

## IZVEŠTAJ SA JAVNE RASPRAVE O NACRTU ZAKONA O OBRADI PODATAKA O LIČNOSTI U OBLASTI UNUTRAŠNJIH POSLOVA

• **Poverenik za informacije od javnog značaja i zaštitu podataka o ličnosti dao je sledeće komentare na Nacrt zakona:**

1) S obzirom na gore navedeno, a budući daje odredbama Nacrta zakona predviđeno da se istim „uređuje obrada podataka o ličnosti...u oblasti unutrašnjih poslova” odnosno da se odredbe tog zakona „odnose na obradu podataka prilikom primene policijskih ovlašćenja, mera i radnji i obavljanja poslova iz nadležnosti Ministarstva unutrašnjih poslova...”, što podrazumeva obradu podataka o ličnosti kako u posebne svrhe, tako i u opštem režimu, najpre je potrebno u Nacrtu zakona jasno razgraničiti obradu podataka koju Ministarstvo unutrašnjih poslova, odnosno policija vrši u svrhe sprečavanja, istrage i otkrivanja krivičnih dela, gonjenja učinilaca krivičnih dela ili izvršenja krivičnih sankcija, uključujući sprečavanje i zaštitu od pretnji javnoj i nacionalnoj bezbednosti, od obrade podataka o ličnosti koju isto vrši u opštem režimu obrade podataka.

U vezi sa navedenim komentaram, ističemo da u Zakonu o zaštiti podataka o ličnosti nije vidljiva jasna razlika između obrade podataka u dva različita režima (opštem i posebnom), a da je navedeno upravo izvršeno kroz predmetni nacrt zakona, odnosno da je u Nacrtu zakona vidljiva razlika u pogledu obrade podataka u posebne svrhe, koja je vezana za deo policijskih poslova, koje je definisao Nacrt zakona o unutrašnjim poslovima, prepoznatih u čl. 5-12. Nacrta zakona, dok se obrada podataka o ličnosti u opštem režimu vezuje za ostale policijske i druge poslove iz nadležnosti Ministarstva unutrašnjih poslova, prepoznatih u čl. 13-18. Nacrta zakona.

2) Takođe, a imajući u vidu da je predmet Nacrta zakona „uređivanje obrade podataka o ličnosti”, te bi samim tim istim trebalo urediti sve relevantne aspekte obrade podataka, ukazujemo da pojedini bitni aspekti obrade nisu istim uređeni kao npr. uslovi za dozvoljenost obrade, postupak obrade, nije uređeno adekvatno pozivanje na posebne propise kojima je utvrđen pravni osnov odnosno pravne obaveze tj. zakonom propisana ovlašćenja rukovodaca za koje je predviđena obrada neophodna, dok pojedini aspekti obrade podataka nisu na dovoljno jasan i precizan način uređeni.

U vezi sa navedenim komentaram, najpre ističemo da u Zakonu o zaštiti podataka o ličnosti utvrđena obaveza propisivanja javnog interesa i poštovanja pravila srazmernosti obrade podataka, dok je propisivanje uslova dozvoljenosti obrade podataka o ličnosti u opštem režimu ostavljeno kao mogućnost, ne i obaveza.

Zatim, ukazujemo da su u Nacrtu zakona, u smislu dozvoljenosti obrade, definisani ciljevi obrade svih podataka koje Ministarstvo obrađuje, i to: zaštita bezbednosti građana i imovine i ostvarivanja prava i drugih na zakonu zasnovanih interesa fizičkih i pravnih lica, poštovanje pravnih obaveza, obavljanja poslova u javnom interesu ili izvršenja zakonom propisanih nadležnosti Ministarstva i zaštita životno važnih interesa lica na koje se podaci odnose ili drugog fizičkog lica. Pored navedenog, u Nacrtu zakona su definisane kategorije lica čiji se podaci obrađuju, određeni su podaci o ličnosti, rokovi čuvanja i vrste korisnika podataka.

3) Stoga, predviđenu supsidijarnu primenu ZZPL, u odredbi člana 1. stav 2. Nacrta zakona treba izmeniti budući da je ZZPL sistemski zakon sa kojim je potrebno usaglasiti odredbe predmetnog zakona.

**Primedba je prihvaćena i ugrađena u Nacrt zakona.**

4) Koncept predmetnog Nacrta zakona, kojim je predviđeno propisivanje tzv. „skupova podataka“ koji, kako je navedeno, predstavljaju „maksimalan obim koje Ministarstvo može da obrađuje, u zavisnosti od svrhe obrade“, koji se „obrađuju samostalno ili se kombinuju međusobno, odnosno sa dodatnim podacima, propisanim ovim ili drugim zakonom“, te da se predviđeni skupovi podataka, koji podrazumevaju veliki obim podataka, od kojih pojedini predstavljaju posebnu vrstu podataka o ličnosti u smislu člana 17, odnosno 18. ZZPL i koji se mogu obrađivati pod uslovima propisanim istim, nije u saglasnosti sa načelima propisanim ZZPL kojima je, između ostalog, propisano da podaci o ličnosti moraju biti primereni, bitni i ograničeni na ono što je neophodno u odnosu na svrhu obrade („minimizacija podataka“). Takođe, sam predmet zakona predviđa da se ovim Nacrtom zakona određuju podaci, te upućivanje na dodatne podatke, propisane drugim zakonom, kao i dodavanja „...“ na kraju nabiranja podataka čime navedeni podaci nisu konačni, ne odgovara normi koja uređuje predmet ovog zakona.

U vezi sa navedenim komentaram, najpre ističemo da su u članu 3. Nacrta zakona predviđeni različiti skupovi podataka, koji se obrađuju samostalno, u zavisnosti od svrhe obrade i kategorije lica na koje se podaci odnose, što je utvrđeno u kasnijim odredbama. Navedeni skupovi su definisani na opšti način, imajući u vidu da se mogu obrađivati u najmanje dve različite svrhe, dok su dodatni podaci izdvojeni u tim kasnijim odredbama, u odnosu na određenu svrhu i kategoriju lica i mogu se obrađivati samo u tu konkretnu svrhu, odnosno za tu konkretnu kategoriju lica. Dodajemo i da se pojam „drugi podaci“ odnosi na podatke koji ne predstavljaju podatke o ličnosti, a nužni su za obavljanje poslova iz nadležnosti Ministarstva, kao i da je, u skladu sa komentaram koji se odnosi na Načelo minimizacije podataka, izvršena dodatna korekcija teksta Nacrta zakona.

5) Dodatno, ukazujemo na to da je članom 5. stav 1. tačka 2) ZZPL propisano da se podaci o ličnosti moraju prikupljati u svrhe koje su konkretno određene, izričite, opravdane i zakonite i dalje se ne mogu obrađivati na način koji nije u skladu sa tim svrhama („ograničenje u odnosu na svrhu obrade“). Naime, najpre ukazujemo na to da svrhe obrade podataka predviđene Nacrtom zakona treba da proizlaze iz posebnih zakona kojima su uređena pitanja koja se na istu odnose i kojima su uređene nadležnosti i ovlašćenja Ministarstva unutrašnjih poslova odnosno Policije (npr. „prevencija kriminala“, „unapređenje bezbednosti u zajednici“, „sprečavanje i otkrivanje prekršaja i privođenja učinilaca prekršaja“, „sprečavanje nasilja na javnim skupovima“ itd.), odnosno iz kojih proizlazi pravni osnov za obradu podataka o ličnosti.

Sve svrhe obrade predviđene Nacrtom zakona nisu konkretno određene i izričite, već su pojedine preširoko definisane, te ih nije lako razgraničiti sa drugim predviđenim svrhama (kao npr. „prevencija kriminala“, „unapređenje bezbednosti u zajednici“). Takođe, u tom smislu, ukazujemo i na to da je istom normom, predviđena obrada u više različitih svrha, koja predviđa obradu više istih. tzv. „skupova podataka“ u okviru kojih je u svakom pojedinačnom naveden veći broj podataka, a sve to bez predviđenih merila kojima bi se određivalo koji od podataka predviđenih u skupovima jeste zaista primeren, bitan i ograničen na ono što je neophodno u odnosu na pojedinačnu svrhu. Stoga, ukazujemo na to da isto može uneti nejasnoće prilikom tumačenja i primene odredbi ovog zakona koje uređuju postupanje sa podacima o ličnosti, odnosno omogućavaju obradu velikog seta podataka o ličnosti, te povećati verovatnoće prekomerne ili neovlašćene obrade podataka. Nejasnoće i teškoće prilikom tumačenja i primene može uneti i to, a kako je napred navedeno, što su ovlašćenja i nadležnosti Ministarstva unutrašnjih poslova, odnosno Policije uređena u jednom ili više posebnih propisa, a obrada podataka o ličnosti po tom pravnom osnovu propisana ovim Nacrtom zakona.

Tako, npr. više odredbi koje uređuju različite svrhe, uključujući primera radi odredbe čl. 4, 5, 7, 9. itd, sadrže kao odrednicu jednog od lica na koje se podaci odnose o kojem se može vršiti obrada svih podataka na koje upućuje ta odredba, da je to lice „prema kome su primenjena policijska ovlašćenja, mere ili radnje”.

Takođe, primera radi, u više odredbi se koristi termin „događaj” prilikom određivanja lica čiji bi se podaci o ličnosti obrađivali, kao npr. „lice koje je učestvovalo u događaju”, „lice koje je prijavilo događaj”, te ukazujemo na to da isto nije dovoljno jasno i konkretno jer predstavlja opšti pojam koji bi mogao imati široko značenje.

S tim u vezi, ukazujemo na to da takve i slične formulacije, budući da su preširoke, da mogu podrazumevati različite aktivnosti odnosno postupanja Ministarstva unutrašnjih poslova. tj. Policije, te uključivati razne kategorije lica, uz činjenicu da je predviđena mogućnost obrade velikog obima podataka o tim licima, kao i da je u svakoj od odredbi navedeno više svrha obrade, koje u nekim slučajevima nisu konkretno i izričito određene, bi trebalo preispitati i, po potrebi, precizirati.

U vezi sa navedenim komentarima, ističemo da je nadležnost Ministarstva unutrašnjih poslova izvorno utvrđena Zakonom o ministarstvima, a dalje razrađena posebnim zakonima, poput Zakona o policiji, Zakonika o krivičnom postupku, Zakona o prekršajima i dr, dok se ovim Nacrtom zakona uređuje samo obrada podataka o ličnosti koja se vrši prilikom obavljanja policijskih i drugih unutrašnjih poslova.

U pogledu svrha, one su definisane prema predmetu regulisanja navedenih posebnih zakona, odnosno vezuju se za policijske poslove (kako ih sada definiše Nacrt zakona o unutrašnjim poslovima), sprečavanje, otkrivanje i rasvetljavanje krivičnih dela i hapšenje učinilaca krivičnih dela (Zakonik o krivičnom postupku) i prekršaja (Zakon o prekršajima).

Dalje, u pogledu obrade podataka o licu „prema kome su primenjena policijska ovlašćenja, mere ili radnje”, ukazujemo da se različita policijska ovlašćenja, mere ili radnje primenjuju u različitim situacijama, po različitom pravnom osnovu i u različite svrhe, iz kog razloga je ova kategorija lica prepoznata u više članova, odnosno za više različitih svrha obrade, a količina podataka zavisi od vrste ovlašćenja koje se primenjuje u konkretnom slučaju .

Što se tiče termina „događaj”, isti podrazumeva različite situacije, koje se kasnije mogu kvalifikovati kao različita kaznena dela (prekršaji, krivična dela, privredni prestup) ili pojave (elementarna nepogoda, požar, poplava...), što opredeljuje nadležnost postupanja zaposlenih u Ministarstvu, kao i svrhu obrade. Takođe, odvojene su kategorije lica koje je prijavilo događaj od lica koje je učestvovalo u događaju, budući da ne mora uvek nužno da se radi o istom licu.

6) Takođe, u odnosu na član 5. Nacrta zakona ukazujemo da je članom 9. ZZPL propisano da ako se radi o podacima o ličnosti koje obrađuju nadležni organi u posebne svrhe, nadležni organ je dužan da prilikom njihove obrade, ako je to moguće, napravi jasnu razliku između podataka koji se odnose na pojedine vrste lica o kojima se podaci obrađuju, kao što su:

- 1) lica protiv kojih postoje osnovi sumnje da su izvršila ili nameravaju da izvrše krivična dela;
- 2) lica protiv kojih postoji osnovana sumnja da su izvršila krivična dela;
- 3) lica koja su osuđena za krivična dela;
- 4) lica oštećena krivičnim delom ili lica za koja se pretpostavlja da bi mogla biti oštećena krivičnim delom;

5) druga lica koja su u vezi sa krivičnim delom, kao što su svedoci, lica koja mogu da obezbede informacije o krivičnom delu, povezana lica ili saradnici lica iz tač. 1) do 3) ovog člana.

U vezi sa navedenim komentarima, ukazujemo da u članu 5. Zakona o zaštiti podataka o ličnosti nije prepoznato lice protiv koga je podignuta optužnica koja još nije potvrđena, ili protiv koga je podnet optužni predlog, privatna tužba ili predlog za izricanje mere bezbednosti obaveznog psihijatrijskog lečenja, a glavni pretres ili ročište za izricanje krivične sankcije još nije određeno („okrivljeni”), dok sam pojam „okrivljeni” konzumira i pojam „optuženi”, odnosno to je izraz koji služi kao opšti naziv za osumnjičenog, okrivljenog, optuženog i osuđenog, u skladu sa članom 2. stav 1. tačka 2) Zakonika o krivičnom postupku.

7) S tim u vezi, smatramo da je celishodno u tom smislu preispitati i usaglasiti odredbe Nacrta zakona, kao npr. da li je za lice iz stava 1. tačka 1) podtačka (1) člana 5. Nacrta zakona potrebno omogućiti obradu svih podataka iz člana 3. stav 1. Nacrta zakona, kao i dodatnih podataka iz stava 2. člana 5. istog, ukoliko to lice nije iz kategorija predviđenih članom 9. ZZPL.

U pogledu obrade podataka o licu „prema kome su primenjena policijska ovlašćenja, mere ili radnje”, u svrhu sprečavanja, otkrivanja i rasvetljavanja krivičnih dela i hapšenja učinilaca krivičnih dela, ukazujemo da je reč o primeni različitih policijskih ovlašćenja, mera ili radnji, propisanih Zakonom o policiji, Zakonikom o krivičnom postupku i drugim zakonima, koja podrazumeva obradu podataka većeg obima, neophodnih za ostvarivanje napred navedene svrhe, odnosno identifikaciju učinioca krivičnog dela, prikupljanje dokaza, vođenje postupka i postupanjima po nalogu tužilaštva i suda. Obim podataka prikupljen u ovu svrhu veći je od obima podataka koji se obrađuju za lice prema kome su primenjena policijska ovlašćenja, mere ili radnje u neku drugu svrhu, propisanu ovim zakonom, upravo zbog svrhe za koju se prikuplja.

8) Dodatno, ukazujemo na to da je nejasna formulacija iz odredbe stava 2. člana 22. Nacrta zakona koja glasi: „kada se dostavljanje vrši omogućavanjem elektronskog pristupa podacima ovlašćenim korisnicima iz člana 20. ovog zakona”, odnosno kojim propisima su određeni „ovlašćeni korisnici”, utvrđen i regulisan način dostavljanja podataka elektronskim pristupom podacima, da i isto podrazumeva pristup drugih subjekata u „Sisteme za automatsku obradu podataka” predviđene glavom VI ovog Nacrta zakona, uključujući način elektronskog pristupa (kojim podacima i sl).

**Primedba je prihvaćena i ugrađena u Nacrt zakona.**

9) U vezi sa odredbom člana 25. Nacrta zakona kojom se predviđa i uređuje obrada podataka od strane Ministarstva upotrebom sistema audio i video nadzora, video-akustičko snimanje i fotografisanje, ukazujemo na to da iz odredbe tačke 2) stava 1. proizlazi da bi se na ovaj način vršila obrada podataka o ličnosti svih zaposlenih i radno angažovanih lica u Ministarstvu unutrašnjih poslova u svrhu iz člana 15. Nacrta zakona, odnosno u svrhu kontrole pravilnosti i zakonitosti rada. Budući da ministarstvo obavlja različite vrste poslova, od administrativnih do onih koje podrazumevaju primenu policijskih ovlašćenja, mera ili radnji, potrebno je ovu odredbu preispitati i, po potrebi, precizirati.

Primedba je delimično prihvaćena i ugrađena u Nacrt zakona, tako što je navedena odredba korigovana na način da će se snimati ovlašćeno službeno lice, prilikom primene policijskog ovlašćenja. Takođe, snimanje svih lica u objektima Ministarstva nužno je iz razloga zaštite ličnosti i objekata koji u njima borave, kao i tajnih podataka, uređaja i opreme za obradu podataka i druge opreme Ministarstva, te je neophodna primena tehničke mere zaštite u formi video-nadzora, koja se posredno može koristiti i za kontrolu rada zaposlenih koji policijske poslove obavljaju u objektima Ministarstva. Ovim je obuhvaćeno i snimanje u prostorijama za zadržavanje lica, takođe u svrhu kontrole rada zaposlenih i postupanja prema dovedenim i zadržanim licima.

• **Republički sekretarijat za zakonodavstvo dao je sledeće komentare na Nacrt zakona:**

1) Ukazujemo da prema članu 47. Ustava RS niko nije dužan da se izjašnjava o svojoj nacionalnoj pripadnosti, što važi i za verska uverenja (član 43. Ustava). U tom smislu, potrebno je precizirati da se navedeni podaci koji su predviđeni članom 3. stav 1. tačka 10) mogu prikupljati samo uz pristanak lica na koje se odnose. Potrebno je detaljnije propisati i način i postupak prikupljanja tih podataka.

Pored toga, potrebno je precizirati način, postupak, uslove i obim za prikupljanje drugih naročito osetljivih podataka koji se tiču zdravlja (član 3. stav 1. tačka 5), seksualne orijentacije i seksualnog života koji su obuhvaćeni navedenom odredbom zakona.

Napominjemo da posebno nije jasan kontekst prikupljanja podataka o seksualnoj orijentaciji i seksualnom životu. Npr. prema članu 13. podaci o nacionalnosti, veroispovesti, seksualnoj orijentaciji i seksualnom životu se prikupljaju za pripadnike specijalizovanih jedinica civilne zaštite, pri čemu nije jasan kontekst takve potrebe niti svrha prikupljanja tih podataka, posebno imajući u vidu delom i postavljena ustavna ograničenja. Potreba za jasnim preciziranjem svrhe i konteksta u kome se određeni podaci prikupljaju odnosi se i na član 25. koji se odnosi na snimanje i fotografisanje lica na javnom mestu.

U vezi sa navedenim komentarom, ukazujemo da se prilikom izrade Nacrta zakona vodilo računa o podacima koje Zakon o zaštiti podataka o ličnosti svrstava u posebnu vrstu podataka o ličnosti, te da je obrada ove vrste podataka propisana zakonom, u jasno određene svrhe, u slučajevima kada je to neophodno, radi primene zakonom propisanih ovlašćenja, gde pristanak lica nije osnov za obradu podataka. Primera radi, u svrhu sprečavanja, otkrivanja i rasvetljavanja krivičnih dela i hapšenja učinilaca krivičnih dela sa elementima nacionalne, rasne i verske mržnje i netrpeljivosti ili pružanja pomoći žrtvama ovih krivičnih dela.

U pogledu seksualne orijentacije i seksualnog života, ukazujemo da su ti podaci od značaja prilikom obavljanja policijskih poslova u slučajevima kada se na osnovu navika ili sklonosti jednog lica preduzimaju neophodne mere i radnje, pre svega u interesu zaštite prava i sloboda tog lica ili radi otkrivanja krivičnih dela koja su usmerena ka licima usled njihove seksualne opredeljenosti ili seksualnog života. Ovi podaci se obrađuju u konkretne svrhe određene ovim zakonom.

Kada je reč o podacima koji se odnose na seksualnu opredeljenost ili seksualni život, kao nacionalnu pripadnost i veroispovest, primedbe su prihvaćene i izvršene su korekcije u tekstu, tako što je prva grupa podataka svrstana u dodatne podatke koji se obrađuju u konkretnu svrhu i za određenu kategoriju lica, dok se druga grupa podataka obrađuje uz pristanak lica.

- **Građanin Aleksandar Zelenski dao je sledeće komentare na Nacrt zakona:**

Iz ugla demokratskih sloboda i prava, kao i pravne države, mora da se fokusira na balans između legitimnih potreba države za bezbednošću i zaštitom javnog reda, i prava građana na privatnost, pravnu sigurnost i ograničenje državne moći. Pozitivni aspekti Jasno definisana svrha obrade: Zakon propisuje da se podaci mogu obrađivati samo radi zaštite bezbednosti, sprečavanja kriminala i izvršavanja zakonskih nadležnosti. To je u skladu sa principom pravne države da državni organi deluju samo u okviru zakona. Ovo načelo se mora praktičnim merama obezbediti u postupanju! Rokovi čuvanja podataka: Precizno su navedeni rokovi za čuvanje i brisanje podataka (npr. 10 godina za podatke o licima prema kojima su primenjena ovlašćenja, 20 godina za učesnike događaja). Ovo je važan mehanizam protiv proizvoljnog i trajnog zadržavanja podataka, koji takođe zaslužuje eksternu proveru van sistema MUP-a. Proporcionalnost: U članu 3. stoji da se obrađuju samo oni podaci koji su neophodni i srazmerni svrsi. To je ključni princip zaštite ljudskih prava, naravno uz adekvatne mere eksterne kontrole! Potencijalni rizici Širok obim podataka: Zakon dozvoljava obradu veoma osetljivih kategorija (biometrijski podaci, DNK profil, zdravstveno stanje, seksualna orijentacija, imovina). Ovo nosi rizik od prekomerne

intervencije u privatnost ako ne postoje jasni mehanizmi kontrole?! Dugotrajno čuvanje: Iako su rokovi navedeni, neki su veoma dugi (20 godina), što može biti problematično ako ne postoji nezavisna kontrola opravdanosti daljeg čuvanja! Nedostatak nezavisnog nadzora: U tekstu se ne pominje uloga nezavisnog tela (npr. Poverenik za informacije od javnog značaja i zaštitu podataka o ličnosti) u kontroli obrade ovih podataka. Bez takvog nadzora, postoji rizik od zloupotrebe. Obrada podataka bliskih lica: Zakon dozvoljava obradu podataka o članovima porodice, prijateljima i saradnicima lica koja su predmet mera. To može dovesti do kolektivne stigmatizacije i narušavanja prava lica koja nisu direktno povezana sa krivičnim delom! Demokratski i pravni okvir U demokratskoj državi, ovakvi zakoni moraju biti: precizni i ograničeni, da građani znaju kada i zašto se njihovi podaci obrađuju, podložni nezavisnoj kontroli, da postoji institucija koja nadgleda primenu i sprečava zloupotrebe, zasnovani na transparentnosti, da javnost ima uvid u statistiku i praksu primene zakona. U ovom nacrtu postoji dobra osnova u pogledu strukture i jasnoće, ali demokratske slobode i prava bi bile adekvatno zaštićene ako se uvede: jača uloga nezavisnog nadzornog organa, stroži kriterijumi za obradu osetljivih podataka, kraći i fleksibilniji rokovi čuvanja uz redovno preispitivanje, što smatram nužnim korekcijama ovog nacрта!

U vezi sa navedenim komentarima, ukazujemo da se prilikom izrade Nacrta zakona vodilo računa da se obim podataka utvrdi srazmerno svrhama, koje su precizno utvrđene ovim Nacrtom zakona i značajno limitira u odnosu na važeći Zakon o evidencijama i obradi podataka u oblasti unutrašnjih poslova. Tako je npr. utvrđeno da se biometrijski podaci i DNK obrađuju u konkretnu svrhu i za određenu kategoriju lica.

Naime, za razliku od važećeg zakona, u Nacrtu zakona su precizno razvrstane kategorije lica čiji se podaci obrađuju, u odnosu na svrhu obrade i utvrđeni su značajno kraći rokovi čuvanja podataka, za svaku od utvrđenih kategorija lica.

U vezi sa komentarom koji se odnosi na nedostatak nezavisnog nadzora, ističemo da je uloga nezavisnog državnog organa koji vrši nadzor nad primenom propisa u oblasti zaštite podataka o ličnosti regulisan Zakonom o zaštiti podataka o ličnosti, te da se ovim nacrtom zakona ne utiče na postojeći mehanizam nezavisnog nadzora. Takođe, ukazujemo da su ovlašćenja policije koja uključuju obradu podataka o ličnosti upotrebom sistema audio i video nadzora detaljnije regulisana zakonom (Zakonom o policiji, Zakonikom o krivičnom postupku i drugim posebnim zakonima), te da nije neophodno preciznije definisanje dodatnih mera zaštite u ovom Nacrtu zakona.

• **Marko Jović, direktor regulatornih i veleprodajnih poslova A1 Srbija dao je sledeće predloge za izmenu Nacrta zakona:**

1) Predlog izmene člana 3. stav 1. tačka 10)

„10) nacionalna pripadnost, veroispovest, seksualna orijentacija, seksualni život; (...)”

U istom članu stav 2. da glasi:

„U zavisnosti od svrhe obrade, u zbirkama podataka iz stava 1. ovog člana obrađuju se samo oni podaci o ličnosti čija je obrada neophodna i srazmerna svrsi obrade, dok se podaci posebne vrste mogu obrađivati samo ako je za konkretnu zakonsku svrhu izrađen test nužnosti i srazmernosti.”

Takođe, da se posle člana 3 doda član Za, koji glasi:

„Pre početka obrade koja predstavlja visok rizik za prava i slobode lica (biometrija, DNK, široki video-nadzor, masovno prikupljanje lokacijskih podataka, automatizovane analize), Ministarstvo je dužno da sprovede procenu uticaja na zaštitu podataka o ličnosti i dostavi Povereniku za informacije od javnog značaja i zaštitu podataka o ličnosti na mišljenje.”

**Obrazloženje:**

Predloženi član 3. Nacrta zakona dopušta obradu izuzetno širokog spektra podataka, koji uključuju podatke o seksualnoj orijentaciji, religiji, zdravstvene podatke, podatke o imovini, finansijske podatke, biometriju svih vrsta podataka, DNK profil i podatke o navikama, sklonosima, stilu života (član 6. Dodatni podaci).

Mnogi od gore navedenih podataka nisu nužni za obavljanje većine policijskih radnji, a LED Direktiva zahteva da se prilikom obrade ovih podataka sprovede strogi test nužnosti i srazmernosti.

Predloženom izmenom smanjuje se rizik od neopravdanog zadiranja u privatnost i izbegava političko ili socijalno profilisanje, čime se vrši usklađivanje Nacrta zakona sa članovima 4. i 8. LED Direktive, odnosno sa principom minimizacije.

U pogledu uvođenja novog člana Za, A1 je mišljenja da je za najrizičnije obrade (DNK, video-nadzor, geolociranje, biometrija) potrebno obavezno sprovoditi Procenu uticaja na zaštitu podataka, jer se na taj način povećava pravna sigurnost i vrši usklađivanje sa članom 27. LED Direktive i članom 54. Zakona o zaštiti podataka o ličnosti.

U vezi sa navedenim predlozima, ukazujemo da izrada testa neophodnosti i srazmernosti za obradu podataka u pojedinačne svrhe propisane ovim zakonom nije primenljiva, imajući u vidu da se radi o obradi podataka u „posebne svrhe” i da policijski službenici, prilikom primene policijskih ovlašćenja, mera i radnji, nisu ovlašćeni da vrše navedeni test, imajući u vidu da se radi o primeni zakonom propisanih ovlašćenja i ispunjenju zakonskih obaveza. Primera radi, u svrhu sprečavanja, otkrivanja i rasvetljavanja krivičnih dela i hapšenja učinilaca krivičnih dela sa elementima nacionalne, rasne i verske mržnje i netrpeljivosti ili pružanja pomoći žrtvama ovih krivičnih dela, gde policijski službenici moraju proveravati okolnosti i motive izvršenja krivičnog dela.

U pogledu predloga za dodavanje novog člana 3a, obaveza procene uticaja na zaštitu podataka o ličnosti prilikom obrade pojedinih vrsta podataka je propisana Zakonom o zaštiti podataka o ličnosti, kao i obaveza pribavljanja mišljenja Poverenika za informacije od javnog značaja i zaštitu podataka o ličnosti, dok ta obaveza nije isključena ovim zakonom.

2) Predlozi izmene člana 4. stav 4, člana 5. st. 3. i 4 i člana 14. stav 4:

Predlog izmene člana 4. stav 4:

„Podaci iz stava 1. tačka 1) podtač. (3) i (4) ovog člana se čuvaju **SEDAM** godina od dana događaja.”

#### **Obrazloženje:**

LED Direktiva zahteva periodično brisanje i zabranu skladištenja podataka bez jasne svrhe. Predugi rokovi stvaraju disproporciju između svrhe obrade i trajanja zadiranja u privatnost, te je Nacrtom zakona neophodno utvrditi kraće rokove čuvanja podataka.

Predlog izmene člana 5. st. 3. i 4:

„Podaci o licu iz stava 1. tačka 1) podtačka (1) ovog člana brišu se nakon pet godina od dana primene ovlašćenja, mere ili radnje.

Podaci o licu iz stava 1. tačka 1) podtač. (2) i (3) ovog člana, obrađuju se ograničeno (u daljem tekstu: pasivizacija) na period od pet godina, za krivična dela za koja je zaprećena kazna zatvora do četiri godine, odnosno na period od **PET** godina, ako je zaprećena veća kazna zatvora, računajući od dana kada je Ministarstvo obavešteno o tome da:

je krivična prijava odbačena, se odustalo od krivičnog gonjenja,

je pravnosnažno odbijena optužba ili se od nje odustalo,

je krivični postupak pravnosnažno obustavljen ili okončan pravnosnažnom oslobađajućom presudom.”

#### **Obrazloženje:**

LED Direktiva zahteva periodično brisanje i zabranu skladištenja podataka bez jasne svrhe. Predugi rokovi stvaraju disproporciju između svrhe obrade i trajanja zadiranja u privatnost, te je Nacrtom zakona neophodno utvrditi kraće rokove čuvanja podataka.

Predlog izmene člana 14. stav 4:

„Podaci iz stava 1. tačka 1) ovog člana se čuvaju **5** godina, osim ako drugim propisom nije određeno drugačije.”

LED Direktiva zahteva periodično brisanje i zabranu skladištenja podataka bez jasne svrhe. Predugi rokovi stvaraju disproporciju između svrhe obrade i trajanja zadiranja u privatnost, te je Nacrtom zakona neophodno utvrditi kraće rokove čuvanja podataka.

U vezi sa navedenim komentarima, ukazujemo da se prilikom izrade Nacrta zakona vodilo računa da se obim podataka utvrdi srazmerno svrhama, koje su precizno utvrđene ovim Nacrtom zakona i značajno limitira u odnosu na važeći Zakon o evidencijama i obradi podataka u oblasti unutrašnjih poslova.

Takođe, za razliku od važećeg zakona, u Nacrtu zakona su precizno razvrstane kategorije lica čiji se podaci obrađuju, u odnosu na svrhu obrade, utvrđeni su značajno kraći rokovi čuvanja podataka, za svaku od utvrđenih kategorija lica i uveden je pojam pasivizacije kao vid ograničenja radnji obrade samo u svrhu sprečavanja, otkrivanja i rasvetljavanja krivičnih dela i hapšenja učinilaca krivičnih dela.

3) Predlog izmene člana 19. stav 4:

„Na zahtev Ministarstva, subjekti iz stava 2. ovog člana ne obaveštavaju lice na koje se podaci odnose o prenosu podataka, do proteka određenog perioda, koji ne može biti duži od **JEDNE** godine i to samo ukoliko bi takvo obaveštavanje ugrozilo istragu.”

**Obrazloženje:**

A1 je mišljenja da je predložena odredba Nacrta zakona isuviše restriktivno postavljena i da omogućava MUP-u da ne obavesti subjekat o obradi do 5 godina. S toga, predlažemo da se navedena odredba uskladi sa potrebom prava lica na informisanje i na uvid u obrađene podatke.

**Predlog je prihvaćen i ugrađen u Nacrt zakona.**

4) Predlog izmene člana 22:

„Član 22.

O dostavljanju podataka korisnicima iz čl. 20. i 21. ovog zakona se vodi evidencija, koja sadrži podatke o podnosiocu zahteva, podatke koji su dostavljeni, razlog i datum dostavljanja i koji se čuvaju pet godina.

Kada se dostavljanje vrši omogućavanjem elektronskog pristupa podacima ovlašćenim korisnicima iz člana 20. ovog zakona, dostavljanje, odnosno pristup podacima se beleži u korisničkom žurnalu.

Ministar uređuje izgled i način vođenja evidencije iz stava 1. ovog člana.”

Predlog dodavanja člana 22a.

„Prilikom dostavljanja podataka korisnicima iz čl. 20. i 21. ovog zakona, Ministarstvo obavezno sprovodi procenu nivoa zaštite pre prenosa i sa korisnicima iz čl. 20 i 21. zaključuje standardne sporazume u obliku Standardnih ugovornih klauzula u skladu sa Odlukom o utvrđivanju Standardnih ugovornih klauzula, koja je objavljena u „Službenom glasniku Republike Srbije” br. 5/2020 dana 22. januara 2020. godine.

Zabranjeno je dostavljanje podataka korisnicima iz čl, 20 i 21. ovog zakona u slučaju da se korisnici nalaze u zemljama bez adekvatne zaštite.”

**Obrazloženje:**

Trenutni Nacrt zakona dopušta razmenu podataka sa „inicijativama“, „drugim organizacijama“, „uz princip reciprociteta“, bez da definisanja adekvatnosti zaštite kao jasnog kriterijuma za razmenu podataka.

S tim u vezi, neophodno je da se izvrši usklađivanje Nacrta zakona sa odredbama članova 36-38. LED Direktive i sa odredbama Zakona o zaštiti podataka o ličnosti u smislu sprečavanja nezakonitog deljenja podataka.

U vezi sa navedenim komentarima, ukazujemo da je zaključivanje standardnih ugovornih klauzula Zakonom o zaštiti podataka o ličnosti predviđeno kao mogućnost, a ne i obaveza. Ujedno napominjemo da se, prema Zakonu o zaštiti podataka o ličnosti, zaključivanje standardnih ugovornih klauzula ne primenjuje na obradu od strane nadležnih organa, u posebne svrhe.

U vezi sa komentarom koji se odnosi na dostavljanje podataka korisnicima koji se nalaze u zemljama bez adekvatne zaštite, ukazujemo da se u takvim slučajevima podaci prenose samo na osnovu zaključenog posebnog sporazuma, prilikom čijeg zaključivanja se vodi računa o postojanju primerenog nivoa zaštite podataka.

• **Jelena Pejić, ispred Beogradskog centra za bezbednosnu politiku, dala je sledeće predloge za izmenu Nacrta zakona:**

1) Bez preciznog definisanja pojmova koji se koriste u zakonu nemoguće je adekvatno primenjivati zakon. „Pasivizacija“ podataka predviđena je u nekoliko članova Nacrta, a nije jasno šta ona podrazumeva osim da je reč o „ograničenoj obradi podataka“. Ovaj termin ne poznaje ni Zakon o zaštiti podataka o ličnosti (ZZPL), niti evropski propisi u oblasti zaštite podataka o ličnosti (GDPR i LED direktiva iz 2016. godine). Za slučaj da je definisanje ovog pojma predviđeno izmenama i dopunama ZZPL, napominjemo da je u ovom momentu neizvesno kad će te izmene biti usvojene i stupiti na snagu, naročito imajući u vidu je ovaj Nacrt u paketu čije se usvajanje planira do kraja juna 2026. godine radi ispunjavanja obaveza iz Reformske agende Srbije, te zakonopisac ne može da se oslanja na propise koji tek treba da prođu zakonodavnu proceduru. Još bolja opcija je da se ovaj Nacrt usvoji u paketu ili nakon izmena i dopuna Zakona o zaštiti podataka o ličnosti.

**Predlog je prihvaćen i ugrađen u Nacrt zakona.**

2) Rokovi u navedenim članovima (član 25, stav 4; član 26. stav 4; član 27, stav 4) nisu ispravno određeni. Naime, umesto da se propiše rok do kojeg je najduže dozvoljeno čuvati prikupljene podatke navodi se donji prag za čuvanje podataka. Ovo nije u skladu sa Zakonom o zaštiti podataka o ličnosti i standardima definisanim EU propisima, na primer da je „posebno potrebno da se obezbedi da rok u kojem se podaci o ličnosti čuvaju bude ograničen na strogi minimum. (...) Da bi se obezbedilo da se podaci o ličnosti ne drže duže nego što je neophodno, rukovalac mora da odredi rok za brisanje ili periodično razmatranje.“ (GDPR para. 39, takođe videti ZZPL čl. 5, stav 1, tačka 5 i čl. 8, stav 2). Rokovi se ne mogu određivati samo na osnovu tehničke izvodljivosti čuvanja baza podataka već na osnovu srazmernosti svrsi radi koje se podaci obrađuju.

**Predlog je prihvaćen i ugrađen u Nacrt zakona.**

3) U obrazloženju Nacrta zakona navodi se sledeće: „Posebno poglavlje posvećeno je merama zaštite podataka o ličnosti i kontroli primene tih mera.“ „U članu 28. Nacrta zakona opisane su mere zaštite podataka.“ To poglavlje (VII) se, međutim, sastoji samo od jednog člana u kojem su ove mere tek pobrojane, a daleko od toga da su opisane. Neophodno ih je dalje razraditi u samom zakonu umesto da se u potpunosti ostavljaju za podzakonski akt koji donosi ministar.

U vezi sa navedenim komentarima, ukazujemo da mere zaštite propisane ovim zakonom podrazumevaju intervenciju u više postojećih podzakonskih akata, odnosno donošenje novih, u zavisnosti od toga da li je reč o tehničkim, organizacionim ili kadrovskim merama. Tako će određene mere (kadrovske) biti prepoznate kroz Pravilnik o unutrašnjem uređenju i sistematizaciji radnih mesta u Ministarstvu unutrašnjih poslova ili kroz Uredbu o stručnom usavršavanju i osposobljavanju u Ministarstvu unutrašnjih poslova, dok će npr. mere informacione bezbednosti (tehničke) biti razrađene u aktu koji se donosi na osnovu posebnog zakona (Zakona o informacionoj bezbednosti).

Ujedno ukazujemo da su mere zaštite podložne promenama, u cilju njihovog unapređenja, te da su podzakonski akti fleksibilnija forma za njihovo definisanje u odnosu na zakon.

• **Partneri Srbije dali su sledeće predloge za izmenu Nacrta zakona:**

1) Partneri Srbije pozdravljaju odluku da se obrada ličnih podataka u oblasti unutrašnjih poslova uredi posebnim zakonom. Takav pristup je primeren, imajući u vidu specifičnost nadležnosti Ministarstva unutrašnjih poslova i intenzitet zadiranja u pravo na zaštitu podataka o ličnosti. Ipak smatramo da je bilo neophodno ovaj postupak normiranja uskladiti sa paralelnim aktivnostima na izmenama opšteg Zakona o zaštiti podataka o ličnosti (u daljem tekstu: ZZPL), imajući u vidu da je jedan od ciljeva ovih izmena upravo preciznije razdvajanje opšteg i posebnog režima obrade podataka.

U takvoj situaciji, usvajanje posebnog zakona pre okončanja izmena opšteg okvira stvara rizik od normativne neusklađenosti, naročito u pogledu osnovnih pojmova, odnosa opšteg i posebnog režima, rokova čuvanja, prava lica na koje se podaci odnose i mera zaštite. Zato smatramo da je ovaj proces trebalo uskladiti sa izmenama ZZPL, odnosno procesu usvajanja ovog Zakona pristupiti nakon što se usvoje izmene ZZPL-a.

U vezi sa navedenim komentarima, ukazujemo da se prilikom izrade Nacrta zakona vodilo računa o opštim načelima na kojima se temelji obrada podataka o ličnosti na području Evropske unije, a u okvirima koje je postavio Zakon o zaštiti podataka o ličnosti u smislu obrade podataka u posebne svrhe, te da se ne očekuju suštinske izmene tog zakona, koje bi u značajnoj meri dovele do neusklađenosti dva zakona. Takođe, prilikom izrade Nacrta zakona izvršene su konsultacije sa službom Poverenika za informacije od javnog značaja i zaštitu podataka o ličnosti, koji je u toku javne rasprave takođe dao svoje komentare, navedene gore u tekstu.

2) Zakon o obradi podataka primenjuje se i na obradu u posebne svrhe (krivična istraga) i na opštu obradu (upravljanje ljudskim resursima, izdavanje dokumenata). ZZPL propisuje različite standarde za ova dva režima, međutim, u Nacrtu ne postoji njihovo eksplicitno razgraničenje.

U vezi sa navedenim komentarom, ukazujemo da je u Nacrtu zakona načinjena razlika u pogledu obrade podataka u posebne svrhe, koja je vezana za deo policijskih poslova, koje je definisao Nacrt zakona o unutrašnjim poslovima, prepoznatih u čl. 5-12. Nacrta zakona, dok se obrada podataka o ličnosti u opštem režimu vezuje za ostale policijske i druge poslove iz nadležnosti Ministarstva unutrašnjih poslova, prepoznatih u čl. 13-18. Nacrta zakona.

Takođe ukazujemo da način podele svrha obrade podataka na opštu i posebnu, kroz Nacrt zakona, Beogradski centar za bezbednosnu politiku i građanin Aleksandar Zelenski istakli kao pozitivnu novinu u odnosu na važeći zakon.

3) Član 4. kao svrhu navodi „prevenciju kriminala, unapređenje bezbednosti u zajednici i zaštitu zdravlja i života” – što je za policijsku ovlašćenje prihvatljivo, ali za kategorije podataka koje uključuju seksualnu orijentaciju i veroispovest (član 3. tač. 10) u toj istoj svrsi nije konkretno opravdanje. Ovo su posebne kategorije podataka u smislu čl. 17. ZZPL i za njihovu obradu postoje strogi dodatni uslovi.

Dalje, čl. 3. Nacrta propisuje 14 kategorija podataka kao „maksimalni obim“ koji MUP može obrađivati. Ovo je po sebi prihvatljivo, ali problem nastaje jer se isti maksimalni set podataka (uključujući DNK profil, biometrijske podatke, seksualnu orijentaciju, veroispovest) može koristiti za potpuno različite svrhe - od krivične istrage do upravljanja javnim skupovima. Načelo minimizacije zahteva da se za svaku svrhu obrađuje samo minimum neophodan za tu svrhu. Formulacija „u zavisnosti od svrhe obrade, obrađuju se samo oni podaci čija je obrada neophodna“ (čl. 3. st. 2.) nije dovoljna - zakon mora to propisati po svrsi, a ne prepustiti MUP-u da sam proceni.

U vezi sa navedenim komentarom, najpre ističemo da su u članu 3. Nacrta zakona predviđeni različiti skupovi podataka, koji se obrađuju samostalno, u zavisnosti od svrhe obrade i kategorije lica na koje se podaci odnose, što je utvrđeno u kasnijim odredbama. Navedeni skupovi su definisani na opšti način, imajući u vidu da se mogu obrađivati u najmanje dve različite svrhe, zajedno sa dodatnim podacima, koji su posebno izdvojeni i mogu se obrađivati samo u tu konkretnu svrhu.

Ujedno ističemo da je, u skladu sa komentarima u okviru javne rasprave, koji se odnose na Načelo minimizacije podataka, izvršena dodatna korekcija teksta Nacrta zakona.

Dodatno ukazujemo da se prilikom izrade Nacrta zakona vodilo računa o podacima koje Zakon o zaštiti podataka o ličnosti svrstava u posebnu vrstu podataka o ličnosti, te da je obrada ove vrste podataka propisana zakonom, u jasno određene svrhe, u slučajevima kada je to neophodno, radi primene zakonom propisanih ovlašćenja. Primera radi, u svrhu sprečavanja, otkrivanja i rasvetljavanja krivičnih dela i hapšenja učinilaca krivičnih dela sa elementima nacionalne, rasne i verske mržnje i netrpeljivosti ili pružanja pomoći žrtvama ovih krivičnih dela. Takođe, na primeru seksualne orijentacije i seksualnog života, ukazujemo da su ti podaci od značaja prilikom obavljanja policijskih poslova u slučajevima kada se na osnovu navika ili sklonosti jednog lica preduzimaju neophodne mere i radnje, pre svega u interesu zaštite prava i sloboda tog lica ili radi otkrivanja krivičnih dela koja su usmerena ka licima usled njihove seksualne opredeljenosti ili seksualnog života. Ovi podaci se obrađuju u konkretne svrhe određene ovim zakonom.

Konačno, napominjemo da policijski službenici, prilikom primene policijskih ovlašćenja, mera i radnji, nisu ovlašćeni da samostalno vrše procenu neophodnosti i srazmernosti obrade podataka o ličnosti, imajući u vidu da se radi o primeni zakonom precizno propisanih ovlašćenja i ispunjenju zakonskih obaveza.

4) Čl. 3. st. 4 propisuje da MUP „u meri u kojoj je to moguće“ obezbeđuje tačnost. Formulacija „u meri u kojoj je to moguće“ nije u skladu sa načelom tačnosti, koje ne dozvoljava takav blanket izuzetak.

U vezi sa navedenim komentarom, ističemo da navedena formulacija izvorno proističe iz propisa Evropske unije, koja je prihvaćena i u Zakonu o zaštiti podataka o ličnosti.

5) Za neke svrhe (npr. čl. 12. - bezbednosna zaštita određenih ličnosti) zakon dozvoljava obradu „podataka prikupljenih u postupku vršenja bezbednosne provere“ bez preciziranja uslova te provere u samom zakonu - što znači da se ključni sadržaj prepušta podzakonskim aktima, u suprotnosti sa zahtevom čl. 14. ZZPL.

U vezi sa navedenim komentarom, ističemo da je bezbednosna provera uređena zakonom kojim se uređuju unutrašnji poslovi, uključujući i bezbednosnu proveru lica u okviru bezbednosne zaštite određenih pojedinaca.

6) Nacrt koristi pojam „pasivizacija“, ali ga ne definiše, iako ga istovremeno uvodi kao jednu od mera u članu 5. i članu 28. i posebno uređuje u okviru poglavlja „Pasivizacija i brisanje podataka“ u čl. 29. Iz samog teksta nacrta nije jasno da li pasivizacija znači ograničenje obrade,

izdvajanje podataka iz aktivne evidencije, blokiranje pristupa, arhiviranje, pseudonimizaciju ili neki drugi režim obrade. U uporednoj praksi ovaj pojam nije prepoznat, te se pod pasivizacijom uglavnom referiše na anonimizaciju podataka kao meru zaštite identiteta lica. Imajući u vidu da čl. 29. stav 2. predviđa mogućnost ponovnog korišćenja pasiviziranih podataka, očigledno je da se ne radi o anonimizaciji. Dalje, nije jasno ni kakve su pravne posledice pasivizacije, ko može da pristupa pasiviziranim podacima, u koje svrhe, pod kojim uslovima, niti u kakvom je odnosu ovaj institut prema ograničenju obrade i brisanju podataka iz ZZPL. U oblasti u kojoj Ustav zahteva da se prikupljanje, držanje, obrada i korišćenje podataka o ličnosti uređuje zakonom, ovaj institut ne može ostati bez jasnog normativnog sadržaja. Imajući to u vidu, smatramo da uvođenje instituta pasivizacije podataka predstavlja samo ozakonjenje prekomernog čuvanja podataka, koje ne prolazi test ustavnosti i zakonitosti, te da ovaj vid obrade podataka treba brisati iz navedenih članova Nacrta.

**U vezi sa navedenim komentarima, ističemo da su isti prihvaćeni i ugrađeni u Nacrt zakona.**

7) Nacrt kroz nekoliko članova, prepušta ministru, odnosno aktima Ministarstva, pitanja koja moraju biti uređena samim zakonom. To se odnosi, između ostalog, na sadržaj, izgled i način vođenja zbirke podataka, obrazac zahteva za dostavljanje podataka, izgled i način vođenja evidencije o dostavljanju, upotrebu korisničkog žurnala, mere zaštite podataka i način njihovog sprovođenja, kao i način brisanja i pasiviziranja podataka. Nije sporno da se tehnički i operativni detalji mogu biti razrađeni podzakonskim aktima. Međutim, nije prihvatljivo da se podzakonskom normiranju prepuste elementi koji neposredno određuju obim, uslove, dostupnost, trajanje i kontrolu obrade podataka o ličnosti. Ustav Republike Srbije izričito propisuje da se prikupljanje, držanje, obrada i korišćenje podataka o ličnosti uređuje zakonom, dok ZZPL za obradu od strane nadležnih organa u posebnim svrhama insistira na zakonskoj određenosti dalje obrade i na određivanju rokova za brisanje ili periodično preispitivanje potrebe čuvanja. Zbog toga smatramo da zakon mora da uredi najmanje osnovne elemente zbirke podataka, krug ovlašćenih korisnika, uslove pristupa, pravila izdvajanja i kopiranja, osnovne elemente evidencije, kriterijume za pasivizaciju i brisanje, kao i minimalne mere zaštite, dok bi ministru mogla biti prepuštena samo njihova tehnička operacionalizacija.

**U vezi sa navedenim komentaram, ističemo da su u članu 3. Nacrta zakona predviđeni različiti skupovi podataka, koji se obrađuju samostalno, u zavisnosti od svrhe obrade i kategorije lica na koje se podaci odnose, što je utvrđeno u kasnijim odredbama. Navedeni skupovi su definisani na opšti način, imajući u vidu da se mogu obrađivati u najmanje dve različite svrhe, zajedno sa dodatnim podacima, koji su posebno izdvojeni i mogu se obrađivati samo u tu konkretnu svrhu.**

Takođe, u nacrtu zakona definisan je maksimalan obim podataka o ličnosti i utvrđeno je da se, pored podataka o ličnosti, u zbirkama podataka obrađuju i drugi podaci, čija obrada je neophodna za obavljanje poslova iz nadležnosti Ministarstva.

Konačno, dodajemo i to da je, u vezi sa navedenim komentaram, u članu 3. Nacrta zakona precizirano koje podatke mogu da sadrže pojedinačne zbirke koje formira Ministarstvo, te da nema smetnji da navedene zbirke budu propisane podzakonskim aktom, imajući u vidu da neće sadržati podatke koji već nisu propisani zakonom (pored rokova čuvanja, preciznije definisanih mera zaštite, koje su već zakonom predviđene, kao i uslova za obradu podataka utvrđenih u Nacrtu zakona, što suštinski predstavlja osnovne elemente koje treba da sadrži svaka zbirka i koji treba da se bliže definišu podzakonskim aktom, u odnosu na pojedinačnu zbirku).

Ujedno napominjemo da su zbirke podataka o ličnosti ranije formirane, u skladu sa odredbama Zakona o evidencijama i obradi podataka u oblasti unutrašnjih poslova, odnosno

drugih zakona u oblasti unutrašnjih poslova, te da donošenje ovog zakona neće uticati na njihov sadržaj, osim u pogledu rokova čuvanja podataka, a da će se eventualne nove zbirke podataka formirati u skladu sa ovim zakonom, vodeći računa o obimu podataka njime utvrđenim, svrhama obrade, rokovima čuvanja, neophodnosti i srazmernosti, kao i ostalim principima na kojima se zasniva ovaj zakon.

8) Čl. 19. st. 4. Zakona o obradi podataka predviđa da organ vlasti može ne obavestavati lice o prenosu podataka do 5 godina - bez sudske kontrole. ZZPL (član 25.) dozvoljava odlaganje obaveštenja, samo u onoj meri i u trajanju dok je to neophodno i srazmerno u demokratskom društvu u odnosu na poštovanje osnovnih prava i legitimnih interesa fizičkih lica, radi ostvarivanja određenih propisanih interesa. Paušalno određeni rok od pet godina može dovesti do situacije da se ovakvo obavestavanje od strane nadležnog organa namenski odlaže, te podaci prekomerno obrađuju bez znanja lica o takvoj obradi. Ovakva odredba posebno zabrinjava u kontekstu saznanja o primeni mera tajnog nadzora komunikacija, tajnog praćenja i snimanja, kao i dokumentovanih slučajeva primene nelegalnih špijunskih softvera od strane nadležnih organa.

**Predlog je prihvaćen i ugrađen u Nacrt zakona.**

9) Član 20. Nacrta predviđa dostavu podataka stranim državama „na osnovu potvrđenog međunarodnog ugovora ili zaključenog posebnog ugovora“ bez dodatnih garancija adekvatnosti zaštite. Zakonski okvir ne uključuje mehanizam za proveru adekvatnosti zaštite u zemlji prijema, što je standardni zahtev GDPR-a i LED direktive (čl. 35-40.). Primera radi, Ministarstvo informisanja i telekomunikacija Republike Srbije, u februaru 2025. godine, potpisalo je memorandum o saradnji u oblasti IKT sa Iranom - državom sa dokumentovanim i sistemskim kršenjem prava na privatnos, a slične bojazni postoje i u odnosu na međudržavne sporazume potpisane sa NR Kinom. Postojanje međunarodnog sporazuma, bez dodatnih provera i garancija zaštite prava građana i bezbednosti informacija, dovodi do dodatnih rizika ne samo po pravo na privatnost, već i sistem nacionalne bezbednosti Republike Srbije.

Takođe, čl. 20. i 21. Nacrta uređuju dostavljanje podataka, ali ne propisuju unapred kategorije primalaca za svaku svrhu - što zahteva čl. 14. ZZPL.

**U vezi sa komentarom koji se odnosi na dostavljanje podataka korisnicima koji se nalaze u zemljama bez adekvatne zaštite, ukazujemo da se u takvim slučajevima podaci prenose samo na osnovu zaključenog posebnog sporazuma, prilikom čijeg zaključivanja se vodi računa o postojanju primerenog nivoa zaštite podataka.**

**Takođe, ističemo da su kategorije primalaca u dovoljnoj meri prepoznate u Nacrtu zakona (državni organi, organizacije, fizička i pravna lica, međunarodni subjekti...), a da će konkretni primaoci biti preciznije navedeni kroz evidencije radnji obrade, koju Ministarstvo vodi u skladu sa Zakonom o zaštiti podataka o ličnosti.**

10) Posebno problematično rešenje sadržano je u čl. 25 - 27. Nacrta, gde su rokovi čuvanja podataka prikupljenih sistemom audio i video nadzora, sistemom kontrole pristupa i sistemom za beleženje audio zapisa propisani kao najkraći rokovi čuvanja: „najkraće 30 dana“, odnosno „najkraće godinu dana“. Takvo postavljanje rokova nije u skladu sa standardima zaštite podataka o ličnosti. Rok čuvanja u zakonu mora predstavljati krajnju granicu dozvoljenog zadržavanja podataka, a ne minimalni period tokom kojeg se podaci obavezno čuvaju. ZZPL propisuje načelo ograničenja čuvanja, prema kome se podaci mogu čuvati samo onoliko dugo koliko je neophodno zaostvarivanje svrhe obrade, a za obradu koju vrše nadležni organi u posebne svrhe mora biti određen rok za brisanje ili rok za periodičnu ocenu potrebe čuvanja. Minimalni zakonski rokovi, naročito kod sistema koji podrazumevaju kontinuirani nadzor i snimanje kretanja, pristupa i komunikacija, šire prostor za prekomerno zadržavanje podataka i slabe

funkciju zakonskog ograničenja. Zato predlažemo da se u čl. 25-27. rokovi propišu kao najduži rokovi čuvanja.

Takođe, pojedine rokovi u Nacrtu treba preispitati. Na primer, čl. 4. predviđa rok od 20 za čuvanje podataka lica koja su prijavila događaj ili zatražila pomoć, što se za ovakvu svrhu može smatrati prekomernim.

Predlog je delimično prihvaćen i ugrađen u Nacrt zakona. Što se tiče rokova čuvanja podataka lica koja su prijavila događaj, ističemo da pojam „događaj” podrazumeva različite situacije, koje se kasnije mogu kvalifikovati kao različita kaznena dela (prekršaji, krivična dela, privredni prestup) ili pojave (elementarna nepogoda, požar, poplava...), što opredeljuje kasnija postupanja zaposlenih u Ministarstvu, kao i svrhu obrade, iz kog razloga iziskuje i duži rok čuvanja, posebno imajući u vidu da se ti podaci koriste i za ostvarivanje prava lica na koje se podaci odnose u slučajevima kada je tim licima potrebno obezbediti dokaz ili izdati potvrdu da su učestvovali u događaju kao oštećeni ili lica koje je prijavilo događaj/zatražilo pomoć (požari, elementarne nepogode i sl.)...

11) Nacrt ne sadrži odredbe o pravu lica da se na njega ne primenjuju odluka zasnovana isključivo na automatizovanoj obradi. Čl. 38. i 39. ZZPL propisuju ovo pravo i obavezu da zakon koji propisuje automatizovanu obradu mora sadržati mere zaštite. Nacrtu sadrži odredbe o IKT sistemu (čl. 24.) i sistemu audio i video nadzora (čl. 25) koji su po definiciji sistemi automatske obrade – ali bez ikakve odredbe o pravima lica ili merama zaštite u kontekstu automatskog odlučivanja.

U vezi sa navedenim komentarom, ističemo da su prava lica u vezi sa automatizovanom obradom podataka i obaveze rukovaoca u pogledu ograničenja automatizovanog donošenja odluka precizno utvrđeni Zakonom o zaštiti podataka o ličnosti.

12) Čl. 1. st. 2. Zakona o obradi podataka sadrži blanket upućivanje na ZZPL, što nije dovoljno specifično za prava lica u kontekstu posebnog režima obrade. Imajući u vidu invazivnost obrade podataka od strane nadležnih organa u posebne svrhe i moguće posledice obrade po prava i slobode lica, potrebno je predvideti dodatne garancije i načine ostvarenja prava.

**Primerka je prihvaćena i ugrađena u Nacrt zakona.**

**• Advokati Branislav S. Subotin i Željko Kočić iz Novog Sada dali su sledeće predloge za izmenu Nacrta zakona:**

1) Komentar na član 25:

Ova odredba uvodi pravni osnov za masovnu primenu sistema audio i video nadzora u okviru unutrašnjih poslova, koji obuhvata snimanje, fotografisanje i akustičko beleženje lica u različitim situacijama - od javnih prostora gde se primenjuju policijska ovlašćenja, preko objekata MUP, pa sve do šireg prostora u kom se mogu nalaziti lica koja ni na koji način nisu u pravnom odnosu sa organima vlasti. Iako se kao formalni cilj navodi obavljanje poslova iz delokruga policije i bezbednosti, detaljna analiza pokazuje da je norma izuzetno široka i da ne uspostavlja dovoljno jasne i stroge granice između legitimnog nadzora i nedozvoljenog ili nesrazmernog uplitanja u pravo na privatnost.

Najpre, ključni problem leži u veoma širokom obuhvatu lica koja mogu biti predmet snimanja. Odredba ne ograničava nadzor samo na lica koja su predmet konkretne policijske radnje ili istrage, već obuhvata i sva lica koja se zateknu na mestu gde se primenjuju policijska ovlašćenja, kao i lica koja se nalaze u objektima MUP. To u praksi znači da se snimanje vrši bez individualizacije, odnosno bez potrebe da postoji konkretan razlog u odnosu na svako pojedinačno lice. Takvo rešenje vodi ka situaciji u kojoj se veliki broj građana može naći pod stalnim ili povremenim nadzorom, bez jasnog kriterijuma sumnje ili potrebe.

Drugi značajan problem odnosi se na prirodu prikupljenih podataka. Ovde se ne radi samo o vizuelnom nadzoru, već i o audio-vizuelnom i akustičkom snimanju, što znači da se beleži i izgled lica, njegovo ponašanje, kretanje, ali i razgovori i zvukovi iz okruženja. Ovakva vrsta obrade podataka je izuzetno invazivna, jer omogućava detaljnu rekonstrukciju aktivnosti i ponašanja pojedinaca. Kada se tome dodaju i podaci o lokaciji, vreme i precizne geografske koordinate, dobija se sistem koji omogućava veoma precizno praćenje kretanja i aktivnosti lica u prostoru.

Posebno je problematičan deo odredbe koji dozvoljava obradu izuzetno detaljnih podataka o lokaciji, uključujući ulice, raskrsnice, kućne brojeve, kilometražu puta, granične prelaze, pa čak i „bliže nazive lokacija“. Ovako precizno geografsko praćenje u kombinaciji sa video i audio nadzorom stvara mogućnost za formiranje sveobuhvatnih profila kretanja pojedinaca, što predstavlja jedan od najintenzivnijih oblika nadzora u savremenim sistemima bezbednosti. Sa stanovišta prava na privatnost, ovakva kombinacija podataka može dovesti do dubokog uplitanja u lični i porodični život lica.

Još jedan značajan nedostatak odnosi se na rok čuvanja podataka. Odredba predviđa da se podaci čuvaju najmanje 30 dana. Iako se ovaj rok na prvi pogled može činiti ograničenim, problem je u tome što se radi o minimalnom roku, bez jasno određenog maksimalnog ograničenja u samoj normi. To znači da zakon ne sprečava potencijalno duže čuvanje podataka, što otvara prostor za različite interne prakse koje mogu dovesti do neujednačene primene i produženog zadržavanja snimaka.

Dodatno, pristup podacima je ograničen na lica sa posebnim ovlašćenjem u skladu sa aktom ministra. Iako se na prvi pogled radi o mehanizmu kontrole pristupa, u suštini se radi o internom sistemu odlučivanja koji nije dovoljno transparentan niti podložan nezavisnoj kontroli. Ključni problem je što zakon ne propisuje jasne kriterijume ko može dobiti pristup, u kojim situacijama i pod kojim uslovima, već se to prepušta internom uređenju unutar MUP. Na taj način, suštinska pitanja zaštite podataka i privatnosti izmeštaju se iz zakonskog okvira u administrativnu sferu.

Takođe, odredba ne uspostavlja jasne mehanizme spoljašnjeg nadzora nad upotrebom sistema audio i video nadzora. U savremenim pravnim standardima, posebno u kontekstu mera koje uključuju masovno ili široko rasprostranjeno snimanje, nezavisni nadzor (sudski, parlamentarni ili od strane nezavisnih tela za zaštitu podataka) smatra se ključnim elementom zakonitosti. U ovom slučaju, taj element nije eksplicitno predviđen, što slabi garancije protiv zloupotrebe.

Posmatrano kroz princip srazmernosti, koji zahteva da svaka mera koja zadire u osnovna prava mora biti neophodna, pogodna i najmanje restriktivna u odnosu na cilj koj se želi postići, ova odredba ostavlja utisak prekomerne širine. Nadzor se ne ograničava na konkretne situacije rizika ili pojedinačne slučajeve, već se primenjuje na širok spektar prostora i lica. To znači da se umesto ciljanog nadzora uvodi sistem koji ima karakter stalnog ili polustalnog praćenja u određenim zonama.

Još jedan problem je nedostatak jasne definicije šta se dešava sa prikupljenim podacima nakon isteka roka čuvanja. Iako se navodi da se oni čuvaju najmanje 30 dana, ne postoji dovoljno precizno uređenje njihovog brisanja, a naročito ne postoji jasna obaveza automatskog uništavanja ili mehanizam provere da li je do brisanja zaista došlo. U sistemima video nadzora, ovaj aspekt je ključan, jer upravo dugotrajno i nekontrolisano čuvanje snimaka predstavlja jedan od najčešćih izvora zloupotreba.

Sve navedeno ukazuje da ova odredba uspostavlja veoma širok i tehnološki intenzivan sistem nadzora, koji obuhvata veliki broj lica i prostora, uz ograničene procesne i institucionalne

garancije. Iako je cilj - bezbednost i efikasnost rada policije - legitiman, način na koji je norma formulisana ne obezbeđuje dovoljnu ravnotežu između tog cilja i zaštite osnovnih prava. Zbog toga se može zaključiti da odredba nije u potpunosti adekvatna, jer nedovoljno precizno definiše obim nadzora, oslanja se na interne akte umesto na zakonske garancije, ne obezbeđuje jasan i nezavisan nadzor, i omogućava obradu podataka koja može biti nesrazmeria u odnosu na legitimni cilj koji se želi postići.

Predložena odredba kojom se uređuje sistem audio i video nadzora ne pravi jasnu pravnu razliku između video i audio nadzora, iako se radi o suštinski različitim merama sa različitim stepenom uticaja na pravo na privatnost. Upravo ovaj nedostatak dovodi u pitanje njenu usklađenost sa ustavnim garancijama i standardima utvrđenim u praksi Evropskog suda za ljudska prava (ESLJP).

Video nadzor - Video nadzor, kao mera koja podrazumeva beleženje ponašanja lica na javnim mestima, može biti opravdan u svrhu zaštite bezbednosti. Međutim, u konkretnoj odredbi ova mera je postavljena preširoko i bez dovoljno preciznih ograničenja. Naime, formulacije poput „lica na javnom ili drugom mestu" i „drugih lica u objektima Ministarstva" obuhvataju praktično neograničen krug lica, bez jasnih kriterijuma i situacija u kojima se nadzor primenjuje. Tako postavljena mera ima karakter opšteg i nediferenciranog nadzora, što nije u skladu sa zahtevom proporcionalnosti. Pored toga, odredba ne sadrži dovoljno jasna pravila o: uslovima aktiviranja nadzora; obimu i trajanju snimanja; razgraničenju između stalnog i povremenog nadzora; nezavisnoj kontroli primene. Posebno je problematično što se pristup podacima i dalja obrada prepuštaju podzakonskom aktu, čime se ključna pitanja zaštite prava građana izmeštaju iz zakona.

Audio nadzor - Za razliku od video nadzora, audio nadzor predstavlja kvalitativno drugačiju i znatno invazivniju meru, jer omogućava snimanje sadržaja komunikacije. Predložena odredba omogućava: audio snimanje lica na javnim mestima; bez individualizacije i konkretne sumnje; bez prethodne sudske kontrole. Na taj način se faktički uvodi mogućnost masovnog snimanja razgovora građana, što po svojoj prirodi odgovara merama tajnog nadzora komunikacija, ali bez ustavom propisanih garancija. Prema standardima ESLJP, ovakvo mešanje u pravo na privatnost ne može se smatrati neophodnim u demokratskom društvu, budući da: nije ograničeno na konkretne slučajeve; obuhvata neograničen broj lica; nije praćeno adekvatnim garancijama protiv zloupotrebe. Dodatno, priroda audio nadzora je takva da on po pravilu dovodi do nediferenciranog prikupljanja podataka, jer nije moguće selektivno ograničiti koje će komunikacije biti snimljene.

Kombinovanje audio i video podataka - Odredba predviđa i obradu preciznih lokacijskih podataka (uključujući GPS koordinate), što u kombinaciji sa audio zapisima omogućava detaljno praćenje kretanja i komunikacije lica. Ovakva obrada podataka značajno povećava stepen zadiranja u privatnost i rizik od profilisanja.

Opšti nedostatak - izostanak jasnog razgraničenja

Ključni problem odredbe je što: ne pravi razliku između video i audio nadzora i na obe mere primenjuje iste, nedovoljno stroge uslove. Na taj način se omogućava da se najintruzivnija mera (audio nadzor) primenjuje u režimu koji bi eventualno mogao biti prihvatljiv samo za video nadzor.

Predložena odredba:

- u delu koji se odnosi na video nadzor nije dovoljno precizna i proporcionalna
- u delu koji se odnosi na audio nadzor predstavlja nesrazmerno i pravno nedopustivo mešanje u pravo na privatnost i tajnost komunikacija

Shodno tome, neophodno je:

- jasno razdvojiti pravni režim video i audio nadzora
- značajno suziti i precizirati uslove za video nadzor
- izbrisati ili suštinski restriktivno urediti audio nadzor, uz uvođenje sudske kontrole i strogih garancija.

U narednom izlaganju iznosimo detaljnije zamerke na predložene odredbe ovog zakona u kombinaciji sa drugim koji se na njega odnose.

Predloženi član, kojim se ovlašćuje MUP da vrši audio i video nadzor, uključujući video-akustičko snimanje lica na javnim mestima, u objektima MUP i u okviru primene policijskih ovlašćenja, nije u skladu sa ustavnim i konvencijskim standardima zaštite prava na privatnost i tajnost komunikacija, prema praksi Evropskog suda za ljudska prava.

Ovom odredbom se predviđa mogućnost sistematskog audio snimanja lica na javnim mestima i u različitim situacijama bez jasnog ograničenja. Za razliku od video nadzora, koji beleži spoljašnje ponašanje, audio nadzor zahvata sadržaj komunikacije, čime ulazi u sferu koja uživa najviši stepen ustavne zaštite.

Predloženo rešenje faktički omogućava: snimanje razgovora građana bez njihovog znanja, kao i nediferencirano prikupljanje komunikacija svih lica koja se zateknu u nadziranoj zoni. Na taj način se briše granica između javnog nadzora i tajnog prisluškivanja, bez ispunjenja uslova koji se za takve mere inače zahtevaju (sudska odluka, konkretna sumnja, ograničeno trajanje).

Odredba omogućava nadzor: svih lica na javnim mestima; svih zaposlenih i angažovanih lica i svih lica u objektima MUP. Ovako postavljeno ovlašćenje je: opšte nediferencirano (neselektivno) i bez jasnih kriterijuma primene.

Prema standardima ESLJP, mere nadzora moraju biti strogo ograničene i usmerene na konkretne situacije. Masovno prikupljanje audio podataka ne može se smatrati „neophodnim u demokratskom društvu“, jer se isti ciljevi mogu postići manje invazivnim sredstvima. Predloženi član ne sadrži dovoljno jasna i precizna pravila o: konkretnim uslovima pod kojima se uključuje audio snimanje; obimu snimanja (da li je kontinuirano ili selektivno); kriterijumima za izdvajanje i obradu podataka i nadzoru nad licima koja imaju pristup podacima. Posebno je problematično što se pristup podacima uređuje „posebnim aktom ministra“, što ostavlja širok prostor za diskreciju bez zakonskih garancija. Ovakvo rešenje ne ispunjava standard predvidivosti koji zahteva Evropski sud za ljudska prava. Odredba ne predviđa prethodno sudsko odobrenje; nezavisan nadzor nad primenom mere i efektivna pravna sredstva za lica koja su bila predmet nadzora. S obzirom da se radi o obradi komunikacija, ovakva kontrola je neophodna. Njeno odsustvo značajno povećava rizik zloupotrebe.

Iako je propisan minimalni rok čuvanja od 30 dana, nije jasno ograničen maksimalni rok; nije definisano u kojim slučajevima se podaci zadržavaju duže n nije propisano obavezno brisanje podataka koji nisu relevantni. Dodatno, obrada detaljnih lokacijskih podataka (GPS koordinate, precizne adrese i sl.) u kombinaciji sa audio zapisima omogućava duboko profilisanje kretanja i ponašanja lica.

Saznanje da država može snimati razgovore na javnim mestima dovodi do: samocenzure; smanjenja slobode izražavanja i ograničenja društvenih interakcija. Ovaj efekat je u suprotnosti sa demokratskim standardima koje ppgiti Evropski sud za ljudska prava.

Predloženi član u delu koji omogućava audio, odnosno video-akustičko snimanje:

- uvodi nesrazmerno i nedovoljno ograničeno mešanje u pravo na privatnost
- zaobilazi ustavne garancije tajnosti komunikacija
- ne ispunjava uslove zakonitosti, nužnosti i proporcionalnosti

**PREDLOG:**

1. Brisanje odredaba koje omogućavaju audio i video-akustičko snimanje; ili

2. Alternativno, njihovo strogo ograničavanje tako da:

- se primenjuju isključivo u pojedinačnim slučajevima
- podležu prethodnoj sudskoj odluci
- budu vremenski i sadržinski ograničene
- uključuju jasan i nezavisan mehanizam nadzora

U suprotnom, predložena odredba nosi visok rizik da bude ocenjena kao neustavna i nesaglasna sa Evropskom konvencijom o ljudskim pravima.

U vezi sa navedenim komentaram, ističemo da, u skladu sa odredbama važećeg Zakona o policiji, Ministarstvo vrši nadzor i snimanje javnog mesta, što uključuje snimanje ili fotografisanje javnog skupa, kao i audio i video snimanje postupanja policijskih službenika, a u svrhu otkrivanja i rasvetljavanja prekršaja i krivičnih dela, kao i kontrole i analize obavljanja policijskih poslova. Navedena obrada podataka dodatno je uređena odredbama Zakona o evidencijama i obradi podataka u oblasti unutrašnjih poslova, čime je prvi put usaglašavana sa evropskim zakonodavstvom. Ovim nacrtom zakona se obrada podataka putem audio i video nadzora dodatno uređuje u usklađuje sa evropskim normativima u ovoj oblasti, koji su prihvaćeni u Zakonu o zaštiti podataka o ličnosti.

Takođe, odredbama Zakona o zaštiti podataka o ličnosti propisano je da se prilikom uvođenja novih tehnologija u oblasti obrade podataka o ličnosti obavezno vrši procena rizika za zaštitu podataka, te, budući da se ovim nacrtom zakona ne predviđaju nove tehnologije, smatramo da je rizik po prava i slobode građana ostao nepromenjen u odnosu na prethodni period, kada su podzakonskim aktima obezbeđene dodatne mere zaštite podataka o ličnosti koje obrađuje Ministarstvo unutrašnjih poslova u sistemu audio i video nadzora.

Ovim nacrtom zakona je izvršeno je dodatno prilagođavanje odredbama Zakona o zaštiti podataka o ličnosti i učinjena veća transparentnost rada policije, imajući u vidu da Nacrt zakona o unutrašnjim poslova, za koji se ovaj Nacrt zakona prvenstveno veže, predviđa mogućnost snimanja primene svih policijskih ovlašćenja.

U pogledu ograničenja prava pristupa, odnosno nezavisne spoljašnje kontrole pristupa, kao dodatnim merama zaštite podataka, ukazujemo da su Nacrtom zakona propisane osnovne mere zaštite, koje će se dalje razraditi intervencijom u više postojećih podzakonskih akata, odnosno donošenjem novih, u zavisnosti od toga da li je reč o tehničkim, organizacionim ili kadrovskim merama. Na taj način smatramo da će se obezbediti dovoljan mehanizam kontrole pristupa podacima, imajući u vidu različite svrhe u koje se podaci obrađuju. S tim u vezi, ukazujemo da su ovlašćenja policije koja uključuju obradu podataka o ličnosti upotrebom sistema audio i video nadzora detaljnije regulisana zakonom (Zakonom o policiji, Zakonikom o krivičnom postupku i drugim posebnim zakonima), te da nije neophodno preciznije definisanje dodatnih mera zaštite u ovom Nacrtu zakona, dok je, u skladu sa upućenom sugestijom, izvršena korekcija u Nacrtu zakona i ograničen je pristup podacima u zavisnosti od okvira ovlašćenja zaposlenih, utvrđenih opisom poslova radnog mesta, a u svrhu obavljanja poslova iz nadležnosti organizacione jedinice, kao i pasiviziranim podacima, uz posebno ovlašćenje od strane ministra.

U vezi sa komentaram koji se odnosi na nedostatak nezavisnog nadzora, ističemo da je uloga nezavisnog državnog organa koji vrši nadzor nad primenom propisa u oblasti zaštite podataka o ličnosti regulisan Zakonom o zaštiti podataka o ličnosti, te da se ovim nacrtom zakona ne utiče na postojeći mehanizam nezavisnog nadzora.

Takođe, predlog koji se odnosi preciznije određivanje i skraćivanje rokova čuvanja podataka prihvaćen je u Nacrtu zakona.

2) Komentar na član 27:

Ova odredba uređuje upotrebu sistema za beleženje audio zapisa u MUP, pri čemu se predviđa da se snimaju i obrađuju razgovori određenih kategorija lica - građana koji pozivaju hitne službe i druge javne brojeve, kao i zaposlenih i lica koja koriste zaštićene komunikacione sisteme državnih organa. Na prvi pogled, cilj norme jeste obezbeđivanje bezbednosti komunikacija, kontrola rada službi i mogućnost naknadne provere sadržaja razgovora u određenim postupcima. Međutim, detaljnija analiza pokazuje da ova odredba u više aspekata nije u dovoljnoj meri usklađena sa osnovnim standardima zaštite prava na privatnost i zaštitu podataka o ličnosti.

Pre svega, najupadljiviji problem jeste izuzetno širok obuhvat lica čije se komunikacije snimaju. Odredba obuhvata ne samo službena lica u sistemu MUP i bezbednosnih službi, već i građane koji pozivaju brojeve hitnih službi ili druge javno dostupne brojeve telefona. To znači da se audio snimanje ne odnosi samo na usko definisane bezbednosne ili operativne potrebe, već zahvata i komunikaciju opšte populacije u situacijama koje često podrazumevaju stres, hitnost ili ličnu osetljivost. U takvom okolinostima, očekivanje privatnosti je posebno izraženo, jer građani kontaktiraju državne službe radi zaštite života, zdravlja ili imovine.

Drugi značajan problem odnosi se na prirodu same obrade podataka. Ovde se ne radi samo o metapodacima, već o direktnom snimanju audio sadržaja razgovora. To znači da se beleži sam sadržaj komunikacije, uključujući potencijalno osetljive lične informacije, emocionalne izjave, opise događaja, pa čak i podatke koji mogu spadati u posebne kategorije podataka o ličnosti. Snimanje razgovora u realnom vremenu predstavlja jedan od najintenzivnijih oblika intervencije u privatnost, jer omogućava potpuni uvid u komunikaciju između lica i državnog organa.

Dodatno, odredba predviđa i obradu metapodataka kao što su datum, vreme i trajanje razgovora, broj pozivaoca i lokacija uređaja sa kog je poziv upućen. Kombinacija audio zapisa i lokacionih podataka stvara izuzetno detaljan profil ponašanja pojedinaca. Na ovaj način, država ne samo da ima uvid u sadržaj komunikacije, već može rekonstruisati i kretanje, navike i obrasce ponašanja lica koja koriste ove usluge. U savremenom pravu zaštite podataka, ovakva kombinacija podataka se smatra visoko invazivnom, jer omogućava duboku analizu privatnog života.

Posebno je problematičan aspekt koji se odnosi na rok čuvanja podataka. Odredba predviđa da se audio zapisi čuvaju najmanje godinu dana. Takav minimalni rok čuvanja, bez jasno definisanog maksimalnog ograničenja u samom tekstu norme, otvara prostor za potencijalno dugotrajno ili neodređeno čuvanje velikog broja razgovora. U kontekstu principa minimizacije podataka i ograničenja roka čuvanja, koji su osnovni standardi savremene zaštite podataka o ličnosti, ovako postavljeno rešenje može se smatrati nesrazmernim, jer ne pravi dovoljno jasnu razliku između podataka koji su zaista neophodni za duži period i onih koji bi morali biti brzo brisani.

Takođe, pristup snimljenim podacima je veoma restriktivno formulisan, ali istovremeno i nedovoljno transparentan. Predviđa se da pristup ima samo lice sa posebnim ovlašćenjem, u skladu sa internim aktom ministra. Ovde se javlja ozbiljan problem sa stanovišta pravne sigurnosti i kontrole nad obradom podataka. Naime, ključni kriterijumi za pristup tako osetljivim podacima nisu propisani zakonom, već se prepuštaju podzakonskom aktu i internim odlukama izvršne vlasti. To znači da se suštinska garancija zaštite podataka ne nalazi na nivou zakona, već u internoj hijerarhiji organa koji podatke i obrađuje, što značajno slabi nezavisnost i objektivnost kontrole.

Još jedan važan nedostatak ogleda se u odsustvu jasno propisanog spoljašnjeg nadzora. U odredbi se ne vidi uloga nezavisnog tela, suda ili drugog mehanizma koji bi vršio kontrolu nad

tim ko, kada i pod kojim uslovima pristupa snimljenim razgovorima. U savremenim standardima zaštite prava na privatnost, posebno u kontekstu intervencija u komunikacije, nezavisni nadzor se smatra ključnim elementom zakonitosti i proporcionalnosti mere.

Sve navedeno ukazuje da ova odredba uspostavlja sistem koji omogućava veoma intenzivnu obradu komunikacionih podataka velikog broja lica, bez dovoljno preciznih i snažnih pravnih garancija. Iako se ciljevi kao što su bezbednost komunikacija i kontrola rada službi mogu smatrati legitimnim, način na koji je odredba formulisana ne obezbeđuje dovoljan balans između tih ciljeva i prava pojedinaca.

Posmatrano kroz standard srazmernosti, koji zahteva da svaka mera koja zadire u privatnost mora biti neophodna, pogodna i najmanje restriktivna u odnosu na cilj koji se želi postići, ova odredba ostavlja utisak da je obim prikupljanja i čuvanja podataka širi nego što bi bilo neophodno. Naročito je problematično to što se ne pravi dovoljno jasna razlika između različitih kategorija lica i situacija, već se u istom režimu obrade nalaze i građani koji traže pomoć hitnih službi i zaposleni u bezbednosnim strukturama.

Zbog svega navedenog, može se zaključiti da ova odredba nije u potpunosti adekvatna sa stanovišta zaštite prava na privatnost, jer nedovoljno precizno definiše granice obrade, oslanja se na interna akta umesto na zakonske garancije, ne obezbeđuje dovoljno nezavisan nadzor i omogućava obradu podataka koja može biti nesrazmerna u odnosu na deklarisanu ciljeve.

U vezi sa navedenim komentarima, najpre ističemo da su u članu 3. Nacrta zakona predviđeni različiti skupovi podataka, koji se obrađuju samostalno, u zavisnosti od precizno utvrđene svrhe obrade i kategorije lica na koje se podaci odnose. Navedeni skupovi podataka se u odnosu na različite kategorije lica mogu obrađivati isto tako u različite svrhe. Takođe, ukazujemo da je pružanje pomoći građanima koji, u različitim situacijama traže pomoć hitnih službi, zakonom propisana obaveza, odnosno ovlašćenje policije, te da u tom smislu nije neophodno dodatno ograničenje obrade podataka u ovom Nacrtu zakona, imajući u vidu da su one već kao takve propisane.

Dodatno ukazujemo da se prilikom izrade Nacrta zakona vodilo računa o podacima koje Zakon o zaštiti podataka o ličnosti svrstava u posebnu vrstu podataka o ličnosti, te da je obrada ove vrste podataka propisana zakonom, u skladu sa načelima srazmernosti i neophodnosti, u jasno određene svrhe, u slučajevima kada je to neophodno, radi primene zakonom propisanih ovlašćenja.

Konačno, ističemo da će komentari koji se odnose na preciznije određivanje i skraćivanje rokove čuvanja prihvaćeni u Nacrtu zakona.

U vezi sa komentarom koji se odnosi na nedostatak nezavisnog nadzora, ističemo da je uloga nezavisnog državnog organa koji vrši nadzor nad primenom propisa u oblasti zaštite podataka o ličnosti regulisan Zakonom o zaštiti podataka o ličnosti, te da se ovim nacrtom zakona ne utiče na postojeći mehanizam nezavisnog nadzora. Takođe, ukazujemo da su ovlašćenja policije koja uključuju obradu podataka o ličnosti upotrebom sistema audio i video nadzora detaljnije regulisana zakonom (Zakonom o policiji, Zakonikom o krivičnom postupku i drugim posebnim zakonima), te da nije neophodno preciznije definisanje dodatnih mera zaštite u ovom Nacrtu zakona.

### 3) Komentar na član 29:

Ova odredba nastoji da uredi pitanje sudbine ogromnih količina podataka koje MUP već poseduje u svojim evidencijama, tako što uvodi sistem „pasivizacije“ i brisanja nakon proteka određenih rokova. Na prvi pogled, ona predstavlja korak ka usklađivanju sa savremenim principima zaštite podataka o ličnosti, pre svega sa načelom ograničenog čuvanja podataka.

Međutim, dublja analiza pokazuje da je ovo rešenje nedovoljno precizno, normativno neujednačeno i u više aspekata nedovoljno zaštitno za prava pojedinaca.

Osnovni koncept koji se uvodi jeste pasivizacija podataka, što znači da se podaci nakon određenog vremena više ne koriste u operativne svrhe, već samo u strogo ograničene bezbednosne svrhe, kao što su otkrivanje i rasvetljavanje krivičnih dela. Istovremeno, predviđa se i brisanje podataka kada se proceni da više nisu neophodni. Ovakva struktura na prvi pogled deluje kao trostepeni sistem: aktivno korišćenje, pasivna upotreba i konačno brisanje. Međutim, problem je u tome što kriterijum prelaska iz jedne faze u drugu nisu dovoljno jasno i objektivno definisani.

Prvi i najvažniji nedostatak ogleda se u prekomerno dugim rokovima čuvanja podataka. Rokovi od 20, 25 ili čak 10 godina u savremenom kontekstu zaštite podataka o ličnosti smatraju se izuzetno dugim, posebno kada se radi o podacima koji mogu uključivati osetljive informacije iz oblasti krivičnog gonjenja, bezbednosti saobraćaja, javnih okupljanja ili kretanja lica. Princip proporcionalnosti zahteva da se podaci čuvaju samo onoliko dugo koliko je neophodno za konkretnu i jasno definisanu svrhu. Ovde, međutim, zakon polazi od unapred fiksiranih, veoma dugih rokova, bez individualne procene potrebe za čuvanjem konkretnih podataka. To znači da se unapred pretpostavlja da su svi podaci jedne kategorije jednako dugo relevantni, što u praksi nije tačno.

Drugi značajan problem je neodređenost pojma „pasivizacija“. Zakon ne definiše dovoljno jasno šta se tehnički i pravno dešava sa podacima nakon što postanu pasivizirani. Nije jasno da li se oni fizički odvajaju, anonimizuju, logički izoluju ili samo formalno ograniče u pristupu. U odsustvu precizne definicije, postoji rizik da se u praksi pasivizacija svede na administrativnu oznaku bez stvarnog tehničkog ograničavanja pristupa, što bi značilo da se suštinski ništa ne menja u pogledu mogućnosti korišćenja podataka.

Treći ključni problem odnosi se na širok i nedovoljno kontrolisan pristup pasiviziranim podacima. Iako je formalno propisano da se oni mogu koristiti samo u svrhe krivičnog gonjenja, formulacije kao što su „sprečavanje, otkrivanje i rasvetljavanje krivičnih dela“ su veoma široke i obuhvataju čitav spektar policijskih i bezbednosnih aktivnosti. U nedostatku strogih procesnih garancija, sudske kontrole ili nezavisnog nadzora, ovako široko definisane svrhe mogu u praksi opravdati veoma širok spektar pristupa podacima.

Četvrti problem jeste potpuno neodređen mehanizam procene neophodnosti daljeg čuvanja podataka. Zakon kaže da će se podaci brisati ako se periodičnom procenom utvrdi da više nisu neophodni, ali ne propisuje:

- ko vrši tu procenu,
- u kojim vremenskim intervalima,
- po kojim kriterijumima,
- niti da li postoji obaveza nezavisne kontrole.

To znači da se jedna od najvažnijih garancija prava na zaštitu podataka — pravo na brisanje — faktički prepušta internoj proceni organa koji te podatke i koristi. U takvom sistemu postoji strukturni konflikt interesa: isti organ koji ima interes da zadrži podatke odlučuje o tome da li ti podaci treba da budu izbrisani.

Peti, možda najznačajniji problem, jeste prenošenje ključnih elemenata uređenja na ministra, koji uređuje način brisanja i pasivizacije podataka. Ovo znači da se suštinski važna pitanja zaštite prava građana ne uređuju zakonom u dovoljnoj meri, već se prepuštaju podzakonskom aktu jednog člana izvršne vlasti. U ustavnopravnom smislu, to slabi princip pravne siurnosti i predvidivosti, jer građani iz samog zakona ne mogu sa dovoljnom preciznošću znati kako će se njihovi podaci obrađivati, čuvati i brisati.

Sa stanovišta savremenih standarda zaštite podataka o ličnosti, naročito onih koji proizilaze iz evropskog prava i prakse, ključni zahtevi su:

- jasno definisane svrhe obrade,
- minimizacija podataka,
- ograničeni rokovi čuvanja,
- nezavisna kontrola obrade,
- i efektivno pravo na brisanje.

Ova odredba te principe samo delimično ispunjava. Iako formalno uvodi rokove i predviđa brisanje, ona istovremeno ostavlja previše prostora za interpretaciju, interne odluke i izvršnu diskreciju. Upravo zbog toga se ne može smatrati u potpunosti adekvatnom sa stanovišta zaštite prava na privatnost. Zaključno, glavni nedostatak ove odredbe nije u tome što ne pokušava da uredi životni ciklus podataka, već u tome što taj sistem nije dovoljno precizan, transparentan i institucionalno kontrolisan. Umesto jasnog i strogog pravnog okvira koji bi ograničio obradu podataka, dobija se model u kome ključne garancije zavise od internih procena i podzakonskih akata, što sa stanovišta zaštite prava građana nije dovoljno snažno niti dovoljno pravno sigurno rešenje.

U vezi sa navedenim komentarima, ukazujemo da se prilikom izrade Nacrta zakona vodilo računa o podacima koje Zakon o zaštiti podataka o ličnosti svrstava u posebnu vrstu podataka o ličnosti, te da je obrada ove vrste podataka propisana zakonom, u skladu sa načelima srazmernosti i neophodnosti, u jasno određene svrhe, u slučajevima kada je to neophodno, radi primene zakonom propisanih ovlašćenja.

Konačno, ističemo da su komentari koji se odnose na preciznije određivanje i skraćivanje rokove čuvanja i pasivizaciju prihvaćeni u Nacrtu zakona.

U vezi sa komentarom koji se odnosi na nedostatak nezavisnog nadzora, ističemo da je uloga nezavisnog državnog organa koji vrši nadzor nad primenom propisa u oblasti zaštite podataka o ličnosti regulisan Zakonom o zaštiti podataka o ličnosti, te da se ovim nacrtom zakona ne utiče na postojeći mehanizam nezavisnog nadzora. Takođe, ukazujemo da su ovlašćenja policije koja uključuju obradu podataka o ličnosti upotrebom sistema audio i video nadzora detaljnije regulisana zakonom (Zakonom o policiji, Zakonikom o krivičnom postupku i drugim posebnim zakonima), te da nije neophodno preciznije definisanje dodatnih mera zaštite u ovom Nacrtu zakona.