



Inštitut Državljan D, zavod za spodbujanje
informacijske in medijske pismenosti, Ljubljana
Gradnikova ulica 6a
SI-6000 Koper
Slovenija

Zavod Državljan D (zanj Domen Savič)
Gradnikova ulica 6a
6000 Koper

Zadeva: Mnenje in pripombe na Predlog Zakona o spremembah in dopolnitvah Zakona o Slovenski obveščevalno-varnostni agenciji (EVA 2025-1524-0001) z vidika varstva osebnih podatkov in temeljnih človekovih pravic

Spoštovani,

V nadaljevanju podajamo komentar Predlog Zakona o spremembah in dopolnitvah Zakona o Slovenski obveščevalno-varnostni agenciji (EVA 2025-1524-0001) z vidika varstva osebnih podatkov in temeljnih človekovih pravic in opozarjamo na zaskrbljujoče pomanjkljivosti.

Slovenija se, kot vse demokratične države, že desetletja sooča z iskanjem ravnovesja med učinkovitim delovanjem obveščevalno-varnostnih služb in varovanjem temeljnih človekovih pravic – še posebej zasebnosti ter varstva osebnih podatkov.

Pripravljeni predlog novele Zakona o Slovenski obveščevalno-varnostni agenciji (v nadaljevanju: predlog ZSOVA), ki je predmet javne razprave, pomembno razširja obseg pooblastil, dostopnih orodij in metod za delovanje SOVE. Ob tem v slovenski in širši evropski javnosti močno odmevajo pomisleki in opozorila glede možnosti posegov v temeljne svoboščine, pa tudi glede transparentnosti delovanja in zaščite pred zlorabami.

Kot dolgoletni zasebnostni aktivist ocenjujem predlog novele ZSOVA skozi objektiv evropskih in slovenskih pravnih standardov ter skozi prizmo prakse, ki se je oblikovala v zadnjih letih ob prepoznanih varnostih tveganjih, pa tudi ob evidentiranih zlorabah posebnih pooblastil (internacionalno in doma). Že površinsko branje javno objavljenega osnutka razkrije izjemno široko zasnovo novih instrumentov, potencialno luknjičav nadzorni okvir in pomanjkljivo varovalko zlorab v več členih, na kar opozarjajo tudi neodvisni nadzorni organi, predvsem Informacijski pooblaščenec.



1. Nejasnosti določb in preširoka formulacija pooblastil

a) Materialna (ne)določenost in nevarnost arbitrarnih posegov

Ena izmed najočitnejših slabosti novele je ohlapna oziroma izjemno splošna formulacija številnih členov, zlasti tistih, ki se nanašajo na opredelitev namena zbiranja in obdelave osebnih podatkov. V predlaganem osnutku je npr. kot namen zbiranja opredeljeno "varstvo ustavne ureditve Republike Slovenije in zagotavljanje nacionalne varnosti", kar praktično omogoča stalno, vnaprejšnje in precej nerazložno zbiranje osebnih podatkov na zalogo ter njihovo hranjenje brez časovno in vsebinsko določenih omejitev.

Informacijski pooblaščenec izrecno opozarja, da morajo biti v zakonu natančno, jasno, ozko in vnaprej predvidljivo določeni tako nabor osebnih podatkov, ki jih lahko SOVA zbira, kot tudi osebe, na katere se zbiranje nanaša in opredeljeni namenski razlogi za njihovo obdelavo. Brez tega se odpira vrata širokim interpretacijam, samovoljnosti in posledično tudi zlorabam.

b) Primerjava z mednarodnimi standardi

Dober primer prakse ponuja norveška in nizozemska zakonodaja, kjer je nabor dovoljenih ukrepov, podatkov in pogojev za poseg izredno podrobno navedena v zakonu, vsak poseg v podatke pa mora biti sorazmeren, nujen in vnaprej opredeljen; nad vsakim ukrepom je posamično uveden sodni in civilni nadzor.

Brez ciljne omejitve in določnosti tvega Slovenija neskladje tako z Ustavo RS (38. člen), z GDPR, kot tudi z mednarodnimi človekovimi pravicami. Pretekle izkušnje v Sloveniji in tujini potrjujejo, da ohlapne formulacije najpogosteje služijo kot izgovor za netransparentne nadzore, razlago selektivne upravičenosti in celo politično zlorabo nadzornega aparata.



2. Biometrijski podatki: Posegi brez transparentnosti in vsebinskih omejitev

a) Predpisane spremembe: vsebina in nevarnosti

Z novelo bi SOVA pridobila pravico do sistematične obdelave biometričnih podatkov: podobe obraza, telesa, posnetkov gibanja, govora in glasu posameznikov, ki so predmet operativnega obravnavanja. Ti podatki so vezani na posameznikove unikatne, trajne telesne lastnosti (podrobnosti določa tudi ZVOP-2, mednarodno pa GDPR), kar pomeni, da gre za posebno zaščiten, občutljiv steber osebnostne pravice.

Z vidika zasebnostnega aktivista je bistveno vprašanje nujnosti in sorazmernosti – ali je kolektivno zbiranje in hranjenje takšnih podatkov sploh dopustno, sploh glede na možnost zlorabe in skoraj popolno nezmožnost posameznika, da bi v primeru zlorabe kakor koli "zamenjal" svoje biometrične identifikatorje.

b) Pomanjkljivosti predloga

Informacijski pooblaščenec opozarja, da predlog ne vsebuje jasne ločitve med osnovnimi identifikacijskimi in biometričnimi podatki, ne določa natančnih in ozkih namenov uporabe, rokov in pogojev hrambe, ne ločuje postopkov za izjemne primere uporabe – kar je direktno v nasprotju z zahtevami 38. člena Ustave, ZVOP-2 in GDPR. Nečrpen nabor "upravičencev" in možnosti naknadnega prenosa ali povezovanja zbirk (prepoved zveze zbirk je sicer izrecno v ZVOP-2, a premalo poudarjena v predlogu novele) dodatno stopnjuje tveganja.

Evropski standardi obvezno zahtevajo, da je vsak poseg v biometrijo v javnem sektorju utemeljen kot edina mogoča pot (nepresegljiva nujnost), potrjen s strani nadzornega organa in časovno, vsebinsko, tehnično maksimalno omejen, vključno z oceno učinkov na varstvo podatkov (DPIA) in s stalnim civilnim nadzorom.

c) Predlogi za spremembo

- Stroga in izrecna ločitev zbiranja osnovnih osebnih in biometričnih podatkov, opredelitev vrst posegov, specifikacija namenov uporabe in obdobja hrambe, obvezni ex ante in ex post nadzor Informacijskega pooblaščenca ter posebni režim obveščenosti in pravic posameznika;
- Zbiranje biometrijskih podatkov zgolj kot ukrep ultima ratio – obvezna dokazila, da cilj ni dosegljiv na drug način, ter izključitev avtomatiziranega profiliranja brez posamične sodne odredbe.



3. IMSI-lovilci in telekomunikacijski nadzor – nevarnost množičnega nadzora in neustrezne pravne zaščite

a) Problematičnost IMSI-lovilcev

IMSI-lovilci delujejo kot lažne bazne postaje – beležijo signalne podatke o mobilnih napravah v okolici, ne glede na njihovo povezavo s konkretno preiskavo. Temeljni pomislek je, da razen želene identifikacije tarče naprava "pobere" množico "tretjih" oseb, ki niso nikakor povezane s sumom ali interesom nacionalne varnosti.

Ustavno sodišče je že razveljavilo prejšnjo ureditev uporabe IMSI-lovilcev v kazenskem postopku zaradi pomanjkanja jasne in učinkovite ex post sodne kontrole ter neobstoja učinkovite varovalke zoper arbitrarno uporabo ukrepa.

Predlog sicer določa, da poseg lahko odobri zgolj predsednik Vrhovnega sodišča, doba uporabe je 15 dni brez možnosti podaljšanja, uradno naj IMSI-lovilec ne bi omogočal prisluškovanja ali ugotavljanja lokacije komunikacijskih sredstev tretjih oseb, a vse to ostaja na ravni deklaracije; konkretni tehnični nadzorni ukrepi, revizijske sledi in transparentnost delovanja tehnologije niso v praksi izrecno zagotovljeni.

b) Analiza in prikaz tveganj

Nejasni tehnični standardi, možnost masovnega naključnega posega v prometne podatke in dejstvo, da posameznik, čigar podatki so bili zgolj mimogrede "pobrani", ni obveščen niti nima učinkovitega pravnega sredstva, pomenijo očiten odmik od standardov proporcionalnosti in nujnosti, ki jih zahteva sodobna ustavna in evropska doktrina.

Čeprav zakon predvideva določene varovalke (pisna odredba, omejena uporaba, letna poročila, nadzor predsednika sodišča, naknadna obvestila), pa je v slovenskem ustavnopravnem okolju, ob zgodovinskih primerih slabih praks SOVE, to premalo. Odsotnost neodvisne tehnične presoje, obvezne uničitve vseh neustreznih podatkov in možnosti varstva pravic prizadetih posameznikov v postopku je velik manko.

Primerjave z nizozemsko, norveško in kanadsko ureditvijo kažejo, da je treba pri vsakem večjem posegu zahtevo argumentirati z analizo tehničnih tveganj, omogočiti invazivno sodno in civilno spremljanje te analize, voditi avtonomno rekonstrukcijsko evidenco, ter omogočiti posamezniku, da o posegu aktivno izve in navede ugovor.



4. Neposreden dostop do podatkov na napravi (vohunska programska oprema): Največje tveganje za temeljne pravice

a) Narava ukrepa in njegovi problemi

Dovolitev neposrednega dostopa do podatkov na telekomunikacijski napravi (t.i. "spyware", najpogostejše znan pod komercialnimi imeni Pegasus itd.) prinaša SOVI možnost popolnega nadzora: branje sporočil, prisluškovanje tudi šifriranim pogovorom, GPS sledenje, dostop do vseh slik, dokumentov, stikov in gesel uporabnika itd.. Takšen ukrep, ki ga je vrsta držav EU zadnja leta zlorabila (nadzor novinarjev, opozicije) je bil v demokratični stroki že večkrat ocenjen kot nesorazmeren, nevaren in potencialno celo nezdržljiv z ustavno pravico do zasebnosti.

Čeprav novela uvaja, kot je zapisano, nekaj varovalk (zahteva najvišje sodne odobritve, dodatni nadzor pooblaščenca), ostaja ključen problem:

- Katere okoliščine štejejo za zadosten razlog za poseg?
- Omejitev samo na izjemne, konkretno opredeljene in neposredno dokazljive primere?
- Ali je civilni nadzor dovolj neodvisen, če ga imenuje vlada?

Iz dosedanjih izkušenj (Tudi v Sloveniji) izhaja, da vsaka vladna možnost vpliva na kadrovanje nadzornikov zmanjša kredibilnost in učinkovitost nadzora. Evropski nadzornik za varstvo podatkov opozarja, da je tak ukrep dopusten le v najbolj izjemnih primerih, kjer je neposredna, trenutna, izrecno dokumentirana grožnja nacionalni varnosti (terorizem, vojne priprave) in kjer ni nobenega drugega načina za dosego cilja.

b) Primeri zlorab po svetu in pomanjkljivost slovenskega predloga

Nikjer ni garantiranega razkritja vseh uporabljene programske opreme in njenih funkcionalnosti, ni ustreznega javnega, medijskega ali neodvisnega civilnodružbenega eks-post nadzora. V Sloveniji je že sedaj nadzorni sistem, ko gre za posebne ukrepe, v praksi bore učinkovit; zadnja parlamentarna in civilna razkritja so pokazala, da so nadzorni odbori pogosto sami pod političnim vplivom, kadrovske in finančno podhranjeni ter v nekaterih primerih instrumentalizirani s strani vladajočih elit.



5. Pravice posameznika: omejitve, obveščenost, sodno varstvo

a) Pravna ureditev v predlogu in kritika

Predlog ZSOVA bistveno omejuje pravice posameznika, da izve, kateri podatki o njem se obdelujejo, kako in ali lahko uveljavlja popravek, izbris ali vloži pritožbo. Pravica do seznanitve in sodnega varstva je srčika 38. člena Ustave RS ter temeljni standard GDPR (pravica do dostopa, popravka, izbrisa in pritožbe).

V konkretnem besedilu je več rešitev formalnih, brez vsebinskih jamstev: omejitev vpogleda v zbirke je izredno splošna, pogoji, pod katerimi bi oškodovanec lahko bil naknadno obveščen, so nejasni in niso dovolj restriktivni, ob tem je kritično problematičen tudi dolgi, petletni moratorij po 17. členu (možnost obveščanja šele po petih letih, če sploh).

Zaradi posebnosti narave obveščevalne dejavnosti je dopustno določeno omejevanje pravic posameznika, a le v nujni meri, ob strogih pogojih, z možnostjo pravočasnega sodnega varstva in z revizijskimi postopki, v katere mora biti vključena resnično neodvisna institucija (npr. evropski model "privacy representative" na Švedskem ali britanski sistem ombudsmanov s prej znanimi postopki obveščanja posameznika).



6. Pregled nadzora, transparentnost in odgovornost

a) Dvosledni nadzor: sodni, civilni, parlamentarni

Učinkovit in neodvisen nadzor nad obveščevalnimi službami je predpogoj zakonite in legitimne uporabe vseh posebnih sredstev. V Sloveniji so dosedanje izkušnje pokazale vrsto slabosti že v osnovi sistemske ureditve.

Predlog ZSOVA sicer formalizira posamezne nadzore (predsednik Vrhovnega sodišča, Komisija za nadzor varnostnih služb, posamični pooblaščenec za nadzor) ter predvideva poročanje, vendar pa ne naslavlja:

- Neodvisnosti imenovanja in odpoklica nadzornikov
- Pomanjkanja dostopa do vseh informacij – SOVA lahko del informacij zadrži s sklicevanjem na državno ali službeno tajnost
- Določb o pravnih posledicah ugotovljenih kršitev in možnosti sankcioniranja odgovornih posameznikov, vključno z vodstvom SOVE
- Obveznih javnih letnih poročilih z analizo uporabe posebnih ukrepov, z objavo narave posegov in njihove učinkovitosti v agregirani obliki, z možnostjo civilne predstavitve očitkov in odziva organov

Primerjalno najboljši sistemi (npr. norveški EOS Committee, nizozemska in kanadska nadzorstvena telesa) poudarjajo sistemsko dolžnost popolne neodvisnosti nadzora, možnost samoiniciativnega nadzora nad vsemi področji, vključno s proračunom, tehnologijami, kadrovsko politiko in arhivi, ter možnost sankcioniranja in javne objave izsledkov.



7. Usklajenost z Ustavo RS in evropskim pravnim redom

a) 38. člen Ustave RS in 8. člen Evropske konvencije o človekovih pravicah

vsakomur zagotavljata varstvo osebnih podatkov, prepoveduje njihovo uporabo v nasprotju z namenom zbiranja, določa pravico do obveščenosti in do sodnega varstva. Zakon mora jasno določati zbiranje, obdelavo, namen uporabe, nadzor in varovanje tajnosti podatkov.

Načelo sorazmernosti, minimalizma in preseganja zgolj takrat, ko ni mogoče cilj doseči manj invazivno, je v središču tako slovenske kot evropske človekovih pravic.

b) GDPR – Splošna uredba EU o varstvu osebnih podatkov

GDPR zapoveduje načela minimalizma, sorazmernosti, transparentnosti, odgovornosti, pravice posameznika do obveščenosti, izbrisa, omejitve obdelave, pritožbe ter posebne pogoje za obdelavo posebnih vrst podatkov (med katere sodijo tudi biometrični podatki).

Predlog, kot je napisan, ni skladen niti z GDPR niti z ustavnimi zahtevami, saj ne opredeljuje dovolj jasno, vnaprej in predvidljivo, katere podatke v katerih okoliščinah ter v kakšni obliki lahko SOVA zbira, kako dolgo jih lahko hrani, za kakšen izrecen namen in pod katerimi pogoji ter vključenostjo posameznika.



8. Mednarodne prakse in lekcije

Primerjalna praksa poudarja naslednje elemente kot ključno hrbtenico (g)dobrega ravnotežja med obveščevalno-varnostno dejavnostjo in varstvom zasebnosti:

- Jasno določeni nameni in omejitve vsakega posebnega ukrepa, zapisani v javno dostopni zakonodaji;
- Večstopenjski, neodvisen nadzor (sodni, parlamentarni, civilni);
- Transparentnost postopkov in javnih agregiranih poročil;
- Obvezna notifikacija posamezniku, na katerega se je ukrep nanašal, razen v nujnih, izjemno ogrožajočih primerih;
- Stroge določbe za zaščito pridobljenih podatkov, njihovo (samodejno) uničenje v ustreznih rokih ter možnost izbrisa in ugovora posameznika;
- Kazenske in disciplinske sankcije za poskus zlorabe ali prekoračitev pooblastil.

Slovenski predlog pred temi standardi očitno zaostaja: ni jasno postavljenih pogojev, ni zadostnega civilnega nadzora in ni praktičnih instrumentov za preprečevanje zlorab.



9. Mnenja civilne družbe, nevladnih organizacij in odzivi v javni razpravi

Odzivi nevladnih organizacij, stroke, Informacijskega pooblaščenca ter nekaterih civilnih aktivistov so izjemno skeptični. Prevladuje mnenje, da predlagatelj ni utemeljil nujnosti širjenja pooblastil, ni pripravil celovite ocene učinkov na temeljne pravice, ni predvidel ustreznih varovalk in da bi predlog v takšni obliki pomenil nevaren presedan, ki bi lahko v prihodnosti omogočil politično motivirane zlorabe obveščevalnega aparata (npr. politično sledenje, zatiranje nevladnikov, novinarjev in posameznikov).

10. Zgodovinske in praktične lekcije – primeri zlorab

Slovenska realnost, ob upoštevanju primerov v mednarodni skupnosti, opozarja na vrsto slabih praks in resničnih nevarnosti:

- V Sloveniji so bili v preteklosti evidentirani politično motivirani posegi SOVE v novinarsko in civilno sfero, izkoriščanje informacij v politične namene ter celo manipulacije z arhivskim gradivom za diskreditacijo nasprotnikov. Pomanjkanje učinkovitega nadzora je omogočilo vsaj delne zlorabe.
- V tujini so notranje afere Pegasus, predvolilne zlorabe specialnih prisluškovalnih orodij ter razkritja množičnih zbiranj podatkov brez jasnega pravnega temelja, vključno s sistematičnimi napakami pri uničevanju nelegalno pridobljenih podatkov, že privedle do širših javnih škandalov in omejevanja zaupanja v demokratično ureditev.



11. Predlogi za izboljšavo in ključna priporočila

Na podlagi zgoraj navedenega, ob podpori argumentiranih stališč neodvisnih organov in primerjalnopravne analize, predlagam naslednje temeljite spremembe:

1. Jasne, ozke, nedvoumno opredeljene namene, nabor podatkov in pogoje vsakega posebnega ukrepa.

Zlasti pri biometričnih podatkih, IMSI-lovilcih in spyware orodjih dovoli poseg le, če ni mogoče cilj doseči drugače, izrecno opredeli nabor podatkov in natančno vnaprej določi roke in obseg hranjenja.

2. Obvezen, večstopenjski in institucionalno neodvisen nadzor.

Civilni nadzornik naj bo imenovan v sodelovanju z DZ, Informacijskim pooblaščencom in predstavniki civilne družbe; njegovo delo mora biti javno in predmet zunanje revizije.

3. Okrepljene pravice posameznika do obveščenosti, sodnega varstva, izbrisa podatkov, poleg možnosti obveščanja najprej že ob začetku zbiranja.

Zadeva naj bo avtomatsko predmet sodnega preverjanja, če se poseg razširi ali traja dlje kot predpisani rok.

4. Strogo ločiti med preventivnim in represivnim zbiranjem podatkov; zbirke na zalogo so prepovedane.

Tudi v najhujših primerih naj bo dovoljena zgolj revizijska obdelava, avtomatsko uničenje vseh podatkov, ki niso neposredno relevantni za primer.

5. Vse določbe o nadzoru nad spremljanjem mednarodnih sistemov zvez razširiti z obvezno sodno odobritvijo, periodičnim poročanjem in formalno obvezo preverjanja zakonitosti vsakega ukrepa.

6. Okrepiti odgovornost predsednika Vrhovnega sodišča kot zadnjega jamstva – uvesti najvišje standarde iz vrstologije evropskih varovalk (Švedska, Nizozemska, Norveška), kjer lahko sodišče kadarkoli revidira, opozori na nezakonit poseg in zahteva uničenje podatkov ali prekinitev zbiranja.

7. Vzpostaviti periodično javno poročanje o uporabi posebnih ukrepov, agregirano in anonimizirano, a z možnostjo neodvisne civilne presoje glede učinkovitosti, sorazmernosti in nemožnosti arbitrarne zlorabe ali širitve ukrepov na rutinsko raven.



Inštitut Državljan D, zavod za spodbujanje
informacijske in medijske pismenosti, Ljubljana
Gradnikova ulica 6a
SI-6000 Koper
Slovenija

Zaključek

Predlog novele ZSOVA, kakor je napisan jeseni 2025, vsebuje nevarno široka in nejasno opredeljena pooblastila SOVA, ki so izrazito nagnjena v smeri učinkovitega, toda hkrati arbitrarnega in nepreglednega nadzora nad državljani. Posebej ogroženi so temeljni stebri zaščite posameznika pred državo – pravica do zasebnosti, pravica do informacijskega samoopredeljevanja in ekvivalentnost pravne zaščite glede na najstrožje evropske standarde.

V dosežku slovenskih demokratičnih izkušenj, na podlagi domače in tuje prakse, ni prostora za uresničevanje obveščevalnega nadzora izven jasno predpisanih mej in ob absolutno neodvisnem, večstopenjskem nadzoru. Vsak poseg v temeljno zasebnost in osebne podatke je dopusten le ob kičastih varovalkah, sorazmernosti in možnosti pravnega varstva, ki ni formalno, temveč zgledno učinkovito.

Novela ZSOVA v taki obliki ni skladna z duhom Ustave RS, evropskimi direktivami in sodobno demokratično kulturo. Če dobijo prednost varnostno-aparatistične potrebe pred človekovimi pravicami, Slovenija tvega nepopravljive zlorabe ter izbris zaupanja državljanov v pravno in demokratično državo.

direktor zavoda Državljan D