. ni nedvoumno in jasno določeno, v kakšnih razmerah in na kakšen način se ta poseg lahko opravi;
3. iz te določbe ne izhaja zahteva po potrebnih časovnih omejitvah tega posega, ki bi se lahko razlikovali glede na različnost okoliščin;
4. ni določeno jasno merilo ali časovna zamejitev za ugotavljanje dopustnega roka hrambe tako pridobljenih osebnih podatkov – prometnih podatkov in zapisov komunikacij.

zato Informacijski pooblaščenec predlaga,

[34] Kot je povzelo USRS v 23. točki odločbe št. U-I-246/14-20 z dne 24. 3. 2017.
[35] Kot je povzelo USRS v 23. točki odločbe št. U-I-246/14-20 z dne 24. 3. 2017.

da Ustavno sodišče oceni ustavnost prvega in tretjega odstavka 21. člena ZSOVA v luči zgoraj navedenega in ju, če bo tudi samo ocenilo, da nista v skladu z Ustavo, razveljavi oz. ugotovi njuno neskladnost z URS ter naloži Državnemu zboru odpravo tega neskladja v razumnem roku.

Hkrati predlagatelj predlaga, da Ustavno sodišče zadevo obravnava prednostno.

Informacijski pooblaščenec:

Mojca Prelesnik, univ. dipl. prav.
informacijska pooblaščenka

Poslati:

- po pošti naslovniku priporočeno in po e-pošti: info@us-rs.si;
- zbirka dokumentarnega gradiva pri IP.