INFORMACIJSKI POOBLAŠČENEC
Zaloška 59, 1000 Ljubljana, Slovenija
Telefon: 01 230 97 30
Faks: 01 230 97 78
E-pošta: gp.ip@ip-rs.si
www.ip-rs.si
REPUBLIKA SLOVENIJA

Zadeva: 007-10/2016/2
Datum: 8.3.2016

g. Boštjan Šefic, državni sekretar
Ministrstvo za notranje zadeve
Štefanova ul. 2, 1501 Ljubljana
Gp.Mnz@gov.si

Zadeva: Mnenje IP k predlogu Zakona o spremembah in dopolnitvah Zakona o nalogah in pooblastilih (predlog ZNPPol-A, EVA 2015-1711-0006), v okviru medresorskega usklajevanja
Zveza: vaš dopis št. 007-485/2015/3 (207-01) z dne 17. 2. 2016

Spoštovani,

v skladu s svojimi pristojnostmi po 1. odst. 48. člena Zakona o varstvu osebnih podatkov (Uradni list RS, št. 94/07, uradno prečiščeno besedilo, v nadaljevanju ZVOP-1) v zvezi z 2. členom Zakona o informacijskem pooblaščencu (Uradni list RS, št. 113/05 in 51/07 – ZUstS-A, v nadaljevanju ZInfP) vam posredujemo mnenje Informacijskega pooblaščenca (v nadaljevanju: IP) k prejetemu predlogu sprememb in dopolnitev Zakona o nalogah in pooblastilih policije (po vašem dopisu kot zgoraj; v nadaljevanju: predlog ZNPPol-A).

IP pri tem uvodoma pojasnjuje, da je svoje mnenje do sprememb in dopolnitev ZNPPol podal že lani poleti, tekom priprave ZNPPol-A (007-67/2015/3, z dne 2. 9. 2015, prilagamo, pripravljeno na podlagi zaprosila GPU št. 007-227/2015/3 (207-1), z dne 12. 8. 2015). Pri pripravi tokratnega mnenja v okviru medresorskega usklajevanja se zatorej v znatni meri opiramo na odkazano mnenje, pri čemer ugotavljamo, da tam vsebovani predlogi žal v večini niso bili upoštevani. Zato še posebej izpostavljamo prav tiste člene, ki kljub prehodnemu opozorilu po mnenju IP še niso ustrezno usklajeni, in h katerim moramo zatorej ponovno podati negativno mnenje.

Stališče IP do posameznih členov predloga je, kot sledi:

K 3. členu predloga ZNPPol-A (sprememba 11. člena zakona, kriminalistično-obveščevalna dejavnost)
IP je že dlje časa seznanjen s pobudami znotraj policije, ki potekajo v smer izboljšanja procesov kriminalistično-obveščevalne dejavnosti, še zlasti v zvezi z nabavo potrebne programske opreme, pridobivanja znanja in izkušenj, ter internega izobraževanja. Aktivnosti v zvezi s tem na splošno ocenjujemo kot pozitivne in v skladu s siceršnjimi pooblastili policije.

Vendar pa v zvezi z novopredlaganim 2. odstavkom, ki izrecno dopušča možnost pridobivanja podatkov za analizo »iz vseh javnih virov«, ponovno opozarjamo na stališče IP, da policija **ni upravičena na zalogo in na splošno vršiti nadzora »vseh javnih virov«, še zlasti ne objav na družbenih omrežjih, forumih in podobnih spletnih straneh z uporabniško generirano vsebino.** Zbiranje oz. analiziranje podatkov (podrobneje opredeljeno v 112. oz. 122. členu, ki se oba spreminjata v to smer, kot opozarjamo v nadaljevanju) mora namreč po mnenju IP biti omejeno na postopke v zvezi **s konkretnimi kaznivimi ravnanji oz. osumljenci**. Tudi v primeru preventivnega delovanja policije in opravljanja preventivnih dejavnosti mora biti delovanje policije usmerjeno in ne bi smelo vključevati vsesplošnega nadzora nad vsemi.

Kar zadeva odkrivanje kaznivih dejanj (2. al. 1. odst. 4. člena veljavnega ZNPPol), mora biti začetek dela namreč zmeraj pogojen z obstojem indicev ali razlogov za sum, da se vrši določeno kaznivo dejanje, ki se preganja po uradni dolžnosti (1. odst. 148. člena Zakona o kazenskem postopku, Uradni list RS, št. 32/12 – uradno prečiščeno besedilo, 47/13 in 87/14, v nadaljevanju ZKP). Ti razlogi sicer lahko izhajajo tudi iz lastne, neposredne zaznave policista, celo slučajne (npr. ko ni v službi), vendar po mnenju IP navedenih členov ni mogoče tolmačiti tako široko, da bi smel policist oz. policija kot institucija povsem preventivno zbirati podatke o vseh javno dostopnih komunikacijah, v upanju, da bodo nekateri od njih nakazovali na kazniva ravnanja. Tudi pooblastilo javnega opazovanja (1. al. 6. člena ZNPPol), je, že historično, omejeno na odločitve poveljnikov policijskih postaj, da se organizira opazovanje na bolj rizičnih krajih, tipično tistih, ki so gosto naseljeni, kjer se že beleži večje število kaznivih dejanj ali dejanj zoper javni red in mir, oz. kjer je večje število varnostno pomembnih oseb in objektov. Skratka, javna prisotnost policije naj se zagotovi na znano rizičnih krajih, kot tudi občasno na drugih krajih, da ravnanje policije ne postane preveč predvidljivo. Na ta način je organizirana tudi rutinska kontrola prometa. Ne bi pa šlo za dopustno javno opazovanje, če bi policija, pod predpostavko zadostnih kadrovskih zmogljivosti, organizirala javno opazovanje na vseh javnih krajih, 24 ur/dan, vse dni v letu. Takšen stalno prisoten, neselektiven, sistemski množični nadzor, ki bi bil brez utemeljitve v predhodni oceni tveganja ali obstoju (vsaj) indicev ali razlogov za sum, in ki je značilen za policijske države, bi namreč lahko pomenil nedopusten poseg v pravice do zasebnosti in svobodo izražanja. Navedeno izhaja tudi iz nedavne sodbe Evropskega sodišča za človekove pravice v zadevi Zakharov proti Rusiji[1], sodbe Sodišča EU v zadevi Digital rights Ireland[2], in pripadajoče odločbe Ustavnega sodišča, v kateri je to razveljavilo določbe Zakona o elektronskih komunikacijah o obvezni hrambi prometnih podatkov.

Ob tem opozarjamo tudi na 122. člen ZNPPol, ki določa, da policija ne sme uporabljati avtomatizirane obdelave osebnih ali drugih podatkov (obdelava osebnih ali drugih podatkov s sredstvi informacijske tehnologije), s katero bi bila lahko o fizični osebi, pravni osebi ali o drugem subjektu sprejeta odločitev, vložena predlog ali kazenska ovadba ali izdelano poročilo, ki bi brez dodatnega delovanja in odločitve pristojnega uslužbenca policije lahko posegali v pravice ali obveznosti fizične osebe, pravne osebe ali drugega subjekta. Z avtomatizirano obdelavo osebnih ali drugih podatkov, zlasti z združevanjem oziroma primerjanjem osebnih podatkov iz ene ali več zbirk osebnih podatkov, evidenc, javnih knjig, registrov ali drugih zbirk osebnih podatkov, policija ne sme izdelati osebnostnih profilov oseb, na katere se nanašajo osebni podatki, tako da bi se brez dodatnega delovanja in odločitve pristojnega uslužbenca policije lahko sklepalo, da so storili ali da niso storili določenega kaznivega ravnanja ali da so izpovedi določenih oseb zanesljive ali nezanesljive. Prepovedana je avtomatizirana obdelava občutljivih osebnih podatkov za izdelavo osebnostnega profila osebe.

Zbiranje podatkov ne more in ne sme obsegati zbiranja podatkov na zalogo, vsesplošnega nadzora nad vsemi, ali ustvarjati vtisa oz. možnosti takšnega nadzora. Takšno postopanje policije bi namreč, glede na zadnjo prakso Evropskega sodišča za človekove pravice (primera Zakharov proti Rusiji, in še zlasti Szabó in Vissy proti Madžarski[3], lahko pri prebivalcih ustvarjalo občutek stalno prisotnega nadzora, ter s tem nedopustno posegalo v njihove pravice do zasebnosti, varstva osebnih podatkov, varstva človekovega dostojanstva, in tako dalje.

[1] http://hudoc.echr.coe.int/eng#{"itemid":["001-159324"]}

[2] http://curia.europa.eu/juris/document/document.jsf?text=&docid=150642&pageIndex=0&doclang=sl&mode=lst&dir=&occ=first&part=1&cid=1004297

[3] http://hudoc.echr.coe.int/eng#%7B%22itemid%22:%5B%22001-160020%22%5D%7D

K 10. členu predloga ZNPPol-A (sprememba 34. člena zakona, zbiranje obvestil)
Predlog predvideva črtanje policistove izrecne obveznosti iz 2. odst., da vsako osebo, od katere zbira obvestila, predhodno izrecno opozori, da je dajanje obvestil prostovoljno oz. da ima (razen v določenih primerih) pravico do anonimnosti pri podaji obvestil. IP takšni spremembi nasprotuje in opozarja, da **je ni mogoče tolmačiti v smer, da je po novem podaja pojasnil za osebo obvezna, oz. da bi policisti smeli zadevni osebi dajati takšni vtis.** Namen spremembe naj bi namreč bil zgolj v tem, tako obrazložitev, da se policista razbremeni podajanja takšnega obvestila v nekaterih izjemnih situacijah, kjer to resnično ni smiselno. Če je to namen predlagane spremembe, potem mora biti zakonska dikcija takšna, da je ta namen dosežen, da pa niso možne širše interpretacije.

Obvestilo o prostovoljnem podajanju informacij je zelo pomembno za zagotovitev načela prostovoljnosti in anonimnosti, zato morajo biti izjeme, ko takega obvestila ni potrebno predhodno podati, podane dovolj ozko. IP pri tem ponovno opozarja na problematično prakso pri pridobivanju podatkov o uporabnikih različnih spletnih storitev, kjer je policija v številnih primerih svoja pisna oz. ustna zaprosila **formulirala tako, da je bila zaprošena oseba prepričana, da zaprošene podatke, vključno s prometnimi podatki, mora posredovati.** Kot smo že večkrat poudarili v svojih poročilih oz. na medsebojnih sestankih, takšna praksa ne sme biti dopustna. Obveznost posredovanja podatkov obstoji zgolj v primerih, ko to določa 115. člen ZNPPol ali drug zakon. V teh primerih mora biti dopis tudi ustrezno označen kot obvezen (kot zahtevek, ne zaprosilo), in mora opozoriti na posledice neposredovanja. V ostalih primerih pa mora iz dopisa jasno izhajati, da gre za zbiranje obvestil, ter da je odgovor na dopis prostovoljno ravnanje. To naj še posebej drži, ker se v predlogu novega 3. odst. izrecno širi možnost zbiranja obvestil tudi na s.p.-je in pravne osebe.

IP zatorej predlaga, da se **2. odstavek dopolni z dostavkom, ki bi izključil to obveznost zgolj v posebej potrebnih primerih**, ki jih tudi sami navajate v obrazložitvi, npr. »ko že iz samega ravnanja osebe izhaja, da želi prostovoljno dati izjavo«.

K 15. členu predloga ZNPPol-A (sprememba 42. člena, identifikacijski postopek)
IP načeloma pozdravlja natančnejšo opredelitev postopkov oz. sredstev, ki jih policisti smejo uporabljati pri identifikacijskem postopku, v skladu s predlaganim novim 2. odst. 42. člena pa tudi za identifikacijo trupla, ugotovitev identitete ali izsleditev iskane osebe ter za ugotovitev identitete žrtve kaznivih ravnanj.

Vendar pa daje **negativno mnenje** k takšnemu nediskriminatornemu naštevanju vseh tehničnih sredstev, ki so v policiji trenutno na voljo. Nekatera od njih, npr. raba termovizijskih kamer, ali sistemov za avtomatsko primerjavo prstnih odtisov, izdelave profilov ali haplotipov DNK, ali sredstev za optično prepoznavo registrskih tablic, imajo namreč lahko široke vplive na zasebnost posameznikov, ki jih policija tekom iskanja obravnava. Za določene od njih je lahko potrebna tudi predhodna odredba sodišča (npr. za vpogled v zasebno stanovanje s termovizijsko kamero, kar glede na tujo prakso šteje kot hišna preiskava), oz. morajo biti izpolnjeni določeni pogoji (oddaja prstnih odtisov brisa ustne sluznice je obvezna samo v določenih primerih). Tako širokega predloga posledično nikakor ni mogoče sprejeti brez vnaprej opravljene študije vplivov na zasebnost (PIA presoje), ki pa glede tega pooblastila ni bili opravljena. Prav tako predlagani odstavek še vedno ohranja ekspemplifikativno obliko, skratka, našteta sredstva našteva zgolj primeroma, ter še vedno izrecno omogoča uporabo tudi »drugih operativnih in kriminalistično-tehničnih opravil« za namen izvedbe identifikacijskega postopka.

Glede hrambe in brisanja tako zbranih podatkov ocenjujemo, da določba iz 1. odst. 113. člena ni zadostna, ker je ta omejena na rabo »tehničnih sredstev za fotografiranje ter video in avdio snemanje ter tehničnih sredstev za označevanje ali identifikacijo oseb, vozil in predmetov«, kar ne zajema vseh tukaj predlaganih sredstev.

K 43. členu predloga (sprememba 112. člena, zbiranje podatkov)
IP daje **negativno mnenje** k predlagani dopolnitvi 1. odst. 112. člena v smislu, da bi policisti lahko na splošno, »zaradi opravljanja policijskih nalog«, zbirali tudi podatke o »biometičnih značilnostih oseb«. Upoštevaje utemeljitev predloga (zagotovitev skladnosti z 79. členom ZVOP-1, biometrijski ukrepi v javnem sektorju), IP meni, da gre pri tem verjetno za napačno razumevanje pogojev iz omenjenega 79. člena ZVOP-1, saj slednji določa, da se uporabo biometrijskih ukrepov v javnem sektorju lahko »določi le z zakonom, če je to nujno potrebno za varnost ljudi ali premoženja ali za varovanje tajnih podatkov ter poslovne skrivnosti, tega namena pa ni možno doseči z milejšimi sredstvi«. Navedeno določbo je tako treba tolmačiti tako, da je raba biometrijskih ukrepov dopustna **v določenih specifičnih primerih**, kot jih že določajo druge določbe ZNPPol (ugotavljanje identitete, identifikacijski postopek, prepoznava na podlagi fotografije) ali drugi zakoni (npr. kriminalistično-tehnična obdelava ob odvzemu prostosti po ZKP). Posledično uporaba takšnih ukrepov ne more biti dopustna »kar na splošno« pri izvajanju nalog policije.

Kot že obrazloženo pri komentarju k 3. členu predloga, daje IP **negativno mnenje** tudi k predlagani dopolnitvi 2. odst. 112. člena, ki naj bi policiji zavoljo »opravljanja njenih nalog« (kot izhaja iz 1. odst. istega člena) dovoljeval nediskriminatorno zbiranje podatkov »iz javnih virov«.

K 44. členu predloga (nov 112.a člen, zbiranje podatkov o potnikih)
IP v zvezi s projektom zbiranja API in PNR podatkov o letalskih potnikih, njihovi hrambi, ter njihovi analizi v okviru namenske enote kriminalistične policije, uvodoma pozdravlja trud, ki je bil vložen v pripravo kakovostne presoje vplivov na zasebnost (PIA). PIA analiza v zvezi s tako predlaganim novim policijskim pooblastilom po mnenju IP predstavlja zgled dobre prakse.

Upoštevaje navedeno, pa IP še vedno dodaja določene pridržke, kot jih je že podal v preteklosti:

1) dopustnost vključitve podatkov za notranje lete (v RS iz drugih držav članic EU, oz. obratno) za namen izvajanja mejne kontrole na notranji meji, oz. za namen obdelave podatkov v okviru izravnalnih ukrepov. IP zatorej predlaga, da se zbiranje podatkov (1. odst. 112.a člena) v tej fazi **omeji zgolj na pridobivanje podatkov o zunanjih letih**, notranje pa vključi šele po sprejemu takšne določbe v PNR direktivi, oz. po opravljenem tehtanju te direktive pred Sodiščem EU.
2) dopustnost širjenja namenov uporabe API podatkov onkraj meja tistih, določenih v določbah Zakona o letalstvu (ki dopušča njihovo pridobivanje za potrebe nadzora meje, se pravi, naloge, ki so opredeljene v Zakonu o nadzoru državne meje). IP predlaga, da se namen spremeni na tistega, ki že velja v Zakonu o letalstvu (mejna kontrola);
3) dopustnost tako širokega določanja namenov uporabe PNR (booking) podatkov, kot to navaja 3. odst. 112.a člena. **IP zlasti opozarja zoper možnost avtomatizirane tiralične kontrole vseh potnikov na podlagi PNR podatkov**. Namen analize PNR podatkov, kot je predstavljen v PIA analizi, naj bi bil skozi kriminalistično obveščevalno dejavnost (analizo, ocenjevalne kriterije) najti osebe, ki jih mejna kontrola sicer, na podlagi svojih pooblastil, morda ne bi. Zatorej naj se tiralično preverjanje izvaja zgolj za te, na podlagi ocenjevalnih kriterijev sumljive osebe, ne pa kar za vse osebe.
4) Rok hrambe podatkov v neblokirani obliki naj se skrajša na čas, ki je potreben za izvedbo ocene tveganja, kar naj bo največ 1 mesec od datuma prejema podatkov.

K 45 členu predloga (dopolnitev 3. odst. 113. člena, uporaba tehničnih sredstev pri zbiranju podatkov pri nadzoru cestnega prometa)

Nov tretji odstavek dodaja možnost uporabe sistemov za optično prepoznavo registrskih tablic pri nadzoru cestnega prometa, konkretno z namenom ugotavljanja pogojev za udeležbo voznika oz. vozila v cestnem prometu oz. z namenom iskanja oseb in predmetov. Pripadajoča obrazložitev, oz. priložena analiza vplivov na zasebnost utemeljujeta, da bo novo tehnično sredstvo uporabljeno zlasti na avtocestah, kjer zaradi režima prometa klasično ustavljanje vozil v okviru rutinske kontrole prometa ni mogoče.

IP opozarja, da gre pri sistemih avtomatske prepoznave tablic za zelo visoka tveganja glede posega v človekove pravice, zato je nujna predhodna izvedba celovite prosoje vplivov na zasebnost. To zahteva tudi predlog bodoče Splošne uredbe o varstvu osebnih podatkov (ang. *General Data Protection Regulation*), ki v členu 33 za primere, kjer gre za potencialno množičen nadzor javnih površin, zahteva izvedbo tovrstnih presoj. IP zato k utemeljitvi ukrepa, oz. glede priložene presoje vplivov na zasebnost ponovno opozarja, da je analiza pomanjkljiva, saj se analiza **ne opredeljuje do tveganja množične obdelave osebnih podatkov voznikov in vseh ostalih tveganj glede posegov v temeljne človekove pravice.** Identifikacija tveganj je bistvenega pomena – tveganja, ki jih predlagatelj ob pripravi predloga predpisa morebiti ne bi identificiral, utegnejo kasneje izpostaviti splošna in strokovna javnost. Rezultat nepravočasno ali nepopolno identificiranih in naslovljenih tveganj je lahko oster odpor strokovne in splošne javnosti – in to kljub temu, da bi bil ob ustrezni analizi tveganj ukrep sicer povsem sprejemljiv. V interesu predlagatelja je zato, da vsa tveganja pravočasno identificira in obravnava. Nasprotno, analiza izhaja iz stališča, da gre zgolj za »avtomatiziran vpogled [preverjanje registrskih tablic] v določene (in ne vse) policijske evidence, do katerih smejo policisti že zdaj dostopati zaradi opravljanja policijskih nalog«. Poglavje št. 2 z naslovom Analiza tveganj tako v pretežnem delu opisuje prednosti, ki naj bi jih prinesel opisani sistem, ne opravi pa dejanske vsebinske analize tveganj za nesorazmerne posege v temeljne človekove pravice (primerjaj s podobnim poglavjem v kakovostni presoji vplivov, ki je bila opravljana v primeru PNR, poglavje 3.2). Edino identificirano tveganje, kot izhaja iz analize, je, če bi sistem hranil podatke o vseh vozilih, ki bi jih zaznal, dostop do teh podatkov pa ne bi bil natančno urejen. IP že ob hitri presoji ugotavlja še vsaj naslednja tveganja, ki bi morala biti identificirana in obravnavana v presoji vplivov na zasebnost:

TVEGANJA POVEZANA Z ZBIRANJEM PODATKOV

- Kakšno je tveganje, da bo pooblastilo sčasoma uporabljeno nesorazmerno – t.j., da bodo sčasoma postavljeni sistemi za prepoznavo registrskih tablic na toliko mestih, da bo praktično vsako vozilo avtomatsko pregledano? Koliko vozil bo avtomatsko obdelanih in njihovi podatki shranjeni do 30 dni, če bo v uporabi npr. 5 takšnih enot? Ali sploh oziroma kakšne varovalke so predvidene, da se to tveganje obvlada?

- Kakšna so tveganja, da predvidena pooblastila oz. tehnična sredstva niso primerna za dosego cilja? Obstajajo številne metode, s katerimi je mogoče pretentati ANPR sisteme[4] – npr. z različnimi spreji, premazi, ponarejenimi lažnimi tablicami - kakšna tveganja to prinaša?

- Kakšen je obseg in intenzivnost posega v pravice tretjih oseb, kolateralne škode?

- Na kakšen način se bo lahko naknadno izmerila in izkazala učinkovitost novih pooblastil oziroma tehničnih sredstev - s katerimi kazalniki se bo merila učinkovitost novih pooblastil oziroma tehničnih sredstev?

TVEGANJA POVEZANA Z UPORABO PODATKOV

- Kakšne so možnosti uporabe podatkov za druge namene (zlasti za pregon drugih kaznivih dejanj), ter kako zagotoviti, da bodo spoštovane zahteve ZKP v zvezi s tem? Posnetki vozil, s katerimi niso

[4] Glej npr.: https://en.wikipedia.org/wiki/Automatic_number_plate_recognition#Circumvention_techniques

bili storjeni prekrški, in **podatki o osebah in vozilih, ki ne bodo uporabljani za izvedbo policijskih nalog, se bodo lahko hranili do 30 dni glede na predlagane določbe**. S katerimi varovalkami se bo preprečilo, da se teh podatkov, ki jih bo zaradi avtomatske obdelave **bistveno več** kot pri ročnem preverjanju, ne bo uporabilo v druge namene? Kako bodo zavarovani?

DRUGA TVEGANJA

- Katera druga, specifična tveganja obstajajo? Pri vsaki opremi, ki temelji na prepoznavi znakov, obstajajo določene ravni točnosti, ki se lahko odražajo v napačnih zadetkih, bodisi tipa »false positive« (registrska tablica je napačno prepoznana kot iskana) bodisi tipa »false negative« (registrska tablica, ki je iskana, ni prepoznana s strani sistema), ki imajo lahko resne posledice za posameznika oziroma za uspešnost policijskih postopkov. V analizi tveganj bi morali ugotoviti, o kakšnih stopnjah in verjetnostih govorimo, ali so te stopnje sprejemljive ter kako obvladati omenjena tveganja.

Prav tako v presoji vplivov **manjka primerjalno pravna analiza tveganj** – navedena je zgolj preglednica, z državami, ki tovrstne sisteme uporabljajo (8). **Iz katerih razlogov sistema ne uporablja preostalih 21 držav članic[5]?** Kakšne so (pozitivne in negativne) izkušnje tistih, ki sistem uporabljajo? Ali so bila pri uporabi identificirana tveganja, zlorabe? Tovrstna vprašanja bi morala biti analizirana v primerjalno pravni analizi tveganj.

IP opozarja, da zdajšnje preverjanje registrskih številk temelji na odločitvi policista (bodisi pri stoječi bodisi vozeči kontroli), da bo preveril določeno vozilo, medtem ko bo predlagana ureditev vključevala preverjanje vseh vozil, katerih registrsko tablico bo zaznala oprema. To pomeni, da bo kontroliranih **bistveno večje število vozil, vključno seveda z bistveno večjim številom nedolžnih voznikov**, kar je vidik, do katerega se je v analizi potrebno opredeliti. Analiza mora namreč utemeljiti prehod z »občasnega«, na sumu policista ali na metodologiji vzorčenja utemeljenega preverjanja, na nediskriminatorno preverjanje vseh vozil na določenem odseku avtoceste. Navedeno se bo morda po tehtanju izkazalo za sorazmeren poseg v zasebnost, vendar pa je to tehtanje treba opraviti.

Dalje IP **nasprotuje zadnji alineji** (prvega dela) novega 3. odstavka, ki dovoljuje tudi rabo »drugih tehničnih sredstev za ugotavljanje drugih prekrškov«. Tako nedoločna opredelitev ob dejstvu, da predlog spremembe jasno zasleduje okrepitev načela zakonitosti (1. stran predloga), ne more biti sprejemljiva.

IP glede na vse navedeno meni, da analiza tveganja in s tem presoja vplivov nista bili opravljeni v zadostnem obsegu, saj obstajajo številna nenaslovljena tveganja. Dokler to ne bo opravljeno **in brez dodatnih varovalk IP ne more podpreti podanega predloga glede uvedbe avtomatiziraniega preverjanja registrskih tablic.**

[5] Glej npr.:

- The police get the tools they want, Britain loses the liberties it holds dear, dostopno na: http://www.theguardian.com/commentisfree/2014/jan/24/police-tools-liberties-britain-crime-rates
- Boston Police indefinitely suspends license plate reader program: dostopno na: http://arstechnica.com/tech-policy/2013/12/boston-police-indefinitely-suspends-license-plate-reader-program/
- Your car, tracked: the rapid rise of license plate readers, dostopno na: http://arstechnica.com/tech-policy/2012/09/your-car-tracked-the-rapid-rise-of-license-plate-readers/
- UK: Vehicle plate recognition video system ruled illegal: https://edri.org/edrigramnumber11-15uk-vehicle-recognition-system-ruled-illegal/

K 46. členu (nov 5. odstavek 114. člena, uporaba tehničnih sredstev pri izvajanju policijskih pooblastil in spremljanju javnih zbiranj)
Novi peti odstavek dodaja dodatne možnosti uporabe tehničnih sredstev za namene iz tega člena (spremljanje zakonitosti izvajanja pooblastil, spremljanje javnih zbiranj) kot tudi prejšnjega člena (nadzor cestnega prometa), in sicer tako, da določa, da se smejo uporabljati »neposredno ali iz vozila, plovila, **zrakoplova (tudi daljinsko ali avtonomno vodenega)**, zgradb ali drugih objektov«. Kot dalje izhaja iz obrazložitve člena, policija s tem uzakonja zlasti rabo **brezpilotnikov (dronov)**, pri čemer si predstavlja, da bo nanje lahko namestila »zelo različne« senzorske sisteme, najpogosteje pa »sredstva za fotografiranje, video snemanje, naprave za nočno opazovanje, toplotne kamere, …«.

Kot je IP že poudaril ob več priložnostih, oz. kot navajamo v svojem Poročilu o brezpilotnih letalnikih, http://www.ip-rs.si/fileadmin/user_upload/Pdf/porocila/Brezpilotni_letalniki_-_porocilo_IP.pdf, brezpilotniki kot taki zavoljo svojih dobrih letalskih zmogljivosti, cenenosti, prikritosti, oz. splošne fleksibilnosti prinašajo bistveno novo razsežnost izvajanja nadzora nad posamezniki in skupinami, zavoljo česar nadzora z brezpilotnikom ni mogoče neposredno enačiti z nadzorom z isto vrsto senzorne naprave, ki jo izvede policija bodisi s tal, bodisi s helikopterja. **Posledično IP vztraja, da se pred uzakonitvijo njihove rabe skupaj s posamičnimi senzornimi sredstvi izdela temeljita analiza vplivov na zasebnost**. K splošni uzakonitvi rabe brezpilotnikov s poljubnimi senzornimi sistemi, kot je predlagano, pa lahko IP poda le **negativno mnenje**.

Še dalje daje IP **negativno mnenje** k novemu 7. odstavku, ki bi omogočal rabo tehničnih sredstev »v lasti drugih državnih organov in pravnih oseb«, v kolikor so po tehničnih lastnostih primerljivi s tipiziranimi sredstvi v lasti policije. Izposoja tujih sredstev, še zlasti pa javno-zasebno partnerstvo v tem smislu, odpira možnost bistveno širše rabe sredstev, in s tem njihovo morebitno neutemeljeno rabo za množični nadzor. Še zlasti v primeru javno-zasebnih partnerstev za potrebe prekrškovnega nadzora, s klavzulo o delitvi plačane kazni, je to lahko posebej problematično. Kot potencialno vprašljiva primera izpostavljamo poskus financiranja hitrostnih radarjev v Mariboru, ter primer iz ZDA, kjer je zasebno podjetje policijska vozila brezplačno opremilo s senzorji za optično prepoznavo registrskih tablic za potrebe izvršbe že zapadlih kazni, pri čemer si je pridržalo znatni delež izterjanih kazni, kot tudi zagotovilo dostop do kopije vseh obdelanih registrskih tablic za uporabo v morebitne druge namene (glej https://www.techdirt.com/articles/20160126/12092833435/cops-getting-free-license-plate-readers-exchange-25-take-all-driver-data-vigilant-can-slurp.shtml). Podobni so primeri uporabe opreme za zaznavanje vožnje v rdečo luč, kjer so zaradi pritiskov zasebnega partnerja po dobičku, skrajšali obdobje trajanja rumene luči, da bi se tako povečalo število prekrškov in s tem zaslužka zasebnega partnerja. Takšni primeri kažejo, da je rabo sposojenih, še zlasti zasebnih sredstev potrebno zelo skrbno ovrednotiti s stališča njihovega vpliva na zasebnost, kar v danem primeru ni bilo opravljeno.

K 51. členu predloga (sprememba 122. člena, avtomatizirana obdelava osebnih in drugih podatkov)
Navedeni člen vrinja nov prvi odstavek, ki **na splošno dopušča avtomatizirano obdelavo vseh zbranih osebnih in drugih podatkov**, vključno z biometričnimi podatki in zbranimi podatki iz javnih virov (43. člen predloga), kot tudi podatkov o letalskih potnikih (44. člen predloga, kot zgoraj). S tem **v celoti spreminja obstoječi pomen člena,** ki je do sedaj vseboval zgolj dve prepovedi avtomatizirane obdelave podatkov, in sicer tako, da je prepovedoval avtomatizirano pripravo kazenskih ovadb oz. izdelavo osebnostnih profilov o določenih osebah, brez da bi odločitev za to na podlagi individualiziranih kriterijev opravil pristojni uslužbenec policije. Obrazložitev tako korenite spremembe je kratka, in sicer naj bi avtomatizirana obdelava »v današnjem času [predstavljala] temelj poslovnih procesov«, z namenom »da isto delo opravimo v krajšem času in z manjšimi človeškimi resursi in nižjimi stroški«.

IP k določitvi tako široke možnosti avtomatizirane obdelave osebnih podatkov, brez vsakršnih omejitev (namenov, izključitve občutljivih osebnih podatkov, idr.) in brez ustrezne obrazložitve, **ne more dati pozitivnega mnenja.**

K 52. členu (dopolnitev 123. člena, evidence policije)
IP daje **pozitivno mnenje** k predlogu uvedbe evidence oseb za izločitev, t.j. evidence DNK profilov policijskih delavcev, ki sodelujejo pri odvzemu oz. analizi vzorcev DNK, da se v primeru kontaminacije njihov profil ne bi vpisal v evidenco DNK preiskav, oz. poslal tujim državam na podlagi ustreznih mednarodnih sporazumov.

IP daje **pozitivno mnenje** k predlogu uvedbe evidence gradiv spolnega izkoriščanja oseb, upoštevaje, da obveznost uvedbe takšne evidence izvira iz prevzetih obveznosti RS po Direktivi 20011/92/EP o boju proti spolni zlorabi in spolnemu izkoriščanju otrok ter otroški pornografiji, in da so dobro opredeljene metode hrambe in uporabe tako zbranih podatkov, kot so določene v sledečih členih.

IP daje **pozitivno mnenje** k predlogoma uvedbe evidence oseb, prijavljenih na let (API podatki) oz. evidence oseb iz sistema rezervacij letalskih kart (PNR podatki), **upoštevaje zgoraj navedene pridržke** iz mnenja k 44. členu predloga.

K 53. členu predloga (sprememba 125. člena, vsebina evidenc)
IP daje **pozitivno mnenje** k predlaganim redakcijskim in terminološkim popravkom vsebine posameznih evidenc. Prav tako daje pozitivno mnenje k dodanim elementom v evidencah prekrškov (odnos med storilcem in oškodovancem, zavoljo priprave podrobnejših statistik nasilja v zakonski, zunajzakonski oz. partnerski zvezi, oz. v družini) oz. dogodkov (fotografije, avdio in videoposnetki), ter k vsebinam novopredlaganih evidenc (evidenca prikritih in namenskih kontrol, evidenca oseb za izločitev, evidenca gradiv spolnega izkoriščanja mladoletnih oseb, obe evidenci letalskih potnikov).

V zvezi z dodajanjem možnosti hrambe haplotipa DNK IP najprej **prosi za posodobljen seznam bioloških preiskav, v katerih naj bi se ugotavljalo haplotip DNK, saj lahko šele na tej podlagi presodimo, za kakšne vrste posege v zasebnost gre.** Tekoči seznam na spletni strani Oddelka za biološke preiskave pri NFL je iz l. 2010 (http://www.policija.si/images/stories/GPUNFL/PDF/BIOseznam.pdf), zadnje letno poročilo policije pa v relevantnem segmentu navaja, da je NFL v zadnjih letih dodal nekatere nove vrste preiskav.

K 54. členu predloga (sprememba 126. člena, posebna pravila za vpisovanje podatkov v evidence)
IP predlaga, da se v navedeni člen doda, da se tudi v primerih odvzema prstnih odtisov oz. odvzema brisa ustne sluznice za potrebe identifikacije osebe oz. za potrebe iskanja osebe tako zajetih podatkov ne vpisuje v pripadajočo evidenco. V danih primerih namreč potreba po zajetih podatkih preneha takoj po tem, ko se osebo najde, oz. ko se potrdi njeno identiteto. Dalje pogoje in razloge za vpis določajo specialni predpisi (ZKP, predpisi o tujcih, prosilcih za azil, idr.), ki vpisa v primeru identifikacijskega postopka ali iskanja osebe ne predvidevajo.

K 56 členu predloga (sprememba 128. člena, roki hrambe podatkov)
IP na splošno daje pozitivno mnenje k predlogu spremenjene druge alineje, ki določa še dodatne kriterije za hitrejši izbris podatkov iz tekočih (aktivnih) evidenc DNK profilov oz. haplotipov, fotografiranih oz. daktiloskopiranih oseb (evidence po 8., 14. in 15. točki). Kot je tudi navedeno v obrazložitvi predloga, se čas

hrambe podatkov v aktivnem delu navedenih evidenc še podrobneje usklajuje z izrekom predmetne odločbe Ustavnega sodišča št. U-I-312/11 (http://odlocitve.us-rs.si/sl/odlocitev/US30334). **Pri tem IP prosi za pojasnilo glede primerov, ko je mogoč vpis v navedene evidence v postopku s prekrški,** saj ni jasno, ali obstaja možnost zajema teh podatkov v prekrškovnih postopkih.

Vendar pa IP daje negativno mnenje k novemu 2. odstavku, ki predvideva ohranitev hrambe podatkov v navedenih evidencah vse do zastaranja kazenskega pregona tudi v primerih, ko bi bil kazenski postopek zoper osebo pravnomočno zaključen njej v prid, v kolikor bi šlo za težje kaznivo dejanje ali če bi bilo mogoče iz (zelo široko definiranih okoliščin) sklepati na ponovitveno nevarnost. Kot je namreč jasno poudarilo Ustavno sodišče v zadevi U-I-312/11, nadaljnja hramba podatkov za (oproščenega) posameznika ni nujna za dosego zakonodajalčevega cilja. Podobno je Evropsko sodišče za človekove pravice v zadevi S in Marper proti Združenemu Kraljestvu[6] odločilo, da predstavlja takšna nadaljnja hramba kršitev njihovih pravic po Evropski konvenciji o človekovih pravicah. Tako široka izjema od predhodnega brisanja pa bi povsem izvotlila možnost, da se podatki nedolžnih posameznikov v doglednem času pobrišejo iz evidence, v kateri naj bi se primerno hranile obsojene oz. vsaj še osumljene osebe.

K 56. členu predloga (sprememba 129. člena, blokiranje podatkov)
IP ponovno daje negativno mnenje k vsebini tega člena, kolikor omogoča, da se podatki iz evidenc fotografiranih oz. daktiloskopiranih oseb oz. evidenci DNK profilov in haplotipov, o osebah, zoper katere je bil kazenski postopek pravnomočno končan njim v prid, še naprej hranijo »v blokirani obliki«, kar pomeni, da so še vedno dosegljivi za potrebe preiskave vseh kaznivih dejanj, ki se preganjajo po uradni dolžnosti. IP predlaga, da se ti podatki po prenehanju roka za hrambo v aktivni evidenci neposredno izbrišejo, ker gre vendarle za nedolžne osebe. Takšna razlaga je, kot je izpostavljeno že zgoraj, edina možna glede na sodbi Ustavnega sodišča RS oz. Evropskega sodišča za človekove pravice v zgoraj navedenih primerih.

S spoštovanjem,

Mojca Prelesnik, univ.dipl.prav.,
Informacijska pooblaščenka

6 https://www.coe.int/t/dghl/standardsetting/dataprotection/Judgments/S.%20AND%20MARPER%20v.%20THE%20UNITED%20KINGDOM%20EN.pdf