**Pregled odziva javnega posvetovanja**

**o**

**predlogu stališč Republike Slovenije**

**do**

**Predloga uredbe Evropskega parlamenta in**

**Sveta o določitvi harmoniziranih pravil o umetni inteligenci (Akt o umetni inteligenci) in**

**spremembi nekaterih zakonodajnih aktov Unije**

Avtorji: mag. Samo Zorc, Nadja Kamenšek, Martina Furlan

Povzetek

Poročilo vsebuje analizo odgovorov na javno posvetovanje o predlogu stališč Slovenije do Akta o umetni inteligenci EU. Stališče predstavlja dopolnitev in prenovo stališča Slovenije z dne 10. 9. 2021. Ministrstvo za digitalno preobrazbo je za prenovo stališča objavilo predloge stališč ter pripravilo javno spletno posvetovanje za odziv in komentarje javnosti, ki je bilo na voljo v obliki spletnega vprašalnika od 2. 3. 2023 do 17. 3. 2023. Spletno posvetovanje je v splošnem pokazalo strinjanje s pripravljenimi predlogi stališč, pri čemer so bila najbolj podprta stališča o primerljivih kaznih za EU institucije, o biometrični identifikaciji kot uporabi umetne inteligence (UI) visokega tveganja, o tehnično jasni definiciji ter o ciljih sistemskega urejanja. Relativno so se respondenti najmanj strinjali s stališčem o sistemskem urejanju v delu, ki se nanaša na uporabo UI na področju nacionalne varnosti, vojaške uporabe in glede sistemov dvojne rabe, s stališčem o tehnično jasni in razumljivi definiciji sistemov UI v delu, ki se nanaša na vprašanje klasifikacije enostavnih sistemov, kjer človek določi pravila ročno, med sisteme UI ter s stališčem o načinu urejanja umetne inteligence splošnega namena. Odgovori bodo ustrezno uporabljeni pri pripravi končnih stališč Slovenije do Akta o umetni inteligenci.

Kazalo

[1 Uvod 3](#_Toc132124852)

[2 Pregled odziva 3](#_Toc132124853)

[2.1 Respondenti 3](#_Toc132124854)

[2.2 Pregled vseh stališč 4](#_Toc132124855)

[2.3 Usklajeni mednarodni pristop 5](#_Toc132124856)

[2.4 Sistemsko urejanje (I) - obseg regulacije 7](#_Toc132124857)

[2.5 Sistemsko urejanje (II) - obseg regulacije 8](#_Toc132124858)

[2.6 Sistemsko urejanje (III) - obseg regulacije 8](#_Toc132124859)

[2.7 Urejanje na podlagi tveganja uporabe za človekove pravice in varnost 9](#_Toc132124860)

[2.8 Horizontalni pristop 10](#_Toc132124861)

[2.9 Tehnično jasna in razumljiva definicija sistema UI (I) 11](#_Toc132124862)

[2.10 Tehnično jasna in razumljiva definicija sistema UI (II) 12](#_Toc132124863)

[2.11 Tehnično jasna in razumljiva definicija sistema UI (III) 13](#_Toc132124864)

[2.12 Ureditev regulacije Umetne inteligence splošnega namena 14](#_Toc132124865)

[2.13 Ureditev raziskav in razvoja 14](#_Toc132124866)

[2.14 Prilagodljivost regulacije hitremu razvoju in inovacijam 15](#_Toc132124867)

[2.15 Jasna in podrobnejša opredelitev kriterijev visokega tveganja 16](#_Toc132124868)

[2.16 Metodologija opredelitve sistemov UI visokega tveganja (I) 17](#_Toc132124869)

[2.17 Metodologija opredelitve sistemov UI visokega tveganja (II) 18](#_Toc132124870)

[2.18 Razložljivost in avtonomnost UI 19](#_Toc132124871)

[2.19 Javna varnost 20](#_Toc132124872)

[2.20 Prepovedane prakse 21](#_Toc132124873)

[2.21 Biometrična identifikacija kot uporaba UI visokega tveganja 22](#_Toc132124874)

[2.22 Učinkovit upravljavski okvir 23](#_Toc132124875)

[2.23 Učinkovito pravno varstvo 24](#_Toc132124876)

[2.24 Primerljive kazni za EU institucije 25](#_Toc132124877)

[3 Zaključek 26](#_Toc132124878)

[4 Priloga I - Vprašalnik 27](#_Toc132124879)

# Uvod

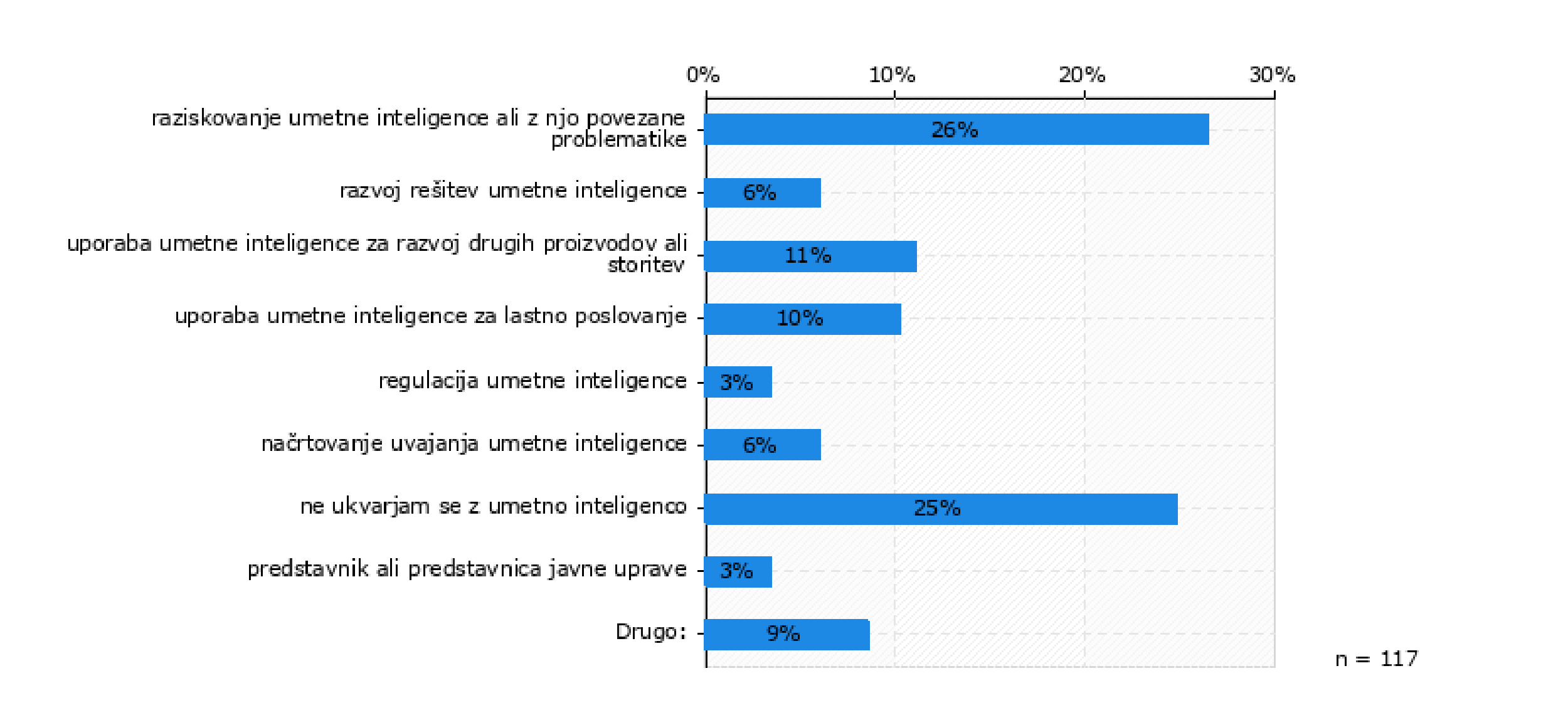
Slovenija aktivno sodeluje pri načrtovanju in izvajanju politik na področju umetne inteligence (UI) tako na ravni EU kot tudi v mednarodnem okolju. Osnovni dokument, ki opredeljuje aktivnosti na tem področju, je Nacionalni program spodbujanja razvoja in uporabe umetne inteligence v Republiki Sloveniji do leta 2025 (NpUI), ki določa vizijo, cilje in koncept podpore razvoju in uvajanju umetne inteligence v Sloveniji. NpUI naslavlja tudi regulacijo, ki sledi viziji zagotavljanja skladnosti z etičnimi načeli, varstvom človekovih pravic in zagotavljanja varnosti pri razvoju in uporabi zaupanja vredne UI. Slednje je osnova tudi za sodelovanje pri pripravi regulative za UI na ravni EU.

Evropska komisija je 21. 4. 2021 objavila predlog Uredbe evropskega parlamenta in sveta o določitvi harmoniziranih pravil o umetni inteligenci (Akt o umetni inteligenci) in spremembi nekaterih zakonodajnih aktov unije COM(2021) 206. Slovenija je na predlog akta v skladu z NpUI podala svoje generalno stališče dne 10. 9. 2021 (EPA 2043-VIII, EU U 1015)[[1]](#footnote-2), ki je bilo osnova za usklajevanje predloga uredbe na Svetu za promet, telekomunikacije in energijo (PTE). Pri usklajevanju predloga uredbe si je Slovenija prizadevala za njegovo izboljšanje v smislu večje jasnosti, konsistentnosti in predvidljivosti za vse relevantne deležnike. Decembra 2022 je Svet PTE pripravil usklajen osnutek uredbe in dosegel splošni pristop. Usklajen osnutek je trenutno v postopku trialoga predmet usklajevanja v Evropskem parlamentu. Glede na spremembe prvotnega predloga Evropske komisije se je Slovenija odločila preveriti svoja dosedanja stališča in jih po potrebi prenoviti glede na spremembe besedila aktualnega predloga tudi z vidika predlogov, ki jih je podajala v času usklajevanja predloga na Svetu PTE. Temu je bilo namenjeno tudi javno posvetovanje, ki je bilo izvedeno v obliki spletnega vprašalnika v času od 2. 3. 2023 do 17. 3. 2023, kjer je imela javnost za vsako stališče možnost podajanja stopnje strinjanja ter pisnega komentarja ali predlogov. Ministrstvo za digitalno preobrazbo je spletno posvetovanje uradno najavilo na svoji spletni strani ter povabilo javnost k sodelovanju, hkrati pa tudi aktivno pozvalo k sodelovanju vse ključne nacionalne deležnike na področju UI. Pregled odziva je naveden v nadaljevanju.

# Pregled odziva

## Respondenti

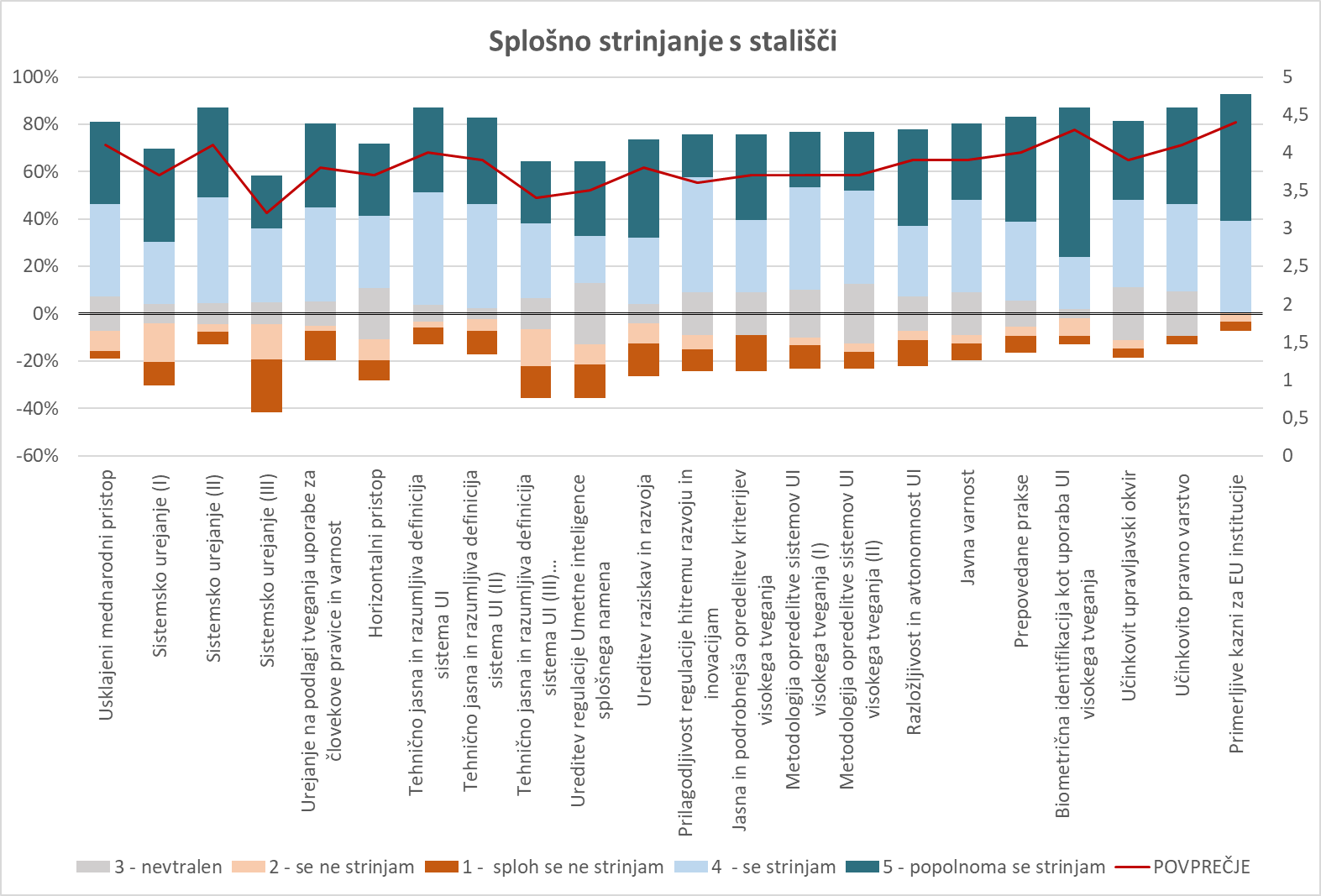
Na vprašalnik je odgovorilo skupaj 132 respondentov, od katerih jih je 37 izpolnilo vprašalnik v celoti, 95 pa delno. Največ respondentov z vidika lastne deklaracije o osebni dejavnosti v povezavi z umetno inteligenco je raziskovalcev UI (26 %), druga največja skupina respondentov je takih, ki se ne ukvarjajo z UI (25 %), tretjo največjo skupino sestavljajo taki, ki uporabljajo UI za razvoj proizvodov ali storitev (11 %).



Slika 1 Vrsta in delež respondentov

## Pregled vseh stališč

Respondenti so se v povprečju strinjali s predlogi stališč RS do AIA. V največji meri se strinjajo s stališčem o primerljivih kaznih za institucije EU, o biometrični identifikaciji kot uporabi UI visokega tveganja, o tehnično jasni definiciji ter o ciljih sistemskega urejanja. Najmanj so se respondenti strinjali s stališčem o sistemskem urejanju (v delu, ki se nanaša na uporabo UI na področju nacionalne varnosti, vojaške uporabe in glede sistemov dvojne rabe), o tehnično jasni in razumljivi definiciji (v delu, ki se nanaša na enostavne sisteme, kjer človek določi pravila ročno) ter o urejanju umetne inteligence splošne uporabe.



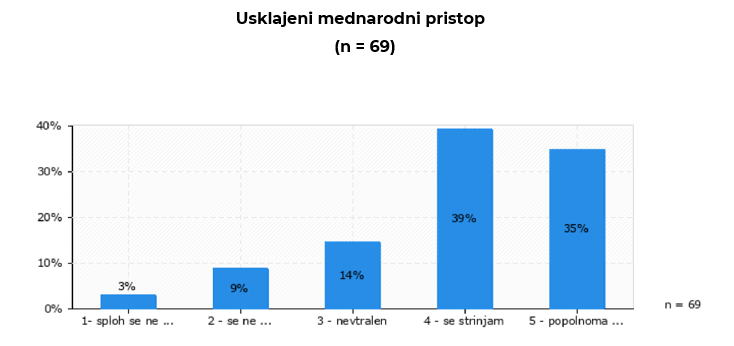
Slika 2 Splošno strinjanje s stališči

## Usklajeni mednarodni pristop

Slovenija se na podlagi pristopa do umetne inteligence (UI) v nacionalnem programu za umetno inteligenco (NpUI) vključuje v vse najpomembnejše mednarodne aktivnosti in tako sodeluje na vseh ravneh načrtovanja in izvajanja politik na ravni EU[[2]](#footnote-3), ter na mednarodni ravni v organizacijah, kot so OECD (delovna skupina AIGO[[3]](#footnote-4)), Svet Evrope (Odbor za UI – CAI[[4]](#footnote-5)), Globalno partnerstvo za umetno inteligenco (GPAI[[5]](#footnote-6)), UNESCO (IRCAI[[6]](#footnote-7)), Urad visokega komisarja za človekove pravice, in drugih relevantnih iniciativah.

Slovenija se v skladu z vizijo NpUI pri vseh aktivnostih zavzema za raziskave, razvoj in uporabo vrhunskih, etičnih in varnih tehnologij s področja UI ter njihov prenos v človeku prijazne in zaupanja vredne storitve in proizvode skladne s človekovimi pravicami in temeljnimi svoboščinami, na človeka osredotočen način in v njegovo dobro.

Glede na zelo raznovrstne aktivnosti, ki jih izvajajo omenjene organizacije, se Slovenija na mednarodni ravni zavzema za čim večje mednarodno sodelovanje ter poenotenje razumevanja, pristopov ter načrtovanja in izvajanja politik na področju UI, ki bi zagotovili bodoči razvoj in uporabo UI v družbi, skladno s prej omenjenimi izhodišči.



Slika 3 Usklajeni mednarodni pristop

**S stališčem se strinja 74 % respondentov, ne strinja se 12 % respondentov, 14 % je nevtralnih.**

Pri tem en respondent opaža, da je proaktivnost regulacije nujna in ključna in da »*širša vključenost strokovne in laične javnosti in večja medijska pokritost obravnavanih regulatornih tematik na temo UI bi nedvoumno prispevala k večji meri legitimnosti tako sprejetih regulatornih predlogov, ki so po opozorilih vodilnih mednarodno uveljavljenih gospodarskih družb, ki izvajajo inovacije s področja UI nujne v proaktivni izvedbi namesto v reaktivni regulaciji področja UI, ker bi slednje predstavljalo večja nepredvidljiva sistemska tveganja za širšo svetovno družbo in njeno temeljno ureditev. /…/ Proaktivnost /…/ je po mnenju stroke bistvena in se zaradi potencialnih tveganj z njo ne sme odlašati*«. Drugi respondent ugotavlja, da »*digitalni svet ne pozna fizičnih meja in je vanj umetna inteligenca močno vpeta*«,zato se mu zdi»*poenoteno razumevanje in pristop do oblikovanja politik ključnega pomena pri omogočanju efektivnega in predvsem doslednega izvajanja politik, vezanih na regulacijo*«. En respondent se sprašuje, »*kakšen vpliv bo imela Slovenija pri preprečevanju uporabe UI za nedemokratične, za ljudi nesprejemljive namene, kar se po svetu že dogaja*«. Drugi respondent pa poudarja, da se mora zavzemanje za etične in varne tehnologije in njihov prenos v človeku prijazne in zaupanja vredne storitve in proizvode »*spremeniti z nujno uporabo načela previdnosti s ključnim izhodiščem človekovih pravic in temeljnih svoboščin, v človeku in javno zdravje dobrih in varnih tehnologij s področja UI /…/*«. Čeprav en respondent ugotavlja, da »*se Slovenija kritično ukvarja s spremembami na področju sodobnih tehnologij*«, pa drugi opozarja, da »*članstvo v mednarodnih organizacijah in usklajeni skupni pristop so dobrodošli, a ne zagotavljajo, da se bo na podlagi tega res zagotovila etičnost rešitev ter uporaba človeku prijaznih rešitev, ki spoštuje človekove pravice in temeljne svoboščine /…/*«.

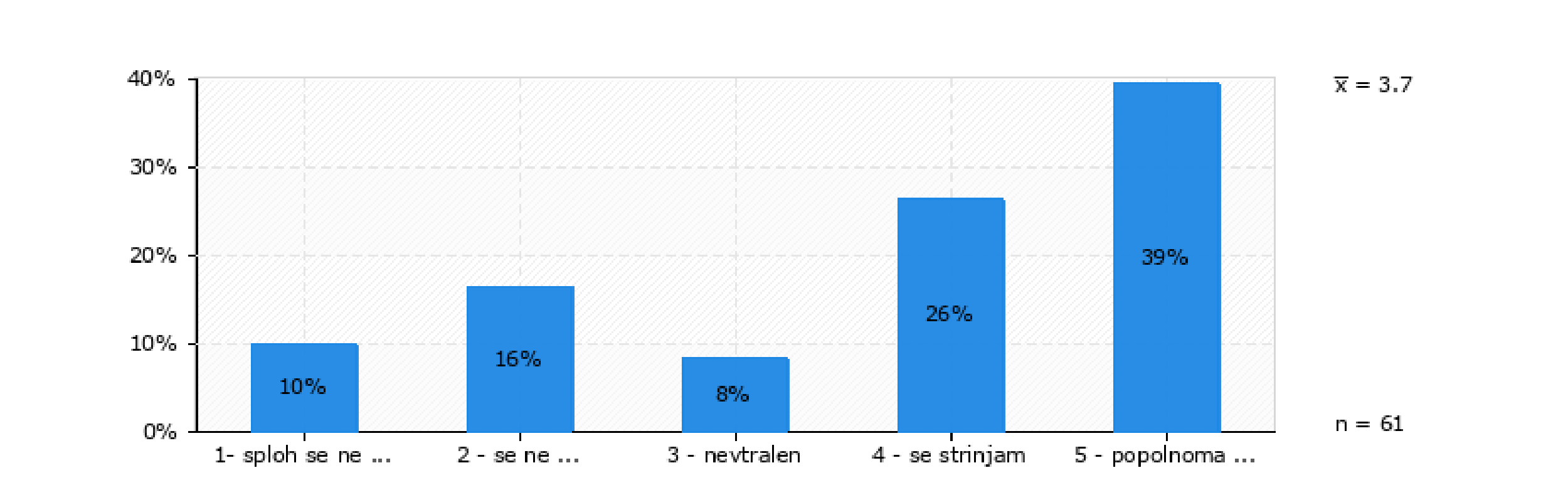
## Sistemsko urejanje (I) – obseg regulacije

Slovenija podpira predlog zakonske ureditve razvoja in uporabe UI, ki prinaša sistemski način ureditve različnih vplivov, učinkov in izzivov, ki jih uvajanje umetne inteligence prinaša v družbo.

Slovenija ne podpira ločenega urejanja problematike za različna vsebinska ali sektorska področja (npr. javna varnost, dvojna uporaba v civilne in vojaške namene, sektorsko urejanje), temveč podpira in želi enotno krovno ureditev, ki bi zagotovila dejansko preglednost in predvidljivost razvoja in uporabe UI za vse deležnike v EU, s tem pa pospešila zagotovitev prepotrebnega zaupanja javnosti v UI.

**S stališčem se strinja 65 % respondentov, 26 % respondentov se ne strinja, 8 % respondentov pa je nevtralnih.**

O usmeritvi zagotavljanja preglednosti in predvidljivosti respondent opozarja na to, da si, glede na to, »*da so vrhunski tehnološki strokovnjaki iz silicijeve doline sami priznali, da povečini več nimajo celotnega uvida v delovanje njihovih lastnih sistemov*«, ne predstavlja, »*kako bi lahko (s počasnostjo, s katero se uvaja in spreminja zakonodaja) bili sposobni "predvideti" razvoj in uporabo UI*«. O podpori krovni in enotni ureditvi drugi respondent razmišlja, da je »*/…/ potrebno zagotoviti, da se ta krovna in splošna vodila lahko prevedejo na bolj specifična področja in da omogočajo čim manj prostora za različne interpretacije, saj s tem odpirajo prostor za zlorabe, ki lahko prinašajo velika tveganja*«.Podobno drugi respondent opozarja, da je »*krovna politika smiselna, ampak lahko vodi v podoptimalne rešitve v posameznih sektorjih, ki bi potencialno potrebovali drugačen pristop do UI /…/*«. Ob tem en respondent opozarja, da morajo biti »*vsi posegi UI v civilno sfero /…/ transparentni in pod nadzorom tudi civilne družbe*«, drugi respondent pa ob tem navaja, da se »*pri zaščiti človekovih pravic in temeljnih svoboščin ne smejo dogajati razlike in da morajo vse različne rešitve na raznolikih področjih spoštovati ista načela. Vprašanje pa je, ali je pristop ene krovne ureditve res izvedljiv /…/*«. En respondent glede tega omenja, da »*bi bilo potrebno za potrebe vojske in izvajanja varnostnih politik določiti posebne standarde uporabe (vključno z ločenim nadzorom)*«.



Slika 4 Sistemsko urejanje (I) – obseg regulacije

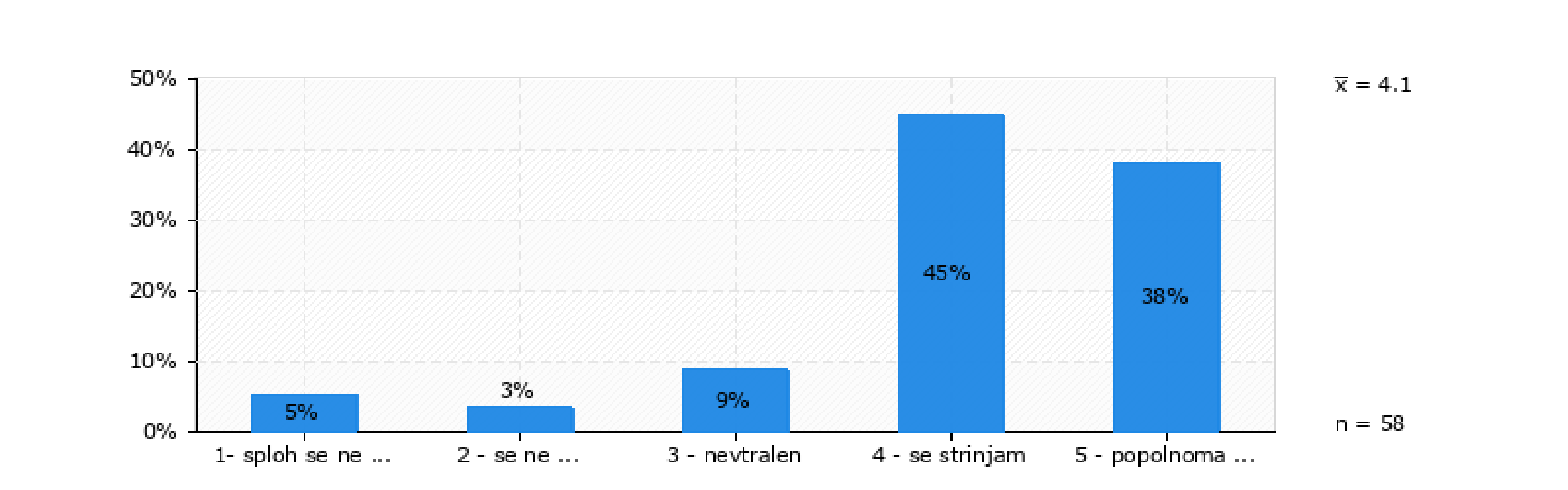
## Sistemsko urejanje (II) – obseg regulacije

Republika Slovenija se strinja s potrebo po doseganju opredeljenih štirih specifičnih ciljev, ki jih v tem smislu zasleduje Akt o umetni inteligenci (Akt o UI):

* zagotoviti, da so sistemi UI varni za uporabo in skladni z zakonodajo o človekovih pravicah in temeljnih svoboščinah ter vrednotami EU;
* zagotoviti pravno varnost za olajšanje naložb in inovacij na področju UI;
* izboljšati upravljanje in učinkovito izvrševanje zakonodaje o človekovih pravicah in temeljnih svoboščinah ter varnostnih zahtevah proizvodov in storitev, ki temeljijo ali vključujejo UI;
* olajšati razvoj enotnega trga za uporabo zakonite, varne in zaupanja vredne UI ter preprečiti razdrobljenost trga.

**83 % respondentov se s predlogom strinja, 8 % respondentov se s predlogom ne strinja, 9 % respondentov je do predloga nevtralnih.**

Glede podpore regulaciji, ki zasleduje omenjene cilje, respondent razmišlja, da bi morali cilji »*nasloviti tudi področje delovnih mest in spremembe, ki jih uvajanje umetne inteligence prinaša v delovna okolja*, */…/ poskrbeti za ustrezno ozaveščanje javnosti ter posodobitev izobraževanja*« ter da bi morali dodati »*zavezo k omogočanju svobodne UI (tako kot je pomembno zagotavljanje sistema, ki omogoča svobodno kodo)*«.



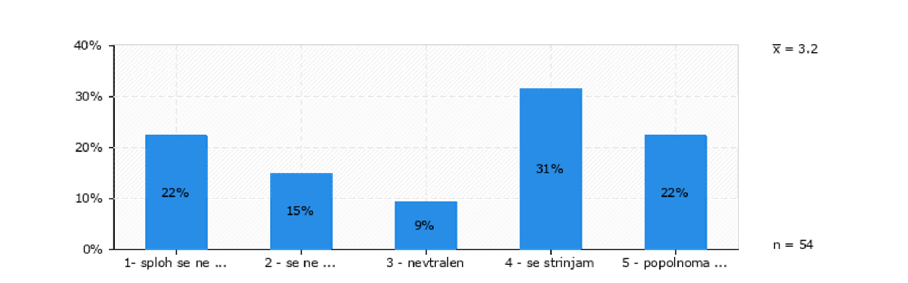
Slika 5 Sistemsko urejanje (II) – obseg regulacije

## Sistemsko urejanje (III) – obseg regulacije

Slovenija podpira usmeritev, da se iz Akta o UI izključi področje nacionalne varnosti in vojaška raba, vendar se v skladu z NpUI tudi na teh področjih zavzema za ustrezno upoštevanje etičnih načel in človekovih pravic. Ob tem se Slovenija zavzema za čim jasnejšo pravno razmejitev med civilno in vojaško uporabo sistemov UI ter za to, da se vsi sistemi UI, ki omogočajo dvojno rabo, obravnavajo skladno z Aktom o UI.

**53 % respondentov se strinja s stališčem, 37 % respondentov se ne strinja s stališčem, 9 % pa je nevtralnih.**

Pri tem respondenti opozarjajo na to, da je treba »*imeti enaka pravila (ai act) v smiselni rabi, vendar ločen nadzor, ter seveda jasno opredeliti, kaj sodi pod navedeni področji*«. En respondent meni, da je treba »*vojaško industrijo močno omejiti, kajti militarizacija UI sistemov je izjemno problematična. Prehitra implementacija znotraj vojske zna narediti nezaupanje javnosti v UI sisteme na splošno*«. Respondenti menijo, da je »*zaveza k ustreznemu upoštevanju človekovih pravic in temeljnih svoboščin preveč ohlapna. Beseda ustrezno tukaj poda preveč svobode, saj je njen pomen različen za različne ljudi in zato omogoča podlago za kršenje določenih pravic, če se to zdi “ustrezno”. Še posebno na polju nacionalne varnosti in vojaške rabe se lahko dogajajo izjeme v uporabi UI, ki ne spoštujejo človekovih pravic in temeljnih svoboščin«.*



Slika 6 Sistemsko urejanje (III) – obseg regulacije

## Urejanje na podlagi tveganja uporabe za človekove pravice in varnost

Slovenija podpira urejanje UI, ki temelji na tveganju in ne regulira vseh različnih sistemov UI na različnih področjih uporabe enako. Ob tem se zavzema za pristop, s katerim se ne regulira same tehnologije, temveč njeno uporabo v različnih kontekstih. V ta namen se jasno in transparentno opredeli hierarhijo različnih segmentov uporabe glede na potencialna tveganja ter za različne segmente opredeli ustrezne zahteve regulacije.

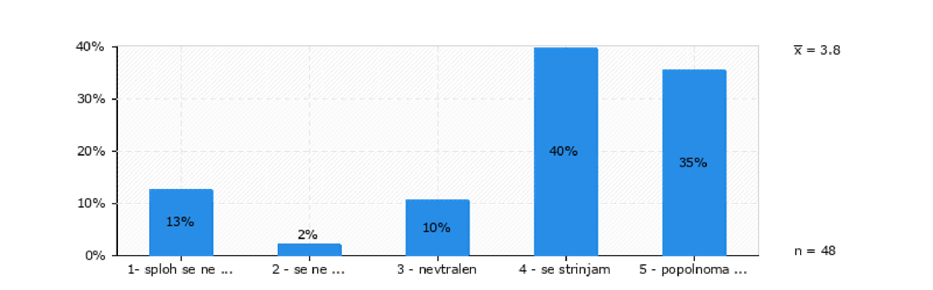
S tega vidika Slovenija opozarja in se zavzema za čim bolj jasno opredelitev kriterijev po katerih se ocenjuje stopnja tveganja, ki bi dovolj podrobno in kvalitetno razločila med različnimi scenariji uporabe, s tem pa različnimi stopnjami tveganja, ki jih slednji prinašajo.

Z vidika vrste tveganj Slovenija podpira opredelitev glavnih ciljev zagotavljanja ustreznega regulativnega režima za UI, tj. tveganje kršenja človekovih pravic in temeljnih svoboščin na eni strani ter tveganja varnosti proizvodov in storitev na drugi.

Zaradi kompleksnosti v zvezi s tem opozarjamo tudi na potrebo po zagotovitvi jasnosti in predvidljivosti zakonodaje glede odgovornosti posameznih deležnikov. Akt o UI mora zagotoviti ustrezne informacije o delovanju sistemov UI v celotni dobavni verigi, ki bi omogočale ugotavljanje, preverjanje in nadzor skladnosti delovanja sistemov UI in deležnikov z opredeljenim regulativnim okvirom ter učinkovito pravno varstvo vseh oseb, na katere sistem UI vpliva. Slovenija se bo zavzemala za tiste rešitve predloga, katerih namen je zagotoviti pravni okvir, ki bo pri razvoju in uporabi sistemov umetne inteligence zagotavljal učinkovito spoštovanje človekovih pravic in temeljnih svoboščin.

**S stališčem se strinja 75 % respondentov, 15 % respondentov se ne strinja, 10 % respondentov pa je nevtralnih.**

Glede urejanja tveganja uporabe za človekove pravice en respondent razmišlja, da je »*ključna* še *zlasti odgovornost posameznih deležnikov pravnih in fizičnih oseb in sledljivost spremembam, ki jih ti deležniki vnašajo v sistem*«.Drugi pa menijo, da mora »*tveganje biti opredeljeno s človekovimi pravicami in temeljnimi svoboščinami v središču* *in ne s strani raznolikih sektorjev (rights-based assessment instead of sector-based)*«.Prav tako jih»*izjemno skrbi trenutni pristop, ki ureja različno UI z nizkimi in visokimi tveganji.* /…/ *Opredelitev nizkih in visokih tveganj je ohlapna in omogoča izigravanje – namesto razlikovanja naj bo pristop osnovan na zaščiti človekovih pravic in temeljnih svoboščin in naj za vse rešitve predvideva enake varovalke*. /…/ *Trenutni pristop problematizira tehnologije, ampak ključna problema pri etičnosti UI rešitev sta upravljanje z njimi in nadzor*«. V povezavi s tveganji en respondent meni, da se velika tveganja »*pojavljajo z načinom uporabe UI sistemov, ne zgolj z njenim razvojem. Ta tveganja vključujejo hotena (morebitna zlonamerna) in nehotena (pomanjkanje znanja) .*«.



Slika 7 Urejanje na podlagi tveganja uporabe za človekove pravice in varnost

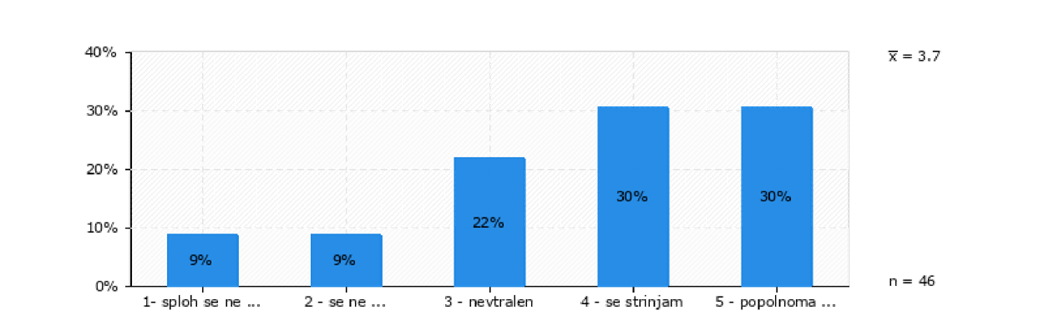
## Horizontalni pristop

Slovenija tudi nadalje podpira pripravo enotne horizontalne uredbe o UI na ravni EU, da bi tako vzpostavili koherenten temeljni okvir za bodoči razvoj in uporabo UI ne glede na različna področja ali kontekste uporabe, predvsem, ko gre za visoko tvegane sisteme UI. Slovenija podpira trenutno zasnovo Akta o UI, ki je zasnovana za urejanje dajanja proizvodov in storitev na trg in pri tem ne nadomešča obstoječe zakonodaje za različne vrste proizvodov in storitev, temveč jo dopolnjuje z vidika zahtev in pogojev tako za sisteme UI kot tudi za vse deležnike, ki pri tem nastopajo.

Z vidika obsega urejanja pa Slovenija opozarja in se zavzema tudi za ustrezno prenovitev ostale zakonodaje, ki ureja tudi druge vidike razmerij med deležniki (npr. odgovornost za proizvode z napako, civilna odgovornost, kazenska odgovornost, pravice potrošnikov itd.), ko gre za razvoj in uporabo UI in ta ni zajeta v Aktu o UI (kot npr. regulacija dajanja proizvodov in storitev na trg).

**60 % respondentov se s stališčem strinja, 18 % respondentov se ne strinja, 22 % respondentov je nevtralnih.**

En respondent razmišlja o tem, da so »*proizvodi z vgrajeno UI izjemno specifični, zato je potrebna še posebna previdnost in razmislek pri prenovi obstoječe zakonodaje. predvsem iz stališča odgovornosti, saj zajema področje UI vsaj faze načrtovanja, razvoja in uporabe. Ob vsaki stopnji so pojavljajo specifična tveganja in razmejitev odgovornosti je različna za različne deležnike. Še posebej velik izziv bo predstavljala "napačna" uporaba*«.



Slika 8 Horizontalni pristop

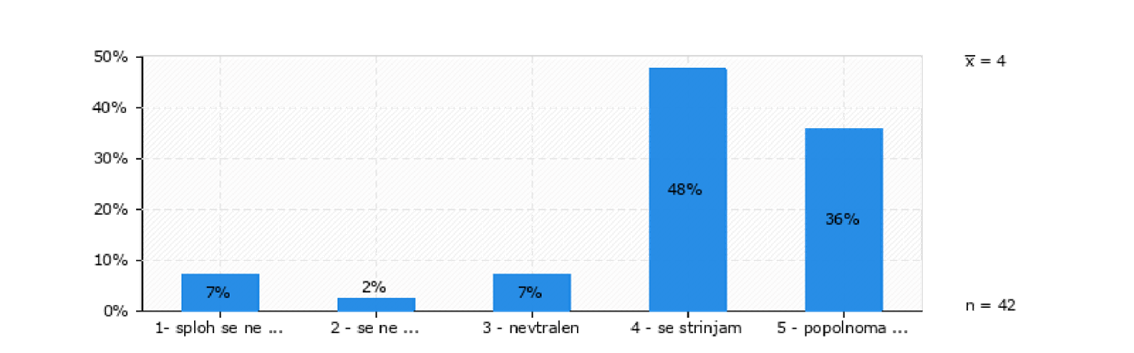
## Tehnično jasna in razumljiva definicija sistema UI (I)

Slovenija pozdravlja uporabo definicije »sistema umetne inteligence« organizacije OECD, mednarodno usklajene ter sprejete definicije sistema UI na tehnični ravni, kot osnovo za opredelitev umetne inteligence v uredbi. V zvezi s trenutno opredeljeno definicijo v Aktu o UI se Slovenija zavzema predvsem za:

* jasno definicijo sistema UI, ki bi predvsem na tehnični ravni zagotovila razumevanje predmeta regulacije za vse zadevne strani;
* jasno opredelitev obsega regulacije Akta o UI, ki ne more biti opredeljena v okviru same definicije sistema UI;
* ustrezno definicijo sistema UI, ki bi omogočila skladnost Akta o UI z drugimi mednarodnimi zakonodajnimi in drugimi dokumenti v mednarodnem okolju ter s tem njegovo široko mednarodno relevanco;
* ustrezno strukturo definicije sistema UI v aktu, ki omogoča hitro in enostavno prilagoditev na podlagi hitrega razvoja UI;
* jasen pristop k temu, da ne reguliramo tehnologije, temveč njeno uporabo.

**60 % respondentov se s stališčem strinja, 18 % respondentov se ne strinja, 22 % respondentov je nevtralnih.**

En respondent razmišlja o tem, da je potrebna »*uskladitev pravne regulacije z nadnacionalnimi in nacionalnimi tehničnimi standardi z namenom zagotovitve skladnosti in varnosti proizvodov /…/*«. Drugi opozarja, da je »*sposobnost hitrega prilagajanja zakonodaje /.../ ob hitri dinamiki razvoja UI ključnega pomena za dosledno regulacijo*«. V zvezi s tem en respondent navaja, da je pomembno, »*da se UI definira izjemno natančno in ozko, brez uporabe ohlapnih izrazov, ki omogočajo različno razumevanje, kar je pomembno predvsem za zagotovitev jasnih pravnih okvirov za zaščito človekovih pravic*«. Ob tem pa drug respondent opozarja, da bo z vidika uporabe potrebna »*dodatna pozornost na opredelitev uporabe UI, saj le-ta zajema različne deležnike in lahko se pojavlja vrsta različnih tveganj (nerazumevanje delovanja UI, napačna umestitev v poslovni proces, napačni podatki)*«.



Slika 9 Tehnično jasna in razumljiva definicija sistema UI (I)

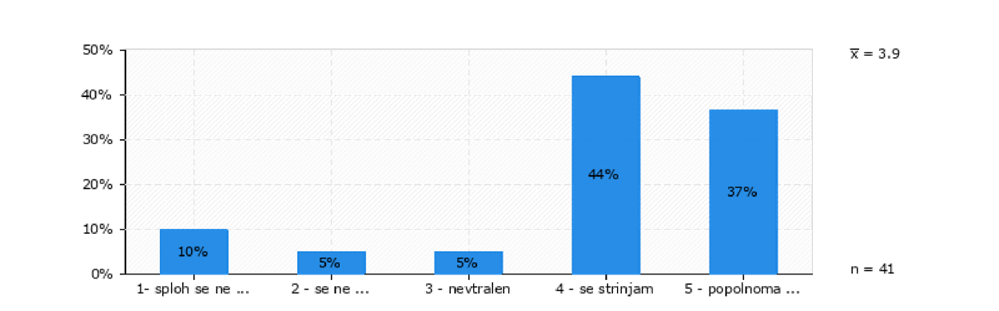
## Tehnično jasna in razumljiva definicija sistema UI (II)

Slovenija se zavzema za opredelitev sistema UI na podlagi OECD definicije, ki je povzeta tudi v NpUI, kjer za jasno ločitev sistemov UI od drugih sistemov oziroma splošne programske opreme predlaga v definiciji UI eksplicitno omembo treh bistvenih funkcionalnih značilnosti sistemov UI, tj. učenja (generiranje modela), modeliranja (preoblikovanje modela) ter sklepanja (uporaba modela).

Trenutna definicija sistema UI v Aktu o UI je omejena predvsem na uporabo strojnega učenja in pristopa temelječega na logiki in znanju, kar po našem mnenju ne zadošča, saj sistemi UI ne temeljijo le na pristopih, ki temeljijo na logiki in znanju, ampak običajno tudi na različnih drugih pristopih, kot so npr. evolucijski pristopi (npr. genetski algoritmi), hevristične metode iskanja in optimizacije, metode planiranja itd., ki torej pravno ne bi bili regulirani kot UI, čeprav jih običajno tja razvrščamo.

**S stališčem se strinja 81 % respondentov, 15 % respondentov se ne strinja, 5 % respondentov je nevtralnih.**

En respondent meni, da je ključno vprašanje definicije, da »*UI sistemi delujejo statistično, kar pomeni, da obstaja bias*«, drugi glede definicije opozarja, da je »*strojno učenje podmnožica UI*«. Drugi respondent opozarja na to, da se področja UI s časom razvijajo, in meni, da *»že če pogledamo zgodovinsko rabo termina, opazimo, da je v preteklosti opisoval stvari, ki jih danes ne bi klasificirali kot UI*«.Omenja, da»*mora biti definicija široka, predvsem pa odprta, da bo lahko regulirala nove pristope pod novimi imeni, ki bodo zagotovo prišli. Vseeno je pomembno, da se izrazi, ki so uporabljeni v definiciji, dobro premislijo in so nedvoumni, da ne dopuščajo različnih razumevanj, v izogib tveganjem za zaščito človekovih pravic*«.V zvezi s širino definicije drugi respondent opozarja, da»*razširitev pojma vodi do pretirane regulacije in birokracije*«*.*



Slika 10 Tehnično jasna in razumljiva definicija sistema UI (II)

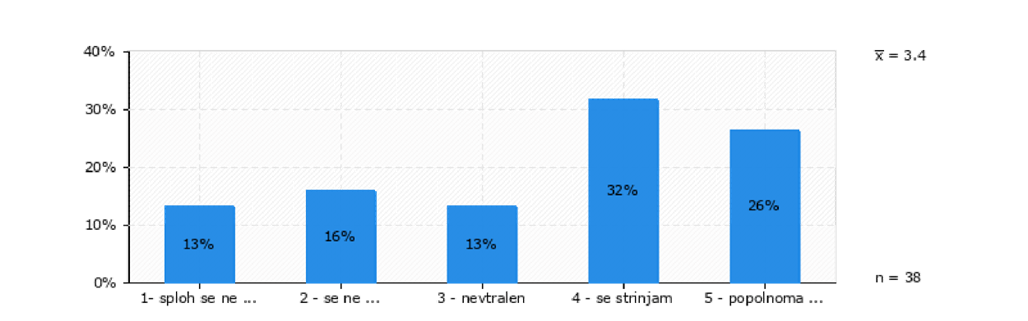
## Tehnično jasna in razumljiva definicija sistema UI (III)

Slovenija ne podpira stališča, da se sistem, ki za samodejno izvajanje operacij uporablja pravila, ki jih opredelijo izključno fizične osebe, ne bi smel šteti za sistem UI. Menimo namreč, da ti vseeno predstavljajo sisteme UI (npr. ekspertni sistemi), čeprav jih morda ne želimo regulirati. V zvezi s tem predlagamo, da se tovrstne vidike opredeli v obsegu regulacije in ne v sami definiciji.

Zaradi večje fleksibilnosti Slovenija zagovarja prvotni predlog določitve pristopov in tehnik za implementacijo omenjenih treh funkcionalnosti in samo v povezavi z njimi, ne samo v recitalih, temveč tudi na način, da bi jih lahko v prvih letih uporabe uredbe lažje dopolnili glede na stanje tehnike (npr. v prilogi, kot je bilo prvotno predvideno).

**S stališčem se strinja 58 % respondentov, 29 % respondentov se ne strinja, 13 % je nevtralnih.**

Komentarji se precej razlikujejo, pri čemer en respondent meni, da pomeni UI le »*uporabo strojnega učenja*«, drugi pa podpirajo vključitev sistemov, ki uporabljajo pravila: »*absolutno se strinjam, kajti ravno avtonomni sistemi lahko sodijo med najbolj tvegane, podpiram prvotni predlo*g«.



Slika 11 Tehnično jasna in razumljiva definicija sistema UI (III)

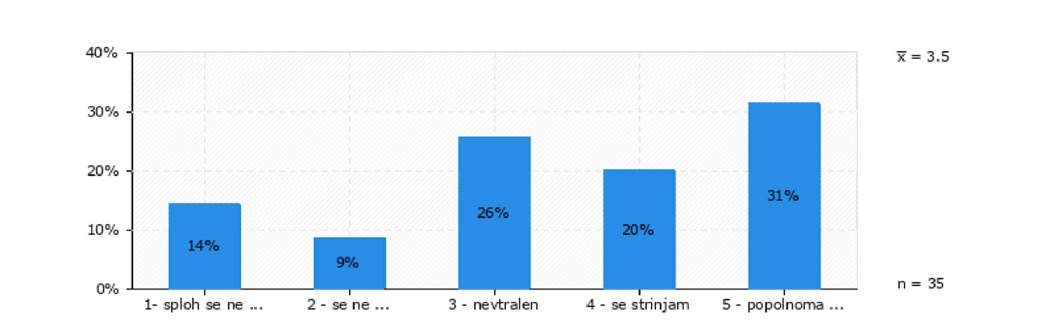
## Ureditev regulacije Umetne inteligence splošnega namena

Slovenija se v Aktu za UI zavzema za jasno definicijo umetne inteligence splošnega pomena (UISP) kot posebne vrste sistemov UI, ki potrebujejo posebno obravnavo, saj gre za sisteme, ki nimajo vnaprej določenega »predvidenega namena« uporabe (intended purpose). Ti sistemi lahko opravljajo splošno uporabne funkcije, kot so prepoznavanje slike/govora, ustvarjanje zvočnih ali video vsebin, odkrivanje vzorcev, odgovarjanje na vprašanja, prevajanje in drugo. Lahko se uporabijo v zelo različnih kontekstih in področjih ter integrirajo v okviru različnih drugih sistemih UI.

Glede na to, da osnovni koncept akta temelji na predvidenem namenu uporabe, v skladu s čimer so urejeni tudi pogoji in obveznosti sistema UI samega kot tudi pravice in dolžnosti posameznih deležnikov, se Slovenija strinja z izključitvijo UISP iz regulacije do trenutka, ko se UISP dejansko da na trg (samostojno ali v okviru drugih sistemov UI) ali uporabi v konkretnem primeru. V tem trenutku mora tovrstni sistem postati predmet regulacije, ne glede na to ali predstavlja oziroma se uporablja v okviru UI visokega tveganja ali ne.

**S stališčem se strinja 51 % respondentov, 23 % respondentov se ne strinja, 26 % respondentov je nevtralnih.**

En respondent trdi, da je treba regulirati »*le tisto, kar je absolutno nujno. Širjenje področja regulacije na zalogo je škodljivo za družbo in za gospodarstvo*«. Drugemu respondentu se to zdi problematična regulacije UISP z vidika odprte kode, saj »*če imaš UI knjižnico, ki jo nekdo uporabi v svojem produktu in da na trg, zakaj bi UI knjižnica postala predmet regulacije?*«. Tretji respondent se sprašuje o ustreznosti trenutne definicije UISP z vidika »*ali GPT-4 recimo dosega merila za UISP?*«,in meni, da mora bitidefinicija UISP»*bolj jasna*«.



Slika 12 Ureditev regulacije umetne inteligence splošnega namena

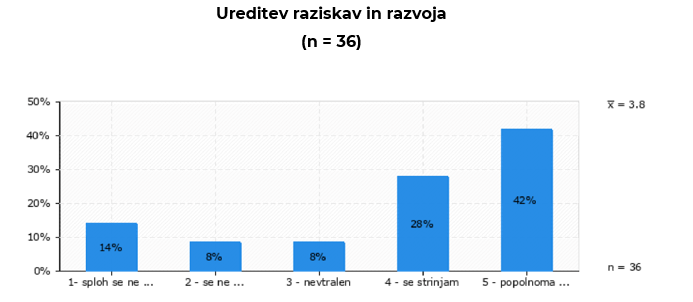
## Ureditev raziskav in razvoja

Raziskave in razvoj sta ključni področji, ki omogočata iskanje in reševanje vedno novih problemov, ki se bodo pojavljali v povezavi z razvojem, uvajanjem in uporabo UI v družbi. Raziskovalno-razvojna dejavnost ponuja nove modele, algoritme in rešitve UI ter z njimi povezane izzive, ki z drugimi področji znanosti odstirajo neznano in zato omogočajo razumevanje tako pozitivnih kot tudi negativnih učinkov, ki jih UI povzroča.

V skladu s tem Slovenija podpira izključitev raziskovalno-razvojne dejavnosti iz obsega regulacije Akta o UI skupaj s sistemi UI, ki se uporabljajo izključno za raziskave in razvoj. Te izjeme pa Slovenija podpira le pod pogojem, da se raziskovalno-razvojna dejavnost izvaja v skladu s priznanimi etičnimi in strokovnimi standardi za znanstvene raziskave.

**S stališčem se strinja 70 % respondentov, 22 % respondentov se ne strinja, 8 % respondentov je nevtralnih.**

En respondent glede podpore izjeme za RR-dejavnost pod pogojem, da se ta izvaja s priznanimi etičnimi in strokovnimi standardi, opozarja, da se bo to »*zelo težko argumentiralo oz. dokazovalo*«.Drugi respondent glede izjeme svari, da se vedno »*pojavljajo potrebe, da se določen segment raziskav izloči s polja transparentnosti in s tem povzročajo škodo UI tudi tam, kjer ima pozitivne pridobitve za ljudi*«. Tretji respondent predlaga, da je »*potrebno tudi dopolniti ustrezne univerzitetne izobraževalne programe za bodoče UI raziskovalce z ustreznimi vsebinami (etični in strokovni standardi) – sedaj tega namreč ni*«*.*



Slika 13 Ureditev raziskav in razvoja

## Prilagodljivost regulacije hitremu razvoju in inovacijam

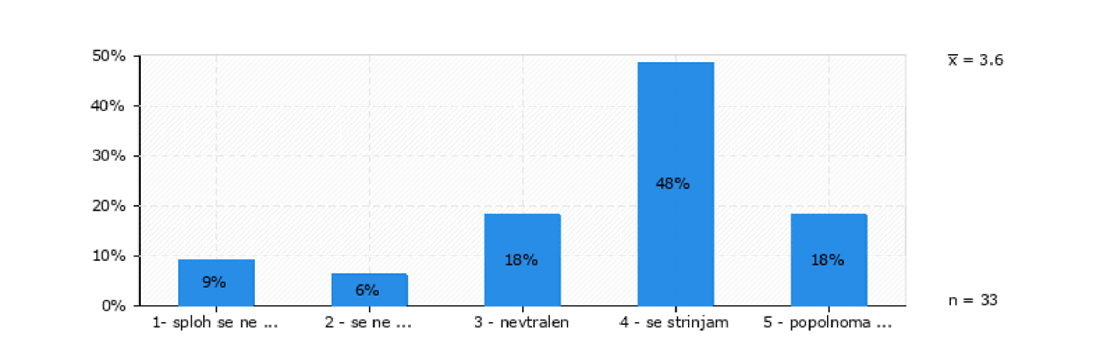
Slovenija podpira odprto in prilagodljivo ureditev, ki bi omogočala prilagajanje hitremu razvoju in rešitvam UI ter podporo okolju za spodbujanje inovacij prihodnjega razvoja umetne inteligence, zlasti s strani malih in srednih podjetij (MSP).

V tem smislu Slovenija podpira vzpostavitev regulativnih peskovnikov, ki omogočajo izdelavo in preverjanje skladnosti prototipov v realnih tržnih nadzorovanih okoliščinah že v zgodnjih fazah razvoja. Prav tako Slovenija podpira možnost razvoja in testiranja sistemov UI visokega tveganja izven peskovnikov, če je to v skladu z opredeljenimi pogoji, kot jih določa uredba, vendar meni, da je pri tem izjema za organe javne varnosti glede potrebe po pridobitvi informirane privolitve oseb, ki so vključene v testiranje, preohlapno določena in potrebuje jasnejšo opredelitev.

Slovenija se zavzema, da so regulativni peskovniki prednostno dostopni ne samo mikro podjetjem, temveč tudi MSP. Hkrati Slovenija za MSP podpira izjemo za ponudnike sistemov UI v povezavi z vzpostavitvijo in uporabo sistemov za upravljanje kvalitete ali zahtev za UISP.

**S stališčem se strinja 66 % respondentov, 15 % respondentov se ne strinja, 18 % respondentov je nevtralnih.**

En respondent meni, da se »*testiranje sistemov UI visokega tveganja izven peskovnikov sliši kot katastrofalna ideja, še posebej, ko pride do organov javne varnosti. Tam bi veljalo tovrstno rabo čim bolj zamejiti, če ne celo prepovedati, saj že imamo izkušnje tako v Evropi kot drugje po svetu, kjer raba UI v organih javne varnosti praktično ni imela pozitivnih posledic*«.Drugi respondent pa je bolj skeptičen do izvedljivosti, saj meni, da so »*regulatorni peskovniki sicer lepo zamišljeni*«,vendar dvomi,»*da bodo peskovniki dejansko delovali v praksi*«, ter predlaga »*vzpostavitev ustrezne podpore, ki bo zagotavljala razvoj in uporabo UI z ustreznimi standardi. Ta pravila sedaj namreč niso popolnoma jasna (se še razvijajo), vendar bi lahko nek takšen draft zagotovili tudi že sedaj (preko morda EDIH, ali kakšnega drugega servisa)*«.



Slika 14 Prilagodljivost regulacije hitremu razvoju in inovacijam

## Jasna in podrobnejša opredelitev kriterijev visokega tveganja

Slovenija se zavzema za jasno opredelitev meril za določitev primerov uporabe UI, ki potrebujejo strožje vrednotenje in nadzor, tj. visoko tvegane umetne inteligence, ter v tem kontekstu jasno definicijo kategorij metod umetne inteligence, ki jih uredba dejansko zajema, kar mora biti posebej izraženo v kriterijih za opredelitev visoko tvegane UI.

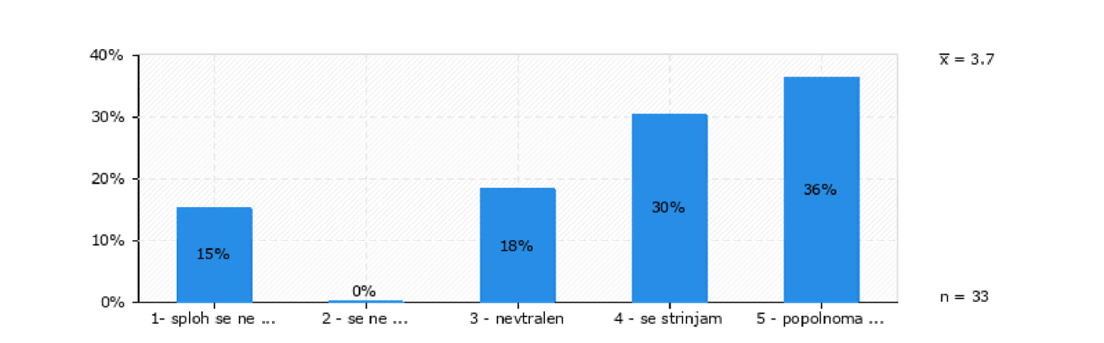
Trenutni kriteriji za oceno tveganja v Aktu o UI pa po mnenju Slovenije ne zmorejo opisati vseh vidikov uporabe sistemov UI na dovolj podrobni ravni in zato ne omogočajo, da bi se regulacija ustrezno prilagajala stvarnosti realnega sveta. Ključno je, da metoda za ocenjevanje tveganj, ki jo predvideva Akt o UI, omogoča odslikavanje dejanskega stanja in slednjega ne generalizira več, kot je treba.

Slovenija zato podpira uporabo klasifikacijskega okvira za sisteme UI, ki ga je pripravil OECD. Ta okvir podrobno opredeljuje tako značilnosti sistema UI samega kot tudi okolje in vpliv nanj, segmentirane v pet kategorij:

* vpliv na ljudi in planet,
* ekonomski kontekst,
* značilnost podatkov in vhodnih navodil, na podlagi katerih sistem UI vzpostavlja model zunanjega okolja, v katerem deluje,
* uporabljen model UI za predstavitev zunanjega okolja ter
* vrsto nalog in rezultatov, ki jih sistem producira.

**S stališčem se strinja 66 % respondentov, 15 % respondentov se ne strinja, 18 % respondentov je nevtralnih.**

En respondent se strinja s predlogom in glede kriterijev opozarja, da »*trenuten predlog akta ni ustrezen, zato ga je potrebno izboljšati*«.Drugi respondent potrjuje že prej izraženo mnenje, da se načeloma »*ne strinjamo z razlikovanjem med rešitvami z nizkim in visokim tveganjem in ponavljamo pomislek glede razlikovanja. Naj bo pristop osnovan na zaščiti človekovih pravic in temeljnih svoboščin in naj za vse rešitve predvideva enake varovalke*«, ter se glede tega naslanja »*na priporočila, ki jih je pripravil EDRI (European digital rights network)*«, saj meni, da je opredelitev kriterijev visokega tveganja»*poenostavljena in zaradi tega omogoča izjeme*«.



Slika 15 Jasna in podrobnejša opredelitev kriterijev visokega tveganja

## Metodologija opredelitve sistemov UI visokega tveganja (I)

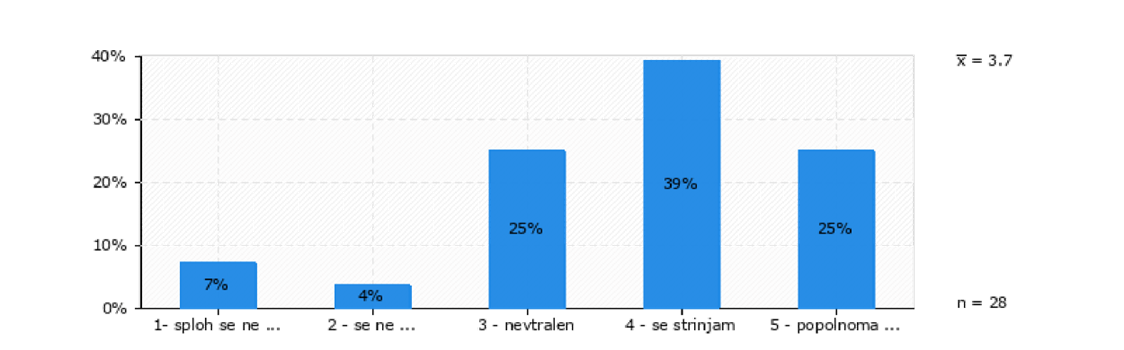
Slovenija zaradi jasnosti, enostavnosti in pravne predvidljivosti, podpira metodologijo določanja področij in sistemov UI visokega tveganja, kot je zasnovana v Aktu o UI, kjer se za samostojne sisteme UI določajo področja in sistemi UI, ki predstavljajo visoko tveganje. Področja so opredeljena v Prilogi III.

Vendar pri tem opozarja, da slednje lahko pripelje do pretiranega generaliziranja in s tem problema prilagajanja konkretnim okoliščinam uporabe sistemov UI v posameznih realnih kontekstih, kjer se lahko tudi povsem netvegana uporaba šteje za visoko tvegano in obratno. Slednje lahko zmanjšuje interes za uvajanje UI na določenih področjih opredeljenih kot visoko tvegana, čeprav to glede na dejanska tveganja morebiti ne bi bilo smiselno.

Za zagotavljanje zaupanja javnosti je potrebno zagotoviti čim boljše prilagajanje realnim okoliščinam, zato Slovenija podpira zadnji kompromisni predlog Akta o UI, ki v dvostopenjski sistem opredelitve področij in sistemov UI visokega tveganja v Prilogi III dodaja dodaten kriterij. Ta preverja, ali je rezultat sistema UI v razmerju do zadevnega ukrepa ali odločitve, ki jo je treba sprejeti, zgolj pomožen, in zato ni verjetnosti, da bi vodil v pomembno tveganje za zdravje, varnost ali temeljne pravice.

**S stališčem se strinja 66 % respondentov, 13 % respondentov se ne strinja, 20 % respondentov je nevtralnih.**

Respondenti pravijo: »*Se strinjam z dvostopenjsko ureditvijo: s krovno generalno ureditvijo regulacije in subsidiarno segmentno po področjih (z lastnimi specifikami), kot to navaja zakonodajalec v predlogu,*« in opozarjajo na previdnost, saj »*raziskave kažejo na človeško pristranskost, kjer strojnim odločitvam zaupamo veliko bolj, kot bi bilo treba.*« Drugi respondent nasprotno meni, da »*trenutna opredelitev ni najboljša, saj je preveč generična in usmerjena bolj na domenska področja*«.



Slika 16 Metodologija opredelitve sistemov UI visokega tveganja (I)

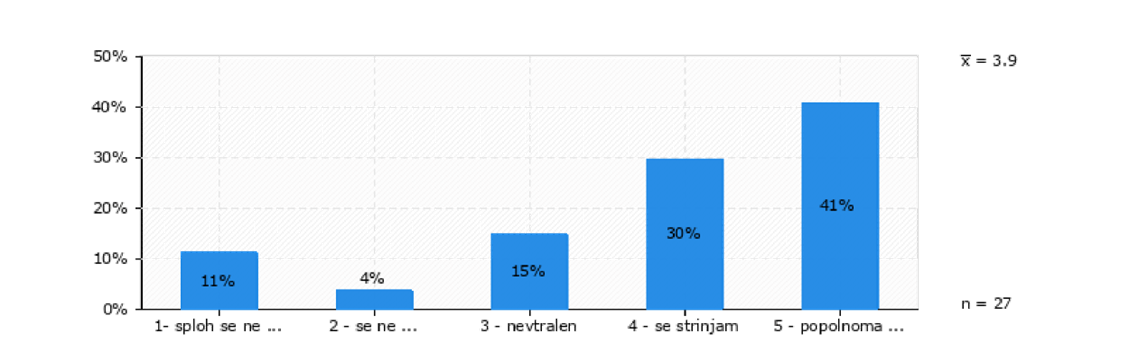
## Metodologija opredelitve sistemov UI visokega tveganja (II)

Slovenija podpira zadnji kompromisni predlog Akta o UI, ki v dvostopenjski sistem opredelitve področij in sistemov UI visokega tveganja v Prilogi III dodaja dodaten kriterij o razmerju sistema UI do zadevnega ukrepa ali odločitve.

Vendar pa Slovenija meni, da to ni dovolj. Zato predlaga, da se za vsako področje in sisteme UI visokega tveganja, glede na to, da so pri vsakem od področij za oceno tveganja lahko relevantne povsem različne okoliščine uporabe, ne samo vprašanje pomožnosti rezultata, posebej pripravi jasen in enostaven odločitveni sistem za opredelitev okoliščin, ki prinašajo visoko tveganje. V tem kontekstu Slovenija opozarja, da je za opredelitev teh okoliščin treba uporabiti kriterije, ki bolj kompleksno in celovito opisujejo same sisteme UI in kontekst njihove uporabe, kar se nanaša na že omenjeni predlog, da se za to uporabi klasifikacijski okvir OECD.

**S stališčem se strinja 64 % respondentov, 11 % respondentov se ne strinja, 25 % respondentov je nevtralnih.**

Respondent opozarja, da naj »*merila za presojo stopnje ocene tveganj po našem predlogu temeljijo izključno na vsebini. V nasprotnem primeru bi tvegali diskrepanco med podano oceno in "de facto" vsebinsko presojo, ki sta lahko ali pa tudi nista skladni*«. Drugi respondenti menijo, da »*mora biti pri opredelitvi kriterijev primarni rights-based approach.*«. En respondent opozarja, da je »*v definicijo najbolj tveganih UI sistemov je potrebno dodati način uporabe in dodati presojo učinkov ter nadzor nad uporabo dovolj frekventno.*«.



Slika 17 Metodologija opredelitve sistemov UI visokega tveganja (II)

## Razložljivost in avtonomnost UI

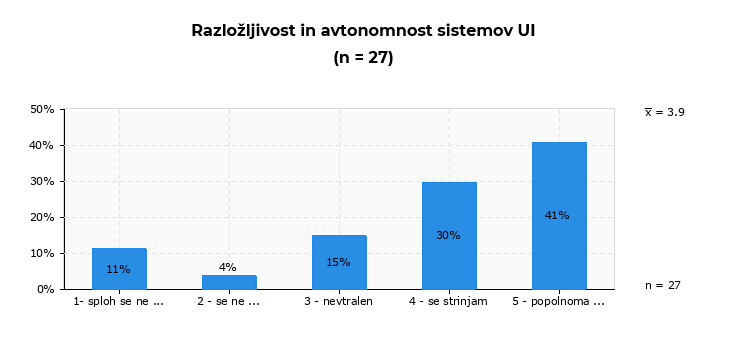
Slovenija se zavzema za obravnavo problema razložljivosti različnih modelov in algoritmov UI.

To je ključnega pomena v posebnih okoliščinah uporabe UI, kjer so obrazložitve odločitev sistemov UI ključni pravni in tehnični predpogoj za uporabo rezultatov sistemov UI v določenih področjih uporabe, kot je na primer uporaba UI v postopkih odločanja v pravosodju ali upravnih organih, posebej v primerih, ko gre za avtomatizirane postopke odločanja.

Slednje v Aktu o UI trenutno ni posebej izpostavljeno, razen v kolikor je obravnavano v okviru sistemov UI visokega tveganja v pravosodju (področje pravosodja in demokratičnih procesov v Prilogi III). Slovenija se zato zavzema, da na področju pravosodja, še posebej sistemi UI visokega tveganja, ne delujejo avtonomno brez človeškega nadzora in da človek vedno sprejema sodne odločitve.

**S stališčem se strinja 71 % respondentov, 15 % respondentov se ne strinja, 15 % respondentov je nevtralnih.**

Do stališča je kritičen respondent, ki pravi, da »*kriterij razložljivosti nikakor ne sme biti pogoj za uporabo UI. To bi povsem zatrlo evropsko UI industrijo, zmanjšalo število inovacij in zmanjšalo koristi državljanom. hkrati bi tak kriterij povzročil še nadaljnjo monopolizacijo ponudbe UI le na največja podjetja, saj je tak dodaten regulatorni pogoj izjemno drag za podjetje*«. Drugi predlagajo, da je rabo UI na področju pravosodja »*na splošno treba omejiti*« oziroma opozarjajo, da uporaba UI lahko pomeni »*neupravičen poseg v avtonomnost uradnikov in sodnikov, zlasti če gre za prikrito objektivno psihološko okužbo s predlogom odločitve in bi kot taka povzročila pristranskost v postopku, kar je nedopustno,* *zato predlagamo da zakonodajalec jasno poda primere, v katerih se pravosodni ali upravni organi lahko zgolj utemeljeno in obrazloženo poslužujejo zgoraj navedenih tehnologij, z namenom da jih ne bi zlorabljali in uporabljali "per se" brez lastnega intelektualnega inputa, kar bi lahko predstavljalo potencialno bistveno kršitev pravic strank v postopku*«, ter menijo, da morajo tovrstni sistemi »*delovati kot orodje/podpora človeškim odločitvam (nikakor ne avtonomno)*«, ob tem pa opozarjajo, da slednje ne velja le za pravosodje temveč, da so »*takšni primeri tudi v bančništvu in kakršnem koli razvrščanju, ki ima lahko znatne finančne ali druge škodljive posledice*«.



Slika 18 Razložljivost in avtonomnost UI

## Javna varnost

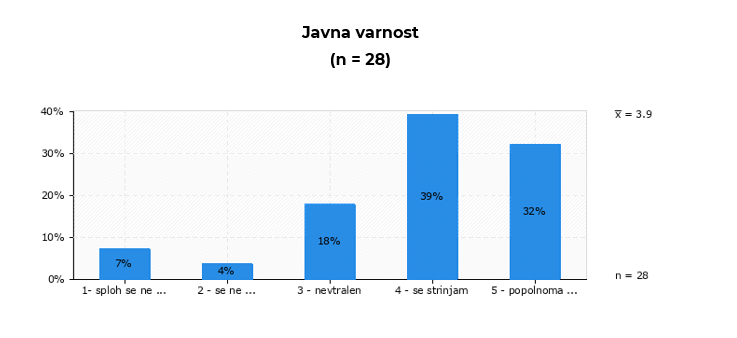
Slovenija meni, da je posebno pozornost treba posvetiti uspešni in učinkoviti uporabi sistemov UI za zagotavljanje javne varnosti. Brez uporabe novih tehnologij, kot je UI, se bo nivo zagotavljanja javne varnosti znižal. To velja tudi z vidika preprečevanja kaznive uporabe sistemov umetne inteligence, ki se predvsem z generativnimi modeli umetne inteligence vse bolj pojavlja na zelo raznolikih področij (npr. informacijska varnost, mediji, socialna omrežja, nezaželene vsebine, sovražni govor itd.).

V skladu z nacionalnim programom NpUI se Slovenija zavzema, da mora uporaba UI na področju javne varnosti odražati evropske vrednote in načela ter vedno podpirati in zagotavljati spoštovanje človekovih pravic in temeljnih svoboščin.

Slovenija se zavzema, da so sistemi UI za razpoznavanje globokih ponaredkov na področju organov javne varnosti v Prilogi III opredeljeni kot sistemi UI visokega tveganja, ko gre za preverjanje in ali dokazovanje avtentičnosti in resničnosti (authenticity and truthfulness).

**S stališčem se strinja 71 % respondentov, 11% respondentov se ne strinja, 18 % respondentov je nevtralnih.**

Respondenti utemeljujejo sledeče: »*Strinjamo se s tem, da je za boj proti škodljivi rabi umetne inteligence potrebno poznavanje in uporaba umetne inteligence (“to velja tudi z vidika preprečevanja kaznive uporabe sistemov umetne inteligence, ki se predvsem z generativnimi modeli umetne inteligence vse bolj pojavlja na zelo raznolikih področjih (npr. informacijska varnost, mediji, socialna omrežja, nezaželene vsebine, sovražni govor itd.)”), ne strinjamo pa se s tem, da je uporaba UI nujna (oziroma ključna) za zagotavljanje javne varnosti«.* Drugi pa se strinjajo *»/…/ z navedenim ob predpostavki spoštovanja temeljnih postulatov in ustavnih pravic demokratične družbe, zlasti z ozirom na pravico do svobode govora, mišljenja, izražanja vesti veri, izobraževanja, zbiranja in združevanja ob predpostavki spoštovanja enke mere pravic in človekovega dostojanstva ostalih. Skrbi nas zloraba terminov iz navedka: "to velja tudi z vidika preprečevanja kaznive uporabe sistemov umetne inteligence, ki se predvsem z generativnimi modeli umetne inteligence vse bolj pojavlja na zelo raznolikih področij (npr. informacijska varnost, mediji, socialna omrežja, nezaželene vsebine, sovražni govor itd.)" za druge prikrite namene. Navedeni termini so pomensko odprti in to predstavlja potencial za zlorabo z zasledovanjem drugih prikritih namenov pod pretvezo zagotavljanja javne varnosti, kar zaradi nejasne postopkovne definiranosti ni legitimno z vidika vrednot demokratične in pluralne družbe«*.



Slika 19 Javna varnost

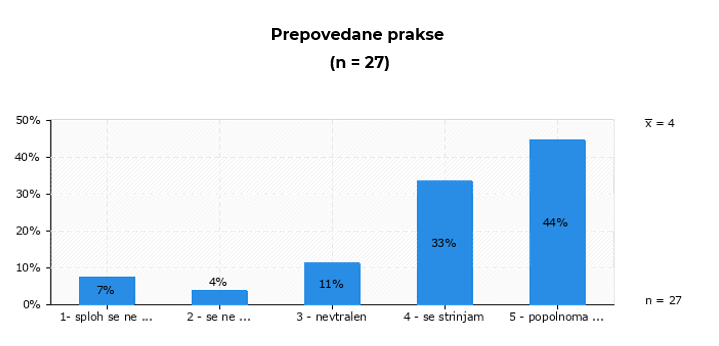
## Prepovedane prakse

Slovenija se strinja s predlogom prepovedanih praks uporabe sistemov UI. V zvezi z oddaljeno biometrično identifikacijo na javnih mestih v realnem času, se poleg prepovedi izvajanja teh aktivnosti s strani organov javne varnosti, kjer se to lahko izvaja le pod striktnimi pogoji, ki so opredeljeni v Aktu o UI, zavzema tudi za prepoved izvajanja teh aktivnosti s strani zasebnega sektorja. Prav tako se Slovenija zavzema za omejitev socialnega rangiranja, kot je opredeljena v uredbi, ne samo na javni sektor, temveč tudi na zasebnega.

Glede prepovedi sistemov UI, ki izkoriščajo katere koli šibke točke določene skupine oseb, se Slovenija zavzema za to, da slednje poleg skupin oseb na osnovi njihove starosti in invalidnosti vključuje tudi skupine oseb na osnovi njihovega posebnega socialnega ali ekonomskega položaja.

**S stališčem se strinja 77 % respondentov, 11 % respondentov se ne strinja, 11 % respondentov je nevtralnih.**

En respondent razmišlja, da je »*predlog prepovedanih praks izjemno pomanjkljiv*«, in se ne strinja z »*izjemami za izvajanje biometrične identifikacije na javnih mestih v realnem času s strani organov javne varnosti*« ter meni, da je v skladu s predlogi organizacije EDRI gledetega»*v uredbo v člen 5 treba dodati več prepovedanih praks: 1) uporaba zasebnih sistemov za prepoznavo obrazov ali drugih zasebnih zbirk biometričnih podatkov za uporabo s strani javnih organov, 2) ustvarjanje ali razširitev prepoznavanja obraza ali drugih biometričnih zbirk podatkov z neciljanim ali posplošenim “scrapingom” biometričnih podatkov iz družbenomedijskih profilov ali posnetkov CCTV ali drugih enakovrednih metod*«.Glede prepovedi sistemov UI, ki izkoriščajo katere koli šibke točke določene skupine oseb, v skladu s skupno izjavo evropskih nevladnih organizacij, kjer sodeluje tudi sam, meni, da »*je treba poleg starosti, invalidnosti, socialnega in ekonomskega položaja dodati tudi migracijski status (torej prepovedati migracijski nadzor)*«.



Slika 20 Prepovedane prakse

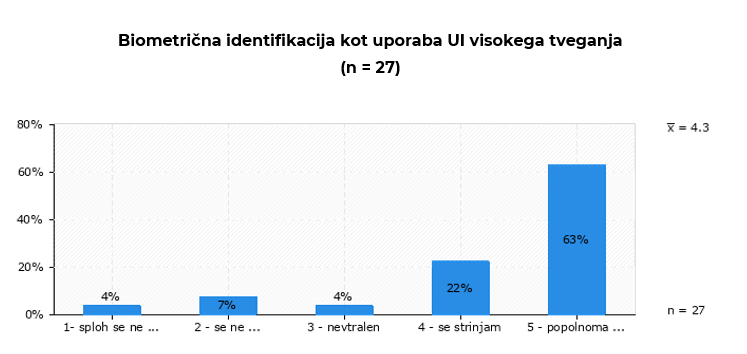
## Biometrična identifikacija kot uporaba UI visokega tveganja

Slovenija se zavzema, da bi kot UI visokega tveganja poleg oddaljene biometrične identifikacije opredelili tudi bližnjo. Primer tega je uporaba identifikacije z uporabo naprav, ki se uporabljajo s stikom osebe oziroma "na bližino", pri čemer ne gre samo za prepoznavo obrazov, temveč tudi vseh drugih biometričnih znakov, kot so delovanje srca, prepoznava prstnih odtisov itd.

Slovenija meni, da bi morali biti vsi sistemi biometrične identifikacije, ki se uporabljajo brez dogovora z osebo, ki je predmet identifikacije, opredeljeni kot UI visokega tveganja.

**S stališčem se strinja 85 % respondentov, 11 % respondentov se ne strinja, 4 % respondentov je nevtralnih.**

Respondent meni, da je v skladu s predlogi organizacije EDRI »*potrebno izboljšanje definicije oddaljene biometrične identifikacije*« in pri tem opozarja, da »*se oddaljeni biometrični nadzor nanaša na to, kako je sistem zasnovan in nameščen, in ne samo na to, ali so posamezniki, na katere se nanašajo osebni podatki, privolili v nadzor ali ne, se ta opredelitev uporablja tudi, če so opozorila nameščena na lokaciji, ki je pod nadzorom sistema oddaljenega biometričnega nadzora, saj strinjanje ni eksplicitno. Znak na ulici ne predvideva strinjanja.*«.



Slika 21 Biometrična identifikacija kot uporaba UI visokega tveganja

## Učinkovit upravljavski okvir

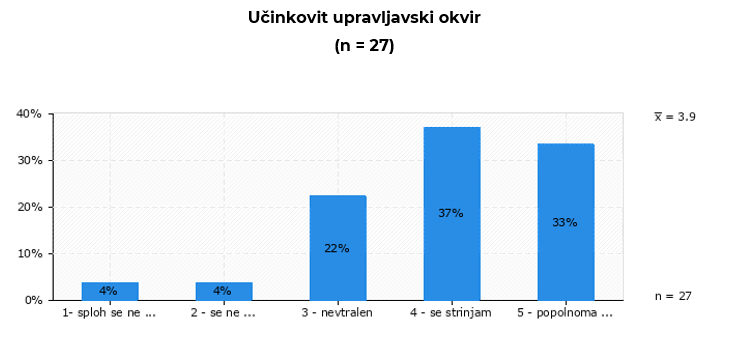
Slovenija spodbuja uporabo obstoječega sistema za preverjanje skladnosti delovanja sistemov UI, kar vključuje sisteme za akreditacijo, certifikacijo in nadzor, predvsem pa tudi na nacionalni ravni. Vendar se strinja s predlogi, da je treba zagotoviti enotno obravnavo sistemov UI na celotnem področju EU, kar zahteva intenzivno sodelovanje tako med državami EU kot tudi med državo in Evropsko komisijo.

Zato podpira vlogo Evropskega odbora za umetno inteligenco, ki ga sestavljajo predstavniki držav članic in Komisije in bo prispeval k učinkovitemu sodelovanju nacionalnih nadzornih organov in Komisije. Menimo, da ima ključno vlogo predvsem takrat, ko gre za čezmejne preiskave nadzora trga, tudi v zvezi s pojavom sistemskih tveganj, ki lahko izhajajo iz uporabe posameznih sistemov UI.

Slovenija pri tem izpostavlja problematiko kapacitet in znanja na področju UI potrebnega za izvajanje nadzornih funkcij, aktivnosti preverjanja skladnosti in sledenja razvoju stanja tehnike na področju UI. Podpira predloge, ki bi zagotavljali stabilen in dolgoročen upravljavski okvir za celotno EU.

**S stališčem se strinja 70 % respondentov, 8% respondentov se ne strinja, 22 % respondentov je nevtralnih.**

Respondenti menijo, da je potreben »*/.../ jasen model nadzora in regulacije. V vašem stališču manjka poudarek, da se potrebuje tudi nadzor javnosti in civilne družbe. Ta nadzor je treba vključiti v izhodiščni sistem. Obenem je ključnega pomena tudi transparentnost implementacije, ki naj bo zagotovljena z javnimi dostopnimi informacijami in bazami o uporabi UI*« ter da je »*poleg zagotavljanja ustreznih kompetenc nadzornih organov potrebno in celo nujno zagotoviti tudi ustrezen proces, ki vključuje redno preverjanje oz. nadzor*«.



Slika 22 Učinkovit upravljavski okvir

## Učinkovito pravno varstvo

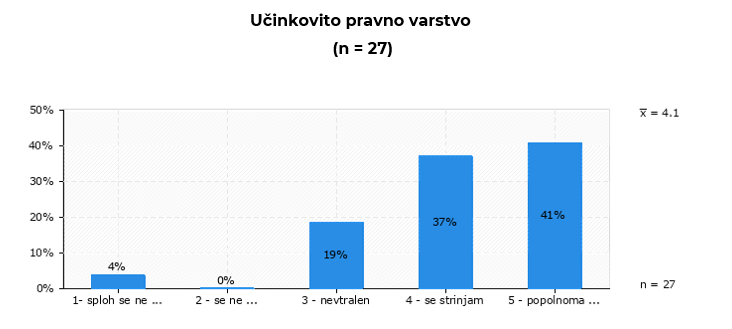
Slovenija se zavzema za zagotovitev učinkovitega pravnega varstva oseb, na katere učinkuje sistem UI, saj meni, da trenutna verzija Akta o UI ne zagotavlja vseh pogojev, ki jih za to potrebujejo osebe, na katere vpliva delovanje UI sistema (tretje osebe).

Slovenija meni, da bi morala uredba zagotoviti ustrezen pretok informacij od ponudnika do uporabnika in od uporabnika do tretjih oseb (kot prizadetih oseb), tako da bi lahko uporabnik ali potrošnik oziroma tretje osebe imeli vse potrebne informacije za poročanje o težavah s sistemom UI. S tem bi imeli možnosti pridobitve ustrezne rešitve in zagotovljeno pravico do učinkovitega pravnega varstva.

Da bi zagotovili pravilno uporabo sistema UI, mora ponudnik v tehnični dokumentaciji, kot jo opisuje Priloga IV, zagotoviti ustrezne informacije, tudi v zvezi s tretjimi osebami, ki jih uporaba sistema UI zadeva. Uporabnik mora te informacije pridobiti od ponudnika, kar vključuje tako način interakcije sistema UI z okoljem kot tudi to, kako varno uporabljati sistem UI zase in za tretje osebe (ob upoštevanju tako predvidenega namena kot tudi razumno predvidljive napačne uporabe). Bistveno je, da ima uporabnik določene informacije, ki jih lahko pridobi le od ponudnika, kar vključuje predvsem predvidljive okoliščine ter delovanje in natančnost sistema UI, ki bi lahko povzročile tveganje za zdravje in varnost ali temeljne pravice in svoboščine njega ali tretjih oseb. To je ključno za obveznost uporabnika, da o delovanju sistema UI ustrezno obvesti tudi tretje osebe, kadar so bile morda kršene varnost, zdravje ter človekove pravice in temeljne svoboščine teh oseb, da le-ti lahko začnejo preiskavo ali aktivnosti za popravo sprejetih odločitev.

**S stališčem se strinja 78 % respondentov, 4 % respondentov se ne strinja, 19 % respondentov je nevtralnih.**

Respondent poziva »*odločevalce za dopolnitev in zagotovitev več procesno-postopkovnih jamstev v postopku, da o delovanju sistema UI ustrezno obvesti tudi tretje osebe, kadar so bile morda kršene varnost, zdravje ter človekove pravice in temeljne svoboščine teh oseb, da le-ti lahko začnejo preiskavo ali aktivnosti za popravo sprejetih odločitev*«.Meni, da je »*definicija "tretjih oseb" namreč v zgornjem tretjem odstavku presplošna in nejasna*«, zato odgovorne pozivam*, »da se termin jasno in nedvoumno definira, z namenom preprečitve zlorab in neupravičenega širjenja pristojnosti in zlorab le-teh z namenom pridobitve podatkov (zlasti osebnih) in njihovega posredovanja tretjim osebam, ki bodisi so, bodisi niso, upravičeni prejemniki, obdelovalci ali hranitelji osebnih ali metapodatkov drugih oseb (tveganje prekomerne širitve pristojnosti na tretje osebe in dostop do podatkov drugih oseb)*«. Drugi respondent med drugim meni, da »*bi bilo treba prilogo 4 dopolniti in prečistiti. Predvsem manjkajo izjemno pomembna poročila o prepoznanih biasih vhodnih podatkov ter njihovo propagiranje skozi življenje cikla UI sistema*«.



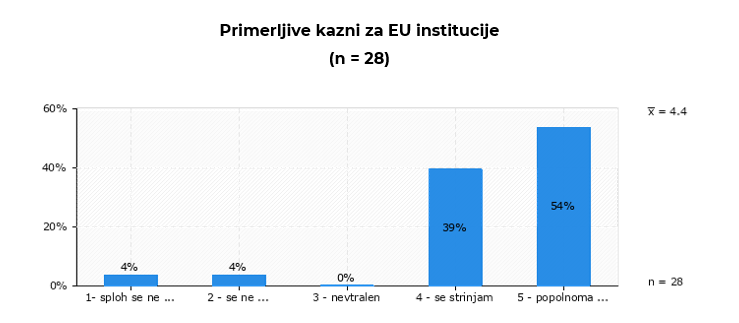
Slika 23 Učinkovito pravno varstvo

## Primerljive kazni za EU institucije

Slovenija meni, da morajo biti kazni proporcionalne in namenjene spodbujanju etičnega in pravno skladnega delovanja vseh deležnikov. V tem smislu menimo, da bi morale biti kazni za vse primerljive deležnike enake, tudi za EU institucije, za katere v trenutnem osnutku s tega vidika kazni odstopajo.

**S stališčem se strinja 93 % respondentov, 8 % respondentov se ne strinja, 0 % respondentov je nevtralnih.**

Respondenti se strinjajo, da je treba »*pripraviti primerljiv okvir za opredelitev višine kazni za različne deležnike (javne zavode, institucije, zasebne družbe, itd.)*« ter da bi morale biti kazni za zlorabo EU institucije in državnih organov »*bistveno višje*«.



Slika 24 Primerljive kazni za EU institucije

# Zaključek

Spletno posvetovanje je v splošnem pokazalo na relativno strinjanje s pripravljenimi predlogi stališč, pri čemer so bila najbolj podprta stališča o primerljivih kaznih za institucije EU, o biometrični identifikaciji kot uporabi UI visokega tveganja, o tehnično jasni definiciji ter o ciljih sistemskega urejanja.

Stališča, s katerimi so se respondenti relativno najmanj strinjali, so bila stališče o sistemskem urejanju v delu, ki se nanaša na uporabo UI na področju nacionalne varnosti, vojaške uporabe in glede sistemov dvojne rabe, kjer pa je iz komentarjev možno razumeti nestrinjanje predvsem s tem, da se Slovenija strinja z izvzetjem nacionalne varnosti in vojaške rabe iz Akta o umetni inteligenci. Menimo, da gre v tem primeru za nejasno zapisano stališče, saj se s tem stališčem Slovenija ne odmika od ciljev in načel opredeljenih v prejšnjih stališčih, temveč se strinja, da zaradi pravne ureditve EU, tega ni mogoče urejati na ravni EU, saj sta ti področji v izključni pristojnosti nacionalnih držav. Ostali dve stališči, s katerima so se respondenti prav tako relativno najmanj strinjali, pa predstavljata stališče o tehnično jasni in razumljivi definiciji, ki se nanaša na vprašanje, ali sisteme, ki za samodejno izvajanje operacij uporabljajo pravila, ki jih opredeli izključno fizična oseba, štejemo kot sisteme UI, ter stališče o urejanju umetne inteligence splošnega namena, kjer se komentarji nanašajo na pomisleke o smiselnosti tovrstne regulacije teh sistemov, potrebnosti primerne definicije UI splošnega namena ter na vprašanje ustreznosti predlaganega urejanja tovrstnih sistemov, ko so ti dostopni pod licencami odprte kode.

Respondenti so imeli možnost podati tudi splošni komentar, kjer pozivajo »*k proaktivnemu pristopu k regulaciji UI (AI), kot izhaja iz predlagateljevega predloga ukrepov*« ter poudarjajo »*pomen zagotovitev sistema procesnih jamstev v zvezi s pravno in tehnično (standardi skladnosti) regulacijo UI (AI) z namenom preprečitve arbitrarnosti, zagotavljanjem spoštovanja in skladnosti s človekovimi pravicami in temeljnimi svoboščinami, mednarodnih pravom, konvencijam in danim zavezam z namenom preprečitve zlorabe in vzpostavitve sistema samoomejevanja s strani vsakokratne oblasti in oseb v poziciji moči, navezujoče se na UI (AI)*«. Hkrati opozarjajo tudi na to, da bi bilo treba »*korporacije, ki neupravičeno uporabljajo UI v nasprotju z zakoni /…/ in delujejo v škodo že pridobljenih človekovih pravic, strožje regulirati*«.

# Priloga I – Vprašalnik

1. <https://imss.dz-rs.si/IMiS/ImisAdmin.nsf/ImisnetAgent?OpenAgent&2&DZ-MSS-01/f92832e6b73881f528e3ccc8d0c3b0268cb891c57e6428c7d1120c6267ee4d4a>. [↑](#footnote-ref-2)
2. https://digital-strategy.ec.europa.eu/en/policies/artificial-intelligence [↑](#footnote-ref-3)
3. <https://oecd.ai/en/network-of-experts>. [↑](#footnote-ref-4)
4. <https://www.coe.int/en/web/artificial-intelligence/cai>. [↑](#footnote-ref-5)
5. <https://gpai.ai/>. [↑](#footnote-ref-6)
6. <https://ircai.org/>. [↑](#footnote-ref-7)