

Priporočila glede zagotavljanja zaščite temeljnih pravic v primeru rabe umetnointeligenčnih sistemov na področjih, ki so v Aktu o UI izvzeta ali pogojno prepovedana

Uredba (EU) 2024/1689 Evropskega parlamenta in Sveta z dne 13. junija 2024 o določitvi harmoniziranih pravil o umetni inteligenci in spremembi uredb (ES) št. 300/2008, (EU) št. 167/2013, (EU) št. 168/2013, (EU) 2018/858, (EU) 2018/1139 in (EU) 2019/2144 ter direktiv 2014/90/EU, (EU) 2016/797 in (EU) 2020/1828 (v nadaljevanju: Akt o umetni inteligenci oziroma Akt o UI), ki regulira dajanje na trg in uporabo umetnointeligenčnih sistemov v Evropski uniji, je stopil v veljavo avgusta 2024. Februarja 2025 so se začele uporabljati določbe glede prepovedanih praks, ki pomenijo nesprejemljivo tveganje za varnost in temeljne pravice državljanov. S tem pa so v veljavo stopile tudi nekatere izjeme, ki so za zaščito pravic zaskrbujoče.

Akt o UI denimo ne velja za uporabo umetnointeligenčnih sistemov za izključno vojaške, obrambne ali nacionalne varnostne namene. Izključitev nacionalne varnosti je upravičena s členom 4(2) Pogodbe o Evropski uniji, ki določa, da zlasti nacionalna varnost ostaja v izključni pristojnosti vsake države članice. Obenem je seznam prepovedanih praks predvsem spisek pogojnih prepovedi. Zato ostaja skrb, da bodo te vrzeli v predpisu izkoriščene za slabitev demokracije in demokratičnih procesov ter pravne države, kar bo imelo zastrašujoč učinek na javno zbiranje, pravico do protesta, zasebnost in druge temeljne pravice, ki so med drugim zagotovljene v Listini Evropske unije o temeljnih pravicah (v nadaljevanju: Listina EU)¹ in Ustavi Republike Slovenije (v nadaljevanju: Ustava).

Uporaba umetnointeligenčnih sistemov na področju nacionalne varnosti

Oprelitev nacionalne varnosti in bistvenih varnostnih interesov je primarno v pristojnosti držav članic. Čeprav v slovenski zakonodaji nimamo jasno definiranega pojma nacionalne varnosti,² je Sodišče EU v združenih zadevah C-511/18, C-512/18 in C-520/18 (La

¹ Listina Evropske unije o temeljnih pravicah, UL C 202, 7. 6. 2016.

² O razumevanju tega pojma v nacionalnem okviru je sicer v določeni meri mogoče sklepati iz Resolucije o strategiji nacionalne varnosti (Uradni list RS, št. 59/19), ki opredeljuje nacionalne interese in nacionalnovarstvene cilje, a ne predstavlja zavezujočega pravnega dokumenta in pojma nacionalne varnosti kot takega ne definira.

Quadrature du Net) z dne 6. 10. 2020³ postavilo okvirno definicijo nacionalne varnosti. Navedlo je, da ta pristojnost ustreza prvobitnemu interesu, ki je zaščititi bistvene funkcije države in temeljne interese družbe, ter vključuje preprečevanje in kaznovanje dejavnosti, ki lahko resno destabilizirajo temeljne ustavne, politične, gospodarske ali družbene strukture države ter zlasti neposredno ogrozijo družbo, prebivalstvo ali državo kot tako, kot so zlasti teroristična dejanja. Sodišče EU pri tem poudarja, da se odstopanja v skladu z določbami o varnosti držav članic nanašajo na izjemne in jasno opredeljene primere, ki ne predstavljajo splošne izjeme in ki naj se razlagajo restriktivno.

Države članice so upravičene sprejeti ustrezne ukrepe za zagotovitev svoje varnosti. A čeprav uporaba UI na področju nacionalne varnosti ni regulirana z Aktom o UI, pa taki ukrepi niso v celoti izven področja uporabe prava EU. Ti ukrepi morajo biti v skladu s splošnimi načeli prava EU, med drugim z načelom sorazmernosti, ki zahteva, da odstopanja ostanejo v mejah tega, kar je primerno in potrebno za doseg zastavljenega cilja.⁴ Države članice morajo dokazati, da so takšni ukrepi potrebni, sorazmerni in spoštujejo bistvo temeljnih pravic. To stališče je zastopano tudi v sodni praksi ESČP, ki članice zavezuje, da mora neodvisen organ preveriti nujnost in zakonitost ukrepov.⁵ To lahko zahteva večjo preglednost in odgovornost nacionalnih varnostnih agencij, kar je lahko izziv glede na pogosto zaupno naravo njihovega delovanja.

Navkljub izjemi morajo nacionalno varnostni organi skrbno oceniti zakonitost uporabe UI sistemov iz dveh razlogov. Prvič, bistveno je zagotoviti, da se ti sistemi uporabljajo izključno za namene nacionalne varnosti, kot to določa 3. točka člena 2(3) Akta o UI. Manj resna je zaznana grožnja za nacionalno varnost, strožje postanejo omejitve, da bi se ukrep lahko opredelil kot izrecna uporaba v te namene. S tem je zagotovljeno, da so nadzorni ukrepi omejeni na obravnavanje resničnih groženj. Drugič, izvesti je treba oceno sorazmernosti konkretnega ukrepa v skladu z Listino EU in Ustavo, tudi če je raba izven področja urejanja Akta o UI. V sklopu testa sorazmernosti se pri tem presoja primernost, nujnost in sorazmernost v ožjem pomenu (*strictu sensu*). Primernost bo verjetno manj pomembna, saj se lahko vprašanja v zvezi z njo ujamejo v oceno izključne uporabe iz samega akta. Nujnost se bo nanašala predvsem na obsežnost ukrepa. Večja kot je nevarnost, več manevrskega prostora je dovoljenega glede ekstenzivnosti. Zaradi tega bo ključno, da bodo države članice in njihovi organi uvedli robustne zaščitne ukrepe, ukrepe za preglednost (odvisno od tega, kako preglednost vpliva na sposobnost zagotavljanja

³ Sodišče EU, združene zadeve C-511/18, C-512/18 in C-520/18 (*La Quadrature du Net*) z dne 6. 10. 2020, URL: <https://curia.europa.eu/juris/document/document.jsf?jsessionid=356695CB12AF6B8B04830FAB2D40762A?text=&docid=232084&pageIndex=0&doclang=SL&mode=lst&dir=&occ=first&part=1&cid=11509485>, pridobljeno na 27. 8. 2025.

⁴ Slepak, Vitaly, *National security clause: law and practice of European Union and Eurasia Economic Union*, 2019, J. Phys.: Conf. Ser. 1406, URL: <https://iopscience.iop.org/article/10.1088/1742-6596/1406/1/012002/pdf>, str. 3-4, pridobljeno na 27. 8. 2025.

⁵ Evropsko sodišče za človekove pravice, *Janowiec in drugi v. Rusija*, št. 55508/07 in 29520/09 z dne 21. 10. 2013, URL: <https://hudoc.echr.coe.int/eng?i=001-127684>, pridobljeno na 2. 9. 2025.

učinkovitega delovanja) in neodvisne nadzorne mehanizme za zagotavljanje skladnosti s temeljnimi pravicami. To izhaja predvsem iz presoje sorazmernosti v ožjem smislu. Kakovost zaščitnih ukrepov se mora povečati glede na to, kako verjeten je nezakonit dostop.⁶

Opozarjamo tudi na problematiko prekrivanja aktivnosti s področja nacionalne varnosti in področij preprečevanja, odkrivanja ali preiskovanja kaznivih dejanj, ki spadajo pod Akt o UI. Glede na opredelitev preprečevanja, odkrivanja ali preiskovanja kaznivih dejanj v Aktu o UI, ki omogoča široko interpretacijo, je v določenih primerih mogoče prekrivanje s pojmom nacionalne varnosti, posledično pa obstaja nevarnost zlorab.⁷ Direktne akcije ali protesti bodo lahko denimo podvrženi umetnointeligenčnemu nadzoru, ki ni omejen z Aktom o UI, v primeru, da bo policija aktivnosti, ki se jih da utemeljiti tako z nacionalno varnostjo kot tudi s preprečevanjem, odkrivanjem in preiskovanjem kaznivih dejanj, utemeljila s sklicevanjem na nacionalno varnost (glej npr. primer Palestine Action v Združenem kraljestvu).⁸ Vsakršne deljene zmogljivosti med organi za nacionalno varnost in organi pregona bo treba spremljati in nadzorovati, da se zagotovi skladnost z Aktom o UI in drugim pravom EU.⁹ Obstajati bi morala tudi jasna razmejitev med dejavnostmi, ki spadajo na področja preprečevanja, odkrivanja ali preiskovanja kaznivih dejanj in področje nacionalne varnosti.

Zaradi teh razlogov se bodo države članice morale znajti v kompleksnem pravnem okolju, kjer njihova izključna pristojnost na področju nacionalne varnosti ni tako absolutna, kot se zdi na prvi pogled, pri uporabi UI na področju nacionalne varnosti pa bo treba med drugim upoštevati tudi splošna načela prava EU.

Upoštevajoč povedano priporočamo, da odgovorni pripravijo in sprejmejo resolucijo ali protokol uporabe umetnointeligenčnih sistemov za namene nacionalne varnosti, ki bo pokrival vse zgoraj omenjene kompleksnosti takšne rabe (tudi primere prekrivanja pristojnosti). S tem bo država zagotovila, da se morebitne izjeme glede prepovedanih uporab ne razlagajo široko, s čimer bo preprečila morebitne zlorabe in prekoračitve s strani organov nacionalne varnosti.

⁶ Laag, Emil, Beyond the Scope? The National Security Exemption and AI-Based Surveillance: Examining the Impact on EU Citizens' Rights in the Age of Artificial Intelligence, URL: <https://gupea.ub.gu.se/handle/2077/85320>, str. 32, 33, pridobljeno na 27. 8. 2025.

⁷ Powell, Rosamund, The EU AI Act: National Security Implications, 2024, URL: <https://cetas.turing.ac.uk/publications/eu-ai-act-national-security-implications>, pridobljeno na 30. 8. 2025.

⁸ United Nations, UK: Palestine Action ban 'disturbing' misuse of UK counter-terrorism legislation, Türk warns, 25. 7. 2025, URL: <https://www.ohchr.org/en/press-releases/2025/07/uk-palestine-action-ban-disturbing-misuse-uk-counter-terrorism-legislation>, pridobljeno na 3. 9. 2025.

⁹ CETaS Explainer: The EU AI Act – National Security Implications, https://cetas.turing.ac.uk/sites/default/files/2024-07/cetas_explainer_-_the_eu_ai_act_-_national_security_implications.pdf, str. 8, pridobljeno 30. 8. 2025.

Uporaba visokotveganih umetnointeligenčnih sistemov na področju preprečevanja, odkrivanja in preiskovanja kaznivih dejanj

Že pred oblikovanjem in sprejemom končnega besedila Akta o UI so mnogi opozarjali na nevarnosti rabe določenih umetnointeligenčnih sistemov in zagovarjali njihovo popolno prepoved. Navkljub močnemu odporu v aktu ostajajo nekatere *pogojne* prepovedi, ki so opredeljene v členu 5. EDPB in EDPB sta denimo opozorila,¹⁰ da gre za tako širok nabor izjem glede prepovedanih rab, da bo tudi s predvidenimi omejitvami potencialno število osumljencev ali storilcev kaznivih dejanj skoraj vedno "dovolj visoko", da opraviči nadaljnjo uporabo prepovedanih umetnointeligenčnih sistemov za odkrivanje osumljencev.

Evropska komisija je februarja 2025 objavila smernice o prepovedanih praksah,¹¹ ki so namenjene zagotavljanju dosledne, učinkovite in enotne uporabe Akta o UI po vsej Evropski uniji. A smernice same po sebi niso zavezujoče, hkrati pa niso dovolj jasne glede določitve izjem.

Prav tako je ključno poudariti, da se nobena od prepovedi smiselno ne nanaša na kontekst migracij in nadzora meja, na kar že dolgo opozarjajo civilnodružbene organizacije, denimo koalicija Protect not surveil.¹² Seznam visokotveganih sistemov ne zajema številnih umetnointeligenčnih sistemov. Izključuje denimo škodljive sisteme, kot so bralniki prstnih odtisov ali orodja napovedne analitike, ki se uporabljajo za napovedovanje, prepovedovanje in omejevanje migracij.

Akt o UI uvaža tudi izjeme, povezane z obveznostmi glede preglednosti in transparentnosti rabe v kontekstu migracij ter kazenskega pregona, kar spodkopava učinkovit javni nadzor. Zaradi tega prizadeti ljudje, civilna družba in novinarji ne bodo mogli vedeti, kje in v kakšnih kontekstih so uporabljeni nekateri najbolj škodljivi umetnointeligenčni sistemi. Zagovarjamo načelo, da je uporaba sistema v policijskih postopkih ali pri nadzoru meja, pri katerem delovanje in posledice niso v celoti pojasnjeni, nesprejemljiva.

Obenem opozarjamo, da mehanizmi odgovornosti po incidentih in kršitvah temeljnih pravic ne bodo prinesli veliko tolažbe žrtvam. V večini primerov regulacija in nadzor

¹⁰ EDPB-EDPS Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), URL: https://edps.europa.eu/system/files/2021-06/2021-06-18-edpb-edps_joint_opinion_ai_regulation_en.pdf, str. 12, pridobljeno na 27. 8. 2025.

¹¹ Evropska komisija, Smernice o prepovedanih praksah, 2025, URL: <https://digital-strategy.ec.europa.eu/s/library/commission-publishes-guidelines-prohibited-artificial-intelligence-ai-practices-defined-ai-act>, pridobljeno na 30. 8. 2025.

¹² #ProtectNotSurveil, The EU AI Act, URL: <https://protectnotsurveil.eu/#calls>, pridobljeno na 27. 8. 2025.

začneta veljati šele po tem, ko je kršitev storjena, pred tem pa zaščite ne nudita. Žrtve so pogosto posamezniki ali družbene skupine, ki so že tako ranljive in nimajo niti informacij niti kapacitet za vložitev pritožbe.

Kar zadeva uporabo sistemov za biometrično identifikacijo na daljavo v javno dostopnih prostorih za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj, Akt o UI razlikuje med identifikacijo v realnem času in naknadno identifikacijo. Prva vključuje zajemanje, primerjavo in identifikacijo v živo, medtem ko slednja te funkcije opravlja retrospektivno z uporabo predhodno zbranih podatkov, kot so denimo posnetki s kamer. Akt o UI sisteme za naknadno biometrično identifikacijo opredeljuje kot visoko tvegane in načeloma prepoveduje rabo sistemov za biometrično identifikacijo na daljavo v realnem času v javno dostopnih prostorih za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj, pri čemer še vedno dovoljuje nekaj pomembnih izjem, ki so zaskrbljujoče. V Sloveniji trenutno nimamo zakonodajne podlage za uporabo biometrične identifikacije na daljavo v realnem času v javno dostopnih prostorih, medtem ko je naknadna identifikacija dovoljena. A razlikovanje med uporabo tehnologije v realnem času in naknadno uporabo je arbitrarno, razlika pri pogojih uporabe pa je ogromna, saj so pogoji za uporabo naknadne identifikacije precej ohlapni. Razlike med rabama se pojavljajo predvsem glede postopka odobritve. Člen 5(3) Akta o UI določa, da mora sodni organ ali neodvisni upravni organ, katerega odločitev je zavezujoča, izdati odobritev pred uporabo sistemov za biometrično identifikacijo na daljavo v javno dostopnih prostorih v realnem času. V izjemnih nujnih primerih lahko organi pregona tehnologijo uporabljajo brez odobritve, če zaprosijo za odobritev v 24 urah. Kar pa zadeva sisteme naknadne identifikacije, člen 26(10) določa, da organi pregona zahtevajo predhodno odobritev od istih organov bodisi pred uporabo sistema bodisi najpozneje 48 ur po njegovi uporabi. Pri poznejši zahtevi za odobritev prav tako ni potrebna zahteva po nujnosti. Poleg tega odobritev ni potrebna, kadar se sistem uporablja za identifikacijo potencialnega osumljenca.¹³

Pri uporabi lahko prihaja tudi do zlorab, ki so protipravne. Že sum kakršnega koli kaznivega dejanja lahko upraviči uporabo sistema za naknadno identifikacijo. Organi pregona bi lahko denimo kopičili slike obrazov, pridobljene z neciljanim skeniranjem, in poskušali identificirati posameznike v svojih podatkovnih bazah po tem, ko so bile slike posnete. Takšna uporaba bi spodkopala človekove pravice prav tako kot identificiranje v realnem času: v obeh primerih bi lahko organi pregona med drugim poskušali identificirati udeležence javnega političnega protesta tudi brez obstoja suma ali dokazov, da so

¹³ Giannini, Tas, AI Act and the Prohibition of Real-Time Biometric Identification, Much ado about nothing?, 10. 12. 2024, URL: <https://verfassungsblog.de/ai-act-and-the-prohibition-of-real-time-biometric-identification/>, pridobljeno na 27. 8. 2025.

protestniki kršili kakršne koli zakone.¹⁴ Uporaba tovrstnih biometričnih aplikacij lahko zato privede do množičnega nadzora in kršitve temeljnih pravic, kot so pravica do zasebnosti, svobode izražanja in mirnih protestov. Prav tako krepí neravnovesje moči med tistimi, ki opazujejo, in tistimi, ki so opazovani; strah pred identifikacijo celo mesece po udeležbi na javnem dogodku lahko denimo znatno vpliva na uresničevanje pravice do svobode izražanja in zbiranja. Čeprav Akt o UI prepoznava tveganja za pravice posameznikov v primeru uporabe tovrstnih biometričnih tehnologij za identifikacijo, pa tveganj ne obravnava ustrezno in določa nejasne izjeme od prepovedi rabe.

Nekatere vlade v EU žal že izkoriščajo pravne vrzeli za uporabo množičnega nadzora, ki jih dopušča Akt o UI. V Avstriji je vlada uporabila biometrični sistem za identifikacijo podnebnih aktivistov na protestih, na Madžarskem pa so sprejeli zakon, ki dovoljuje uporabo tehnologije za prepoznavanje obrazov na paradah ponosa.

Upoštevaloč povedano priporočamo, da odgovorni razmislijo o bolj restriktivnih ukrepih glede uporabe prepovedanih praks za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj, posebej na področjih migracij, upravljanja meja in uporabe biometrične identifikacije na daljavo. Predvsem pa naj ne sprejmejo dodatne zakonodaje, ki bi odobrila ali dovolila rabo določenih umetnointeligenčnih sistemov za odkrivanje, preprečevanje, preiskovanje ali pregon kaznivih dejanj, s čimer bi omogočila izogib obveznostim glede transparentnosti in pravice posameznikov do obveščenosti iz člena 50 Akta o UI.

Člen 26(10) Akta o UI ureja naknadno biometrično identifikacijo na daljavo in dovoljenje, ki je za rabo te identifikacije potrebno, pri čemer so omejitve oziroma pogoji blažji, kot pri biometrični identifikaciji na daljavo v realnem času. Člen določa, da uvajalec visokotveganega sistema UI za naknadno biometrično identifikacijo na daljavo predhodno ali brez nepotrebnega odlašanja in najpozneje v 48 urah zaprosi sodni organ ali upravni organ, katerega odločitev je zavezujoča in je predmet sodnega nadzora, za uporabo tega sistema, razen če se ta uporablja za prvotno identifikacijo morebitnega osumljenca na podlagi objektivnih in preverljivih dejstev, neposredno povezanih s kaznivim dejanjem. Države članice bodo morale postopek tovrstnega dovoljenja podrobneje določiti. **Priporočamo, da se na zakonski ravni na jasen način uredita postopek pridobitve dovoljenja in postopanje v primeru zavrnitve, tako da bodo relevantni organi zavezani jasnim omejitvam, hkrati pa bo zagotovljena ustrezna raven varstva človekovih pravic.**

¹⁴ The Human Rights Risks of Facial Recognition AI Tech in Policing and Immigration Must be Properly Recognised in the EU AI Act, Center for Democracy and Technology Europe, <https://cdt.org/insights/brief-human-rights-risks-of-facial-recognition-ai-tech-in-policing-and-immigration-must-be-properly-recognised-in-the-eu-ai-act/>, pridobljeno na 27. 8. 2025.

Čeprav primarno zagovarjamo stališče, da potrebujemo več preventivnih ukrepov na področju kazenskega pregona, in posledično ne podpiramo uporabe zgoraj omenjenih tehnologij, razumemo, da se bodo takšne tehnologije v praksi uporabljale. Upoštevajoč vse zgoraj omenjene nevarnosti za pravice in potencialne za kršitve ali protipravno rabo **priporočamo, da se javnosti omogoči nadzor nad uporabo tovrstnih sistemov v javnem registru UI. Obenem mora država tudi interno zagotoviti sistem monitoringa naročanja, implementacije in uporabe tovrstnih sistemov ter učinkovit sistem takojšnje prekinitve rabe sistemov ob vsakršni ugotovitvi kršitve temeljnih pravic.**

Danes je nov dan, Inštitut za druga vprašanja je neodvisna neprofitna organizacija, ustanovljena leta 2013, ki deluje na presečišču tehnologije, demokracije in digitalnih pravic. S kombinacijo razvoja odprtokodnih orodij, zagovorništva in sodelovanja s skupnostmi si prizadevamo za večjo preglednost institucij in dejavno vključevanje javnosti v politične procese. Inštitut ima status organizacije v javnem interesu na področju informacijske družbe. Aktivno se ukvarjamo z regulacijo in odgovorno uporabo novih tehnologij, s posebnim poudarkom na umetni inteligenci. S svojim znanjem prispevamo k sooblikovanju nacionalnih politik, naši sodelavci sodelujejo v strokovnem svetu za obravnavo strokovnih vprašanj in svetovanje pri implementaciji Akta o UI ter v postopku priprave Nacionalnega programa o UI 2030. Svoje delo umeščamo v širši evropski kontekst kot člani mreže za digitalne pravice EDRi, svojo zavezanost k transparentnosti pa dokazujemo s projekti, kot je Register uporabe UI v javnem sektorju.

Kontaktna oseba: Jasmina Ploštajner, jasmina@danesenovdan.si

Pravna mreža za varstvo demokracije je iniciativa, ki nudi pravno podporo posameznikom_cam ter organizacijam, ki se zaradi nenasilnega javnega delovanja znajdejo v pravnih postopkih. S pravnimi mnenji, stališči in pozivi varujemo demokratično, odprto, svobodno in solidarno družbo.*