

Ministarstvo unutrašnjih poslova

Bulevar Mihajla Pupina 2

Beograd

Predmet: Komentari na Nacrt Zakona o obradi podataka o ličnosti u oblasti unutrašnjih poslova

1. Načelni komentar

Partneri Srbija pozdravljaju odluku da se obrada podataka o ličnosti 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.

2. Opšti i poseban režim obrade nisu jasno razgraničeni.

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.

3. Svrhe obrade nisu uvek „konkretne, izričite i opravdane“.

Čl. 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 (čl. 3. tač. 10) u toj istoj svrsi nije dovoljno 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.

4. Načelo tačnosti podataka ne dozvoljava paušalne izuzetke

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 dopušta takav blanket izuzetak.

5. Uslovi za dozvoljenost obrade nisu uvek propisani.

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.

6. Članovi 5, 28 i 29 - uvođenje „pasivizacije podataka“ kao neosnovan vid prekomernog čuvanja podataka

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 članu 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 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 uređuju 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.

7. Suštinska pitanja obrade ne smeju biti prepuštena ministru i internim aktima Ministarstva

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 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 uređuju 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 sam da uredi najmanje osnovne elemente zbirke podataka, krug ovlašćenih korisnika, uslove pristupa, pravila izdvajanja i kopiranja, osnovne elemente evidencija, kriterijume za pasivizaciju i brisanje, kao i minimalne mere zaštite, dok bi ministru mogla biti prepuštena samo njihova tehnička operacionalizacija.

8. Izuzeci od načela transparentnosti moraju biti neophodni i srazmerni u demokratskom društvu

Čl. 19. st. 4. Zakona o obradi podataka predviđa da organ može **ne obavještavati lice o prenosu podataka do 5 godina** - bez sudske kontrole. ZZPL (član 25) dozvoljava odlaganje obaveštenja, samo u onoj meri i u onom trajanju dok je to neophodno i srazmerno u demokratskom društvu u odnosu na poštovanje osnovnih prava i legitimnih interesa fizičkih lica, radi ostvarenja određenih propisanih interesa. Paušalno određen rok od pet godina može dovesti do situacije da se ovakvo obavješćavanje od strane nadležnih 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.¹

9. Član 20 - Razmena podataka sa stranim državama bez provere adekvatnosti zaštite prava u zemlji prijema

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 provere 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. potpisalo je memorandum o saradnji u oblasti IKT sa Iranom -državom sa dokumentovanim i sistemskim kršenjima prava na privatnos,²a 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, dovode 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.

10. Članovi 25 - 27 – rokovi za audio i video nadzor moraju biti određeni kao najduži, a ne kao najkraći

¹ [Serbia: "A Digital Prison": Surveillance and the suppression of civil society in Serbia - Amnesty International](#)

² [MINISTRI RISTIĆ I HAŠEMI POTPISALI MEMORANDUM O SARADNJI U OBLASTI IKT IZMEĐU SRBIJE I IRANA](#)

Posebno problematično rešenje sadržano je u čl. 25. - 27. nacrtu, 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 za ostvarivanje svrhe obrade, a za obradu koju vrše nadležni organi u posebnim svrhama 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.

11. Mere zaštite prava lica u slučaju automatizovane obrade nisu propisane

Nacrt a ne sadrži odredbe o pravu lica da se na njega ne primenjuje 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 odredbu 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.

12. Nacrt ne sadrži poglavlje o pravima lica čiji se podaci obrađuju, niti upućuje sistematski na ZZPL u tom smislu.

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 invanzivnost 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.