

TVEGANJA UPORABE UMETNE INTELIGENCE PRI PREISKOVANJU IN ODKRIVANJU KAZNIVIH DEJANJ V KAZENSKIH POSTOPKIH IN NADZORU MEJA TER UPRAVLJANJU MIGRACIJ

KATJA KOLARIČ^{1,2}

¹ Univerza v Mariboru, Pravna fakulteta, Maribor, Slovenija
katja.kolaric3@student.um.si

² Okrožno sodišče Ptuj, Ptuj, Slovenija
katja.kolaric@sodisce.si

EU je prva na svetu sprejela Akt o umetni inteligenci, ki je pravni okvir za razvoj umetne inteligence. Poglavje obravnava uporabo umetne inteligence pri odkrivanju in preprečevanju kaznivih dejanj, zlasti na področju organiziranega kriminala, terorizma, zagotavljanja varnosti državljanov EU, obvladovanja migracij in nadzora meja. Strojno učenje umetne inteligence lahko privede do pristranskosti in diskriminacije zaradi algoritmov, na katerih te aplikacije temeljijo. Kakovost uporabljenih podatkov vpliva na rezultate aplikacij, kar povečuje inherentno pristranskost. Akt o umetni inteligenci poudarja, da je treba prepovedati uporabo umetne inteligence, če ni združljiva s temeljnimi pravicami, zapisanimi v Listini Evropske unije o temeljnih pravicah. Splošna uporaba umetne inteligence za namene množičnega nadzora je nesorazmerna. Ključno je uravnoteženje varstva pravic posameznikov in učinkovito izvajanje policijskih nalog. Pri uporabi umetne inteligence za preiskovanje kaznivih dejanj je nujno upoštevati Etične smernice za uporabo umetne inteligence, saj imajo odločitve resne posledice za življenje in svobodo posameznikov.

DOI
[https://doi.org/
10.18690/um.pf.11.2025.12](https://doi.org/10.18690/um.pf.11.2025.12)

ISBN
978-961-299-086-2

Ključne besede:

Akt EU o umetni
inteligenci,
etična raba umetne
inteligence,
varstvo temeljnih pravic,
umetna inteligenca
kazenskih postopkih,
upravljanje migracij,
digitalna forenzika,
prepovedane prakse rabe
umetne inteligence,
visoko tvegani sistemi.



Univerzitetna založba
Univerze v Mariboru

DOI
[https://doi.org/
10.18690/um.pf.11.2025.12](https://doi.org/10.18690/um.pf.11.2025.12)

ISBN
978-961-299-086-2

RISKS OF USING ARTIFICIAL INTELLIGENCE IN LAW ENFORCEMENT, CRIMINAL PROCEEDINGS, BORDER CONTROL AND MIGRATION MANAGEMENT

KATJA KOLARIČ^{1,2}

¹ University of Maribor, Faculty of Law, Maribor, Slovenia
katja.kolaric3@student.um.si

² District court Ptuj, Ptuj, Slovenia
katja.kolaric@sodisce.si

Keywords:

EU Artificial Intelligence Act, ethical use of artificial intelligence, protection of fundamental rights, artificial intelligence in criminal proceedings, migration management, digital forensics, prohibited practices in the use of artificial intelligence, high-risk systems.

The EU is the first in the world to adopt the Artificial Intelligence Act, a single legal framework for its development. This chapter discusses the use of artificial intelligence in crime prevention, border control and migration. Artificial intelligence helps detect crime, improve law enforcement methods and investigate financial and cybercrime. However, at the same time, it can threaten fundamental rights under the Charter of Fundamental Rights of the European Union. Mass surveillance is disproportionate, and algorithmic bias can lead to discrimination. The quality of data affects the results, increasing inherent bias. It is crucial to balance the protection of rights with the effective implementation of police tasks. It is essential to follow the Ethical Guidelines when using artificial intelligence for criminal investigations, as decisions have serious consequences for the life and freedom of individuals.



University of Maribor Press

1 Uvod

Pojem umetna inteligenca je bil v različnih obdobjih v zadnjih 60-ih letih zelo različno definiran in uporabljen. Vključuje najrazličnejše tehnologije, s pomočjo katerih računalniki analizirajo svoje okolje in na tej podlagi ukrepajo za doseganje določenih ciljev. Gre za dejavnosti, do nedavnega omejene na zmožnosti človeka. Pravna opredelitev umetne inteligence bi morala temeljiti na ključnih značilnostih sistemov umetne inteligence.¹ Pojma umetne inteligence in strojnega učenja se pogosto uporabljata kot sopomenki, čeprav to nista. Strojno učenje je tehnika, ki pomaga povezovati in obdelovati velike količine podatkov in se ob tem kaj novega naučiti. Umetna inteligenca pa je bistveno širši pojem in vključuje področja računalniškega vida, robotike in obdelave naravnega jezika, pa tudi druge pristope, ki ne vključujejo tehnologij strojnega učenja. Umetna inteligenca se danes uporablja v različnih fazah sodnih postopkov, pri čemer vsaka faza vključuje specifične primere uporabe. V fazi preiskave in zbiranja dokazov lahko algoritmi strojnega učenja pomagajo pri analizi velikih količin podatkov, kot so elektronska sporočila in dokumenti, ter identifikaciji relevantnih informacij.² Na mednarodnem področju poteka med državami na različnih kontinentih boj za prevlado. Mednarodne študije primerov kažejo, da si napovedna analitika in tehnologije umetne inteligence vse bolj utirajo pot v mednarodne zadeve, diplomacijo in obveščevalne službe. Tehnologije, ki se uporabljajo pri upravljanju migracij, so na mednarodnem področju neregulirane in posegajo v človekove pravice. Obstaja nevarnost, da države na migrantih preskušajo nove tehnologije. Tehnologije, ki se uporabljajo pri upravljanju migracij, posegajo v človekove pravice. Sledljivi migranti upravičujejo uporabo tehnologije in zbiranja podatkov pod krinko nacionalne varnosti ali celo pod krinko humanitarnosti in razvoja.³ Uredba (EU) 2024/1689 Evropskega parlamenta in Sveta 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) 2020/1828⁴ (Akt o umetni inteligenci) je pričela veljati 13. junija 2024 in je prvi predpis, ki podaja pravila glede uporabe umetno-inteligenčnih sistemov. Tudi izven EU se vzpostavlja koncept algoritemske etike, ki povzema nujnost vključevanja etičnega nadzora v algoritmične sisteme in potrebo po normativno-operativnem

¹ Nacionalni program spodbujanja razvoja in uporabe umetne inteligence v Republiki Sloveniji do leta 2025.

² Več o tem Selinšek, 2021, stran 223.

³ Molnar, 2019.

⁴ UL L 2024/1689, 12. 7. 2024.

okvirju, ki vključuje moralno razmišljanje skozi celoten življenjski cikel umetne intelligence – od zasnove do uvedbe, od regulacije do organizacijskega upravljanja.⁵

Namen tega poglavja v monografiji je obravnavati pravno opredelitev umetne intelligence v EU s posebnim poudarkom na uporabi umetne intelligence v kazenskem pravu, uporabnosti digitalnih dokazov ter uporabi umetne intelligence pri nadzoru meja in upravljanju migracij. Etične smernice za zaupanja vredno umetno inteligenco iz leta 2019 je razvila neodvisna strokovna skupina na visoki ravni za umetno inteligenco (AI HLEG), ki jo je imenovala Evropska komisija (Etične smernice), saj do tedaj umetna inteligenca ni bila regulirana s posebnim predpisom. V teh smernicah je AI HLEG razvila sedem nezavezujočih etičnih načel za umetno inteligenco, ki naj bi pomagala zagotoviti, da je umetna inteligenca zaupanja vredna in etično zanesljiva. Teh sedem načel vključuje človeško delovanje in nadzor, tehnično robustnost in varnost, zasebnost in upravljanje podatkov, preglednost, raznolikost, nediskriminacijo in pravičnost ter družbeno in okoljsko blaginjo in odgovornost.⁶ Akt o umetni inteligenci je v tem poglavju monografije obravnavan tudi z namenom zagotavljanja načel varovanja človekovih pravic in varovanja temeljnih pravic in vrednot uporabnika ter etičnih in pravnih načel za uporabo umetnointeligentnih sistemov v kazenskem pravu.

V drugem razdelku je obravnavana pravna opredelitev umetne intelligence v EU in Akt o umetni inteligenci, v tretjem razdelku uporaba umetne intelligence v kazenskem pravu, v četrtem pa uporaba digitalnih dokazov v predkazenskih in kazenskih postopkih. Peti razdelek naslavlja uporabo umetne intelligence za nadzor meja in upravljanje migracij, v šestem razdelku so povzeta etična načela za uporabo umetne intelligence, v sedmem pa nesprejemljivo tveganje in prepovedane prakse. V osmem razdelku so zapisane zaključne ugotovitve.

⁵ Celsi, Zomaya, 2025.

⁶ Etične smernice neodvisne strokovne skupine na visoki ravni za umetno inteligenco, ki jo je ustanovila Evropska komisija, (2018), dostopno na: [ethics_guidelines_for_trustworthy_ai-sl_88015DAF-E3CC-BBB8-AFE06902735B11DE_60438](https://ethics-guidelines-for-trustworthy-ai-sl-88015DAF-E3CC-BBB8-AFE06902735B11DE_60438) (1).pdf87, (obiskano: 6. 1. 2025).

2 Pravna opredelitev umetne inteligence v EU

2.1 Umetnointeligenčni sistemi

Umetnointeligenčne sisteme je mogoče zlahka uporabljati v številnih različnih gospodarskih in družbenih sektorjih, tudi čezmejno, in lahko enostavno krožijo po vsej EU.⁷ Akt o umetni inteligenci izpostavlja, da je ključna značilnost umetnointeligenčnih sistemov njihova sposobnost sklepanja,⁸ ki se nanaša na proces pridobivanja izhodnih podatkov, kot so napovedi, vsebina, priporočila ali odločitve, ki lahko vplivajo na fizično in virtualno okolje ter na sposobnost umetnointeligenčnih sistemov, da izpeljejo modele ali algoritme ali oboje iz vhodnih vrednosti ali podatkov.⁹ Tehnike, ki omogočajo sklepanje pri vzpostavljanju sistema umetne inteligence, vključujejo pristope strojnega učenja, ki se tega, kako doseči določene cilje, učijo iz podatkov, ter pristope, ki temeljijo na logiki in koordiniranem znanju. Zmogljivost umetnointeligenčnih sistemov za sklepanje presega osnovno obdelavo podatkov, saj omogoča učenje, oblikovanje zaključkov in modeliranje. Izraz »temelječ na napravah« se nanaša na dejstvo, da umetnointeligenčne sisteme poganjajo stroji.¹⁰ Visokokakovostni podatki in dostop do njih imajo ključno vlogo pri zagotavljanju strukture in zmogljivosti številnih umetnointeligenčnih sistemov.¹¹ Akt o umetni inteligenci v 3. členu določa pomembnost terminološke uskladitve pojma »umetnointeligenčnih sistemov«, ki naj bo jasno opredeljen in tesno usklajen z delom mednarodnih organizacij, ki se ukvarjajo z umetno inteligenco, da bi zagotovili pravno varnost, olajšali mednarodno zbliževanje ter hkrati zagotavljali prožnost, ki bo omogočala prilagajanje hitremu tehnološkemu razvoju na tem področju. Cilj harmonizacijske zakonodaje je, da v skladu z vrednotami EU spodbuja uvajanje na človeka osredotočene ter zaupanja vredne in varne umetne inteligence, hkrati pa zagotavlja visoko raven varovanja zdravja, varnosti in temeljnih pravic, kot so določene v Listini Evropske unije o temeljnih pravicah. Pri razvrstitvi umetnointeligenčnega sistema med sisteme visokega tveganja je zlasti pomemben obseg škodljivega vpliva sistema umetne inteligence na temeljne pravice, varovane z Listino Evropske unije o temeljnih pravicah¹² in Evropsko konvencijo o človekovih

⁷ Akt o umetni inteligenci, uvodna točka 3.

⁸ Prav tam, uvodna točka 12.

⁹ Evropska komisija, 2025.

¹⁰ Več o tem glej Akt o umetni inteligenci, uvodna točka 12.

¹¹ Več o tem glej Akt o umetni inteligenci, uvodna točka 67.

¹² UL C 326, 26. 10. 2012, strani 391–407.

pravicah (EKČP).¹³ Gre za pravico do človekovega dostojanstva, spoštovanja zasebnega in družinskega življenja, varstvo osebnih podatkov, svobodo izražanja in obveščanja, svobodo zbiranja in združevanja, pravico do nediskriminacije, pravico do izobraževanja, varstvo potrošnikov, pravice delavcev, pravice invalidov, enakost spolov, pravice intelektualne lastnine, pravico do učinkovitega pravnega sredstva in nepristranskega sodišča, pravico do obrambe in domneve nedolžnosti ter pravico do dobrega upravljanja. Iz temeljnih načel uporabe umetne inteligence, upoštevanih v določbah Akta o umetni inteligenci, izhaja, da imajo otroci posebne pravice, zapisane v 24. členu Listine Evropske unije o temeljnih pravicah in v Konvenciji Združenih narodov o otrokovih pravicah,¹⁴ ki zahtevata upoštevanje šibkih točk otrok ter nalagata zagotavljanje zaščite in varstva, ki sta potrebna za njihovo dobro počutje. Pri ocenjevanju resnosti škode, ki jo lahko povzroči sistem umetne inteligence, je treba upoštevati tudi pravico do visoke ravni varstva okolja, ki je zapisana v Listini Evropske unije o temeljnih pravicah in se izvaja v politikah EU tudi v zvezi z zdravjem in varnostjo oseb. Pristop k umetni inteligenci, osredotočen na temeljne pravice, temelji na pravni ureditvi, kjer je za spoštovanje, zaščito in izpolnjevanje pravic odgovorna država. Na ta način bi morala biti zagotovljena visoka raven pravnega varstva pred morebitno zlorabo novih tehnologij.

Akt o umetni inteligenci tako zagotavlja jasno pravno podlago za razvoj umetne inteligence, v kateri bosta sklicevanje na temeljne pravice in njihova uporaba v praksi trdno zasidrana.¹⁵ Nekaterе države članice so že preučile možnost sprejetja nacionalnih predpisov, s katerimi bi zagotovile, da je umetna inteligenca zaupanja vredna in varna ter da se razvija in uporablja v skladu z obveznostmi glede temeljnih pravic. Različna nacionalna pravila lahko povzročijo razdrobljenost notranjega trga in zmanjšajo pravno varnost za operaterje, ki razvijajo, uvažajo ali uporabljajo sisteme umetne inteligence. Zato bi bilo treba zagotoviti dosledno in visoko raven varstva po vsej EU, da bi dosegli zaupanja vredno umetno inteligenco in hkrati preprečili razlike, ki ovirajo prosti pretok, inovacije, uvajanje in uporabo umetnointeligenčnih sistemov ter z njimi povezanih proizvodov in storitev na notranjem trgu, in sicer z določitvijo enotnih obveznosti za operaterje ter

¹³ Zakon o ratifikaciji Konvencije o varstvu človekovih pravic in temeljnih svoboščin, spremenjene s protokoli št. 3, 5 in 8 ter dopolnjene s protokolom št. 2, ter njenih protokolov št. 1, 4, 6, 7, 9, 10 in 11 (MKVCP), Uradni list RS–MP, št. 7/94.

¹⁴ Uradni list SFRJ–MP, št. 15/90, Akt o notifikaciji nasledstva glede konvencij Organizacije združenih narodov in konvencij, sprejetih v mednarodni agenciji za atomsko energijo (Uradni list RS–MP, št. 9/92).

¹⁵ FRA, Agencija Evropske unije za temeljne pravice, 2024.

zagotovitvijo enotnega varstva prevladujočih razlogov javnega interesa in pravic oseb na notranjem trgu na podlagi 114. člena Pogodbe o delovanju Evropske unije¹⁶ (PDEU).¹⁷ Na nacionalnih ravneh bo na posameznih podpodročjih potrebna zakonska regulacija pravil o umetni inteligenci. Republika Slovenija na državni ravni še ni sprejela predpisa, ki bi urejal področje umetne inteligence. Kadar je zakonska ureditev nujna zaradi same narave posamezne pravice, njena opustitev povzroči protiustavno pravno praznino.¹⁸ Evropski parlament in Evropska komisija sta se dokaj intenzivno ukvarjala s harmonizacijo prava EU o umetni inteligenci.¹⁹ Z dodatnimi prihodnjimi in deloma že sprejetimi pravnimi dokumenti EU naj bi države članice zagotovile harmonizacijo pravnih predpisov, ki bi se nanašali na umetno inteligenco. Akt o umetni inteligenci podaja podlage za zaščito javnih interesov, kot so zdravje, varnost in varovanje temeljnih pravic. Harmonizacija naj bi za najhujše zlorabe s področja umetne inteligence obsegala tudi kazenskopravno zaščito.²⁰

Umetna inteligenca pomembno prispeva k prepoznavanju groženj in preprečevanju napadov, vendar njen razvoj odpira tudi številna tveganja. Med drugim se umetna inteligenca uporablja v izboljšanih nadzornih brezpilotnih letalih – dronih, ki spremljajo javne dogodke, proteste ali območja z visoko stopnjo kriminala za nadzor množic in ukrepanje v sili. Z namenom analize socialnega vedenja umetna inteligenca spremlja spletne dejavnosti in označuje sumljivo vedenje ali komunikacijo, orodja umetne inteligence pa spremljajo družbene medije tudi glede morebitnih groženj in dejavnosti tolpe.²¹ Umetna inteligenca utegne postati stalen del našega kazenskega pravosodja, saj omogoča preiskovalno analizo dokazov predvsem v fazi izločanja dokazov in je v pomoč pri sprejemanju odločitev.²²

¹⁶ UL C 326, 26. 10. 2012, strani 47–390.

¹⁷ Tako Akt o umetni inteligenci, uvodna točka 3.

¹⁸ Testen v Šturm (ur.), 2011, stran 198.

¹⁹ Evropski parlament je naročil tudi številne raziskovalne študije, da bi pridobil znanstveno podlago za zakonodajne dejavnosti na čelu tehnološkega razvoja in varstva podatkov, med drugim študijo o vplivu Splošne uredbe o varstvu podatkov (GDPR) na umetno inteligenco, študijo o biometričnem prepoznavanju in zaznavanju vedenja, študijo o metaverzumu in nedavno študijo o pravu in IKT. Več o tem glej Maciejewski et al., 2024.

²⁰ Ferlinc, 2024.

²¹ Glej <https://www.europarl.europa.eu/topics/sl/article/20200827STO85804/kaj-je-umetna-inteligenca-in-kako-se-uporablja-v-praksi> (obiskano: 6. 1. 2025).

²² Več o tem Selinšek, 2021, strani 219–232.

Potrebno je zagotoviti, da bodo organi poznali in razumeli omejitve, zmogljivosti in tveganja pri uporabi sistemov umetne inteligence, vključno s tveganjem pristranskosti zaradi avtomatizacije. Evropski parlament je leta 2021 v postopku oblikovanja načel za uporabo umetne inteligence v kazenskih postopkih s sprejetjem Resolucije Evropskega parlamenta z dne 6. oktobra 2021 o umetni inteligenci v kazenskem pravu in njeni uporabi v policiji in pravosodnih organih na področju kazenskih zadev (2020/2016(INI))²³ (Resolucija o umetni inteligenci) še posebej izpostavil, da je za ustrezno odgovornost in pristojnost potrebno obsežno specializirano usposabljanje v zvezi z etičnimi pravili, morebitnimi nevarnostmi, omejitvami in pravilno uporabo tehnologije umetne inteligence, zlasti policijskega in pravosodnega osebja. Treba je prepoznati možnosti za pristranskost, saj lahko nabori podatkov, na katerih temelji delo umetnointeligenčnega sistema, temeljijo na diskriminatornih in pristranskih podatkih.²⁴

Obstaja nevarnost, da policijsko delo, ki ga ustvarja umetna inteligenca, temelji na sklopih učnih podatkov z elementi rasizma, kar neizogibno privede do rasistične pristranskosti izsledkov, ocen in priporočil. Zato naj države članice spodbujajo protidiskriminacijske politike in pripravijo nacionalne akcijske načrte proti rasizmu pri policijskem delu in v pravosodnem sistemu. Služba Evropskega parlamenta za raziskave v nedavno opravljeni raziskavi »Umetna inteligenca na mejah EU« izpostavlja, da bi razvoju in uvajanju zmogljivih tehnologij umetne inteligence koristilo popolno razumevanje in razmisleki o širših vidikih, vključno z zgodovinskimi koreninami tehnologij ter prevladujočimi družbenimi in političnimi pogledi in pričakovanji. Sprejemanje tehnologije brez soočanja s pastmi, kot sta tehnološki determinizem in mit o tehnološki nevtralnosti, bi dodatno slabilo temeljne pravice preglednosti in zavezanosti odgovornosti.²⁵

Resolucija o umetni inteligenci je izpostavila nesorazmerje moči med tistimi, ki uporabljajo tehnologijo umetne inteligence, in tistimi, ki so ji podvrženi. Organi preprečevanja, odkrivanja in preiskovanja kaznivih dejanj in pravosodni organi pod nobenim pogojem ne smejo uporabljati umetne inteligence tako, da bi postala dejavnik neenakosti, socialnih napetosti ali izključenosti. Izpostaviti je občutljive vidike uporabe orodij umetne inteligence, ki ne sme vplivati na pravice osumljencev

²³ UL C 132, 6. 10. 2021, strani 17–26.

²⁴ Akt o umetni inteligenci, uvodna točka 59.

²⁵ Dumbrava, 2021.

do obrambe, še posebej glede na tveganja ob uporabi le-te. Posebna previdnost velja pri pridobivanju tehtnih informacij o načinu pridobivanja izsledkov umetne inteligence, katere rezultati so lahko na videz prepričljivi. Posebno pozornost je treba nameniti položaju preiskovanega posameznika, ki bo moral izpodbijati rezultate takšnih preiskav na sodišču.

Iz uvodnih točk Akta o umetni inteligenci izhaja jasno zavedanje, da je poleg koristnih uporab umetno inteligenco mogoče tudi zlorabiti tako, da bi nastala nova in močna orodja za manipulacijo, izkoriščanje in družbeni nadzor. Take prakse so še posebej škodljive in zlonamerne ter bi jih bilo treba prepovedati, ker so v nasprotju z vrednotami EU glede spoštovanja človekovega dostojanstva, svobode, enakosti, demokracije in pravne države ter temeljnimi pravicami, določenimi v Listini Evropske unije o temeljnih pravicah, vključno s pravico do nediskriminacije, varstva podatkov in zasebnosti ter pravicami otroka. Z umetno inteligenco omogočene manipulativne tehnike se lahko uporabljajo za napeljevanje posameznikov k neželenemu vedenju ali za njihovo zavajanje tako, da se jih spodbuja k odločitvam na način, ki spodkopava in ovira njihovo avtonomijo, odločanje in svobodno izbiro.²⁶

V ZDA so v obdobju po letu 2020 opravljali raziskave,²⁷ ki izpostavljajo princip učenja s pristopom in metodologijo, ki sta pozornost usmerila na pravne okvire ZDA in ustavne premisleke, kot sta enaka zaščita pravic in postopkovna pravičnost, glede na tveganja, ki nastanejo v okviru orodij, ki so nepregledna in dovzetna za pristranskost. Izpostavili so, da je za obravnavo vprašanj ključnega pomena bolj globalen pristop, vključno s primerjavo z drugimi nacionalnimi pristopi in upoštevanjem nadnacionalnih pravnih in upravnih režimov. V ta namen so se pridružili projektu Sienna, ki ga je koordinirala Univerza v Twenteju (Nizozemska), s Trilateralnim raziskovanjem (Združeno kraljestvo), ki deluje kot namestnik koordinatorja. Projekt, katerega cilj je bil preslikati globalno pravno in regulativno okolje za široko paleto umetne inteligence in robotskih tehnologij, je imel enajst partnerjev in dva pridružena partnerja iz Evrope, Azije, Afrike in ZDA. Ključen cilj je bil obravnavati etična vprašanja na nastajajočih tehnoloških področjih človeške genomike, izboljšave človeka in interakcije človek-stroj. Projekt je prejel sredstva v okviru programa EU za raziskave in inovacije H2020. Poleg tega je Center sodeloval

²⁶ Akt o umetni inteligenci, uvodne točke 29, 59 in 60.

²⁷ Bergman Klein center, 2018.

z laboratorijem za digitalno vključevanje kanadske vlade, da bi obravnaval širše posledice umetne inteligence in sorodnih tehnologij za človekove pravice. Cilj tega tekočega projekta je oceniti vpliv tehnologij umetne inteligence v okviru Splošne deklaracije o človekovih pravicah.²⁸ Z razvojem nabora gradiv, ki poudarjajo tveganja, ki jih umetna inteligenca lahko predstavlja za človekove pravice, se opredeljujejo najboljše prakse za prepoznavanje, ublažitev in odpravo teh tveganj. Hkrati ta gradiva priznavajo tudi priložnosti, ki jih takšne tehnologije ponujajo za izboljšanje rezultatov na področju človekovih pravic.²⁹

2.2 Akt EU o umetni inteligenci

Akt o umetni inteligenci določa harmonizirana pravila za dajanje na trg in za uporabo sistemov umetne inteligence v EU, prepoved nekaterih praks umetne inteligence, posebne zahteve za visoko tvegane sisteme umetne inteligence in obveznosti za operaterje takih sistemov. Določa tudi harmonizirana pravila o preglednosti za nekatere sisteme umetne inteligence, harmonizirana pravila za dajanje na trg umetnointeligenčnih modelov za splošne namene, pravila o spremljanju trga, nadzoru trga, upravljanju in izvrševanju ter ukrepe v podporo inovacijam, s posebnim poudarkom na malih in srednjih podjetjih, vključno z zagonskimi podjetji. Cilj je izboljšanje delovanja notranjega trga z določitvijo enotnega pravnega okvira, predvsem za razvoj, dajanje na trg ter za uporabo umetnointeligenčnih sistemov v EU v skladu z vrednotami EU. Namen je spodbujati uvajanje na človeka osredotočenih in zaupanja vrednih umetnointeligenčnih sistemov ter hkrati zagotoviti visoko raven varovanja varnosti in temeljnih pravic.³⁰

Akt o umetni inteligenci za sisteme opredeljuje štiri ravni tveganja: minimalno tveganje, omejeno tveganje, visoko tveganje in nesprejemljivo tveganje,³¹ ne uvaja pa pravil za umetno inteligenco, ki se šteje za minimalno ali brez tveganja. V to kategorijo spada velika večina umetnointeligenčnih sistemov, ki se trenutno uporabljajo v EU.³² Iz uvodne točke 97 Akta o umetni inteligenci izhaja, da se umetnointeligenčni modeli za splošne namene, vključno z velikimi generativnimi

²⁸ Uradni list RS–MP, št. 24/2018.

²⁹ Raso et al., 2018.

³⁰ Glej tudi GOV.SI, 1. 8. 2024, dostopno na: <https://www.gov.si/novice/2024-08-01-danes-je-začela-veljati-evropska-uredba-o-umetni-inteligenci-prva-taka-celovita-zakonodaja-na-svetu/> (obiskano: 6. 1. 2025).

³¹ Evropska komisija, 2024.

³² Prav tam.

umetnointeligenčnimi modeli, lahko uporabljajo za najrazličnejše naloge. Ti modeli se učijo iz velikih količin podatkov. Pomembno je, da ima ponudnik sistema, ki vključuje umetnointeligenčni model za splošne namene, dostop do vseh potrebnih informacij, da lahko zagotovi, da je sistem varen in skladen z Aktom o umetni inteligenci. Ponudniki modelov s sistemskimi tveganji so dolžni ocenjevati in zmanjševati tveganja, poročati o resnih incidentih, izvajati najsodobnejše preizkuse in ocene modelov ter zagotavljati kibernetško varnost svojih modelov.³³

Umetnointeligenčni sistemi, ki se razvrstijo kot sistemi velikega tveganja, so opredeljeni v poglavju III Akta o umetni inteligenci, če je umetnointeligenčni sistem vgrajen kot varnostna komponenta v proizvode, ki jih zajema obstoječa zakonodaja o proizvodih (Priloga I), ali če sam predstavlja take proizvode. To je lahko na primer medicinska programska oprema, ki temelji na umetni inteligenci, če naj bi se umetnointeligenčni sistem uporabljal v primeru velikega tveganja iz Priloge III k Aktu o umetni inteligenci. Na seznamu so navedeni primeri uporabe s področij, kot so izobraževanje, zaposlovanje, preprečevanje, odkrivanje in preiskovanje kaznivih dejanj ali migracije. Umetnointeligenčni sistem se razvrsti kot sistem velikega tveganja, če je namenjen za katerega koli od primerov uporabe, določene v Prilogi III Akta o umetni inteligenci, in zajema osem področij: (1) biometrija, (2) kritična infrastruktura, (3) izobraževanje in poklicno usposabljanje, (4) zaposlovanje, upravljanje delavcev, (5) dostop do bistvenih zasebnih in javnih storitev, (6) preprečevanje, odkrivanje in preiskovanje kaznivih dejanj, (7) migracije, nadzor meje ter (8) pravosodje in demokratični procesi.³⁴ Umetnointeligenčni sistem, ki predstavlja sistem visokega tveganja, je lahko vgrajen kot varnostna komponenta v proizvode, ki jih zajema obstoječa zakonodaja o proizvodih (Priloga I), ali sam predstavlja take proizvode. V skladu z Aktom o umetni inteligenci bodo za umetnointeligenčne sisteme velikega tveganja veljale posebne zahteve: ustrezni sistemi za oceno in zmanjšanje tveganja, visokokakovostni nabori podatkov, ki se uporabljajo v sistemu, da se čim bolj zmanjša tveganje diskriminatornih rezultatov, beleženje dejavnosti za zagotovitev sledljivosti rezultatov, podrobno dokumentacijo z vsemi potrebnimi informacijami o sistemu in njegovem namenu, da lahko organi ocenijo njegovo skladnost, jasne in ustrezne informacije uvajalcu, ustrezni ukrepi za

³³ Akt o umetni inteligenci uvaja posebne obveznosti razkritja za zagotovitev, da so ljudje obveščeni, kadar je to potrebno za ohranitev zaupanja. Na primer, pri uporabi umetnointeligenčnih sistemov, kot so klepetalni boti, bi bilo treba ljudi opozoriti, da komunicirajo s strojem, da lahko sprejmejo informirano odločitev. Povzeto po Evropska komisija, 2024.

³⁴ Evropska komisija, 2024.

človeški nadzor, visoka raven robustnosti, kibernetske varnosti in natančnosti.³⁵ V Aktu o umetni inteligenci je tako izpostavljena standardizacija teh sistemov.³⁶

Uvajalci umetnointeligenčnih sistemov najbolje razumejo, kako se bo visoko tvegani umetnointeligenčni sistem dejansko uporabljal, in lahko tako opredelijo potencialna velika tveganja, ki niso bila predvidena v fazi razvoja, saj natančneje poznajo okoliščine uporabe, osebe ali skupine oseb, ki bodo verjetno izpostavljene, vključno z ranljivimi skupinami. Uvajalci visoko tveganega umetnointeligenčnega sistema imajo ključno vlogo pri skrbi za zaščito temeljnih pravic, kar dopolnjuje obveznosti ponudnika pri razvoju sistema (26. člen Akta o umetni inteligenci). Iz uvodnih točk 28, 38 in 39 Akta o umetni inteligenci izhaja, da je pri uporabi visoko tveganih umetnointeligenčnih sistemov, ki se uporabljajo za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj, potrebno obveznost izvajati v skladu z 10. in 13. členom Direktive (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.³⁷

Umetnointeligenčni sistemi, posebej namenjeni uporabi v upravnih postopkih s strani davčnih in carinskih organov ter finančno obveščevalnih enot, ki izvajajo upravne naloge analiziranja informacij na podlagi prava EU o preprečevanju pranja denarja, naj ne bi bili opredeljeni kot visoko tvegani umetnointeligenčni sistemi. Sisteme sicer uporabljajo organi za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj za namen preprečevanja, odkrivanja, preiskovanja in pregona kaznivih dejanj. Orodij umetne inteligence pa ne bi smeli uporabljati na način, ki bi prispeval k neenakosti ali izključenosti.

Iz uvodne točke 60 Akta o umetni inteligenci tudi izhaja, da je med sisteme visokega tveganja primerno razvrstiti sisteme umetne inteligence, ki so na podlagi ustreznega prava EU in nacionalnega prava dovoljeni za uporabo na področju migracij, azila in upravljanja nadzora meja ter poligrafov in podobnih orodij, za ocenjevanje nekaterih

³⁵ Prav tam.

³⁶ Pri izvajanju teh zahtev imajo ključno vlogo harmonizirani standardi EU. Ko bodo ti standardi objavljeni, se bo za umetnointeligenčne sisteme, razvite v skladu z navedenimi standardi, domnevalo, da so skladni s pravili (t. i. domneva o skladnosti). Več o tem Evropska komisija, 2024.

³⁷ UL L 119, 4. 5. 2016, strani 89–131.

tveganj, ki jih predstavljajo fizične osebe, ki vstopajo na ozemlje države članice ali zaprosijo za vizum ali azil, za pomoč pristojnim javnim organom pri obravnavi, vključno s povezano oceno zanesljivosti dokazov, prošnji za azil, vizumov in dovoljenj za prebivanje, ter s tem povezanih pritožb zaradi ugotavljanja upravičenosti fizičnih oseb, ki zaprosijo za status, za namene odkrivanja, priznavanja ali identifikacije fizičnih oseb v okviru upravljanja migracij, azila in nadzora meja, z izjemo preverjanja potnih listin. Na področju migracij in azila je pomembna točnost in preglednost teh sistemov, ne pa diskriminatornost. Ob tem pa je potrebno dosledno zagotavljanje temeljnih pravic zadevnih oseb, zlasti pravice do prostega gibanja, nediskriminacije, varstva zasebnega življenja in osebnih podatkov, mednarodnega varstva ter dobrega upravljanja.

V določbi 5. člena Akta o umetni inteligenci so določena nesprejemljiva tveganja.³⁸ Gre za sklop posebno škodljivih načinov rabe umetne inteligence, ki je v nasprotju z vrednotami EU, ker krši temeljne pravice, zaradi česar so prepovedani. Prepovedane prakse so: izkoriščanje ranljivosti oseb, prirejanje in uporaba sublimiranih tehnik, družbeno točkovanje za javne in zasebne namene, individualno napovedno policijsko delo, ki temelji izključno na profiliranju oseb, neciljno zbiranje slik obrazov s spleta ali posnetkov sistema televizije zaprtega kroga (CCTV) za vzpostavitev ali razširitev podatkovnih zbirk, prepoznavanje čustev na delovnem mestu in v izobraževalnih ustanovah, razen iz zdravstvenih ali varnostnih razlogov (tj. spremljanje stopnje utrujenosti pilota), biometrična kategorizacija fizičnih oseb za sklepanje o njihovi rasi, političnem prepričanju, članstvu v sindikatu, verskem ali filozofskem prepričanju ali spolni usmerjenosti. Še vedno bo mogoče označevanje ali filtriranje naborov podatkov in razvrščanje podatkov na področju preprečevanja, odkrivanja in preiskovanja kaznivih dejanj, biometrična identifikacija na daljavo v realnem času v javno dostopnih prostorih s strani organov kazenskega pregona, ob upoštevanju omejenih izjem.^{39, 40} Priloga III zajema osem področij, na katerih je

³⁸ Informacijski pooblaščenec RS je posebej opozoril na uporabo določb I. in II. poglavja Akta o umetni inteligenci, ki so se začele uporabljati 2. februarja 2025, vključujoč prepovedi uporabe določenih umetointeligenčnih sistemov, ki jih ta predpis določa. Gre za sisteme umetne inteligence za družbeno ocenjevanje (t. i. social scoring) ter sklepanje o čustvih posameznikov v šolstvu in na delovnih mestih. Prav tako so prepovedane tudi določene oblike napovedovanja domnevnih izvršitev kaznivih dejanj in druge.

³⁹ Več o tem Resolucija o umetni inteligenci, točka 25.

⁴⁰ Akt o umetni inteligenci, uvodni točki 17 in 43.

lahko uporaba umetne inteligence še posebej problematična, in našteva konkretne primere uporabe za vsako področje.⁴¹

3 Umetna inteligenca v kazenskem pravu

Resolucija o umetni inteligenci ugotavlja, da orodja in aplikacije umetne inteligence uporablja sodstvo po vsem svetu, tudi pri odločanju o priporu, pri izrekanju kazni, izračunu verjetnosti ponovitve kaznivega dejanja, določanju pogojne kazni, spletnem reševanju sporov, upravljanju sodne prakse in olajševanju dostopa do prava. Resolucija o umetni inteligenci tudi ne prezre, da uporaba umetne inteligence izkrivlja in zmanjšuje možnosti za nebelce in manjšine. Dodati je, da se ta orodja in aplikacije v EU, z izjemo nekaj držav članic, trenutno večinoma uporabljajo v civilnih zadevah.

V digitalni forenziki so metode uporabljane v uvodnih fazah digitalnega forenzičnega procesa, kjer se triaža uporablja za izločitev nerelevantnih podatkov, da ostane za poglobljeno preiskavo oziroma ročni pregled kolikor toliko obvladljiva količina podatkov. Razvila se je tudi dodatna veja forenzike – protiforenzika, ki označuje programsko opremo in naprave oziroma predstavlja ukrepe, ki preiskovalcem preprečujejo oziroma jim otežijo pridobivanje podatkov s preiskovane digitalne naprave. Pomembno je, da preiskovalci vedo, kako ti ukrepi delujejo, da lahko potem uspešno izvedejo preiskave.⁴²

Organi preprečevanja in preiskovanja kaznivih dejanj tako uporabljajo aplikacije umetne inteligence, kot so tehnologija za prepoznavanje obrazov, na primer za iskanje po zbirkah podatkov o osumljencih in identifikacijo žrtev trgovine z ljudmi ali spolnega izkoriščanja in zlorabe otrok, tehnologije za avtomatizirano prepoznavanje registrskih tablic, identifikacijo govorcev, identifikacijo govora, branje z ustnic, zvočni nadzor (tj. mehanizmi za odkrivanje strelav), avtonomne raziskave in analize identificiranih zbirk podatkov, napovedi (napovedno policijsko delo in analiza kriminalnih žarišč), orodja za zaznavanje vedenja, napredna virtualna obdukcijska orodja, ki so v pomoč pri določanju vzroka smrti, avtonomna orodja za odkrivanje finančnih goljufij in financiranja terorizma, spremljanje družbenih

⁴¹Evropska komisija, 2024; Akt o umetni inteligenci, Shaping Europe's digital future, dostopno na: <https://digital-strategy.ec.europa.eu/sl/factpages/ai-act> (obiskano: 25. 1. 2025).

⁴² Brezovnik, 2016, stran 20.

medijev (strganje in nabiranje podatkov za rudarjenje povezav), ter sistemi avtomatiziranega nadzora, ki vključujejo različne detekcijske zmogljivosti (kot so detekcija srčnega utripa in toplotne kamere). Te aplikacije so lahko poleg drugih morebitnih ali prihodnjih aplikacij tehnologije umetne inteligence na področju preprečevanja, odkrivanja in preiskovanja kaznivih dejanj različno zanesljive in natančne ter lahko različno vplivajo na varstvo temeljnih pravic in dinamiko kazenskoopravnih sistemov. Dodati je, da se številna tovrstna orodja uporabljajo v tretjih državah, a bi bila v skladu z zakonodajnim okvirom in sodno prakso EU nezakonita. Rutinska uporaba algoritmov lahko kljub nizki stopnji lažno pozitivnih rezultatov privede do tega, da število napačnih opozoril močno preseže število pravih opozoril.⁴³

V tej zvezi je treba omeniti, da sodišča redno uporabljajo dokaze, pridobljene z analizami elektronskih naprav, potovalnih računalnikov na osebnih vozilih, preiskav DNK in bioloških sledov. V predkazenskem postopku policija za izločitev možnih osumljencev uporablja tudi metodo poligrafa. V uvodni točki 59 Akta o umetni inteligenci je poudarjeno, da je primerno, da se številni umetnointeligenčni sistemi, če je njihova uporaba dovoljena na podlagi zadevnega prava EU in nacionalnega prava, namenjeni uporabi v okviru preprečevanja, odkrivanja in preiskovanja kaznivih dejanj, razvrstijo med sisteme visokega tveganja, kjer so točnost, zanesljivost in preglednost še posebej pomembni, da se preprečijo škodljivi vplivi, ohrani zaupanje javnosti ter zagotovita odgovornost in učinkovito sodno varstvo. Med preiskovanjem ali pregonom kaznivih dejanj bi morali visoko tvegani umetnointeligenčni sistemi pri ocenjevanju tveganja, v izogib situacijam, da lahko fizična oseba postane žrtev poligrafov in podobnih orodij za ocenjevanje zanesljivosti dokazov, glede na naravo dejavnosti in s tem povezana tveganja, vključevati zlasti sisteme umetne inteligence, specializirane za namen uporabe organov preprečevanja, odkrivanja in preiskovanja kaznivih dejanj ali institucij, organov, uradov ali agencij EU v podporo tem organom. Ob ocenjevanju in presoji tveganja ponovitvene nevarnosti je treba zagotavljati, da odločitev ne nasprotuje prepovedim iz 5. člena Akta o umetni inteligenci in ne temelji izključno na podlagi oblikovanja profilov fizične osebe, ocene osebnostnih lastnosti in značilnosti ali preteklega kaznivega ravnanja fizičnih oseb ali skupin za oblikovanje profilov med odkrivanjem, preiskovanjem ali pregonom kaznivih dejanj. Oseba ima v skladu s

⁴³ Glej Resolucija o umetni inteligenci, točka M.

pravom EU pravico, da ni predmet odločitve, ki ima zanjo pravne učinke ali nanjo znatno vpliva in temelji izključno na avtomatizirani obdelavi podatkov.

4 Uporabnost digitalnih dokazov

Resolucija o umetni inteligenci postavlja zahtevo, da je za učinkovito uveljavljanje pravic do obrambe in preglednost nacionalnih kazensko-pravnih sistemov nujen poseben, jasen in natančen pravni okvir, ki bo urejal pogoje, načine in posledice uporabe orodij umetne inteligence na področju preprečevanja, odkrivanja in preiskovanja kaznivih dejanj in pravosodja, ter določal pravice oseb, ki so njihove tarče, pa tudi učinkovite pritožbene in odškodninske postopke, vključno s pravnimi sredstvi.⁴⁴ Poudarja, da imajo stranke v kazenskem postopku pravico, da so seznanjene s postopkom zbiranja podatkov in s tem povezanih ocen, ki se izvedejo ali pridobijo z uporabo aplikacij umetne inteligence. Domneva nedolžnosti predstavlja enega temeljnih stebrov demokratične države, ki svojo oblast utemeljuje na vladavini prava. Gre za ustavno varovano pravico v določbi 27. člena Ustave RS,⁴⁵ ki je v Zakonu o kazenskem postopku⁴⁶ (ZKP) zapisana v določbi 3. člena. Ti določbi določata, da oseba, ki je obdolžena kaznivega dejanja, velja za nedolžno, dokler njena krivda ni ugotovljena s pravnomočno sodbo. To pomeni, da dokazno breme nosi tožilec. Enako besedilo vsebujeta tudi drugi odstavek 6. člena EKČP in 11. člen Splošne deklaracije o človekovih pravicah. Šepec v zvezi s tem izpostavlja, da izjave in dokazi v kazenskem postopku, ki vzbujajo sum, da je obdolženi storil kaznivo dejanje, vse do pravnomočnega končanja postopka niso sporne z vidika drugega odstavka 6. člena EKČP, na primer, ko gre za izvajanje odločanja o priporu ali izvajanje preiskovalnih ukrepov.⁴⁷

Z vidika hrambe podatkov ter presoje in nadaljnje validacije digitalnih dokazov, pridobljenih s pomočjo umetne inteligence, ki se uči na podlagi podatkov iz različnih podatkovnih baz, je izpostaviti zavezujočo odločbo USRS U-I-312/11,⁴⁸ v kateri je Ustavno sodišče ugotovilo neustavnost prve alineje prvega odstavka 63. člena tedaj

⁴⁴ Prav tam.

⁴⁵ Uradni list RS, št. 33/91-I, 42/97 – UZS68, 66/00 – UZ80, 24/03 – UZ3a, 47, 68, 69/04 – UZ14, 69/04 – UZ43, 69/04 – UZ50, 68/06 – UZ121,140,143, 47/13 – UZ148, 47/13 – UZ90,97,99, 75/16 – UZ70a in 92/21 – UZ62a.

⁴⁶ Uradni list RS, št. 176/21-uradno prečiščeno besedilo, 96/22 – odl. US, 2/23 – odl. US, 89/23 – odl. US in 53/24.

⁴⁷ Šepec et al., 2023, strani 60 in 61.

⁴⁸ ECLI:SI:USRS:2014:U.I.312.11.

veljavnega Zakona o policiji.⁴⁹ Ta določba je omogočala, da so se profili oseb, ki so bile osumljene, niso pa bile pravnomočno obsojene, lahko hranili vse do zastaranja pregona za predmetno kaznivo dejanje. Trajna hramba profilov DNK oseb, za katere bi veljala domneva nedolžnosti, ni bila nujna za doseg namenov odkrivanja obravnavanega in prihodnjega kaznivega dejanja. Ustavno sodišče je opozorilo, da je pri trajni hrambi obstajala velika nevarnost za stigmatizacijo teh oseb (34. člen Ustave RS), ki bi bile obravnavane enako, kot če bi bile obsojene. Pooblastila za trajno hrambo niso ustrezala merilu nujnosti. Uveljavitev novih dokaznih metod z uporabo umetne inteligence bo nedvomno postavljena pred nove sodne izzive z vidika presoje že uveljavljenih načel in standardov varovanja pravic osumlencev. Tudi Resolucija o umetni inteligenci izrecno izpostavlja, da avtomatizirano odločanje ne sme temeljiti na posebnih vrstah osebnih podatkov, razen če so vzpostavljeni ustrezni ukrepi za varstvo pravic in interesov posameznika, na katerega se podatki nanašajo.⁵⁰ Resolucija poziva, naj se na javnih mestih trajno prepove uporaba avtomatizirane analize in/ali prepoznavanja na podlagi drugih človeških značilnosti, kot so hoja, prstni odtisi, DNK, glas ter drugi biometrični in vedenjski znaki. Obenem poziva k moratoriju uvedbe sistemov prepoznavanja obrazov za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj pri identifikaciji, razen če se uporabljajo izključno za identifikacijo žrtev kaznivih dejanj, dokler ne bodo tehnični standardi popolnoma v skladu s temeljnimi pravicami, rezultati pa nepristranski in nediskriminatorni, ob upoštevanju strogih zaščitnih ukrepov proti zlorabi in strogega demokratičnega nadzora in spremljanja, ter zagotovitvi, da je uporaba tehnologij nujna in sorazmerna.⁵¹

Akt o umetni inteligenci izpostavlja pravico do človeške presoje. V skladu z domnevo nedolžnosti bi bilo treba fizične osebe v EU zmeraj presojati glede na njihovo dejansko ravnanje. Preiskovancev nikoli ne bi smeli presojati na podlagi ravnanja, ki ga predvideva umetna inteligenca, ali zgolj na podlagi oblikovanih profilov, osebnostnih lastnosti ali značilnosti, kot so državljanstvo, kraj rojstva, kraj prebivališča, število otrok, stopnja zadolženosti ali vrsta avtomobila, ki jih izdela umetnointeligenčni sistem, brez dokazov o utemeljenih razlogih za sum, da je bila ta oseba vpletena v kriminalno dejavnost na podlagi objektivnih preverljivih dejstev in brez človeške ocene. Zato bi bilo treba prepovedati ocene tveganja, ki se izvajajo v

⁴⁹ Uradni list RS, št. 66/09 – uradno prečiščeno besedilo, 22/10, 26/11 – odl. US, 58/11 – ZDT-1, 40/12 – ZUJF, 96/12 – ZPIZ-2, 15/13 – ZNPPol in 15/13 – ZODPol.

⁵⁰ Resolucija o umetni inteligenci in Akt o umetni inteligenci, uvodna točka 70.

⁵¹ Glej tudi točke 6.3, 6.4. in 6.5 tega poglavja.

zvezi s fizičnimi osebami, da se oceni verjetnost, da bodo te osebe storile kaznivo dejanje, ali da se predvidi dejansko ali potencialno kaznivo dejanje samo na podlagi oblikovanja profilov teh fizičnih oseb ali ocene njihovih osebnostnih lastnosti in značilnosti. Ta prepoved se ne nanaša na sisteme umetne inteligence, ki opravljajo analizo tveganja, ki ne temelji na oblikovanju profilov oseb ali na osebnostnih lastnostih in značilnostih posameznikov za oceno verjetnosti finančnih goljufij s strani podjetij na podlagi sumljivih transakcij ali za orodja, ki izvajajo analizo tveganja, ki omogočajo napovedovanje verjetnosti lokalizacije prepovedanih drog ali nezakonitega blaga s strani carinskih organov, na primer na podlagi znanih trgovskih poti.⁵²

V pravni teoriji *Selinšek* obširneje obravnava kazenskopravni vidik uvajanja avtomatizacije in drugih novosti v digitalnih forenzičnih preiskavah. Čeprav so temelji digitalne forenzike (računalniška znanost, fizika, elektronika) razmeroma trdni in v osnovi podprti z matematično znanostjo (ENFSI, 2015), je njeno delovno področje – ob upoštevanju hitrega razvoja tehnologije in s tem povezane podatkovne ekspanzije – očitno torej preveč dinamično, da bi se (že) lahko ustalila kot splošno priznana znanstvena disciplina s trdnimi teoretičnimi in metodološkimi temelji. Kot je bilo že navedeno, to za pravosodne organe kot osrednje uporabnike njenih storitev predstavlja posebne izzive. Uporaba znanstveno nepreizkušenih tehnik za dokazovanje v kazenskem postopku je inherentno problematična, zato digitalni dokazi pogosto le s težavo zadostijo strogim zahtevam po zanesljivosti digitalnih forenzičnih dokazov. Ob odsotnosti univerzalnih pravil oziroma standardov za izvajanje digitalnih forenzičnih procesov, digitalni forenziki te preiskave opravljajo predvsem na podlagi svojih izkušenj in politike svoje organizacije, kar lahko na globalni, pa tudi na regionalni in v večjih državah celo nacionalni ravni, ustvarja precejšnjo neenakost pri izkoriščanju potenciala digitalnih forenzikov v kazenskih postopkih. Za izvedenska dela forenzikov veljajo znanstveni kriteriji, ki načeloma veljajo za izvedenska dela v kazenskih postopkih.⁵³

Med temeljnimi in najpomembnejšimi načeli kazenskega procesnega prava in postopka je načelo iskanja materialne resnice,⁵⁴ ki izhaja iz določbe 17. člena ZKP. To načelo izrecno zavezuje sodišče in državne organe, ki sodelujejo v kazenskem

⁵² Akt o umetni inteligenci, uvodna točka 42.

⁵³ Selinšek, 2021, stran 226.

⁵⁴ Gorkič in Šugman Stubbs, 2010, stran 371.

postopku (torej policijo in državno tožilstvo), da morajo po resnici in popolnoma ugotoviti dejstva, pomembna za izdajo zakonite odločbe, pri čemer morajo enako pazljivo preizkusiti in ugotoviti tako dejstva, ki obdolženca obremenjujejo, kakor tudi dejstva, ki so mu v korist.⁵⁵ Prav tako je predsednik senata v okviru pravil procesnega vodstva dolžan skrbeti za to, da se zadeva vsestransko razčisti. Posamezna načela v kazenskem postopku pomenijo odstop od načela materialne resnice. Med drugimi gre za prepoved upoštevanja tistih spoznanj, do katerih ni prišlo na način, določen z zakonom, in je predvidena njihova ekskluzija ne glede na to, da kažejo na resničnost obstoja pravno pomembnih dejstev.⁵⁶ Upošteva drugi odstavek 18. člena ZKP za nedovoljene štejejo dokazi, ki so bili pridobljeni s kršitvijo ustavno določenih človekovih pravic in temeljnih svoboščin, dokazi, ki so bili pridobljeni s kršitvijo določb kazenskega postopka in je zanje v tem zakonu določeno, da se sodna odločba nanje ne more opreti, ali ki so bili pridobljeni na podlagi takega nedovoljenega dokaza. V skladu s 83. členom ZKP sodišče po uradni dolžnosti ali na predlog stranke izloči navedene dokaze iz spisov takoj, ko ugotovi, da gre za nedovoljen dokaz. Dokaze, pridobljene na pravno nedovoljen način, torej s kršitvijo ustavno določenih pravic in temeljnih svoboščin oziroma s kršitvijo nekaterih določb kazenskega postopka, ter dokaze, pridobljene na podlagi nedovoljenega dokaza (sadeži zastrupljenega drevesa), pristojni sodnik izloči iz spisa.

Načelo pravičnega sojenja je kot temeljno pravno načelo, ki zajema vse temeljne pravice posameznika, zajeto v 6. členu EKČP, na podlagi katerega obstaja obsežna sodna praksa Evropskega sodišča za človekove pravice (ESČP). Postopek po pravilih domačega zakona, ki krši ustavna načela in splošno sprejete mednarodne standarde, ne more biti zakonit. EKČP je namreč uvedla naddržavno varstvo človekovih pravic in s tem korenito posegla v suverenost nacionalnih držav.⁵⁷ Med drugim zahteva, da so preiskovalne metode, uporabljene v konkretnem primeru, preizkušene in zanesljive. Kot eno ključnih zagotovil, da bodo državni organi spoštovali pravičnost postopka, velja omeniti ekskluzijo dokazov.⁵⁸ S stališča presoje zanesljivosti digitalnih dokazov⁵⁹ Selinšek izpostavlja, da forenzični priročniki in standardi večinoma molčijo o konceptu »veljavnega digitalnega dokaza« oziroma ne vzpostavljajo procedure za validacijo digitalnih dokazov. Tudi na pravnem področju

⁵⁵ Gorkič, Šugman Stubbs in Fišer, 2020, strani 122–127.

⁵⁶ Dežman et al., 2003, stran 271.

⁵⁷ Ribičič, 2007, strani 121.

⁵⁸ Šepec et al., 2023, strani 49 in 50.

⁵⁹ Selinšek, 2021, stran 226.

ni posebnih postopkov za validacijo teh dokazov, ampak veljajo enaka pravila kot za vse druge dokaze. *Selinšek* s tega vidika opozarja, da uvajanje avtomatizacije v digitalne forenzične preiskave sproža naslednja (medsebojno povezana) vprašanja: vprašanje zanesljivosti avtomatiziranih digitalnih forenzičnih (pod)procesov, vprašanje zanesljivosti avtomatiziranih digitalnih forenzičnih orodij in vprašanje vsebinske celovitosti oziroma zanesljivosti (delno) avtomatizirano pridobljenih digitalnih dokazov. Osrednji izziv pri prepuščanju dela preiskovalnih dejavnosti računalniškemu programu (algoritmu) je torej zagotavljanje zanesljivosti izsledkov, kar je zelo pomembno v vseh pravnih postopkih, absolutno bistveno pa v kazenskem postopku, kjer lahko pravična (oprostilna ali obsodilna) sodba temelji le na objektivno in celovito ugotovljenem dejanskem stanju.⁶⁰

Da je digitalni dokaz uporaben na sodišču, mora biti pravno dopusten in imeti ustrezno dokazno vrednost. Digitalni dokaz je pravno dopusten, kadar je pridobljen, shranjen in analiziran v skladu z določbami ZKP.⁶¹ Pravna dopustnost se, kot je bilo navedeno, presoja z vidika ustavnih in zakonskih standardov, določenih za postopanje z dokazili. Sodišče je vezano na ekskluzijska pravila, katerih dokazov zaradi nezakonitega načina pridobitve ne sme upoštevati.⁶² *Selinšek* še pojasnjuje, da pri presoji dokazne vrednosti digitalnih dokazov velja načelo proste presoje dokazov kot eno temeljnih načel kazenskega postopka. Sicer je treba pri presoji še posebej upoštevati naravo oziroma značilnosti digitalnih dokazov. *Selinšek* opozarja, da mora digitalni forenzični dokaz v tem okviru izpolnjevati naslednje elemente: avtentičnost (vsebinska verodostojnost, vključno z izkazano vzročno zvezo med dokazom in domnevnim storilcem kaznivega dejanja in med dokazom in elektronsko napravo, v kateri je shranjen); neokrnjenost oziroma integriteto (dokaz, predločen sodišču, mora biti popolnoma enak (nespremenjen), kot je obstajal ali nastal v času storitve kaznivega dejanja); preverljivost (ključno je izvajanje preiskave na identični kopiji nosilca dokaza in pravilno dokumentiranje dela v obliki skrbniške verige). Izpostavlja

⁶⁰ Prav tam, strani 224–228.

⁶¹ Pravna podlaga za obravnavo digitalnih dokazov izhaja iz določb Zakona o elektronskem poslovanju in elektronskem podpisu (Uradni list RS, št. 98/04 – uradno prečiščeno besedilo, 61/06 – ZEPT, 46/14, 121/21 – ZEISZ in 130/22 – ZN-H), kjer je v 4. členu navedeno, da se elektronskim podatkom ne sme odreči dokazne vrednosti zgolj za to, ker so v elektronski obliki. Prav tako se je Republika Slovenija s podpisom Zakona o ratifikaciji Konvencije o kibernetiski kriminaliteti in Dodatnega protokola h Konvenciji o kibernetiski kriminaliteti (Uradni list RS–MP, št. 17/2004), ki obravnava inkriminacijo rasističnih in ksenofobičnih dejanj, storjenih v informacijskih sistemih, zavezala, da bo spremenila notranjo zakonodajo, kar je storila z dopolnitvijo določb 219.a in 223.a člena ZKP. Dodana sta bila dva člena, ki sta začrtala smernice preiskav digitalne forenzike. Več o tem glej Brezovnik, 2016, stran 17.

⁶² Šepec et al., 2023, stran 189.

pa tudi vsebinsko celovitost (dokaz je treba ovrednotiti samostojno in tudi v povezavi z drugimi dokazi v tem primeru) in zanesljivost (način pridobitve dokaza in ravnanje z njim ne smeta vzbujati dvoma o avtentičnosti in verodostojnosti dokaza).⁶³

Narava dokazov, pridobljenih z umetno inteligenco, je lahko problematična z vidika zakonitosti njihove pridobitve. Če pridobitev digitalnih dokazov ne terja njihove ekskluzije, je dokaze treba presoјati glede na druge dokaze v spisu. S stališča uporabnosti v sodnih postopkih gre digitalne dokaze presoјati kot vsak drug dokaz, pri čemer sodna praksa tudi izpostavlja, da je treba pri uporabi izsledkov umetne inteligence zagotoviti kritično presoјo rezultatov raziskav, ki jih izdelata umetna inteligenca. Če bodo posamezniki preveč zaupali navidezno objektivnim in znanstvenim orodjem umetne inteligence ter ne bodo pomislili, da so lahko njihovi rezultati napačni, nepopolni, neustrezni ali diskriminacijski, lahko to privede do kršitev pravic. Pomembno je, da imamo realna pričakovanja glede teh tehnoloških rešitev in da se ne obljublja popolne rešitve na področju preprečevanja, odkrivanja in preiskovanja kaznivih dejanj in odkritje vseh storjenih kaznivih dejanj. Resolucija o umetni inteligenci še navaja, da obstoječi zaščitni ukrepi, kot je zaščitni ukrep »človek v zanki« (ki zahteva človeško interakcijo) in pravica do pojasnila, morda ne bodo zadostovali za obvladovanje tveganj. Kot se je izkazalo v primeru raziskovalnega projekta, ki ga financira EU in se osredotoča na razvoj tehnologij za zaznavanje čustev, je treba povečati preglednost in nadzor nad financiranjem raziskav umetne inteligence, zlasti na pomembnih področjih, kot je nadzor meja in varnosti. V zvezi s tem poudarja, da lahko uporaba umetne inteligence vpliva na človekove odločitve in vse faze kazenskega postopka. Zato morajo organi, ki uporabljajo sisteme umetne inteligence, spoštovati izredno visoke pravne standarde in zagotoviti človeško posredovanje, zlasti pri analizi podatkov, ki izhajajo iz teh sistemov.

5 Uporaba umetne inteligence pri nadzoru meja in upravljanju migracij

To področje predstavlja presečišče zakonskih določb, ki regulirajo javno in nacionalno varnost, določb o priseljevanju ter varovanju človekovih pravic in temeljnih svoboščin.⁶⁴ EU se pri prizadevanjih za okrepitev mejne kontrole in

⁶³ Selinšek, 2021, stran 227.

⁶⁴ Molnar et al. v Kenyon (ur.), 2018, stran 2.

zmanjševanja varnostnih tveganj, povezanih s težjimi kriminalnimi dejanji in terorizmom, usmerja k uporabi umetne inteligence. Namen uporabe umetnointeligenčnih sistemov je izboljšati učinkovitost in uspešnost pregledov na zunanjih mejah, okrepiti preprečevanje nezakonitega priseljevanja in boj proti njemu ter prispevati k visoki ravni varnosti na območju EU. Da se ohrani zaupanje javnosti v migracijski in azilni sistem, varnostne ukrepe in zmogljivosti EU za upravljanje zunanje meje, je treba zagotoviti interoperabilnost med informacijskimi sistemi EU, in sicer sistemom vstopa/izstopa (SVI), vizumskim informacijskim sistemom (VIS), evropskim sistemom za potovalne informacije in odobritve (ETIAS), sistemom Eurodac, schengenskim informacijskim sistemom (SIS) in evropskim informacijskim sistemom kazenskih evidenc za državljane tretjih držav. Za doseg tega je kot sestavne dele interoperabilnosti treba vzpostaviti evropski iskalni portal (ESP), skupno storitev za ugotavljanje ujemanja biometričnih podatkov (skupna BMS), skupno odložišče podatkov o identiteti (CIR) in detektor več identitet (MID).⁶⁵ Tudi kaznovalna in varnostna politika v Republiki Sloveniji naslavlja in izpostavlja rastoči pomen obrambe in varovanja državnega teritorija.⁶⁶ Za namene preverjanja identitete oziroma identifikacije centralizirani informacijski sistemi mejnih kontrol in varnostnih služb EU v vedno večji meri uporabljajo biometrične tehnologije. Tehnologija avtomatizirane identifikacije prstnih odtisov se trenutno uporablja v treh informacijskih sistemih: schengenskem informacijskem sistemu, v evropskem sistemu za primerjavo prstnih odtisov (Eurodac) in vizumskem informacijskem sistemu.⁶⁷ Umetna inteligenca se bo za državljane tretjih držav (ki niso članice EU) uporabljala tudi v drugih dveh sistemih, sistemu vstopa in izstopa in v informacijskem sistemu kazenskih evidenc. Interoperabilnost informacijskih sistemov EU bi morala omogočiti, da se sistemi med seboj dopolnjujejo, kar bi olajšalo pravilno identifikacijo oseb.⁶⁸ Evropski parlament je tekom priprav na sprejetje Akta o umetni inteligenci izpostavil občutljive vidike uporabe umetne inteligence na področju nadzora mej in migracijske politike.⁶⁹ Slovenska Amnesty

⁶⁵ Publications office of the EU, dostopno na: <https://op.europa.eu/en/publication-detail/-/publication/c8823cd1-a152-11ea-9d2d-01aa75ed71a1/language-en> (obiskano: 6. 1. 2025).

⁶⁶ Glej tudi Šalamon et al. v Korošec, Filipčič, Zdolšek (ur.), 2019.

⁶⁷ Tako tudi Dumbrava, 2025.

⁶⁸ Uredba (EU) 2019/817 Evropskega parlamenta in Sveta z dne 20. maja 2019 o vzpostavitvi okvira za interoperabilnost informacijskih sistemov EU na področju meja in vizumov (UL L 135, 22. 5. 2019, strani 27–84) in Uredba (EU) 2019/818 Evropskega parlamenta in Sveta z dne 20. maja 2019 o vzpostavitvi okvira za interoperabilnost informacijskih sistemov EU na področju policijskega in pravosodnega sodelovanja, azila ter migracij (UL L 135, 22. 5. 2019, strani 85–135). Več o tem tudi <https://eur-lex.europa.eu/legal-content/SL/TXT/?uri=LEGISSUM:4400468> (obiskano: 13. 2. 2025).

⁶⁹ Dumbrava, 2021.

International,⁷⁰ Ministrstvo za digitalno preobrazbo Republike Slovenije in druge podpisnice so se tekom priprave stališč k predlogu Akta o umetni inteligenci zavzeli za zaščito pravic marginaliziranih ljudi, tujcev migrantov, beguncev, iskalcev azila in drugih z neurejenim migrantskim statusom.⁷¹ Avtomatski sistemi odločanja, ki se uporabljajo v kontekstu priseljavanja in beguncev, lahko vplivajo na sposobnost ljudi, da uveljavljajo svojo svobodo gibanja, pravico do potovanja in pravice do mobilnosti.⁷²

V raziskavi *Artificial intelligence at EU borders*, 2021, *Dumbrava* ugotavlja, da z namenom nadzora meja in obvladovanja migracij v EU obstajajo štiri glavne vrste aplikacij umetne inteligence, ki se uporabljajo ali se razmišlja o njihovi uporabi v okviru mejnega nadzora in varovanja meja: biometrična identifikacija (avtomatsko prepoznavanje prstnih odtisov in obrazov), zaznavanje čustev, algoritemska ocena tveganja in orodja umetne inteligence za spremljanje, analizo in napovedovanje migracijskih tokov. Kljub napredku razvoja tehnologij biometrične identifikacije se natančnost rezultatov še vedno razlikuje v odvisnosti od uporabljene tehnologije in je odvisna od kontekstualnih dejavnikov. Tehnologija avtomatiziranega prepoznavanja obrazov se še ne uporablja v informacijskih sistemih EU, vendar je pričakovati, da bodo v bližnji prihodnosti sistemi za preverjanje in/ali identifikacijo obdelovali obrazne slike. Tehnologije za zaznavanje čustev na mejah in drugod predstavljajo eno najbolj kontroverznih aplikacij umetne inteligence. Sicer trenutno na mejah EU ni nameščenih nobenih sistemov za zaznavanje čustev, so pa takšne tehnologije za izboljšanja nadzora meja v številnih pobudah in projektih, ki jih financira EU. Poleg preverjanja identifikacije znanih oseb se algoritmi umetne inteligence uporabljajo tudi za identifikacijo zanimivih neznanih oseb na podlagi posebnih podatkovnih profilov tveganja. Algoritemsko profiliranje za ocenjevanje varnostnih tveganj in ilegalnih (nedovoljenih) migracij se trenutno razvija v okviru vizumskega informacijskega sistema in evropskega sistema za izmenjavo potovalnih informacij o potnikih. Avtomatizirano oceno tveganja izvajajo države članice v okviru medsebojne izmenjave obveščevalnih podatkov o potnikih. EU prav tako vlaga v orodja za spremljanje, analiziranje in napovedovanje migracijskih trendov in varnostnih groženj, ki temeljijo na umetni inteligenci. Evropski urad za podporo

⁷⁰ Amnesty International Slovenija, 2023, dostopno na: <https://www.amnesty.si/akt-o-umetni-inteligenci>, (obiskano: 6. 1. 2025).

⁷¹ Enako tudi Amnesty International, 2024, dostopno na: <https://www.amnesty.org/en/documents/pol40/7772/2024/en/> (obiskano: 6. 1. 2025).

⁷² Več o tem Molnar et al., 2018.

azilnih vprašanj trenutno uporablja sistem zgodnjega opozarjanja in napovedovanja za napovedovanje števila prošenj za azil. Evropska komisija in agencije EU na področju svobode, varnosti in prava raziskujejo druge aplikacije na tem področju tudi v okviru razvoja sistema Frontex, Eurosur in središča za inovacije Europol. *Ciudad Fontecha* je opravila novejšo podrobnejšo raziskavo uvajanja tehnologij umetne inteligence za varovanje mej in obvladovanje migracij. V okviru študije je izpostavljen pomen uvajanja novih tehnologij za namene mejnega nadzora ter varnostne in azilne politike in pomen sočasnega varovanja pravic. Izpostavljena je tudi kritika evropskih sistemov interoperabilnosti, ki naj bi jo zaradi nevarovanja pravic državljanov tretjih držav podale številne človekoljubne organizacije.⁷³ Tudi kanadska vlada vlaga v nova prizadevanja za varnost meja in identifikacijo. Kanadska vlada vključuje razširitev prizadevanj za zbiranje prstnih odtisov tujih državljanov in premik v smeri razvoja koncepta digitalne identitete znanega popotnika, za olajšanje ocene tveganja pred preverjanjem in varnostnih postopkov, na primer z omogočanjem priseljenskih poti, ki temeljijo na tveganju.⁷⁴ Tehnologija sama po sebi ni demokratična in vpliva na človekove pravice, kar je še posebej pomembno upoštevati v kontekstu prisilnih migracij, ko je tehnologija uporabljena zoper priseljence in deluje nehumano.⁷⁵ Iz uvodne točke 60 Akta o umetni inteligenci izhaja, da bi umetnointeligenčni sistemi na področju migracij, azila in upravljanja nadzora meja, ki jih ta predpis zajema, morali biti skladni z ustreznimi postopkovnimi zahtevami iz Uredbe (ES) št. 810/2009 Evropskega parlamenta in Sveta z dne 13. julij 2009 o vizumskem zakoniku Skupnosti z dne 13. julija 2009 o vizumskem zakoniku Skupnosti,⁷⁶ Direktive 2013/32/EU Evropskega parlamenta in Sveta z dne 26. junija 2013 o skupnih postopkih za priznanje ali odvzem mednarodne zaščite,⁷⁷ in drugega ustreznega prava EU. Države članice ali institucije, organi, uradi ali agencije EU v nobenem primeru ne bi smeli uporabljati umetnointeligenčnih sistemov na področju migracij, azila in upravljanja nadzora meja kot sredstev za izogibanje svojim mednarodnim obveznostim iz Konvencije Združenih narodov o statusu beguncev.⁷⁸ Prav tako se ne smejo uporabljati za

⁷³ Ciudad Fontecha, 2023.

⁷⁴ Več o tem Molnar et al., 2018, stran 22.

⁷⁵ Molnar, 2019.

⁷⁶ UL L 243, 15. 9. 2009, strani 1–58.

⁷⁷ UL L 180, 29. 6. 2013, strani 60–95.

⁷⁸ Konvencijo Združenih narodov o statusu beguncev je sprejela Diplomatska konferenca Združenih narodov o statusu beguncev in oseb brez državljanstva 28. julija 1951 v skladu z resolucijo št. 429 (V) Generalne skupščine z dne 14. decembra 1950. Veljati je začela 22. aprila 1954.

kakršno koli kršitev načela nevračanja ali za odrekanje varnih in učinkovitih zakonitih poti na ozemlje EU, vključno s pravico do mednarodne zaščite.⁷⁹

6 Etična načela za uporabo umetnointeligenčnih sistemov v kazenskem pravu

6.1 Uvodno

Resolucija o umetni inteligenci izpostavlja, da nobenemu sistemu umetne inteligence, ki se uporablja na področju preprečevanja, odkrivanja in preiskovanja kaznivih dejanj in pravosodja, ne bi smelo biti omogočeno, da posega v telesno celovitost ljudi ali posameznikom podeljuje pravice ali nalaga pravne obveznosti. Opozarja tudi, da mora v okviru pravosodja in preprečevanja, odkrivanja ter preiskovanja kaznivih dejanj vsako odločitev, ki ima pravni ali podobni učinek, vedno sprejeti človek. Ta lahko odgovarja za sprejete odločitve. Tisti, ki so podvrženi sistemom, ki temeljijo na umetni inteligenci, morajo imeti možnost uporabe pravnih sredstev. Resolucija tudi navaja, da ima oseba v skladu s pravom EU pravico, da ni predmet odločitve, ki ima zanj pravne učinke ali nanjo znatno vpliva, in temelji izključno na avtomatizirani obdelavi podatkov, kot tudi, da človek ne more podati neodvisne ocene, če se zanaša le na podatke, profile in priporočila, ki jih ustvarjajo stroji. Pravica do človeškega posredovanja je pomembna zaradi morebitnih hudih negativnih posledic, zlasti na področju preprečevanja, odkrivanja in preiskovanja kaznivih dejanj ter pravosodja. V zvezi s tem tudi Etične smernice izpostavljajo, da lahko uporaba umetne inteligence vpliva na človekove odločitve in vse faze kazenskega postopka. Zato morajo organi, ki uporabljajo sisteme umetne inteligence, spoštovati izredno visoke pravne standarde in zagotoviti človeško posredovanje. Resolucija opozarja, da je pri analizi podatkov, ki izhajajo iz teh sistemov, treba ohraniti diskrecijsko pravico sodnikov in odločanje za vsak primer posebej. Zato poziva k prepovedi uporabe umetne inteligence in sorodnih tehnologij za predlaganje sodb. Izpostavljeno je, da morajo izvršitveni organi, ko v okviru pravosodnega sodelovanja odločajo o prošnji za izročitev (ali predajo) drugi državi članici ali tretji državi, oceniti, ali je morda zaradi uporabe orodij umetne inteligence v državi prosilki ogrožena temeljna pravica do poštenega sojenja. Zato je bil naslovljen poziv na Evropsko komisijo, naj izda smernice, kako to ocenjevati v

⁷⁹ Več o tem glej Akt o umetni inteligenci, uvodna točka 60.

okviru pravosodnega sodelovanja v kazenskih zadevah. Zato bi morale države članice v skladu z veljavno zakonodajo poskrbeti, da so posamezniki obveščeni, kadar jih organi preprečevanja, odkrivanja in preiskovanja kaznivih dejanj ali pravosodni organi obravnavajo z uporabo aplikacij umetne inteligence.⁸⁰

6.2 Načelo preglednosti, nepristranskosti in pravičnosti

Raznolikost, nediskriminacija in pravičnost vključujejo preprečevanje nepoštenih pristranskosti, dostopnost in univerzalno zasnovo ter sodelovanje deležnikov. Preglednost vključuje sledljivost, razločljivost in obveščanje, kot navajajo Etične smernice. Gre za različne elemente postopkovne pravičnosti, ki so pomembni za sprejetje avtomatiziranih sistemov odločanja, vključno s pravico do zaslišanja, pravico do poštenega, nepristranskega in neodvisnega odločevalca, pravico do obrazložitve (vedno bolj znana tudi kot pravica do pojasnila) in pravico do pritožbe zoper neugodno odločitev, ki naj jih vključujejo avtomatizirani sistemi odločanja.⁸¹ V okviru pravosodja in preprečevanja, odkrivanja ter preiskovanja kaznivih dejanj mora vsako odločitev, ki ima pravni ali podoben učinek, vedno sprejeti človek, ki lahko odgovarja za sprejete odločitve. Resolucija o umetni inteligenci izpostavlja, da morajo imeti tisti, ki so podvrženi sistemom, ki temeljijo na umetni inteligenci, možnost uporabe pravnih sredstev, prav tako pa ima oseba v skladu s pravom EU pravico, da ni predmet odločitve, ki ima zanj pravne učinke ali nanjo znatno vpliva in temelji izključno na avtomatizirani obdelavi podatkov. Resolucija o umetni inteligenci še opozarja, da je zaradi zapletenosti razvoja in upravljanja sistemov umetne inteligence izziv, kako pravilno določiti odgovornost za morebitno škodo, ter narekuje, da je treba oblikovati jasen in pravičen sistem za dodelitev pravne odgovornosti in krivdne sposobnosti za morebitne škodljive posledice teh naprednih digitalnih tehnologij. Poziva k uporabi previdnostnega načela pri vseh aplikacijah umetne inteligence na področju preprečevanja, odkrivanja in preiskovanja kaznivih dejanj ter poudarja, da mora pravno odgovornost vedno nositi fizična ali pravna oseba. Na nabore podatkov, ki jih uporabljajo sistemi umetne inteligence (za učenje in delovanje), lahko negativno vplivajo vključitev nenamerne zgodovinske pristranskosti, nepopolnost in slabi modeli upravljanja. Nadaljevanje take pristranskosti bi lahko povzročilo (ne)posredne predsodke do nekaterih skupin ali ljudi in njihovo diskriminacijo, kar bi lahko še povečalo predsodke in marginalizacijo.

⁸⁰ Resolucija o umetni inteligenci, točke 12–17.

⁸¹ Molnar et al., 2018, strani 32–45.

Škoda lahko nastane tudi zaradi namernega izkoriščanja pristranskosti (potrošnikov) ali sodelovanja v nelojalni konkurenci, na primer z izenačevanjem cen s koluzijo ali nepreglednim trgom. Kadar je to mogoče, je treba ugotovljivo in diskriminacijsko pristranskost odstraniti v fazi zbiranja podatkov. Na način razvoja sistemov umetne inteligence (npr. programiranje algoritmov) lahko negativno vpliva tudi nepoštena pristranskost. To bi se lahko preprečilo z vzpostavitvijo postopkov nadzora za jasno in pregledno analizo in obravnavo namena, omejitev, zahtev in odločitev sistema. Poleg tega je mogoče z zaposlovanjem ljudi iz različnih okolij, kultur in disciplin zagotoviti raznolikost mnenj, kar bi bilo treba spodbujati, kot to poudarjajo Etične smernice.⁸² Nabori podatkov in algoritemski sistemi, ki se na različnih stopnjah obdelave uporabljajo pri razvoju umetne inteligence, robotike in sorodnih tehnologij, lahko povzročijo neposredno in posredno diskriminacijo skupin ljudi, zlasti ker podatki, ki se uporabljajo za učenje algoritmov za napovedano policijsko delo, vplivajo na prednostne naloge nadzora in lahko ohranijo ali povečajo obstoječe predsodke.⁸³ Uvodne točke 64 do 68 Akta o umetni inteligenci tako navajajo, da lahko tveganja, povezana z umetnointeligenčnimi sistemi, nastanejo zaradi načina zasnove takih sistemov, kakor tudi iz tega, kako se ti uporabljajo. Uvajalci lahko tako opredelijo potencialna velika tveganja, ki niso bila predvidena v fazi razvoja. Po potrebi bi morali obvestiti fizične osebe, da se zanje uporablja visoko tvegani sistem umetne inteligence. Informacije bi morale vključevati predvideni namen sistema in vrsto odločitev, ki jih sprejema. Uvajalec bi moral fizične osebe obvestiti tudi o njihovi pravici do obrazložitve, določeni v Aktu o umetni inteligenci.⁸⁴

6.3 Načelo človeške avtonomije

Človeško delovanje in nadzor vključuje temeljne pravice, človeško delovanje in človeški nadzor.⁸⁵ Temeljne pravice, na katerih temelji EU, so namenjene zagotavljanju spoštovanja svobode in avtonomije ljudi. Ljudje, ki komunicirajo s sistemi umetne inteligence, morajo imeti možnost, da se še naprej v celoti in dejansko samostojno odločajo in sodelujejo v demokratičnem procesu. Gre za skupine temeljnih pravic, posebej primerne za zajem sistemov umetne inteligence. Številne od teh pravic so v določenih okoliščinah pravno izvršljive v EU, tako da je upoštevanje njihovih pogojev po zakonu obvezno. Tudi po tem, ko je dosežena

⁸² Etične smernice, stran 22.

⁸³ Glej Resolucija o umetni inteligenci, točka 22.

⁸⁴ Akt o umetni inteligenci, uvodne točke 64–68.

⁸⁵ Etične smernice, stran 19.

skladnost s pravno izvršljivimi temeljnimi pravicami, pa nam lahko etično razmišljanje pomaga razumeti, kako lahko razvoj, uvajanje in uporaba umetne inteligence vključujejo temeljne pravice in njihove temeljne vrednote, ter zagotoviti natančnejša navodila, ko si prizadevamo ugotoviti, kaj bi morali narediti s tehnologijo in ne kaj (trenutno) lahko naredimo z njo.⁸⁶

6.4 Načelo varovanja temeljnih pravic

Temeljni instrument pravnega okvira EU za varstvo temeljnih pravic, ki se nanaša na uporabo umetne inteligence, je Listina Evropske unije o temeljnih pravicah, ki skupaj z nenapisanimi splošnimi načeli prava EU predstavlja glavni vir temeljnih pravic v EU. Listina vsebuje širok spekter temeljnih pravic in ima enako pravno veljavnost kot Pogodbi EU ter zavezuje vse institucije in organe EU, pa tudi države članice, ko izvajajo pravo EU (prvi odstavek 51. člena). Številne pravice iz Listine Evropske unije o temeljnih pravicah so enake tistim iz EKČP. Njihova vsebina in obseg morata biti enaka ustreznim pravicam, zagotovljenim z EKČP (tretji odstavek 52. člena Listine). Vendar ta določba ne preprečuje širšega varstva po pravu EU.⁸⁷ Temeljne pravice je mogoče najti tudi v določbah Pogodb EU (glej npr. drugi odstavek 6. člena PEU ter naslova V in X PDEU) in drugih dokumentih sekundarne zakonodaje EU.⁸⁸ Načelo poudarja, da je treba prepovedati uporabo umetne inteligence, če ni združljiva s temeljnimi pravicami. Pri tem se opira na neodtujljive pravice iz mednarodnega prava o človekovih pravicah, Pogodb EU in Listine Evropske unije o temeljnih pravicah, ki določajo spoštovanje človekovega dostojanstva, svobodo posameznika, spoštovanje demokracije, pravičnosti in pravne

⁸⁶ Prav tam, stran 14.

⁸⁷ Načelo varovanja temeljnih pravic, povzeto v uvodu Resolucije o umetni inteligenci v kazenskih zadevah in njeni uporabi v policiji in pravosodnih organih na področju kazenskih zadev, izhaja iz Pogodbe o EU (UL C 202, 7. 6. 2016, strani 47–390), zlasti 2. in 6. člena, PDEU, zlasti 16. člena, Listine Evropske unije o temeljnih pravicah, zlasti členov 6., 7., 8., 11., 12., 13., 20., 21., 24. in 47., EKČP, Konvencije Sveta Evrope o varstvu posameznika glede na avtomatsko, obdelavo osebnih podatkov (ETS 108) in protokola o njeni spremembi (konvencija 108+), Strasbourgške konvencije (28. 1. 1981, ETS št. 108), Evropske etične listine za uporabo umetne inteligence v pravosodnih sistemih in njihovem okolju, ki jo je pripravila Evropska komisija za učinkovitost pravosodja (CEPEJ) pri Svetu Evrope (2018), Sporočila Komisije z dne 8. aprila 2019 o krepitvi zaupanja v umetno inteligenco, osredotočeno na človeka (COM(2019)0168) final, 8. 4. 2019), Etičnih smernic za zaupanja vredno umetno inteligenco, ki jih je 8. aprila 2019 objavila strokovna skupina Komisije na visoki ravni za umetno inteligenco (Strokovna skupina na visoki ravni za umetno inteligenco, Etične smernice za zaupanja vredno umetno inteligenco, 8. 4. 2019), Bele knjige Komisije z dne 19. februarja 2020 o umetni inteligenci – evropski pristop k odličnosti in zaupanju (COM(2020)0065 final, UL C 65, 19. 2. 2020) in drugih. Več o tem Resolucija o umetni inteligenci, strani 17 in 18.

⁸⁸ FRA, Agencija Evropske unije za temeljne pravice, (2021), Pravilno ravnanje v prihodnje, stran 5, dostopno na: https://fra.europa.eu/sites/default/files/fra_uploads/fra-2020-artificial-intelligence_sl.pdf, <https://eur-lex.europa.eu/legal-content/SL/TXT/?uri=LEGISSUM:4365508> (obiskano: 13. 2. 2025).

države, enakost, nediskriminacijo in solidarnost, vključno s pravicami oseb, ki jim grozi izključenost. Državljeni imajo različne pravice, vključno z volilno pravico, pravico do dobrega upravljanja ali dostopa do javnih dokumentov in pravico do naslavljanja peticij na upravo. Sistemi umetne inteligence ponujajo velik potencial za izboljšanje razsežnosti in učinkovitosti vlade pri zagotavljanju javnih dobrin in storitev družbi. Hkrati bi lahko primeri uporabe umetne inteligence negativno vplivali na pravice državljanov, ki bi jih bilo zato treba zaščititi. Kadar se uporablja pojem »pravice državljanov«, to ne pomeni zanikanja ali zanemarjanja pravic državljanov tretjih držav in oseb z neurejenim statusom v EU (ali oseb, ki nezakonito prebivajo v EU), saj imajo državljani tretjih držav prav tako pravice po mednarodnem pravu in zato tudi na področju umetne inteligence.⁸⁹ Resolucija o umetni inteligenci izpostavlja, da morajo biti vse rešitve umetne inteligence na področju kazenskega prava ter preprečevanja, odkrivanja in preiskovanja kaznivih dejanj in pravosodja v skladu z Listino Evropske unije o temeljnih pravicah in EKČP, ki prav tako nalagata v celoti spoštovati načela človekovega dostojanstva, nediskriminacije, svobode gibanja, domneve nedolžnosti in pravice do obrambe, vključno s pravico do molka, svobodo izražanja in obveščanja, svobodo zbiranja in združevanja, enakosti pred zakonom, načela enakosti orožij ter pravice do učinkovitega pravnega sredstva in poštenega sojenja. Našteto je treba zagotavljati pri splošni rabi umetne inteligence ter še posebej na področju preprečevanja, odkrivanja in preiskovanja kaznivih dejanj in pravosodja. Resolucija o umetni inteligenci tudi opozarja na tveganje, da bi uporaba umetne inteligence pri preprečevanju, odkrivanju in preiskovanju kaznivih dejanj vključevala številna potencialno visoka in nesprejemljiva tveganja za varstvo temeljnih pravic posameznikov, kot so nepregledno odločanje, različne oblike diskriminacije in napake, neločljivo povezane z osnovnim algoritmom, ki se lahko s povratnimi učinki še povečajo, ter tveganja za varstvo zasebnosti in osebnih podatkov ter svobode izražanja in obveščanja, domnevo nedolžnosti, pravico do učinkovitega pravnega sredstva in poštenega sojenja. Poudarja, da avtomatizirano odločanje ne sme temeljiti na posebnih vrstah osebnih podatkov, razen če so vzpostavljeni ustrezni ukrepi za varstvo pravic in svoboščin ter zakonitih interesov posameznika, na katere se nanašajo osebni podatki. Izražena je namreč skupna politična volja držav članic za zagotovitev spoštovanja temeljnih pravic pri uporabi sistemov umetne inteligence na področju preprečevanja, odkrivanja in preiskovanja kaznivih dejanj in pravosodja. Te pravice izhajajo iz

⁸⁹ Etične smernice, strani 12 in 13.

določb 2. in 3. člena PEU, Listine Evropske unije o temeljnih pravicah, zlasti v členih 7., 8., 11., 12., 13., 20., 21., 24. in 47., EKČP in drugih predpisov.

6.5 Pravica do zasebnosti in varstvo podatkov

Zasebnost in upravljanje podatkov vključuje spoštovanje zasebnosti, kakovost in celovitost podatkov ter dostop do njih. Uvodne točke Akta o umetni inteligenci izpostavljajo pomembnost varstva posameznika pri obdelavi osebnih podatkov, ki na ravni EU predstavlja eno od temeljnih človekovih pravic na podlagi 8. člena Listine Evropske unije o temeljnih pravicah. Temeljna pravica do varstva osebnih podatkov je zajamčena zlasti z Uredbo (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES (Splošna uredba o varstvu podatkov)⁹⁰ in Uredbo (EU) 2018/1725 Evropskega parlamenta in Sveta z dne 23. oktobra 2018 o varstvu posameznikov pri obdelavi osebnih podatkov v institucijah, organih, uradih in agencijah Unije in o prostem pretoku takih podatkov ter o razveljavitvi Uredbe (ES) št. 45/2001 in Sklepa št. 1247/2002/ES⁹¹ Evropskega parlamenta in Sveta ter Direktivo (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 Evropskega parlamenta in Sveta o varstvu osebnih podatkov, ki se obdelujejo v okviru policijskega in pravosodnega sodelovanja v kazenskih zadevah.⁹²

Direktiva 2002/58/ES Evropskega parlamenta in Sveta z dne 12. julija 2002 o obdelavi osebnih podatkov in varstvu zasebnosti na področju elektronskih komunikacij⁹³ poleg tega varuje zasebno življenje in zaupnost komunikacij, vključno z zagotavljanjem pogojev za shranjevanje osebnih in neosebnih podatkov na terminalski opremi in za dostop do teh podatkov z nje. Navedeni pravni akti EU so podlaga za vzdržno in odgovorno obdelavo podatkov, tudi kadar nabori podatkov vključujejo kombinacijo osebnih in neosebnih podatkov.⁹⁴ Država zagotavlja

⁹⁰ UL L 119, 4. 5. 2016, strani 1–88.

⁹¹ UL L 295, 21. 11. 2018, strani 39–98.

⁹² UL L 119, 4. 5. 2016, strani 89–131.

⁹³ UL L 201, 31. 7. 2002, strani 37–47.

⁹⁴ Akt o umetni inteligenci, uvodna točka 10.

dostopnost odprtih podatkov javnega sektorja širokemu krogu uporabnikov,⁹⁵ zavedajoč se vloge različnih socialnih omrežij in platform, ki generirajo, zbirajo in hranijo podatke, povezovanje podatkov iz različnih virov javnega in zasebnega sektorja na področjih jezikovnih virov, opazovanja okolja, zdravja, prostorskega načrtovanja, prometa ter njihovega povezovanja s podatki industrijskega sektorja, finančnega sektorja in turizma, ob jasnem zavedanju, da je široko povezovanje različnih virov neosebnih podatkov lahko problematično tudi z vidika varovanja zasebnosti,⁹⁶ posebej v kontekstu uporabe orodij umetne inteligence, ki lahko tudi na podlagi teh podatkov zelo dobro in natančno določijo (profilirajo) posamezne osebe in njihove aktivnosti in s tem posredno vplivajo tudi na področje regulacije osebnih podatkov. Ustrezen pravni okvir mora zato ustrezno odgovoriti tudi na te izzive. Obenem lahko te aplikacije ogrozijo temeljne pravice ljudi, zato je vsakršna splošna uporaba umetne inteligence za namene množičnega nadzora nesorazmerna.⁹⁷

6.6 Načelo nediskriminacije

Etične smernice opozarjajo, da je treba enako spoštovati moralne vrednosti in dostojanstvo vseh ljudi. To presega nediskriminacijo, ki dopušča razlikovanje med različnimi situacijami na podlagi objektivnih razlogov. Pri umetni inteligenci enakost pomeni, da delovanje sistema ne sme dati nepošteno pristranskih rezultatov. Podatki, ki se uporabljajo za učenje sistemov umetne inteligence, bi morali biti čim bolj vključujoči in predstavljati različne skupine prebivalstva. Za to je potrebno spoštovanje potencialno ranljivih oseb in skupin, kot so delavci, ženske, invalidi, etnične manjšine, otroci, potrošniki ali druge osebe, ki jim grozi izključenost.⁹⁸ Izpostaviti velja pomisleke, da se zaradi napovedi umetne inteligence na podlagi značilnosti določene skupine oseb krepijo obstoječe oblike diskriminacije. Močno si je treba prizadevati za preprečevanje samodejne diskriminacije in pristranskosti in pozivati k zanesljivim dodatnim zaščitnim ukrepom, kadar se sistemi umetne inteligence na področju preprečevanja, odkrivanja in preiskovanja kaznivih dejanj in

⁹⁵ Nacionalni program spodbujanja razvoja in uporabe umetne inteligence v Republiki Sloveniji do leta 2025, dostopno na: [file:///C:/Users/uporabnik/Downloads/NpUI-SI-2025%20\(6\).pdf](file:///C:/Users/uporabnik/Downloads/NpUI-SI-2025%20(6).pdf) (obiskano: 6. 1. 2025).

⁹⁶ V Kanadi so tako primeroma opozorili, da izsledki preverjanja lahko vsebujejo občutljive podatke, vključno z dostopom do baze podatkov kanadskega policijskega informacijskega centra (CPIC), ki v skladu z zakonom o duševnem zdravju vsebuje občutljive zdravstvene podatke, vključno s poskusi samomora in nalogi za prijetje. Povzeto po Molnar et al., 2018.

⁹⁷ Resolucija o umetni inteligenci, točka H.

⁹⁸ Etične smernice, stran 13.

pravosodja uporabljajo za mladoletnike.⁹⁹ Nabori podatkov in algoritemski sistemi, ki se na različnih stopnjah obdelave podatkov pri razvoju umetne inteligence, robotike in sorodne tehnologije uporabljajo pri razvrščanju, ocenjevanju in napovedovanju, lahko povzročijo različno obravnavo ter neposredno in posredno diskriminacijo skupin ljudi.¹⁰⁰ Podatki, ki se uporabljajo za učenje algoritmov za napovedno policijsko delo, vplivajo na sedanje prednostne naloge nadzora in lahko posledično ohranijo in povečajo obstoječe predsodke. Skupine, odgovorne za zasnovo, razvoj, preskušanje, vzdrževanje, uvajanje in nabavo sistemov umetne inteligence za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj, ter pravosodje, so dolžni zmanjšati tveganja za diskriminacijo. Resolucija o umetni inteligenci izpostavlja, da povečana uporaba biometričnih podatkov v informacijskih sistemih EU povečuje tveganje za nezakonito profiliranje (podobe obraza lahko na primer razkrijejo etnično poreklo). Tudi če profiliranje ne temelji na biometričnih ali osebnih podatkih, lahko druge vrste podatkov in/ali njihove kombinacije, ki se uporabljajo za algoritemsko profiliranje, povzročijo diskriminacijo na podlagi prepovedanih razlogov. Odločitve na področju preprečevanja, odkrivanja in preiskovanja kaznivih dejanj so skoraj vedno odločitve, ki imajo zaradi izvršilne narave organov preprečevanja, odkrivanja in preiskovanja kaznivih dejanj in njihovih ukrepov pravni učinek za osebo, na katero se nanašajo. Resolucija o umetni inteligenci opozarja, da obstaja tveganje, da se odločitve v zvezi z življenjskim ciklom in uporabo aplikacij umetne inteligence na področju pravosodja in kazenskega pregona ne bi sprejemale na pregleden način in se pri tem ne bi popolnoma varovale temeljne pravice¹⁰¹ ter bi se ohranjali obstoječa diskriminacija, pristranskost in predsodki. Že v preteklosti je bilo izpostavljeno, da številne tehnologije za identifikacijo, ki temeljijo na algoritmih in se trenutno uporabljajo, nebelce, pripadnike nekaterih etničnih skupnosti, osebe LGBTI, otroke, starejše in ženske nesorazmerno pogosteje napačno identificirajo in klasificirajo ter jim s tem povzročajo škodo. Posamezniki imajo pravico, da so pravilno identificirani, pa tudi pravico, da sploh niso identificirani, razen če identifikacijo zahteva zakon zaradi utemeljenih in legitimnih javnih interesov. Resolucija o umetni inteligenci prav tako navaja, da so odločitve na področju preprečevanja, odkrivanja in preprečevanja kaznivih dejanj skoraj vedno odločitve, ki imajo zaradi izvršilne narave organov preprečevanja, odkrivanja in preiskovanja kaznivih dejanj in njihovih ukrepov pravni

⁹⁹ Resolucija o umetni inteligenci, točka 9.

¹⁰⁰ Etične smernice, stran 22.

¹⁰¹ Akt o umetni inteligenci, uvodni točki 48 in 59.

učinek za osebo, na katero se nanašajo.¹⁰² Nadalje poudarja, da prepoved diskriminacije izhaja iz vrste mednarodnih in domačih pravnih norm, med njimi 14. člena EKČP, 2. člena PEU, 21. in 23. člena Listine Evropske unije o temeljnih pravicah ter 14. člena Ustave RS. Ta pravni okvir ne le prepoveduje diskriminacijo, temveč tudi poskuša zagotavljati, da so vsi, ne glede na osebne značilnosti, deležni enakih pravic in pravnega varstva in da jim je zagotovljena pravica do pravnega sredstva in poštenega sojenja, kar krepi zaupanje v pravosodni sistem in družbeno pravičnost, pa tudi preprečuje tveganja za svobodo in varnost posameznikov.¹⁰³

6.7 Načelo kakovosti in varnosti

Tehnična robustnost in varnost vključuje odpornost proti napadom in varnost, rezervni načrt in splošno varnost, točnost, zanesljivost in ponovljivost. Uvodne točke Akta o umetni inteligenci izpostavljajo, da bi v okviru uporabe tega predpisa, skladno z zahtevo po pismenosti na tem področju, bilo treba vsem zadevnim akterjem v verigi zagotoviti vpoglede, potrebne za zagotovitev ustrezne skladnosti s tem predpisom in njegovo pravilno izvrševanje. Ponudniki umetnointeligenčnih sistemov velikega tveganja bodo morali izvajati tudi sisteme za upravljanje kakovosti in tveganj, da bi zagotovili skladnost z novimi zahtevami ter čim bolj zmanjšali tveganja za uporabnike in izpostavljene osebe. Akt o umetni inteligenci postavlja zahtevo, da je treba zagotoviti ustrezno spremljanje zmogljivosti umetnointeligenčnih sistemov v realnem življenju, saj ti predstavljajo tveganja za varnost in temeljne pravice, ki so morda povezane z njihovo uporabo. Prav tako je primerno določiti posebne odgovornosti za uvajalce.¹⁰⁴ S stališča kakovosti in varnosti se točnost nanaša na sposobnost sistema umetne inteligence, da pravilno razvršča informacije v ustrezne kategorije ali oblikuje pravilne napovedi, priporočila in odločitve na podlagi podatkov ali modelov. Če se občasnim netočnim napovedim ni mogoče izogniti, je pomembno, da lahko sistem navede, kako verjetne so te napake. Visoka stopnja točnosti je še posebno pomembna v situacijah, ko sistem umetne inteligence neposredno vpliva na človeška življenja.¹⁰⁵ Umetnointeligenčni sistemi velikega tveganja, ki jih uvajajo javni organi ali subjekti, ki delujejo v njihovem imenu, bodo morali biti registrirani v javni podatkovni zbirki EU, razen če se ti sistemi uporabljajo na področjih preprečevanja, odkrivanja in preiskovanja kaznivih

¹⁰² Resolucija o umetni inteligenci, točki 8 in 9, glej tudi točke L–P.

¹⁰³ Več o tem Škrjanc, 2024.

¹⁰⁴ Evropska komisija, 2024.

¹⁰⁵ Etične smernice, stran 20.

dejanj ali migracij. Sisteme, ki se uporabljajo na področjih preprečevanja, odkrivanja in preiskovanja kaznivih dejanj ali migracij, bo treba registrirati v nejavnem delu podatkovne zbirke, ki bo dostopen le ustreznim nadzornim organom. Da bi zagotovili skladnost v celotnem življenjskem ciklu umetnointeligenčnega sistema, bodo organi za nadzor trga izvajali redne revizije, olajševali spremljanje po dajanju na trg ter ponudnikom omogočili, da prostovoljno poročajo o vseh hudih incidentih ali kršitvah obveznosti glede temeljnih pravic, ki jih opazijo. V izjemnih primerih lahko organi odobrijo izjeme za nekatere umetnointeligenčne sisteme velikega tveganja, ki se dajo na trg. Zahteve bodo v primeru kršitve nacionalnim organom omogočile dostop do informacij, ki so potrebne za preiskavo tega, ali je uporaba umetnointeligenčnega sistema skladna s pravom.¹⁰⁶ Resolucija o umetni inteligenci izpostavlja pomen razumljivosti rezultatov, saj bi moral biti organom preprečevanja, odkrivanja ali preiskovanja ali pravosodnim organom v EU dovoljen nakup le orodij in sistemov, katerih algoritmi in logika so preverljivi in dostopni vsaj policiji in sodstvu ter neodvisnim revizorjem, da jih lahko ocenijo, pregledajo in preverijo, prodajalci pa jih ne smejo zapreti ali označiti kot lastniške, da se zagotovijo tehnična preglednost, zanesljivost in točnost. Pravosodni organi in organi preprečevanja, odkrivanja in preiskovanja kaznivih dejanj naj zagotovijo proaktivno popolno preglednost zasebnih podjetij, ki jim zagotavljajo sisteme umetne inteligence za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj in pravosodja. Za dosego tega namena Resolucija o umetni inteligenci priporoča uporabo odprtokodne programske opreme, kjer je to mogoče.

6.8 Načelo »pod nadzorom uporabnika«

Uporabniki bi morali imeti možnost sprejemati samostojne informirane odločitve glede sistemov umetne inteligence. Zagotoviti bi jim bilo treba znanje in orodja za zadovoljivo razumevanje sistemov umetne inteligence in interakcijo z njimi ter jim po možnosti omogočiti, da razumno sami ocenijo ali izpodbijajo sistem. Sistemi umetne inteligence bi morali posameznike podpirati pri sprejemanju boljših, bolj informiranih odločitev v skladu z njihovimi cilji. Človeški nadzor pomaga zagotavljati, da sistem umetne inteligence ne ogroža človekove avtonomije ali povzroča drugih škodljivih učinkov. Nadzor se lahko doseže z mehanizmi upravljanja, kot so pristopi s človekovim posredovanjem (HITL, human-in-the-

¹⁰⁶Evropska komisija, 2024.

loop), človekovim nadzorom (HOTL, human-on-the-loop) ali človekovim odločanjem (HIC, human-in-command).¹⁰⁷ Resolucija o umetni inteligenci v točki 17 poziva k algoritemski razločljivosti, preglednosti, sledljivosti in preverljivosti, saj so nujen del nadzora, da bodo razvoj, uvajanje in uporaba sistemov umetne inteligence za pravosodje ter preprečevanje, odkrivanje in preiskovanje kaznivih dejanj skladni s temeljnimi pravicami in jim bodo državljani zaupali.

7 Nesprejemljivo tveganje in prepovedane prakse

Akt o umetni inteligenci podaja celovit pristop do področij dovoljenega in nedovoljenega delovanja. Določba 5. člena kot sklop posebno škodljivih uporab umetne inteligence, ki so v nasprotju z vrednotami EU, ker kršijo temeljne pravice in so zato prepovedane, opredeljuje sisteme za sklepanje o čustvih na delovnem mestu, prakse izkoriščanja ranljivosti oseb, prirejanje in uporabo subliminalnih tehnik, družbeno točkovanje za javne in zasebne namene ter rasno profiliranje. Za zagotovitev odgovorne in sorazmerne uporabe teh sistemov je pomembno določiti, da bi bilo treba v vsakem od teh izrecno naštetih in ozko opredeljenih primerov upoštevati nekatere elemente, predvsem glede narave razmer, zaradi katerih je bila zahteva vložena, ter posledic uporabe za pravice in svoboščine vseh zadevnih oseb, ter zaščitnih ukrepov in pogojev, predvidenih za uporabo. Poleg tega bi bilo treba uporabo sistemov za biometrično identifikacijo na daljavo v realnem času v javno dostopnih prostorih za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj uporabljati le za potrditev identitete specifično ciljnega posameznika in bi morala biti omejena na to, kar je nujno potrebno za časovno obdobje ter geografsko in osebno področje uporabe, pri čemer je treba upoštevati zlasti dokaze ali znake v zvezi z grožnjami, žrtvami ali storilcem. Zanimariti se tudi ne sme izjemne občutljivosti rabe biometričnih podatkov. Uvodne točke 14 do 20 Akta o umetni inteligenci izpostavljajo, da so biometrični podatki posebna kategorija osebnih podatkov ter da je primerno, da se več kritičnih primerov uporabe biometričnih sistemov razvrsti kot visoko tveganih, če je njihova uporaba dovoljena na podlagi ustreznega prava EU in nacionalnega prava. Obdelava biometričnih podatkov je dopustna na način, ki ne bo povzročal neselektivnega nadzora ali izogibanja pogojem prepovedi in strogim izjemam za biometrično identifikacijo na daljavo v realnem času. Resolucija o umetni inteligenci apelira, da je biometrična kategorizacija in

¹⁰⁷ Etične smernice, stran 19.

biometrična identifikacija fizičnih oseb za sklepanje o njihovi rasi, političnem prepričanju, članstvu v sindikatu, verskem ali filozofskem prepričanju ali spolni usmerjenosti prepovedana praksa. Še vedno bo mogoče označevanje ali filtriranje naborov podatkov in razvrščanje podatkov na področju preprečevanja, odkrivanja in preiskovanja kaznivih dejanj. Iz Resolucije o umetni inteligenci tudi izhaja, da je uporaba biometričnih podatkov širše povezana z načelom pravice do človekovega dostojanstva, ki je temelj vseh temeljnih pravic, ki jih zagotavlja Listina Evropske unije o temeljnih pravicah. Nevladne organizacije še posebej izpostavljajo, da nepregledna narava odločanja o priseljevanju in beguncih ustvarja okolje, zrelo za algoritemsko diskriminacijo.¹⁰⁸

Akt o umetni inteligenci v 3. členu podaja opredelitev pojmov.¹⁰⁹ Pojem »biometrična kategorizacija« je opredeljen kot razvrstitev fizičnih oseb v posebne kategorije na podlagi njihovih biometričnih podatkov. Takšne posebne kategorije se lahko nanašajo na spol, starost, barvo las, barvo oči, tetovaže, vedenjske ali osebnostne lastnosti, jezik, vero, pripadnost narodnostni manjšini in spolno ali politično usmerjenost. To ne vključuje sistemov za biometrično kategorizacijo, ki so izključno pomožni element, neločljivo povezan z drugo komercialno storitvijo, kar pomeni, da tega elementa iz objektivnih tehničnih razlogov ni mogoče uporabiti brez glavne storitve, njegova vključitev ali funkcionalnost pa ni sredstvo za izogibanje uporabi pravil iz tega predpisa.¹¹⁰

Pojem »sistem za biometrično identifikacijo na daljavo« je treba opredeliti funkcionalno kot sistem umetne inteligence, namenjen identifikaciji fizičnih oseb (ene ali več) brez njihovega dejavnega sodelovanja, običajno na daljavo, s primerjavo biometričnih podatkov osebe z biometričnimi podatki iz referenčne podatkovne zbirke, ne glede na uporabljeno tehnologijo, procese ali vrste biometričnih podatkov. To izključuje sisteme umetne inteligence za biometrično preverjanje, tudi avtentikacijo, katerih edini namen je potrditi, da je določena fizična oseba res tista, za katero se predstavlja, in potrditi identiteto fizične osebe izključno z namenom dostopa do storitve, odklepanja naprave ali varnostnega dostopa do prostorov. Ta izključitev je utemeljena z dejstvom, da bodo imeli taki sistemi verjetno manjši vpliv na temeljne pravice fizičnih oseb v primerjavi s sistemi za biometrično identifikacijo

¹⁰⁸ Amnesty International, 2024, dostopno na: <https://www.amnesty.org/en/documents/pol40/7772/2024/en/> (obiskano: 6. 1. 2025).

¹⁰⁹ Akt o umetni inteligenci, uvodne točke 12–20.

¹¹⁰ Prav tam, uvodna točka 16.

na daljavo, ki se lahko uporabljajo za obdelavo biometričnih podatkov velikega števila oseb brez njihovega dejavnega sodelovanja.¹¹¹ Pri sistemih »v realnem času« se zajemanje biometričnih podatkov, primerjava in identifikacija izvedejo takoj ali skoraj takoj, v vsakem primeru pa brez večje zamude. V zvezi s tem ne bi smelo biti prostora za izogibanje pravilom Akta o umetni inteligenci o uporabi zadevnih sistemov umetne inteligence »v realnem času«, saj je predvidena možnost manjših zamud. Sistemi »v realnem času« vključujejo uporabo gradiva »v živo« ali »skoraj v živo«, kot je videoposnetek, ki ga ustvari kamera ali druga naprava s podobno funkcionalnostjo. Pri »naknadnih« sistemih so bili biometrični podatki že zajeti, primerjava in identifikacija pa se izvedeta šele po daljšem času. To vključuje gradivo, kot so slike ali videoposnetki, ki jih ustvarjajo kamere CCTV ali zasebne naprave in je bilo ustvarjeno pred uporabo sistema v zvezi z zadevnimi fizičnimi osebami. Kot tveganje so izpostavljene tehnične netočnosti sistemov umetne inteligence, namenjenih za biometrično identifikacijo fizičnih oseb na daljavo, ki lahko vodijo do pristranskih rezultatov in diskriminatornih učinkov. Tveganje takšnih pristranskih rezultatov in diskriminatornih učinkov je zlasti pomembno v zvezi s starostjo, etnično pripadnostjo, raso, spolom ali invalidnostjo. Glede na tveganja, ki jih predstavljajo sistemi za biometrično identifikacijo na daljavo, bi jih bilo treba razvrstiti kot sisteme visokega tveganja.¹¹²

Poleg tega bi bilo kot sisteme visokega tveganja treba opredeliti sisteme umetne inteligence, namenjene uporabi za biometrično kategorizacijo, v skladu z občutljivimi lastnostmi ali značilnostmi, zaščitenimi na podlagi prvega odstavka 9. člena Uredbe 2016/679, ki ureja rabo biometričnih podatkov, če ti niso prepovedani s to uredbo, in sisteme za prepoznavanje čustev, ki niso prepovedani s to uredbo. Iz uvodne točke 30 Akta o umetni inteligenci izhaja, da bi bilo treba prepovedati sisteme za biometrično kategorizacijo, ki temeljijo na biometričnih podatkih fizičnih oseb, kot so obraz ali prstni odtisi posameznika, za sklepanje ali ugotavljanje o političnem prepričanju posameznika, članstvu v sindikatu, verskem ali filozofskem prepričanju, rasi, spolnem življenju ali spolni usmerjenosti. Prepoved ne bi smela zajemati zakonitega označevanja, filtriranja ali kategorizacije naborov biometričnih podatkov, pridobljenih v skladu s pravom EU ali nacionalnim pravom na podlagi biometričnih podatkov, kot je razvrščanje slik glede na barvo las ali oči, ki se lahko

¹¹¹ Prav tam, uvodna točka 17.

¹¹² Prav tam. Primerjaj tudi Resolucija o umetni inteligenci, točka 25.

na primer uporabljajo na področju preprečevanja, odkrivanja in preiskovanja kaznivih dejanj.¹¹³

Akt o umetni inteligenci v točki h) prvega odstavka 5. člena določa, da je kot prepovedana praksa opredeljena uporaba sistemov umetne inteligence za biometrično identifikacijo fizičnih oseb na daljavo v realnem času v javno dostopnih prostorih za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj, kar je posebej hudo poseganje v pravice in svoboščine zadevnih oseb, kolikor lahko vpliva na zasebno življenje velikega dela prebivalstva, vzbuja občutek stalnega nadzora ter posredno odvrča od uresničevanja svobode zbiranja in drugih temeljnih pravic. V tretjem odstavku 5. člena Akta o umetni inteligenci je določeno, da bo za vsako uporabo sistema za biometrično identifikacijo na daljavo v realnem času v javno dostopnih prostorih za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj treba pridobiti izrecno in posebno dovoljenje sodnega organa ali neodvisnega upravnega organa države članice, katerega odločitev je zavezujoča. Tako dovoljenje bi bilo treba načeloma pridobiti pred uporabo sistema umetne inteligence za identifikacijo osebe ali oseb. Izjeme od tega pravila bi morale biti dovoljene v ustrezno utemeljenih nujnih primerih iz nujnih razlogov, tj. v primerih, ko je uporaba zadevnih sistemov potrebna do te mere, da je dejansko in objektivno nemogoče pridobiti dovoljenje pred začetkom uporabe sistema umetne inteligence. V takih nujnih primerih bi bilo treba uporabo sistema umetne inteligence omejiti na absolutni minimum, zanjo pa bi morali veljati ustrezni zaščitni ukrepi in pogoji, kot jih določa nacionalno pravo ter kot jih v okviru vsakega posameznega primera nujne uporabe določi organ za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj. Poleg tega bi moral organ za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj v takšnih primerih zaprositi za tako dovoljenje, hkrati pa navesti razloge, zakaj ga ni mogel zahtevati prej, brez nepotrebnega odlašanja in najpozneje v 24 urah. Če se tako dovoljenje zavrne, bi bilo treba takoj prenehati z uporabo sistemov za biometrično identifikacijo v realnem času, povezanih s tem dovoljenjem, vse podatke, povezane s tako uporabo, pa bi bilo treba zavreči in izbrisati. Resolucija o umetni inteligenci opozarja, da je lahko uporaba in zbiranje biometričnih podatkov za namene identifikacije na daljavo, na primer z izvajanjem prepoznavanja obrazov na javnih mestih ter v okviru avtomatiziranega mejnega nadzora, ki se uporablja za mejno kontrolo na letališčih, posebej tvegana za temeljne pravice in da se lahko

¹¹³ Akt o umetni inteligenci, uvodni točki 30 in 39.

posledice razlikujejo glede na namen, okoliščine in obseg uporabe. Tehnične netočnosti sistemov umetne inteligence, namenjenih za biometrično identifikacijo fizičnih oseb na daljavo, lahko namreč vodijo do pristranskih rezultatov in diskriminatornih učinkov. Zato bi bilo treba prepovedati uporabo teh sistemov za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj, razen v izrecno naštetih in ozko opredeljenih primerih, ko je uporaba nujno potrebna za doseg pomembnega javnega interesa, katerega pomen prevlada nad tveganji, kakor je določeno v točki h) prvega odstavka 5. člena Akta o umetni inteligenci. Uvodna točka 33 Akta o umetni inteligenci pojasnjuje, da gre pri izjemah za primer iskanja nekaterih žrtev kaznivih dejanj, vključno s pogrešanimi osebami, nevarnosti za življenje ali fizično varnost oseb ali varnost pred terorističnim napadom ter lokalizacijo ali identifikacijo storilcev ali osumljencev kaznivih dejanj, ki so navedena v prilogi k temu predpisu. Gre za kazniva dejanja, za katera je v zadevni državi članici predpisana zgornja meja zaporne kazni ali ukrepa, vezanega na odvzem prostosti, najmanj štiri leta in so v pravu te države članice opredeljena. Tak prag za zaporno kazen ali ukrep, vezan na odvzem prostosti, v skladu z nacionalnim pravom prispeva k zagotavljanju določenosti, da je kaznivo dejanje dovolj hudo, da bi lahko upravičilo uporabo sistemov za biometrično identifikacijo na daljavo v realnem času. Seznam kaznivih dejanj iz priloge k Aktu o umetni inteligenci temelji na 32-ih kaznivih dejanjih, naštetih v Okvirnem sklepu sveta z dne 13. junija 2002 o evropskem nalogu za prijetje in postopkih predaje med državami članicami (2002/584/PNZ).¹¹⁴ Pri tem je treba upoštevati, da so nekatera od teh kaznivih dejanj v praksi verjetno pomembnejša od drugih, saj bi bila lahko uporaba biometrične identifikacije na daljavo v realnem času predvidoma potrebna in sorazmerna v zelo različnem obsegu za praktično izvajanje lokalizacije ali identifikacije storilca ali osumljenca različnih navedenih kaznivih dejanj ter ob upoštevanju verjetnih razlik v resnosti, verjetnosti in obsegu škode ali morebitnih negativnih posledic. Uporaba sistema za biometrično identifikacijo na daljavo v realnem času v javno dostopnih prostorih se dovoli le, če je ustrezní organ za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj opravil oceno učinka na temeljne pravice in, če v tej uredbi ni določeno drugače, sistem registriral v podatkovni zbirki, kot je določeno v tem predpisu.¹¹⁵

¹¹⁴ UL L 190, 18. 7. 2002, strani 1–20.

¹¹⁵ Akt o umetni inteligenci, uvodne točke 33–38.

V nacionalni zakonodaji Republike Slovenije procesne določbe ZKP še ne vsebujejo ustreznih določb o umetni inteligenci. Za obe področji, kazensko materialno in kazensko procesno pravo, bo zakonodajalec seveda najprej moral preveriti, kako in ali sploh lahko uporabi že sprejete zakonodajne rešitve tudi za sisteme umetne inteligence. Potrebno bo intenzivno delo zakonodajalca, da bo določil, v katerih primerih bo državni tožilec moral pridobiti sodne odredbe in v katerih bo, podobno kot pri uporabi nekaterih prikritih preiskovalnih ukrepov, za odredbe ali dovoljenja pristojen sam ali pa bodo dovolj le policijska pooblastila.¹¹⁶

Uvodna točka 31 Akta o umetni inteligenci opozarja, da lahko umetnointeligenčni sistemi, ki zagotavljajo družbeno točkovanje fizičnih oseb s strani javnih ali zasebnih akterjev, vodijo do diskriminatornih rezultatov in izključitve nekaterih skupin. Kršijo lahko pravico do dostojanstva in nediskriminacije ter vrednote enakosti in pravičnosti. Taki umetnointeligenčni sistemi ocenjujejo ali razvrščajo fizične osebe ali skupine fizičnih oseb na podlagi več podatkovnih točk, povezanih z njihovim družbenim vedenjem v več kontekstih ali znanimi, predpostavljenimi ali predvidenimi osebnimi ali osebnostnimi značilnostmi v določenih časovnih obdobjih. Število družbenih točk, dodeljenih s strani takih sistemov, lahko vodi do škodljivega ali neugodnega obravnavanja fizičnih oseb ali celotnih skupin oseb v družbenih kontekstih, ki niso povezani s kontekstom, v katerem so bili podatki prvotno ustvarjeni ali zbrani, ali do škodljivega obravnavanja. Prav tako je kot prepovedana praksa opredeljeno individualno napovedno policijsko delo, ki temelji izključno na profiliranju oseb. Resolucija o umetni inteligenci ugotavlja, da je napovedno policijsko delo ena od aplikacij umetne inteligence na področju preprečevanja, odkrivanja in preiskovanja kaznivih dejanj, vendar opozarja, da se pri napovednem policijskem delu analizirajo nabori podatkov, potrebni za identifikacijo vzorcev in korelacij, ne more pa se podati odgovor na vprašanje vzročnosti. Glede na različne vrste uporabe prepoznavanja obrazov, kot so med drugim preverjanje/avtentifikacija (tj. ujemanje neposrednega obraza s fotografijo v osebem dokumentu, npr. pametne meje), identifikacija (tj. ujemanje fotografije z zbirko fotografij) in odkrivanje (tj. odkrivanje obrazov v realnem času iz virov, kot je posnetek s CCTV, in njihovo povezovanje s podatkovnimi zbirkami, npr. nadzor v realnem času), pri čemer ima vsaka od njih različne posledice za varstvo temeljnih pravic, je bila izpostavljena kritika glede ciljnega zbiranja slik obrazov s spleta ali

¹¹⁶ Več o tem Ferlinc, 2024.

posnetkov sistema televizije zaprtega kroga (CCTV) za vzpostavitev ali razširitev podatkovnih zbirk. Resolucija o umetni inteligenci problematizira, da akterji preprečevanja, odkrivanja in preiskovanja kaznivih dejanj in obveščevalne službe uporabljajo zasebne zbirke podatkov za prepoznavanje obrazov, kot je Clearview AI, ki je zbirka podatkov, sestavljena iz več kot treh milijard slik, nezakonito zbranih s socialnih omrežij in drugih spletišč, tudi od državljanov EU. Uvodna točka 28 Resolucije o umetni inteligenci opozarja, da je Evropski parlament še posebej izpostavil, da tehnologija Clearview AI v EU ni v skladu z ureditvijo EU o varstvu podatkov. Opravljanje prepoznav mora biti skladno z načeli sorazmernosti in nujnosti ter veljavnim pravom, zahtevami najmanjšega obsega podatkov, točnosti podatkov, omejitve hrambe, varnosti podatkov in odgovornosti skladno s pravom države članice ali pravom EU. Resolucija o umetni inteligenci izpostavlja, da morajo biti tehnični standardi popolnoma v skladu s temeljnimi pravicami. Poziva tudi, naj se na javnih mestih trajno prepove uporaba avtomatizirane analize in/ali prepoznavanja na podlagi drugih človeških značilnosti, kot so hoja, prstni odtisi, DNK, glas ter drugi biometrični in vedenjski znaki, oziroma predlaga moratorij uvedbe sistemov prepoznavanja obrazov za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj pri identifikaciji, razen če se uporabljajo izključno za identifikacijo žrtev kaznivih dejanj, saj je treba zagotoviti, da bodo rezultati nepristranski in nediskriminatorni, ob zagotavljanju strogih zaščitnih ukrepov proti zlorabi in strogega demokratičnega nadzora in spremljanja ter ob zagotovitvi, da je uporaba tehnologij nujna in sorazmerna. Znanstvena veljavnost tehnologije za prepoznavanje čustev, kot so kamere, ki zaznavajo gibanje oči in spremembe velikosti zenice, je na področju preprečevanja, odkrivanja in preiskovanja kaznivih dejanj sporna. Obstajajo resni pomisleki glede znanstvene podlage sistemov umetne inteligence, katerih namen je prepoznavanje čustev ali sklepanje o njih, saj se izražanje čustev med kulturami in okoliščinami ter celo pri enem samem posamezniku zelo razlikuje. Akt o umetni inteligenci pojem »sistem za prepoznavanje čustev« opredeljuje kot umetnointeligenčni sistem za prepoznavanje čustev ali namer ali za sklepanje o čustvih ali namerah fizičnih oseb na podlagi njihovih biometričnih podatkov. Med ključnimi pomanjkljivostmi takšnih sistemov so omejena zanesljivost, premajhna specifičnost in omejena možnost posplošitve. Zato lahko umetnointeligenčni sistemi, ki prepoznavajo čustva ali namere fizičnih oseb na podlagi biometričnih podatkov ali ki iz njih sklepajo, vodijo do diskriminatornih rezultatov ter posegajo v pravice in svoboščine zadevnih oseb. Glede na neravnovesje moči v kontekstu dela ali izobraževanja ter intruzivne narave

teh sistemov bi lahko takšni sistemi povzročili škodljivo ali neugodno obravnavo nekaterih fizičnih oseb ali celotnih skupin fizičnih oseb. Zato bi bilo treba prepovedati dajanje na trg, dajanje v uporabo ali uporabo sistemov umetne inteligence, namenjenih odkrivanju čustvenega stanja posameznikov v situacijah, povezanih z delovnim mestom in izobraževanjem. Ta prepoved ne bi smela zajemati umetnointeligentnih sistemov, danih na trg izključno iz zdravstvenih ali varnostnih razlogov, kot so sistemi za terapevtsko uporabo.¹¹⁷

8 Zaključek

Umetnointeligentne sisteme je mogoče zlahka uporabljati v številnih različnih gospodarskih in družbenih sektorjih, tudi čezmejno, in lahko enostavno krožijo po vsej EU. Nekatere države članice so že preučile možnost sprejetja nacionalnih predpisov, s katerimi bi zagotovile, da je umetna inteligenca zaupanja vredna in varna ter da se razvija in uporablja v skladu s temeljnimi pravicami. Zato bi bilo treba zagotoviti dosledno in visoko raven varstva po vsej EU, da bi dosegli zaupanja vredno umetno inteligenco in hkrati preprečili razlike, ki ovirajo prosti pretok, inovacije, uvajanje in uporabo sistemov umetne inteligence. V Republiki Sloveniji še ni sprejet predpis, ki bi celovito urejal področje umetne inteligence. Opustitev zakonske ureditve, kadar je to nujno zaradi narave posamezne pravice, povzroči protiustavno pravno praznino. V kazenskem pravu in pri uporabi umetne inteligence v policiji in pravosodnih organih na področju kazenskih zadev je uporabo umetne inteligence treba presoјati s stališča sorazmernosti in nujnosti ter na podlagi temeljite ocene posledic dovoljenja za uporabo tehnologij, ki zmanjšujejo vlogo ljudi pri preprečevanju, odkrivanju in preiskovanju kaznivih dejanj in sojenju. Nikakor se ne bi smelo zanemariti vpliva uporabe orodij umetne inteligence na pravice osumljencev do obrambe, zlasti težav pri pridobivanju smiselnih informacij o delovanju teh sistemov in posledično težav pri izpodbijanju njihovih rezultatov na sodišču, zlasti s strani fizičnih oseb, ki so subjekt preiskave in v ranljivem položaju ter so odvisne od izida ukrepov pristojnih javnih organov. Uporaba sistemov umetne inteligence za biometrično identifikacijo fizičnih oseb na daljavo, če lahko vpliva na zasebno življenje velikega dela prebivalstva, vzbuja občutek stalnega nadzora ter posredno odvrča od uresničevanja svobode zbiranja in drugih temeljnih pravic, je opredeljena kot prepovedana praksa. Poleg tega se zaradi takojšnjega učinka in

¹¹⁷ Akt o umetni inteligenci, uvodne točke 27–39, 43 in 44.

omejenih možnosti za nadaljnja preverjanja ali popravke v zvezi z uporabo takih sistemov, ki delujejo v realnem času, povečujejo tveganja za kršitev pravic in svoboščin zadevnih oseb v okviru dejavnosti preprečevanja, odkrivanja in preiskovanja kaznivih dejanj. Zaradi vpliva teh dejavnosti nanje je potrebno premišljeno uvajanje tehnologij umetne inteligence v okviru nadzora meja. Umetna inteligenca prinaša jasne koristi, kot so večja zmogljivost za odkrivanje goljufij in zlorab, boljši in pravočasen dostop do ustreznih informacij, večja zmogljivost pri sprejemanju odločitev in možnosti za večjo zaščito ranljivih ljudi. S stališča uporabnosti v sodnih postopkih gre sicer izsledke umetne inteligence presojati kot vsak drug dokaz, pri čemer sodna praksa za vrednotenje teh dokazov še ni povsem izoblikovana. Resolucija o umetni inteligenci pri tem podaja vrednostna stališča za vrednotenje predmetnih dokazov. Razmah tehnologij omogoča širok nabor novih dokazov, katerih vrednost je inherentno problematična, saj omogočajo zaključke o vzdrževanju utemeljenega suma, a je njihova veljavnost lahko sporna s stališča varovanja temeljnih pravic obtoženih, kar lahko privede do izločitve dokazov. Obenem so sodišča dolžna upoštevati konvencijsko in ustavno sodno prakso, ki zvišuje raven varstva človekovih pravic. Uporaba umetne inteligence vpliva na človekove odločitve in vse faze kazenskega postopka, zato morajo organi, ki uporabljajo sisteme umetne inteligence, spoštovati izredno visoke pravne standarde in zagotoviti človeško posredovanje, zlasti pri analizi podatkov, ki izhajajo iz teh sistemov. Uporaba umetne inteligence v pravosodju prinaša številne prednosti, kot so povečana učinkovitost, natančnost in pravičnost pravnih postopkov. Ključno je, da se pri uporabi umetne inteligence dosledno upoštevajo etična načela, zlasti načelo nediskriminacije, da bi se izognili morebitnim negativnim posledicam za posameznike in družbo kot celoto. EU temelji na ustavni zavezi o varovanju temeljnih in neodtujljivih človekovih pravic, zagotavljanju spoštovanja pravne države ter spodbujanju demokratične svobode in skupnega dobrega. Nepregledna narava odločanja o priseljevanju in beguncih ustvarja okolje, ki je zrelo za algoritemsko diskriminacijo. Etične smernice opozarjajo, da si sistemi umetne inteligence ne bi smeli neupravičeno podrediti ljudi ali jih siliti, zavajati, manipulirati z njimi, jih določati ali zbirati v skupine. Namesto tega bi morali biti zasnovani tako, da povečujejo, dopolnjujejo in krepijo kognitivna, socialna in kulturna znanja in spretnosti ljudi. To pomeni, da bi bilo treba zagotoviti človeški nadzor. Sistemi umetne inteligence lahko tudi bistveno spremenijo delovno področje. Podpirati bi morali ljudi v delovnem okolju in si prizadevati za ustvarjanje smiselne dela.

Literatura

- Amnesty International Slovenija, Akt o umetni inteligenci odpira vrata strukturnemu rasizmu, revija Akcija (2023), dostopno na: <https://www.amnesty.si/akt-o-umetni-inteligenci> (obiskano: 6. 1. 2025).
- Amnesty International, The Digital Border: Migration, Technology and Inequality (2024), dostopno na: <https://www.amnesty.org/en/documents/pol40/7772/2024/en/> (obiskano: 6. 1. 2025).
- Bergman Klein center (2018) Algorithms and Justice Examining the role of the state in the development and deployment of algorithmic technologies, dostopno na: <https://cyber.harvard.edu/sites/default/files/2019-10/2019AIAAlgorithmsJusticeOnePager.pdf> (obiskano: 6. 1. 2025).
- Brezovnik, B. (2016) Digitalna forenzika in digitalni dokazi, organizacijsko statični vidik Fakulteta za varnostne vede univerze v Mariboru, dostopno na: <https://core.ac.uk/download/pdf/67605432.pdf> (obiskano: 12. 2. 2025).
- Celsi, R., Zomaya, A. (2025) Perspectives on managing AI Ethics in Digital age, dostopno na: <https://www.mdpi.com/2078-2489/16/4/318> (obiskano: 25. 8. 2025).
- Ciudad Fontecha, P. (2023) AI in Border Control. Opportunity or threat? An analysis of Artificial Intelligence practices in border control in EU's Member States, dostopno na: https://www.ie-ei.eu/Ressources/FCK/image/Theses/2023/Ciudad_Fontecha_EUDIPIO_Thesis_2023.pdf (obiskano: 6. 1. 2025).
- Dežman, Z., et al. (2003) Kazensko procesno pravo Republike Slovenije (Ljubljana: GV Založba).
- Dumbrava, C. (2021) Artificial intelligence at EU borders, EPRS | European Parliamentary Research Service, dostopno na: [https://www.europarl.europa.eu/RegData/etudes/IDAN/2021/690706/EPRS_IDA\(2021\)690706_EN.pdf?pnspid=k7duqPpaXRCNgvJ6VONLvYSpFVIJhSp5XGZAO9RQ](https://www.europarl.europa.eu/RegData/etudes/IDAN/2021/690706/EPRS_IDA(2021)690706_EN.pdf?pnspid=k7duqPpaXRCNgvJ6VONLvYSpFVIJhSp5XGZAO9RQ) (obiskano: 26. 1. 2025).
- Dumbrava, C. (2025) Measuring irregular migration and returns in the EU, EPRS | European Parliamentary Research Service, dostopno na: [https://www.europarl.europa.eu/RegData/etudes/BRIE/2025/767210/EPRS_BRI\(2025\)767210_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2025/767210/EPRS_BRI(2025)767210_EN.pdf) (obiskano: 26. 1. 2025).
- European Commission: Directorate-General for Migration and Home Affairs & Deloitte (2020) Opportunities and challenges for the use of artificial intelligence in border control, migration and security . Volume 1, Main report, Publications Office, <https://data.europa.eu/doi/10.2837/923610>.
- Evropska komisija (2018) Etične smernice neodvisne strokovne skupine na visoki ravni za umetno inteligenco, dostopno na: [ethics_guidelines_for_trustworthy_ai-sl_88015DAF-E3CC-BBB8-AFE06902735B11DE_60438\(1\).pdf](https://ethics_guidelines_for_trustworthy_ai-sl_88015DAF-E3CC-BBB8-AFE06902735B11DE_60438(1).pdf) (obiskano: 6. 1. 2025).
- Evropska komisija (2024) Akt o umetni inteligenci, Shaping Europe's digital future, dostopno na: <https://digital-strategy.ec.europa.eu/sl/factpages/ai-act> (obiskano: 25. 1. 2025).
- Evropska komisija (2024) Umetna inteligenca – vprašanja in odgovori, Bruselj, dostopno na: https://ec.europa.eu/commission/presscorner/detail/sl/qanda_21_1683 (obiskano: 6. 1. 2025).
- Evropska komisija (2025) Evropski pristop k umetni inteligenci Shaping Europe's digital future, dostopno na: <https://digital-strategy.ec.europa.eu/sl/policies/european-approach-artificial-intelligence> (obiskano: 25. 1. 2025).
- Ferlinc, A. (2024) Umetna inteligenca z vidika uporabe kazenskega prava, V središču, Ius Info, dostopno na: <https://www.iusinfo.si/medijsko-sredisce/v-srediscu/umetna-inteligenca-z-vidika-uporabe-kazenskega-prava-312126> (obiskano: 14. 2. 2025).
- FRA, Agencija Evropske unije za temeljne pravice (2024) Pravilno ravnanje v prihodnje, Umetna inteligenca in temeljne pravice, poročilo, Luxemburg: Urad za publikacije, dostopno na: https://fra.europa.eu/sites/default/files/fra_uploads/fra-2020-artificial-intelligence_sl.pdf,

- <https://eur-lex.europa.eu/legal-content/SL/TXT/?uri=LEGISSUM:4365508> (obiskano: 13. 2. 2025).
- Gorkič, P., Šugman Stubbs, K. (2010) *Praktikum za kazensko procesno pravo* (Ljubljana: GV Založba).
- Gorkič, P., Šugman Stubbs, K., Fišer, Z. (2020) *Temelji kazenskega procesnega prava* (Ljubljana: GV Založba).
- Maciejewski, M., et al. (2024) *Law and ICT (Pravo in IKT)*, Evropski parlament, Generalni direktorat za notranjo politiko Unije, Tematski sektor za pravice državljanov in ustavne zadeve, dostopno na: [https://www.europarl.europa.eu/RegData/etudes/STUD/2024/762738/IPOL_STU\(2024\)762738_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2024/762738/IPOL_STU(2024)762738_EN.pdf) (obiskano: 14. 2. 2025).
- Molnar, P., et al. (2018) *Bots at the Gate, A Human Rights Analysis of Automated Decision Making in Canada's Immigration and Refugee System*, University of Toronto, dostopno na: <https://ihrp.law.utoronto.ca/bots-gate-update> (obiskano: 11. 2. 2025).
- Molnar, P. (2019) *Technology on the margins: AI and global migration management from a human rights perspective*, Cambridge International Law Journal, dostopno na: https://www.researchgate.net/publication/337780154_Technology_on_the_margins_AI_and_global_migration_management_from_a_human_rights_perspective (obiskano: 6. 1. 2025).
- Nacionalni program spodbujanja razvoja in uporabe umetne inteligence v Republiki Sloveniji do leta 2025 (NpUI), dostopno na: <https://www.gzs.si/Portals/Panoga-ZIT/Vsebine/novice-priponke/NpUI-SI-2025.pdf> (obiskano: 6. 1. 2025).
- Raso, F., et al., Bergman Klein center (2018) "Artificial Intelligence and Human Rights"—developed with support from the Digital Inclusion Lab, Global Affairs Canada, dostopno na: <http://ai-hr.cyber.harvard.edu/> (obiskano: 6. 1. 2025).
- Ribičič, C. (2007) *Evropsko pravo človekovih pravic*, Izbrana poglavja (Ljubljana: Pravna fakulteta v Ljubljani).
- Selinšek, L. (2021) *Vpliv avtomatizacije digitalnih forenzičnih preiskav na dokazovanje v kazenskem postopku*, *Revija za kriminalistiko in kriminologijo*, 72(3), strani 219–232.
- Selinšek, L., Malovrh, M., v: Dvoršek, A., Selinšek, L. (ur.), (2008). *Nekateri praktični problemi dokazovanja v kazenskih postopkih*, poglavje digitalni dokazi, Univerza v Mariboru, Pravna fakulteta, Fakulteta za policijsko-varnostne vede, strani 57–77.
- Šalamon, N., et al. v: Korošec, D., Filipčič, K., Zdolšek, S. (ur.) (2019) *Veliki znanstveni komentar posebnega dela kazenskega zakonika KZ-1*, 3. knjiga (Ljubljana: Pravna fakulteta Univerze v Ljubljani, Uradni list Republike Slovenije).
- Šepec, M., et al. (2023) *Zakon o kazenskem postopku s komentarjem*, 1. knjiga (Ljubljana: GV Založba).
- Škrjanc, M. (2024) *Načelo nediskriminacije pri uporabi umetne inteligence v pravosodnih sistemih*, V središču, IUS-INFO, dostopno na: <https://www.iusinfo.si/medijsko-sredisce/v-srediscu/nacelo-nediskriminacije-pri-uporabi-umetne-inteligence-v-pravosodnih-si> (obiskano: 6. 1. 2025).
- Testen, F., Šturm, L. (ur.) (2011) *Komentar Ustave Republike Slovenije, dopolnitev-A* (Kranj: Fakulteta za državne in evropske študije).
- Umetna inteligenca tudi na mejah v EU (2018) *Računalniške novice*, dostopno na: <https://racunalniske-novice.com/umetna-inteligenca-tudi-na-mejah-v-eu/> (obiskano: 14. 2. 2025).

Extended abstract

The most technologically advanced nations of the 21st century will fully exploit AI's benefits. AI systems simulate human cognitive functions, such as learning and decision-making, offering economic, social, and security benefits. However, their application in law enforcement and judicial processes introduces complex challenges, particularly regarding bias, discrimination, and mass surveillance risks.

Recognizing these concerns, the European Commission established an independent high-level expert group, which in 2019 issued the Ethical Guidelines for Trustworthy AI. These guidelines emphasize legality, ethics, and robustness, outlining seven core principles: human oversight, security, privacy, transparency, fairness, social well-being, and accountability. This Chapter will explore the implications of AI in crime prevention, border control, and judicial processes, assessing both its advantages and ethical risks. It will examine the EU's legal human rights-based approach to AI regulation and discuss whether the Artificial Intelligence Act successfully balances security and human rights.

The EU's adoption of the Artificial Intelligence Act (Regulation (EU) 2024/1689) marks a significant step in crime detection, prevention, migration management, and border control, and in the context of the potential aspects of fundamental rights violations in the use of artificial intelligence systems. With this act, the EU becomes the first to implement a unified legal framework for AI development, deployment, and use, ensuring a well-regulated internal market. Ethical Guidelines for Trustworthy AI emphasize legality, ethics, human oversight, technical robustness and security, data privacy, transparency, fairness, non-discrimination and accountability. AI offers major advantages in crime prevention, investigation, and law enforcement, particularly in financial crime, money laundering, terrorism financing, and cybercrime. While these applications enhance security, they also pose risks to fundamental rights. Mass surveillance through AI remains a disproportionate measure, raising ethical and legal concerns. The European Parliament's resolution of 6 October 2021, highlights that AI-based law enforcement tools, particularly machine learning, can reinforce bias and discrimination due to flawed algorithms and biased datasets. Historical data used in AI systems can embed discrimination, disproportionately affecting racial and ethnic groups. Poor data quality worsens AI's inherent bias, further entrenching societal inequalities. Therefore, ensuring a balance between protecting fundamental rights and effective policing is crucial. AI's role in criminal investigations requires careful regulation. While it can enhance efficiency, accuracy, and fairness in legal proceedings, the European Parliament resolution of 6 October 2021 on artificial intelligence in criminal law and its use by police and judicial authorities in criminal matters (2020/2016(INI)) highlights that AI-driven decisions must align with ethical principles to avoid harmful consequences for individuals and society. Non-discrimination remains a key concern, as AI systems can perpetuate biases unless properly managed. Transparency, fairness, and proportionality must be maintained to ensure AI serves justice without infringing on fundamental rights. The EU and its Member States bear responsibility for regulating AI use in law enforcement and judicial processes. Decision-making related to AI systems must be transparent, ensuring that fundamental rights are upheld and biases are not reinforced. AI's deployment in crime prevention and detection must be proportional and necessary, ensuring its use remains constitutional and contributes to a just, humane legal system. By establishing clear legal and ethical boundaries, the EU aims to harness AI's potential while safeguarding human rights.

AI's role in law enforcement should focus on improving security without leading to unjust surveillance, discrimination, or breaches of fundamental freedoms. Ethical AI implementation is essential for maintaining trust and ensuring that technological advancements benefit society equitably.