REPUBLIKA SLOVENIJA
ZAGOVORNIK NAČELA ENAKOSTI

REPUBLIKA SLOVENIJA
ZAGOVORNIK NAČELA ENAKOSTI

Podpisnik:Miha Lobnik
Izdajatelj certifikata:Republika Slovenija
Serijska št. certifikata:6d 0f 14 5e 00 00 00 00
Datum poteka certifikata:16.01.2022
Datum in čas podpisa:14:22, 19.06.2020
Referenčna številka:0701-6/2020/3

Železna cesta 16, 1000 Ljubljana
01 4735 550
gp@zagovornik-rs.si

Ministrstvo za pravosodje
Župančičeva ulica 3
1000 Ljubljana

E: gp.mp@gov.si

Številka: 0701-6/2020/3
Datum: 19. 6. 2020

Zadeva: **Priporočila Zagovornika načela enakosti v zvezi s predlogom Zakona o varstvu osebnih podatkov na področju obravnavanja kaznivih dejanj**

Spoštovani,

na spletnem portalu e-Uprava je bil 9. 6. 2020 javno objavljen predlog Zakona o varstvu osebnih podatkov na področju obravnavanja kaznivih dejanj (ZVOPPOKD), EVA: 2020-2030-0006, s katerim se v slovenski pravni red prenaša Direktiva EU 2016/680.[1] Zagovornik načela enakosti (v nadaljevanju: Zagovornik) je v zvezi s predmetno materijo predlagatelju že podal nekatera priporočila v fazi, ko je bila ta še vključena v celovit predlog novega Zakona o varstvu osebnih podatkov (ZVOP-2).[2] Iz predloga ZVOPPOKD izhaja, da se je vsebina določb, relevantnih z vidika varstva pred diskriminacijo, glede na zadnji predlog ZVOP-2 spremenila. V tem oziru Zagovornik opozarja tudi, da sedemdnevni rok za javno razpravo, kot je bil določen na spletnem portalu e-Uprava, ni v skladu z Resolucijo o normativni dejavnosti,[3] ki za javno razpravo o predlogih zakonov predpisuje 30 do 60 dnevni rok.

Zagovornik se v tem priporočilu, tako kot v primeru zadnjega predloga ZVOP-2, osredotoča na vprašanje **varstva pred diskriminacijo v kontekstu avtomatiziranega odločanja in avtomatizirane obdelave osebnih podatkov** ter na vprašanje pravne podlage za **zbiranje podatkov o t.i. zločinih iz sovraštva**.

*

Zagovornik pozdravlja, da je v 2. členu predloga ZVOPPOKD na sistemski ravni določena prepoved obdelave osebnih podatkov na podlagi nedopustne diskriminacije zaradi različnih osebnih okoliščin, pri čemer definicija osebnih okoliščin ostaja odprta (»ali katerokoli drugo osebno okoliščino«). Varstvo pred diskriminacijo je še posebej pomembno v kontekstu **avtomatiziranega odločanja in avtomatizirane obdelave podatkov**. Uporaba tehnologij umetne inteligence lahko privede tako do diskriminatorne obdelave osebnih podatkov kot tudi do diskriminatornih rezultatov obdelave osebnih podatkov. Na to opozarja tudi Bela knjiga Evropske komisije (EK) o umetni inteligenci, ki kot ključni izziv uporabe umetne inteligence na področju človekovih pravic poleg varstva osebnih podatkov izpostavlja prav potencialne kršitve prepovedi diskriminacije.[4] Na nevarnost diskriminacije pri uporabi umetne inteligence na področju policijsko-pravosodno-varnostnega delovanja opozarjajo tudi druge mednarodne vladne in nevladne organizacije.[5]

---

[1] Direktiva (EU) 2016/680 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov, ki jih pristojni organi obdelujejo za namene preprečevanja, preiskovanja, odkrivanja ali pregona kaznivih dejanj ali izvrševanja kazenskih sankcij, in o prostem pretoku takih podatkov ter o razveljavitvi Okvirnega sklepa Sveta 2008/977/PNZ
[2] Dopis Zagovornika Ministrstvu za pravosodje št. 0070-1/2019/3 z dne 9. 9. 2019 o predlogu ZVOP-2 z dne 14. 8. 2019.
[3] Uradni list RS, št. 95/09, b) točka drugega odstavka 2. poglavja
[4] Evropska komisija, *Bela knjiga o umetni inteligenci - evropski pristop k odličnosti in zaupanju*, COM (2020) 65 final, dostopno na: https://op.europa.eu/en/publication-detail/-/publication/aace9398-594d-11ea-8b81-01aa75ed71a1/language-sl/format-PDF
[5] Glej npr. F. Zuiderveen Borgesius / Svet Evrope (2019) Discrimination, artificial intelligence, and algorithmic decision-making, dostopno na: https://rm.coe.int/discrimination-artificial-intelligence-and-algorithmic-decision-making/1680925d73; Equinet (2020) Regulating for an Equal AI: A New Role for Equality Bodies, dostopno na: https://equineteurope.org/wp-content/uploads/2020/06/ai_report_digital.pdf

Za razliko od preteklih različic ZVOP-2 predlog ZVOPPOKD izrecno ne izpostavlja prepovedi diskriminacije kot posebnega fokusa ocene učinkov avtomatizirane in druge obdelave posebnih podatkov. Prav tako naknadno oziroma ponovno preverjanje odločitev, ki bi temeljijo izključno na avtomatizirani obdelavi osebnih podatkov ni (samodejno) zapovedano, kot je to določal drugi predlog ZVOP-2, temveč se opravi na zahtevo posameznika, ki mu to pravico določa področni zakon. Upoštevajoč navedeno Zagovornik ocenjuje, da se je raven varstva pred diskriminacijo pri uporabi avtomatiziranega odločanja in obdelave podatkov v predlogu ZVOPPOKD glede na zadnji predlog celovitega ZVOP-2 znižala. Prav tako aktualni predlog ne predvideva obvezne ocene učinkov glede tveganj za človekove pravice in temeljne svoboščine ob uvedbi novih sistemov avtomatiziranega odločanja.

***Zagovornik zato predlagatelju priporoča, da v predlogu ZVOPPKD**:*

- *vključi **dodatni pogoj izjeme** od prepovedi odločanja, ki temelji izključno na avtomatizirani obdelavi osebnih podatkov, in sicer, **vsakokratno naknadno (ročno) preverjanje rezultatov avtomatizirane obdelave osebnih podatkov** (9. člen);*
- *v **2. točki četrtega odstavka 49. člena** za besedno zvezo »osebni podatki«, **doda besedilo »,zlasti glede prepovedi diskriminacije«**;*
- *v **petem odstavku 49. člena** določi, da mora pristojni organ pred uvedbo novega sistema za avtomatizirano obdelavo osebnih podatkov **oceno učinka** izvesti **tudi glede tveganj za človekove pravice in temeljne svoboščine, zlasti glede prepovedi diskriminacije,** ter glede **ukrepov za obvladovanje teh***

Zagovornik nadalje opozarja na vprašanje **pravne podlage zbiranja razčlenjenih podatkov o t.i. zločinih iz sovraštva** (*hate crime*). Po raziskavi Agencije EU za temeljne pravice (FRA), pristojni organi v Sloveniji uradnih razčlenjenih podatkov o tovrstnih kaznivih dejanjih ne zbirajo in ne objavljajo.[6] Ti podatki, ki v običajno temeljijo na posebnih vrstah osebnih podatkov oškodovancev (npr. narodnost, spolna usmerjenost, zdravstveno stanje itd.), so v statistični obliki ključni za spremljanje stanja in trendov ter za oblikovanje učinkovitih javnih politik zoper t.i. zločine iz sovraštva.

Zagovornik upošteva, da celovito zbiranje podatkov o kaznivih dejanjih iz sovraštva terja tudi ustrezne prilagoditve kazenskopravne zakonodaje. Vendar pa poudarja, da bi predlog ZVOPPOKD kot sistemski zakon moral predvideti možnost zakonitega obdelovanja osebnih podatkov za namene pridobivanja podatkov o t.i. zločinih iz sovraštva.

Zagovornik predlagatelju zato priporoča**, da **v obrazložitvi 6.** (zakonitost obdelave) **in/ali 7.** (zakonitost obdelave posebnih vrst osebnih podatkov) **člena predloga ZVOPPOKD v okvir izjem od prepovedi obdelave (posebnih vrst) osebnih podatkov izrecno vključi situacije, v katerih je posameznik, na katerega se osebni podatki nanašajo, oškodovanec kaznivega dejanja, katerega motiv je sovraštvo na podlagi osebnih okoliščin.

Zagovornik zaproša Ministrstvo za pravosodje za odziv na njegova priporočila.

S spoštovanjem,

Miha Lobnik
ZAGOVORNIK NAČELA ENAKOSTI

Poslano:
- naslovniku (po e-pošti),
- zbirka dok. gradiva.

V vednost:
- Informacijski pooblaščenec (gp.ip@ip-rs.si)
- Varuh človekovih pravic (info@varuh-rs.si)

[6] FRA (2018) Hate crime recording and data collection practice across the EU, str. 23-25. Dostopno na: https://fra.europa.eu/sites/default/files/fra_uploads/fra-2018-hate-crime-recording_en.pdf

UTEMELJITEV STROKOVNE SLUŽBE ZAGOVORNIKA K PRIPOROČILU ŠT. 0701-6/2020/1

I. PRIPOROČILO

***Zagovornik zato predlagatelju priporoča, da v predlogu ZVOPPKD**:*

- *vključi **dodatni pogoj izjeme** od prepovedi odločanja, ki temelji izključno na avtomatizirani obdelavi osebnih podatkov, in sicer, **vsakokratno naknadno (ročno) preverjanje rezultatov avtomatizirane obdelave osebnih podatkov** (9. člen);*
- *v **2. točki četrtega odstavka 49. člena** za besedno zvezo »osebni podatki«, **doda besedilo »,zlasti glede prepovedi diskriminacije«**;*
- *v **petem odstavku 49. člena** določi, da mora pristojni organ pred uvedbo novega sistema za avtomatizirano obdelavo osebnih podatkov **oceno učinka** izvesti **tudi glede tveganj za človekove pravice in temeljne svoboščine, zlasti glede prepovedi diskriminacije,** ter glede **ukrepov za obvladovanje teh***

Avtomatizirano odločanje in obdelava podatkov na področju delovanja policijskih, pravosodnih in varnostnih organov temeljita na **uporabi tehnologij umetne inteligence**. Medtem, ko lahko to na zadevnem področju prinaša številne prednosti, saj se velike količine podatkov lahko obdelajo v kratkem času, kar je pri obravnavi kaznivih dejanj bistvenega pomena, pa se z avtomatsko obdelavo osebnih podatkov in avtomatskim odločanjem na podlagi teh podatkov odpirajo številna vprašanja posegov v človekove pravice.[7] EK v Beli knjigi o umetni inteligenci zato izpostavlja pomen regulativnih okvirov, ki bodo zagotavljali skladnost z zakonodajo, načeli in vrednotami EU, kot posebej pomembna v tem oziru pa izpostavlja **področja, na katerih je vpliv na pravice posameznikov lahko najbolj neposreden**, pri čemer izpostavlja prav uporabo umetne inteligence za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj in v pravosodju.[8]

Tako Bela knjiga EK kot študije različnih mednarodnih vladnih in nevladnih organizacij[9] v kontekstu potencialnega negativnega vpliva avtomatiziranega odločanja in obdelave podatkov na človekove pravice izpostavljata področji varstva osebnih podatkov ter **diskriminacije**. Vsakršna tehnologija umetne inteligence deluje po načelu razlikovanja, saj uporabljeni algoritmi že po definiciji podatke obravnavajo oziroma obdelujejo neenako.[10] **Problem se pojavi, kadar takšno neenako obdelovanje temelji na osebnih okoliščinah, na podlagi katerih je diskriminacija prepovedana**, in kadar takšna obdelava posledično **vodi v razlikovanje na podlagi osebnih okoliščin**. Avtomatizirana obdelava osebnih podatkov poteka z uporabo stalno razvijajočih se tehnologij, ki temeljijo na strojnem učenju (*machine learning*). Pogoj slednjega je vnos relevantnih učnih podatkov (*training data*), na podlagi katerih se s pomočjo algoritmov oblikujejo končne odločitve. Če so ti učni podatki pristranski (*bias*), obstaja velika verjetnost, da bodo odločitve na podlagi avtomatizirane obdelave osebnih podatkov diskriminatorne. Avtomatizirano odločanje lahko vodi do diskriminacije z neustrezno definicijo spremenljivk in kategorij učnih podatkov, z neustreznim označevanjem učnih podatkov, z nereprezentativno uporabo učnih podatkov (npr. osredotočenje zgolj na skupine z določeno osebno okoliščino) ter z uporabo posrednih osebnih podatkov, ki so močno povezani z določeno zaščiteno osebno okoliščino (t.i. *proxies*).[11]

Na področju, ki ga naslavlja predlog ZVOPPOKD, se kot najbolj problematični področji z vidika diskriminacije izpostavljata izdelovanje profilov za namene **preventivne policijske dejavnosti** (*predictive policing*), ki temelji na avtomatizirani izdelavi profilov tveganj, kdo in kje bo zagrešil kaznivo dejanje, ter uporaba **tehnologije prepoznave obrazov** (*facial recognition technology* - FRT).[12]

---

[7] Glej npr. študijo Sveta Evrope (2017) *Algorithms and Human Rights: Study on the human rights dimensions of automated data processing techniques and possible regulatory implications*, dostopno na: https://edoc.coe.int/en/internet/7589-algorithms-and-human-rights-study-on-the-human-rights-dimensions-of-automated-data-processing-techniques-and-possible-regulatory-implications.html#

[8] *Bela knjiga*, opomba 4 *zgoraj*, str. 11.

[9] Glej opombe 5 in 8 *zgoraj*.

[10] Svet Evrope, opomba 8 *zgoraj*, str. 26.

[11] F. Zuiderveen Borgesius / Svet Evrope (2019) Discrimination, artificial intelligence, and algorithmic decision-making str. 10-13, dostopno na: https://rm.coe.int/discrimination-artificial-intelligence-and-algorithmic-decision-making/1680925d73

[12] Equinet (2020), opomba 5 *zgoraj*, str. 34, 41-48.

Britanski organ za enakost je na primer v svojem senčnem poročilu Odboru OZN za človekove pravice izpostavil, da nekateri javno dostopni podatki kažejo tudi na do 96-odstotno nenatančnost avtomatizirane FRT ter nesorazmerno napačno identifikacijo žensk ter oseb drugih 'ras', zaradi česar so tudi britanska sodišča izpostavila potrebo po dodatnih preiskavah delovanja FRT z vidika prepovedi diskriminacije.[13] Omeniti velja, da FRT uporablja tudi slovenska policija, glede njene uporabe pa ostaja odprtih več vprašanj – od izdelave ocene učinka na varstvo osebnih podatkov in druge človekove pravice do neusklajenosti policije z Informacijskim pooblaščencem glede delovanja predmetne FRT aplikacije.[14] Britanski organ za enakost v omenjenem senčnem poročilu izpostavil tudi nekatere dokaze, ki kažejo, da tehnologija za preventivne policijske dejavnosti krepi vzorce diskriminatorne policijske obravnave (zlasti temnopoltih, etničnih manjšin ter revnih), hkrati pa pristranskim postopkom daje dodatno legitimnost.[15]

Zaradi navedenih in drugih nevarnosti tehnologij umetne inteligence, zlasti na policijsko-pravosodno-varnostnem področju, je bistvenega pomena, da se pred njihovo uporabo izvedejo **ustrezni postopki ocene učinkov**, zlasti z vidika **prepovedi diskriminacije**. EK v Beli knjigi izpostavlja pomen ustvarjanja »ekosistema zaupanja«, ki zagotavlja skladnost uporabe umetne inteligence z EU pravili, vključno z varstvom temeljnih pravic (ter s tem varstvom pred diskriminacijo). Da bi preprečili negativne učinke umetne inteligence, EK izpostavlja potrebo po čim širšem predhodnem ugotavljanju skladnosti, ki bi se ga izvajalo z ocenami različnih učinkov nove tehnologije ter postopkov njene uporabe.[16] V okviru teh postopkov je pomembno, da uporabnik posameznega sistema za avtomatsko obdelavo osebnih podatkov izdela oceno učinka tako glede samega uporabljenega algoritma (način obdelave podatkov in učni podatki) kot tudi glede kakovosti podatkov, ki so v algoritemsko odločanje vneseni (*input data*), in podatkov, ki jih algoritem oblikuje na podlagi predpisanega sklepanja (*inferred labels* – napovedi).[17] Strokovnjaki opozarjajo, da je (predhodno, pa tudi sprotno) preverjanje kakovosti podatkov pomembno zlasti pri tehnologijah, namenjenih preventivnim policijskim dejavnostim, ker modeli ocene tveganj v prvi vrsti temeljijo na podatkih in ne na teoretskih modelih analize tveganj.[18]

Upoštevajoč navedeno Zagovornik predlaga, da se **v 49. členu predloga ZVOPPOKD, ki ureja oceno učinka** in se osredotoča na kontekst »uporabe novih tehnologij«, v 2. točki četrtega odstavka izpostavi, da se ocena tveganj za človekove pravice in svoboščine posameznikov, na katere se nanašajo osebni podatki, opravi **zlasti glede prepovedi diskriminacije**. To je pomembno tudi z vidika določbe tretjega odstavka 9. člena predloga zakona, ki določa, da mora pred sprejetjem zakona, ki določa avtomatizirano odločanje, pristojni predlagatelj izvesti oceno učinka iz 49. člena predloga zakona. Iz zgoraj navedenih razlogov Zagovornik dodatno predlaga, da se **izvedba ocene tovrstnega učinka predpiše tudi za uvedbo vsakršnega novega sistema za avtomatizirano obdelavo osebnih podatkov**, kot to določa peti odstavek 49. člena predloga zakona. Iz obrazložitve k 49. členu izhaja, da je trenutna ureditev namenjena temu, da pristojni organ »načrtuje varnost sistema«, ki bi moral po Zagovornikovi oceni vključevati tudi oceno tveganj za človekove pravice, zlasti glede prepovedi diskriminacije. Ob navedenih Zagovornikovih predlogih in priporočilih velja izpostaviti, da je v kontekstu ocene učinka **poseben poudarek na prepovedi diskriminacije vsebovala že prva različica predloga ZVOP-2**.[19] Druga različica ZVOP-2 je ta poudarek opustila,[20] kar je Zagovornik s svojimi priporočili na dotični predlog tudi naslovil. Kot izhaja iz zgoraj navedenega, Zagovornik ne vidi utemeljenega razloga za opustitev tega poudarka, nasprotno.

Z vidika dodatnih varovalk Zagovornik izpostavlja tudi, da je bilo v drugi različici predloga ZVOP-2 kot **pogoj izjeme od prepovedi** odločanja, ki temelji izključno na avtomatizirani obdelavi osebnih podatkov, določeno **samodejno naknadno preverjanje rezultatov obdelave**.[21]

---

[13] Equality and Human Rights Commission (2020) *Civil and Political Rights in Great Britain*, str. 65-66. Dostopno na: https://www.equalityhumanrights.com/sites/default/files/civil_and_political_rights_in_great_britain_2020.pdf

[14] Aljoša Masten (2020) *Tudi slovenska policija uporablja avtomatsko prepoznavo obrazov*, MMC RTV, https://www.rtvslo.si/slovenija/tudi-slovenska-policija-uporablja-avtomatsko-prepoznavo-obrazov/510776

[15] Opomba 14 *zgoraj*, *prav tam*

[16] *Bela knjiga*, opomba 4 *zgoraj*, glej poglavji D. in F.

[17] FRA (2019) *Data quality and artificial intelligence – mitigating bias and error to protect fundamental rights*, str. 4-5, dostopno na: https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-data-quality-and-ai_en.pdf

[18] Albert Meijer in Martijn Wessels (2019) *Predictive Policing: Review of Benefits and Drawbacks, International Journal of Public Administration* 42(12), dostopno na: https://www.tandfonline.com/doi/full/10.1080/01900692.2019.1575664.

[19] Drugi odstavek 44. člena: »*Pred uvedbo sistema postopkov avtomatiziranega odločanja je treba izvesti posebno osredotočeno oceno učinka po 37. členu tega zakona, ki mora vsebovati tudi oceno učinka na povezane človekove pravice in temeljne svoboščine, **zlasti glede prepovedi diskriminacije**«*.

[20] Tretji odstavek 77. člena.

[21] Prvi odstavek 77. člena *(»/…/ ter če so izvedena naknadna preverjanja rezultatov avtomatizirane obdelave /…/*). Obrazložitev k 77. členu je dodatno utemeljevala, da je bistvo te določbe med drugim, »da mora biti možno in **dejansko izvedeno** naknadno preverjanje rezultatov«.

V prvem odstavku 9. člena ZVOPPOKD je ta standard znižan in je kot pogoj izjeme določeno le, da mora področni zakon, ki dovoljuje uporabo takšnega odločanja, določati pravico posameznika, da zahteva ročni pregled odločitve in da izrazi svoje stališče do odločitve. Zagovornik se zaveda, da se s tem ustrezno prenaša le minimalni standard iz prvega odstavka člena 11 Direktive EU 2016/680. Upoštevajoč zgoraj navedena tveganja, ki jih avtomatizirano odločanje lahko prinaša z vidika prepovedi diskriminacije, pa Zagovornik meni, da bi veljalo v prvi odstavek 9. člena aktualnega predloga zakona vključiti tudi standard, ki je bil postavljen v drugi različici ZVOP-2. To dopušča tudi tretji odstavek 1. člena Direktive EU 2016/680, ki določa, da direktiva »državam članicam ne preprečuje, da za varovanje pravic in svoboščin posameznikov, na katere se nanašajo osebni podatki, ki jih obdelujejo pristojni organi, sprejmejo višjo raven zaščitnih ukrepov od ravni, določene v tej direktivi«.

II. PRIPOROČILO

Zagovornik predlagatelju priporoča**, da **v obrazložitvi k 6.** (zakonitost obdelave) **in/ali 7.** (zakonitost obdelave posebnih vrst osebnih podatkov) **členu predloga ZVOPPOKD v okvir izjem od prepovedi obdelave (posebnih vrst) osebnih podatkov izrecno vključi situacije, v katerih je posameznik, na katerega se osebni podatki nanašajo, oškodovanec kaznivega dejanja, katerega motiv je sovraštvo na podlagi osebnih okoliščin.

Zločini iz sovraštva (*hate crime*) so kazniva dejanja, ki so zoper oškodovance usmerjena zaradi ene ali več njihovih osebnih okoliščin, ki predstavljajo njihovo prirojeno ali pridobljeno lastnost, ki se je ne morejo zlahka odreči, in ki predstavlja sestavni del njihove identitete. Zločini iz sovraštva so neposredno povezani z vprašanjem diskriminacije. Predstavljajo kazniva dejanja, ki so sicer že splošno opredeljena in prepovedana, torej so v vsakem primeru lahko sankcionirana po veljavni zakonodaji. Vendar pa imajo tovrstna kazniva dejanja posebno kvalitativno naravo, saj so storjena s posebnim diskriminatornim nagibom (angl. *bias motive*) in so zoper žrtev usmerjena zaradi storilčevih predsodkov, nestrpnosti ali sovraštva do skupine oseb, ki ji žrtev pripada. Žrtev kaznivega dejanja je torej žrtev v prvi vrsti zaradi svoje osebne okoliščine, npr. barve kože, narodnosti, etničnega porekla, verskega ali drugega prepričanja, migrantskega statusa, spolne usmerjenosti ali identitete itn. Zločin iz sovraštva je proti žrtvi usmerjen zato, ker ta pripada (ali naj bi pripadala v očeh storilca) skupini oseb z določeno osebno okoliščino, do katere storilec goji izrazito negativen oziroma odklonilen odnos. **Gre za posebno hude izraze predsodkov storilcev do teh skupin, ki objektivno kažejo izraze sovraštva in s tem načrtne poskuse, da bi te skupine z grobim zastraševanjem še dodatno potisnili na rob družbe**.

Evropsko sodišča za človekove pravice (ESČP) je skozi prakso oblikovalo stališče, da odsotnost preiskave vzročne povezave med rasističnimi motivi in umorom pomeni kršitev postopkovne dimenzije 14. člena Evropske konvencije o človekovih pravicah (EKČP), tj. prepovedi diskriminacije.[22] Sodišče je odločilo, da ima **država *pozitivno dolžnost* razkriti rasistične motive, ki bi lahko igrali vlogo pri storitvi kaznivega dejanja**, kar pomeni, da morajo pristojni organi »zbrati in zavarovati dokaze, preizkusiti vse praktične poti odkrivanja resnice ter podati popolnoma obrazloženo, nepristransko in objektivno odločitev, brez da bi pri tem izpustili sumljiva dejstva, ki bi lahko bila indikator rasno motiviranega nasilja«.[23] Sodišče je skozi svojo prakso **identično stališče ter povezavo s pozitivnimi dolžnostmi** po postopkovni dimenziji 14. člena EKČP uveljavilo **tudi v odnosu do kršitev zaradi drugih osebnih okoliščin** ter v odnosu do diskriminatornih motivov kaznivih dejanj, ki temeljijo na zgolj domnevani osebni okoliščini žrtev.[24]

Upoštevajoč navedeno FRA opozarja, da bi **odsotnost razkritja in beleženja diskriminatornih motivov** ob obravnavi kaznivih dejanj v policijskih postopkih lahko pomenila **kršitev mednarodnega prava človekovih pravic**, saj je verjetnost, da bi se nato diskriminatorni motiv razkril kasneje tekom kazenskega postopka manjša.[25] Poleg tega FRA poudarja, da je **zbiranje razčlenjenih podatkov o t.i. zločinih iz sovraštva nujno za spremljanje učinkovitosti organov pregona pri odzivih na tovrstna kazniva dejanja ter za oblikovanje učinkovitih in usmerjenih politik**. Objavljanje in razširjanje podatkov v anonimizirani in statistični obliki žrtvam in skupnostim, ki jim pripadajo, sporoča,

[22] *Nachova in drugi proti Bolgariji*, št. 43577/98 in 43579/98, sodba z dne 6. julija 2005
[23] *Prav tam*, 159. odstavek
[24] Za seznam primerov ESČP in njihovo analizo glej FRA. 2018. *Unmasking bias motives in crimes: selected cases of the European Court of Human Rights*. Dostopno na: https://fra.europa.eu/sites/default/files/fra_uploads/fra-2018-unmasking-bias-motives-paper_en.pdf
[25] FRA (2018), opomba 6 *zgoraj*, str. 11

da država kazniva dejanja iz sovraštva obravnava resno, širši javnosti pa, da zločine iz sovraštva spremlja, naslavlja in ima do njih ničelno stopnjo tolerance.[26]

Razčlenjenih podatkov o t.i. zločinih iz sovraštva v Sloveniji ni. Študija FRA kaže, da se Slovenija uvršča v skupino le petih držav članic EU, ki podatkov o zločinih iz sovraštva ne beležijo, ne zbirajo in ne objavljajo.[27] Zagovornik se s problemom odsotnosti ustrezno razčlenjenih podatkov sicer srečuje na različnih področjih pri svojem delu. Upoštevajoč 16. člen Zakona o varstvu pred diskriminacijo (ZVarD)[28] Zagovornik v okviru priprave svojih rednih letnih poročil zbira in objavlja tudi podatke o primerih diskriminacije, obravnavanih pri drugih državnih organih – inšpektoratih (na podlagi ZVarD in drugih pravnih podlagah), policiji (20. člen ZJRM-1 ter 131. in 297. člen KZ-1), Vrhovnem državnem tožilstvu (131. in 297. člen KZ-1) ter sodiščih (na podlagi predpisov, ki vsebujejo prepoved diskriminacije in obveznost enake obravnave ne glede na osebne okoliščine). Iz rezultatov poizvedb, ki jih je Zagovornik izvedel v letih 2017, 2018 in 2019 izhaja, da **noben izmed navedenih naslovnikov podatkov o obravnavanih primerih diskriminacije ne razčlenjuje po osebnih okoliščinah**. Tega ne izvajajo tudi pristojni inšpektorati, ki jim ZVarD v prvem odstavku 16. člena izrecno nalaga, da Zagovorniku enkrat letno posredujejo »/…/ anonimizirane podatke o številu obravnavanih primerov diskriminacije *po posameznih osebnih okoliščinah*, po oblikah diskriminacije in po posameznih področjih /…/«.

Ministrstvo za pravosodje je v odgovoru na eno izmed Zagovornikovih poizvedb[29] kot eno najtežjih nalog na področju boja proti diskriminaciji izpostavilo prepoznavanje elementov sovražnosti pri kaznivih dejanjih ter **vprašanje beleženja različnih oblik diskriminacije**. Hkrati je ministrstvo poročalo, da v zvezi s tem FRA in Uradom za demokratične institucije in človekove pravice pri Organizaciji za varnost in sodelovanje v Evropi (ODIHR) načrtuje izvedbo delavnice, ki bo namenjena osveščanju in izboljšanju delovanja na tem področju in na katerem bodo sodelovali predstavniki policije in državnega tožilstva. Težave pri spremljanju kaznivih dejanj s sovražnim motivom po osebnih okoliščinah oškodovancev je Zagovorniku poročalo tudi Vrhovno državno tožilstvo (VDT). To je izpostavilo potrebo po previdnosti pri opredeljevanju načina evidentiranja in spremljanja tako motiviranih kaznivih dejanj, saj da opredeljevanje spisov oziroma vodenje evidenc po osebnih okoliščinah oškodovancev, zoper katere je sovražni motiv usmerjen, ni dovoljeno.[30]

Slovenski pravni red že sedaj dopušča zbiranje podatkov o primerih diskriminacije, ki jih vodijo Zagovornik in pristojne inšpekcije, po posameznih osebnih okoliščinah, in sicer za namene spremljanja, načrtovanja in vodenja nediskriminacijske politike ter za znanstvenoraziskovalne namene.[31] Zagovornik je zato že v okviru drugega predloga ZVOP-2[32] predlagatelju priporočil, da v okvir določb 73. člena, ki so urejale zakonitost obdelave posebnih vrst osebnih podatkov na policijsko-pravosodno-varnostnem področju, izrecno vključi situacije, v katerih je posameznik, na katerega se osebni podatki nanašajo, oškodovanec kaznivega dejanja, katerega motiv je sovraštvo na podlagi osebnih okoliščin.

Ker se je način ureditve zakonitosti obdelave (tudi posebnih vrst) osebnih podatkov v predlogu ZVOPPOKD spremenil in izrecna navedba omenjenih situacij po oceni Zagovornika konceptualno ne spada v okvir 6. in/ali 7. člena predloga, **Zagovornik predlaga, da se dopustnost obdelave tovrstnih osebnih podatkov** (ob upoštevanju pogojev iz 6. in 7. člena predloga) **izrecno navede v obrazložitvi teh členov**. Po oceni Zagovornika pravna podlaga za obdelavo teh podatkov obstaja. Zakon o nalogah in pooblastilih policije[33] v 1. točki prvega odstavka 125. člena namreč določa, da policija v evidenci kaznivih dejanj vodi tudi podatke o motivu kaznivega dejanja, tega pa v primeru t.i. zločinov iz sovraštva predstavlja prav osebna okoliščina oškodovanca. Prav tako bi se isti podatki načeloma lahko zbirali tudi z ozirom na pravnomočne sodne odločbe o t.i. zločinih iz sovraštva. Pravilnik o kazenskih evidencah[34] v 8. točki prvega odstavka 6. člena kot vsebino kazenske evidence določa prevedbo opisa tipa kaznivega dejanja glede na sistem ECRIS. Okvirni sklep Sveta 2009/315/PNZ z dne 26. februarja 2009 o organizaciji in vsebini izmenjave informacij iz kazenske evidence med državami članicami v delu, ki ni bil spremenjen z Direktivo EU 2019/884, v zadnjem

[26] *Prav tam*
[27] *Prav tam*, str. 21-25
[28] Uradni list RS, št. 33/16 in 21/18 – ZNOrg
[29] Dopis Ministrstva za pravosodje Zagovorniku št. 070-6/2020 z dne 8. 1. 2020
[30] Dopis VDT Zagovorniku št. Ktr-zb-1/6/2020/AF-KK z dne 24. 1. 2020
[31] 16. člen ZVarD
[32] Predlog EVA: 2018-2030-0045 z dne 14. 8. 2019
[33] Uradni list RS, št. 15/13, 23/15 – popr. in 10/17, 47/19
[34] Uradni list RS št. 3/18

stavku člena 11(1) določa, da lahko pristojni organ v okviru izmenjave informacij o obsodbah »pošlje katerekoli druge informacije o kazenskih obsodbah, če so vnesene v kazensko evidenco«. Ti podatki bi lahko pomenili tudi motiv kaznivega dejanja, v predmetnem primeru torej osebno okoliščino oškodovanca. **Temeljni namen** tovrstne obdelave podatkov je **pridobiti agregirani statistični podatek o stanju in trendih** na področju t.i. zločinov iz sovraštva s ciljem **oblikovati in izvijati učinkovitejše ukrepe za njihovo preprečevanje in obravnavo**.