

USTAVNOPRAVNE KRŠITVE DELOVANJA IN UPORABE UMETNOINTELIGENČNIH SISTEMOV

KRISTJAN ZAHRASTNIK

Univerza v Mariboru, Pravna fakulteta, Maribor, Slovenija
kristjan.zahrastnik@um.si

Poglavje obravnava in kritično analizira delovanje in uporabo umetnointeligentnih sistemov z vidika ustavnopravnih kršitev. Posegi v ustavnopravno varovane pravice, ki nastanejo pri delovanju in uporabi umetnointeligentnih sistemov, se pojavljajo na dveh ravneh: pri razvoju in učenju teh sistemov ter pri njihovi uporabi s strani uporabnika. Avtor se pri tem osredotoča na pravice iz ustvarjalnosti (avtorska pravica), varstvo osebnih podatkov, enakost pred zakonom (prepoved diskriminacije), svobodo dela (pravica do dela), svobodo izražanja, pravico do osebnega dostojanstva in varnosti ter varstvo pravic zasebnosti in osebnostnih pravic. V tej zvezi obravnava tudi relevantne pravne akte EU, kot so Akt o umetni inteligenci, Direktiva (EU) 2019/790 o avtorski in sorodnih pravicah na enotnem digitalnem trgu in Akt o digitalnih storitvah.

DOI
[https://doi.org/
10.18690/um.pf.11.2025.6](https://doi.org/10.18690/um.pf.11.2025.6)

ISBN
978-961-299-086-2

Ključne besede:
ustavnopravne kršitve
umetnointeligentnih
sistemov,
avtorska pravica,
varstvo osebnih podatkov,
prepoved diskriminacije,
pravica do dela,
svoboda izražanja,
pravica do osebnega
dostojanstva,
pravica do zasebnosti,
osebnostne pravice



Univerzitetna založba
Univerze v Mariboru

DOI
[https://doi.org/
10.18690/um.pf.11.2025.6](https://doi.org/10.18690/um.pf.11.2025.6)

ISBN
978-961-299-086-2

Keywords:

constitutional violations of
artificial intelligence
systems,
copyright,
protection of personal data,
prohibition of
discrimination,
right to work,
freedom of expression,
right to personal dignity and
safety,
right to privacy,
personality rights

CONSTITUTIONAL VIOLATIONS IN THE OPERATION AND USE OF ARTIFICIAL INTELLIGENCE SYSTEMS

KRISTJAN ZAHRASTNIK

University of Maribor, Faculty of Law, Maribor, Slovenia
kristjan.zahrastnik@um.si

The chapter examines and critically analyses the operation and use of artificial intelligence systems from the perspective of constitutional law violations. Interferences with constitutionally protected rights arising from the operation and application of artificial intelligence systems occur on two levels: during their development and training, as well as in their use by end-users. The author focuses on intellectual property rights (copyright), protection of personal data, equality before the law (prohibition of discrimination), freedom of work (right to work), freedom of expression, right to personal dignity and safety, and protection of the rights to privacy and personality rights. In this context, the author also discusses relevant EU legal acts, such as the Artificial Intelligence Act, Directive (EU) 2019/790 on Copyright and Related Rights in the Digital Single Market, and the Digital Services Act.



University of Maribor Press

1 Uvod

Umetnointeligenčni sistemi imajo mnogo pozitivnih učinkov, kot so izboljššan dostop do informacij, poenostavitev procesov ipd., vendar delovanje in uporaba teh sistemov nista vselej povsem neškodljiva – lahko predstavljata nedopustne posege v pravice iz ustvarjalnosti (avtorska pravica), varstvo osebnih podatkov, enakost pred zakonom (prepoved diskriminacije), svobodo dela (pravica do dela), svobodo izražanja, pravico do osebnega dostojanstva in varnosti ter varstvo pravic zasebnosti in osebnostnih pravic. Namen in cilj tega poglavja v monografiji sta obravnavati in kritično analizirati delovanje in uporabo umetnointeligenčnih sistemov skozi presojo ustavnopravnih kršitev. Pravne kršitve so presojane z ustavnopravnega vidika in odražajo dva sklopa posega umetnointeligenčnih sistemov v ustavno varovane dobrine. Prva enota ponazarja kršitve teh dobrin pri razvoju, učenju in delovanju umetnointeligenčnih sistemov, pri čemer lahko pride do posegov v pravice iz ustvarjalnosti, varstvo osebnih podatkov, enakost pred zakonom ter varstvo pravic zasebnosti in osebnostnih pravic. Druga enota posegov predstavlja ustavne kršitve, ki nastanejo pri uporabi umetnointeligenčnih sistemov. Ogrožene so zlasti pravice iz ustvarjalnosti, varstvo osebnih podatkov, enakost pred zakonom, svoboda dela, svoboda izražanja, pravica do osebnega dostojanstva in varnosti ter varstvo pravic zasebnosti in osebnostnih pravic. Skladno s tem je zasnovana struktura poglavja, v katerem so razvrščeni razdelki po ustavnih pravicah, ki so ogrožene z delovanjem in uporabo umetnointeligenčnih sistemov. Razdelki si smiselno sledijo po zaporedju od začetnih ustavno varovanih človekovih pravic in njihovih kršitev, ki izvirajo iz razvoja, učenja in delovanja umetnointeligenčnih sistemov, do posegov v človekove pravice, ki nastanejo pri končni uporabi sistema s strani uporabnika. Za uvodom je tako v drugem razdelku predstavljen pomen ustavnopravnih kršitev za kategorizacijo sistemov umetne inteligence. Sledi prikaz morebitnih posegov umetnointeligenčnih sistemov v varovane avtorske pravice v tretjem razdelku, pri čemer so obravnavani načini zbiranja podatkov, pomen ustreznega navajanja virov izhodnih podatkov ter obstoječi primeri domnevnih kršitev avtorskih pravic. Četrty razdelek se osredotoča na kršitve varstva osebnih podatkov v skladu z evropsko zakonodajo. V petem razdelku avtor predstavi razloge za pristranskost umetnointeligenčnih sistemov in navede dejanske primere pristranskega delovanja. Šesti razdelek obravnava kršitve pravice do dela in vpliv morebitne opredelitve sistema umetne inteligence kot visokotveganega na uresničevanje te pravice. V sedmem razdelku so obravnavani položaji, v katerih lahko uporaba umetnointeligenčnih sistemov vodi v kršitev

svobode izražanja, osmi razdelek pa se posveča kršitvam pravice do osebnega dostojanstva, zasebnosti in drugih osebnostnih pravic.

To poglavje v monografiji se osredotoča na vse oblike umetnointeligenčnih sistemov, vendar so zaradi njihove priljubljenosti in aktualnosti največkrat v ospredju primeri ustavnopravnih kršitev, ki izhajajo iz delovanja in uporabe generativne umetne inteligence (npr. klepetalni robot ChatGPT). Izraz »delovanje in uporaba« je treba za namene tega prispevka razlagati tako, da po vzoru uvodne točke 1 Uredbe (EU) 2024/1689 Evropskega parlamenta in Sveta z dne 13. junija 2024 o določitvi harmoniziranih pravil o umetni inteligenci in spremembi uredb (ES) št. 300/2008, (EU) št. 167/2013, (EU) št. 168/2013, (EU) 2018/858, (EU) 2018/1139 in (EU) 2019/2144 ter direktiv 2014/90/EU, (EU) 2016/797 in (EU) 2020/1828¹ (Akt o umetni inteligenci) obsega razvoj, dajanje na trg, dajanje v uporabo ter samo uporabo umetnointeligenčnih sistemov.

Delovanje in uporaba umetnointeligenčnih sistemov lahko povzročita negativne posledice v obliki premoženjske ali nepremoženjske škode.² V tem poglavju so obravnavani najpogostejši in najbolj invazivni posegi umetnointeligenčnih sistemov v ustavno varovane dobrine v naslednjem zaporedju: pravice iz ustvarjalnosti (avtorska pravica), varstvo osebnih podatkov, enakost pred zakonom (prepoved diskriminacije), svoboda dela (pravica do dela), svoboda izražanja, pravica do osebnega dostojanstva in varnosti ter varstvo pravic zasebnosti in osebnostnih pravic.

2 Pomen ustavnopravnih kršitev za kategorizacijo umetnointeligenčnih sistemov

Na območju EU³ je za delovanje in uporabo umetnointeligenčnih sistemov zavezujoč Akt o umetni inteligenci. Njegov namen je tudi zagotavljanje visoke ravni varovanja zdravja, varnosti in temeljnih pravic iz Listine Evropske unije o temeljnih pravicah⁴ (Listina) pred škodljivimi učinki umetnointeligenčnih sistemov.⁵ S tem namenom Akt o umetni inteligenci v 5. členu določa, katere prakse dajanja na trg, dajanja v uporabo in uporabe umetnointeligenčnih sistemov so prepovedane. Na

¹ UL L 2024/1689, 12. 7. 2024, strani 1–144.

² Evropska komisija, 2020, stran 10.

³ Podrobneje o področju uporabe Akta o umetni inteligenci glej 2. člen Akta o umetni inteligenci.

⁴ UL C 202, 7. 6. 2016, strani 389–405.

⁵ Prvi odstavek 1. člena Akta o umetni inteligenci.

podlagi tega člena so prepovedani tudi umetnointeligentni sistemi, ki s posebnim ciljem ali na določen način:⁶

- izkoriščajo katero koli ranljivost oseb ali skupin oseb zaradi njihove starosti, invalidnosti ali posebnega družbenega ali ekonomskega položaja;
- z družbenimi točkami ocenjujejo ali razvrščajo osebe ali skupine oseb, pri čemer gre za škodljivo ali neugodno obravnavo nekaterih fizičnih oseb oziroma skupin oseb, ki ni povezana s kontekstom ustvarjanja oziroma zbiranja podatkov oziroma je neupravičena ali nesorazmerna z njihovim družbenim vedenjem.⁷

V uvodni točki 28 Akt o umetni inteligenci prepoveduje zlorabo umetnointeligentnih sistemov, kadar so ti v nasprotju s spoštovanjem: »človekovega dostojanstva, svobode, enakosti, demokracije in pravne države ter temeljnimi pravicami, določenimi v Listini, vključno s pravico do nediskriminacije, varstva podatkov in zasebnosti ter pravicami otroka.« Nespoštovanje oziroma obseg kršitev določenih pravic, vključno s: »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,« tvori temelj za razvrstitev umetnointeligentnega sistema med sisteme visokega tveganja.⁸

Uredba (EU) 2022/2065 Evropskega parlamenta in Sveta z dne 19. oktobra 2022 o enotnem trgu digitalnih storitev in spremembi Direktive 2000/31/ES (Akt o digitalnih storitvah)⁹ v uvodni točki 81 določa, da druga kategorija sistemskih tveganj zadeva: »dejanski ali predvidljivi vpliv storitve na uresničevanje temeljnih pravic, kot so zaščitene z Listino, med drugim človekovega dostojanstva, svobode izražanja in obveščanja, vključno s svobodo in pluralizmom medijev, pravice do zasebnega

⁶ Glede konkretizacije posebnega cilja ali načina glej vsako posamezno točko prvega odstavka 5. člena Akta o umetni inteligenci.

⁷ Predstavljeni sta zgolj dve prepovedni praksi (točka b) in točka c) 5. člena Akta o umetni inteligenci). Prvi odstavek 5. člena obsega seznam osmih prepovedanih praks dajanja na trg, dajanja v uporabo in uporabe umetnointeligentnih sistemov.

⁸ Akt o umetni inteligenci, uvodna točka 48.

⁹ UL L 277, 27. 10. 2022, strani 1–102.

življenja, varstva osebnih podatkov, prepovedi diskriminacije, pravic otrok in varstva potrošnikov».

3 Kršitev avtorskega prava

3.1 Načini pridobivanja podatkov umetnointeligenčnih sistemov

Posegi umetnointeligenčnih sistemov v varovane avtorske pravice so prikazani skozi delovanje generativne umetne inteligence, vendar to ne pomeni, da analiza kršitev ni uporabna tudi za druge umetnointeligenčne sisteme, ki se razvijajo, učijo in delujejo na primerljiv način.

Sistemi generativne umetne inteligence so običajno usposobljeni na obsežnem učnem naboru podatkov, pridobljenem s spleta, ki vključuje veliko količino besedil s spletnih mest, člankov, knjig, objav na družbenih omrežjih ter strokovnih in znanstvenih prispevkov. Pri tem sistemi generativne umetne inteligence niso seznanjeni z avtorskimi pravicami na teh podatkih, temveč uporabljajo besedilo za učenje vzorcev in odnosov med besedami, besednimi zvezami in stavki, čeprav je velika večina besedil, uporabljenih za usposabljanje, varovanih z avtorskimi pravicami.¹⁰

Tehnologija umetne inteligence običajno uporablja naslednje pristope: strojno učenje, globoko učenje, nevronske mreže, kognitivno računalništvo, obdelavo naravnega jezika in računalniški vid.¹¹ Pridobivanje podatkov umetnointeligenčnih sistemov temelji na strganju podatkov, generiranju podatkov, odkupu podatkov in vnosu podatkov.¹² Klepetalni roboti običajno pridobivajo podatke iz lastne podatkovne baze, iskanja po spletu, uporabe aplikacijskega programskega vmesnika, obdelave naravnega jezika, iz podatkovne baze uporabnika in strojnega učenja.¹³ Ključna in primarna vira pridobivanja podatkov za delovanje ter uporabo klepetalnih robotov sta lastna baza podatkov in iskanje po spletu.

Z naraščajočo priljubljenostjo generativne umetne inteligence postaja ključno vprašanje, katere podatke lahko razvijalci umetnointeligenčnih sistemov uporabljajo za usposabljanje svojih modelov brez dovoljenja.¹⁴ Direktiva (EU) 2019/790

¹⁰ Helms in Krieser, 2023.

¹¹ Glej <https://csuglobal.edu/blog/how-does-ai-actually-work> (obiskano: 23. 1. 2025).

¹² Sahathullah, 2023.

¹³ Harris, 2024.

¹⁴ Bocharov et al., 2024.

Evropskega parlamenta in Sveta z dne 17. aprila 2019 o avtorski in sorodnih pravicah na enotnem digitalnem trgu in spremembi direktiv 96/9/ES in 2001/29/ES¹⁵ (Direktiva 2019/790) v 4. členu določa izjeme ali omejitve za besedilno in podatkovno rudarjenje. Na tej podlagi države članice EU določijo izjeme ali omejitve za namene besedilnega in podatkovnega rudarjenja. Slovenski zakonodajalec je besedilno in podatkovno rudarjenje implementiral s 57.a členom Zakona o avtorski in sorodnih pravicah¹⁶ (ZASP). Na podlagi tega člena ZASP je za namene besedilnega in podatkovnega rudarjenja prosto reproduciranje del, do katerih se zakonito dostopa. Reproduciranje je prosto tudi za komercialne namene.¹⁷ Besedilno in podatkovno rudarjenje je treba razumeti kot vsako avtomatizirano analitično tehniko, namenjeno analiziranju elektronskega besedila in podatkov.¹⁸

Splošna izjema za besedilno in podatkovno rudarjenje ne pride v poštev, kadar si avtor pridrži pravico uporabe del, ki so javno dostopna na spletu,¹⁹ ali izrecno in na ustrezen način prepove besedilno in podatkovno rudarjenje takšnih del. To se doseže zlasti s strojno berljivimi sredstvi, kot je na primer protokol za izključevanje spletnih pajkov (ang. Robots Exclusion Standard),²⁰ ki pajkom iskalnikov pove, do katerih URL-jev lahko dostopajo na zadevnem spletnem mestu.²¹ V tej zvezi se je tudi razvil program (Cloudflare), ki ima zmožnost samodejno blokirati bote, ki strgajo vsebine, s čimer lahko upravljavci spletnih strani na enostaven način blokirajo neželene umetnointeligentne pajke.²²

Dopustnost besedilnega in podatkovnega rudarjenja se označuje kot pomemben doprinos k razvoju podatkovne analitike in umetne inteligence v EU,²³ čeprav gre pri tem za vsebinsko omejitev avtorskih pravic. Da se za primere razvoja in učenja umetnointeligentnih modelov uporabljajo tehnike besedilnega in podatkovnega rudarjenja, izhaja že iz Akta o umetni inteligenci.²⁴ Na tej podlagi lahko

¹⁵ UL L 130, 17. 5. 2019, strani 92–125.

¹⁶ Uradni list RS, št. 16/07 – uradno prečiščeno besedilo, 68/08, 110/13, 56/15, 63/16 – ZKUASP, 59/19 in 130/22.

¹⁷ Predlog Zakona o spremembah in dopolnitvah Zakona o avtorski in sorodnih pravicah, EVA 2020-2130-0064, strani 17.

¹⁸ Prvi odstavek 57.a člena ZASP.

¹⁹ Tretji odstavek 57.a člena ZASP.

²⁰ Predlog Zakona o spremembah in dopolnitvah Zakona o avtorski in sorodnih pravicah, EVA 2020-2130-0064, strani 17, 56.

²¹ Glej <https://developers.google.com/search/docs/crawling-indexing/robots/intro> (obiskano: 23. 1. 2025).

²² Bocharov et al., 2024.

²³ Predlog Zakona o spremembah in dopolnitvah Zakona o avtorski in sorodnih pravicah, EVA 2020-2130-0064, stran 34.

²⁴ Akt o umetni inteligenci, uvodna točka 105.

umetnointeligenčni sistemi, četudi komercialnega značaja, z namenom besedilnega in podatkovnega rudarjenja reproducirajo zakonito dostopna dela²⁵ in jih hranijo tako dolgo, kot je to potrebno.²⁶

3.2 Navajanje podatkov umetnointeligenčnih sistemov

Uporaba podatkov za razvoj in učenje umetnointeligenčnih sistemov temelji na Direktivi 2019/790 in ZASP. Izhodni podatki v obliki proizvodov umetnointeligenčnih sistemov so vsaj pri nekaterih pogosto prikazani brez navedbe vnosnih podatkov, četudi jih ti pogosto poosebljajo. Spoštovanje in ustrezno navajanje tujih avtorskih del izhaja že iz osnovne akademske poštenosti in korektnosti.²⁷ Prav tako se z navajanjem uporabljenih virov preprečujejo nekatere oblike plagiatorstva.²⁸ Nekateri umetnointeligenčni sistemi, kot je na primer klepetalni robot ChatGPT, generirajo besedilo z uporabo vzorcev in struktur iz učnih podatkov, zato inherentno ne »podpirajo« določenih trditev ali idej. Namesto tega so njihovi odgovori oblikovani na temelju statističnih verjetnosti in vzorcev v podatkih.²⁹ Na podlagi tega se utemljuje zanemarjanje obveznosti navajanja uporabljenih virov pri oblikovanju določenih proizvodov umetne inteligence. Četudi bi pri tem zavzeli stališče, da umetnointeligenčni sistemi niso obvezani navesti seznama uporabljenih virov, na katerih temelji njihov proizvod, je vključitev navedbe uporabljenih virov še vedno koristna zaradi povečanja kredibilnosti in točnosti izhodnih podatkov.³⁰

Nekateri modeli generativne umetne inteligence ne navajajo uporabljenih virov, s katerimi so oblikovali proizvod. Uporabnik lahko pozove umetnointeligenčni sistem, naj mu poda seznam uporabljenih virov. Odziv umetnointeligenčnega sistema je v posameznih primerih nekorekten in nedostojen, saj ponudi seznam virov, ki so izmišljeni.³¹ Seznam z neresničnimi viri, za katere umetnointeligenčni sistem trdi, da jih uporabil pri oblikovanju proizvoda, je brezpomenski in zavajajoč. Tovrstni odziv umetnointeligenčnih sistemov ne le da zanemarja obveznost

²⁵ Primerjaj Lucchi, 2024, stran 616.

²⁶ Drugi odstavek 57.a člena ZASP in drugi odstavek 4. člena Direktive 2019/790.

²⁷ Primerjaj Beširević in Zahraštnik v Romih (ur.), 2023, stran 120.

²⁸ Kot plagiatorstvo se med drugim šteje predstavljanje tujega dela kot lastnega in kopiranje besedila ali idej tujih del brez navedbe vira. Glej <https://www.biblioblog.si/2011/03/plagiatorstvo-in-njegovo-odkrivanje.html> (obiskano: 24. 1. 2025).

²⁹ Lucchi, 2024, stran 617.

³⁰ Evropska komisija, 2023.

³¹ Primerjaj Day, 2023, strani 1024–1027.

sklicevanja na uporabljene viře, temveč tudi ponazarja prednost oblikovanja lažnega seznama virov pred seznanitvijo uporabnika z dejstvom, da ne more določiti konkretnih virov, ki tvorijo izhodne podatke.

3.3 Primeri domnevnih kršitev avtorskih pravic pri delovanju umetnointeligentnih sistemov

Vprašanje zakonitosti uporabe avtorsko zaščenega gradiva za učenje algoritmov klepetalnih robotov (npr. ChatGPT) in pogojev, pod katerimi je takšna uporaba dovoljena, je že predmet razprave v sodnih sporih. Ker klepetalni robot ChatGPT in drugi sistemi generativne umetne inteligence močno temeljijo na velikih količinah podatkov za učenje, ki lahko vključujejo avtorsko zaščenjena dela, lahko to predstavlja pomembno pravno oviro za njihovo delovanje.³²

Getty Images Inc. je začel sodni postopek proti podjetju Stability AI Limited, pri čemer je trdil, da je Stability AI kršil pravice intelektualne lastnine, vključno z avtorskimi pravicami za vsebine, ki jih ima v lasti ali zastopa Getty Images. Po stališču Getty Images je Stability AI nezakonito kopiral in obdelal milijone slik, zaščenjenih z avtorskimi pravicami, brez pridobitve ustrezne licence in z zasledovanjem lastnih komercialnih interesov, tj. učenje lastnega umetnointeligentnega sistema.³³ Višje sodišče v Angliji in Walesu,³⁴ ki obravnava to zadevo, je 14. 1. 2025 izdalo sodbo, ki se nanaša na določena postopkovna vprašanja³⁵ – meritorno o zadevi še ni odločalo.

The New York Times je vložil tožbo³⁶ proti OpenAI in Microsoftu zaradi kršitve avtorskih pravic. V tožbi je trdil, da so bili milijoni člankov, ki jih je objavil The Times, uporabljeni za usposabljanje avtomatiziranih klepetalnih robotov, ki zdaj konkurirajo časopisu kot viru zanesljivih informacij. V tožbi je navedenih več primerov, ko je klepetalni robot uporabnikom posredoval skoraj dobesečne odlomke iz člankov The Times, ki bi sicer zahtevali plačano naročnino za ogled. Trdil je, da sta OpenAI in Microsoft pri usposabljanju svojih programov umetne

³² Lucchi, 2024, stran 617.

³³ Glej <https://newsroom.gettyimages.com/en/getty-images/getty-images-statement> (obiskano: 24. 1. 2025).

³⁴ Izvorni naziv odločujočega sodišča je High Court of Justice, Business and Property Courts of England and Wales.

³⁵ Zadeva št. IL-2023-000007, Getty Images (US) Inc, Getty Images International UC, Getty Images (UK) Limited, Getty Images Devco UK Limited, iStockphoto LP, Thomas M Barwick Inc proti Stability AI Ltd, [2025] EWHC 38 (Ch), z dne 14. 1. 2025.

³⁶ Tožba je dostopna na naslednji povezavi: https://nytimes-assets.nytimes.com/2023/12/NYT_Complaint_Dec2023.pdf (obiskano: 29. 1. 2025).

intelligence posebno pozornost namenila uporabi novinarskih vsebin The Times zaradi domnevne zanesljivosti in točnosti teh gradiv.³⁷ Domnevne kršitve OpenAI in Microsoft naj bi nastale tako pri usposabljanju umetnointeligenčnih sistemov kot tudi pri izhodnih podatkih v obliki proizvoda.

Tožniki Paul Tremblay, Sarah Silverman,³⁸ Christopher Golden in Richard Kadrey so imetniki avtorskih pravic na svojih knjigah. Tožena stranka, OpenAI, razvija in ponuja programsko opremo umetne intelligence ChatGPT. OpenAI je kopiral avtorske dela (knjige) tožnikov in jih uporabil v svojem učnem podatkovnem naboru. Ko je bil ChatGPT pozvan, da povzame knjige, ki so jih napisali tožniki, je ustvaril natančne povzetke vsebine teh knjig, pri čemer naj bi prišlo do kršitve njihovih avtorskih pravic.³⁹

Omenjene zadeve so še vedno v teku,⁴⁰ zaradi česar način njihovega razpleta trenutno ostaja negotov. Posledično ni jasno, ali bodo sodišča to obravnavala kot kršitev avtorskih pravic. Je pa skoraj nedvoumno, da gre za kršitev, v kolikor bo produkt umetnointeligenčnega sistema dobesedno prepisal določeno varovano avtorsko delo. Ti primeri predstavljajo prve pomembne pravne spore v zvezi z uporabo umetne intelligence in kršitvijo avtorskih pravic. Če bodo tožniki dosegli ugoden izid, bi to lahko imelo velik vpliv na razvoj tehnologije umetne intelligence.⁴¹

4 Kršitev varstva osebnih podatkov

Med tradicionalno varovane vidike zasebnosti sodi tudi varstvo osebnih podatkov.⁴² Varstvo osebnih podatkov se v teoriji redoma opredeljuje s pojmom informacijska zasebnost, ki tvori del človekove zasebnosti.⁴³ Informacijska zasebnost odraža pravico posameznika nad nadzorom informacij o sebi.⁴⁴ Prav to je predmet človekove pravice do varstva osebnih podatkov na podlagi 38. člena Ustave RS.⁴⁵ V tej zvezi pravica do varstva osebnih podatkov obsega različne oblike osebnih

³⁷ Grynbaum in Mac, 2023.

³⁸ Primerjaj »United States District Court, Northern District of California«, Silverman et al. proti OpenAI, Inc. et al., 23-cv-3416, datum vložitve: 7. 7. 2023.

³⁹ »United States District Court, Northern District of California«, Paul Tremblay et al. proti OPENAI, INC. et al., 23-cv-03223-AMO, 23-cv-03416-AMO, z dne 12. 2. 2024.

⁴⁰ Več o podobnih tožbah glej: <https://www.mckoolsmith.com/newsroom-ai-litigation-3> (obiskano: 30. 1. 2025).

⁴¹ Lucchi, 2024, stran 615.

⁴² Farmanj v Avbelj (ur.), 2019, stran 342.

⁴³ Čebulj, 2002.

⁴⁴ Stone et al., 1983, stran 459.

⁴⁵ Čebulj, 2002.

podatkov – ti so lahko v besedilni, zvočni, slikovni obliki ali imajo genetske in druge biometrične značilnosti.⁴⁶

Pri vključevanju generativnih umetnointeligenčnih sistemov v procese podjetij bi moral biti ponudnik teh sistemov dejansko obravnavan kot obdelovalec podatkov v smislu Uredbe (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/ES⁴⁷ (Splošna uredba o varstvu podatkov). V skladu z 28. členom Splošne uredbe o varstvu podatkov bi bilo zato treba s ponudnikom skleniti pogodbo o obdelavi podatkov (ang. data processing agreement ali data processing addendum), s katero se opredelijo pravne obveznosti glede varstva osebnih podatkov. Če ponudnik generativnih umetnointeligenčnih sistemov (npr. OpenAI) ne omogoča sklenitve pogodbe o nerazkritju informacij (ang. non-disclosure agreement) ali pogodbe o obdelavi podatkov, obdelava osebnih podatkov ni zakonita. Zato podjetja, ki želijo obdelovati osebne podatke, uporabljajo podjetniške različice, s katerimi ponudnik svojim strankam zagotavlja pogodbo o obdelavi podatkov.⁴⁸ Na ta način ponudniki priznavajo svojo vlogo obdelovalca podatkov in se zavezujejo, da bodo podatke obdelovali v skladu z navodili svojih strank.⁴⁹

Splošna uredba o varstvu podatkov določa posebna pravila za prenos osebnih podatkov, ki se obdelujejo ali so namenjeni obdelavi po prenosu v tretjo državo.⁵⁰ Če ima ponudnik sedež v tretji državi, morajo podjetja iz EU, ki želijo uporabljati umetnointeligenčni sistem ponudnika, upoštevati pravne posledice prenosa osebnih podatkov v tretje države. Da bi se podjetja izognila uporabi teh posebnih pravil oziroma zagotovitve skladnosti s Splošno uredb o varstvu podatkov, podjetja v praksi pogosto ustanovijo podružnico na območju EU. S tem lahko uporabniki, katerih obdelava osebnih podatkov poteka po Splošni uredbi o varstvu podatkov, sklenejo pogodbeno razmerje s podružnico na območju EU in ne z matičnim podjetjem v tretji državi.⁵¹

⁴⁶ Teršek v Avbelj (ur.), 2019, stran 367.

⁴⁷ UL L 119, 4. 5. 2016, strani 1–88.

⁴⁸ Glej na primer različico »ChatGPT Enterprise«.

⁴⁹ Paschou, 2024. Glej npr. <https://openai.com/policies/data-processing-addendum/> (obiskano: 29. 1. 2025).

⁵⁰ Glej poglavje V Splošne uredbe o varstvu podatkov.

⁵¹ Kot primer kaže izpostaviti ameriško podjetje OpenAI, ki ima sedeže v Kaliforniji, in je s tem namenom ustanovila podružnico OpenAI Ireland Ltd. v Dublinu. Paschou, 2024. Primerjaj <https://openai.com/policies/data-processing-addendum/> (obiskano: 29. 1. 2025).

Usposabljanje generativnih umetnointeligentnih sistemov temelji na ogromni količini javno dostopnih in pridobljenih podatkov s spleta, kar vključuje tudi številne vrste osebnih podatkov.⁵² V zvezi s tem se lahko pojavijo znatna tveganja glede varstva osebnih podatkov, predvsem nevarnost profiliranja in možna izguba nadzora nad osebnimi podatki.⁵³ Zaradi tega trenutno ni jasno, v kolikšnem obsegu generativni modeli umetne inteligence lahko spoštujejo »pravico do izbrisa« oziroma »pravico do pozabe«, kot je določena v 17. členu Splošne uredbe o varstvu podatkov.⁵⁴ Če se izgubi nadzor nad osebnimi podatki, ki so bili uporabljeni kot učni podatkovni nabor, bo praktično nemogoče uveljavljati pravico do izbrisa, četudi ta pripada posamezniku. Nasprotno, če je mogoče enostavno in jasno identificirati osebne podatke, ima posameznik pravico doseči, da upravljavec brez nepotrebnega odlašanja izbriše zadevne osebne podatke, ob predpostavki, da za to obstaja razlog iz 17. člena Splošne uredbe o varstvu podatkov.

5 Pristranskost umetnointeligentnih sistemov

5.1 Razlog pristranskosti umetnointeligentnih sistemov

Sistemi umetne inteligence se učijo sprejemanja odločitve na podlagi učnih podatkov, zato je ključnega pomena oceniti nabor podatkov glede morebitne pristranskosti. Ena od metod je pregled vzorčenja podatkov, da bi ugotovili, ali so določene skupine oseb v učnih podatkih preveč oziroma premalo zastopane ali nedosledno označene (podatkovna pristranskost). Denimo, orodja umetne inteligence za zaposlovanje, ki uporabljajo nedosledno označevanje ali izključujejo oziroma prekomerno ovrednotijo določene značilnosti, lahko neupravičeno izločijo kvalificirane kandidate iz postopka izbire.⁵⁵ Še več, nepopolni in pristranski podatki lahko povzročijo napake in nepravilnosti pri diagnosticiranju kožnih bolezni, kot je melanom.⁵⁶ Ljudje so pri obdelavi podatkov in sprejemanju odločitev lahko pod vplivom lastnih subjektivnih prepričanj in stališč (kognitivna pristranskost). Posledično lahko te pristranskosti vgradijo v sisteme umetne inteligence prek izbire podatkov ali načina njihovega vrednotenja. Na primer, kognitivna pristranskost

⁵² Glej <https://honoralia.com/en/the-right-to-be-forgotten-in-chatgpt/> (obiskano: 29. 1. 2025).

⁵³ Paschou, 2024.

⁵⁴ Glej <https://www.fieldfisher.com/en/insights/does-chatgpt-comply-with-eu-gdpr-regulations-inves> (obiskano: 29. 1. 2025) in Zhang et al., 2024, strani 1–10.

⁵⁵ Glej <https://www.ibm.com/think/topics/shedding-light-on-ai-bias-with-real-world-examples> (obiskano: 20. 1. 2025).

⁵⁶ Adamson in Smith, 2018, strani 1247–1248, Vokinger et al., 2021, stran 2.

lahko povzroči, da se daje prednost podatkovnim naborom, zbranim v določeni državi, namesto da bi vključevali vzorce iz različnih populacij po vsem svetu. Uporaba nepravilnih učnih podatkov lahko privede do algoritmov, ki ponavljajo napake, povzročajo nepravične rezultate ali celo še dodatno krepijo pristranskost, ki je že prisotna v pomanjkljivih podatkih (algoritemska pristranskost). Ta vrsta pristranskosti se lahko pojavi tudi zaradi programskih napak, na primer če razvijalec nepošteno tehta določene dejavnike pri odločanju algoritma zaradi lastne zavestne ali nezavestne pristranskosti. Tako lahko algoritem na podlagi kazalnikov diskriminira med skupinami oseb z določenimi lastnostmi.⁵⁷ Zato sta kakovosten učni nabor podatkov in ustrezna analitična zasnova ključnega pomena za odpravo pristranskosti v delovanju umetnointeligentnih sistemov.⁵⁸

5.2 Dejanski primeri pristranskosti umetnointeligentnih sistemov

V podjetju Amazon so zasnovali in uporabljali računalniške programe za pregledovanje življenjepisov kandidatov za zaposlitev z namenom mehanizacije izbire iskalcev zaposlitve. Leta 2015 je podjetje Amazon ugotovilo, da zasnovani sistem za izbiro kandidatov za delovna mesta programskih razvijalcev in drugih tehničnih položajev ni ocenjeval kandidatov na spolno nevtralen način. Razlog za to je dejstvo, da so bili Amazonovi računalniški modeli usposobljeni za preverjanje prijavljenih kandidatov s proučevanjem vzorcev v življenjepisih, ki so jih kandidati predložili podjetju v preteklih desetih letih. Ker tehnološko industrijo zaznamuje prevlada moških zaposlenih, se je Amazonov sistem priučil, da so moški kandidati bolj zaželeni. Na tej podlagi je negativno ovrednotil življenjepise, ki so vsebovali besedo »ženski«, na primer v izrazu »kapetanka ženskega šahovskega kluba«. Prav tako je nižje ovrednotil življenjepise diplomantk izključno ženskih fakultet.⁵⁹

COMPAS je orodje za oceno tveganja in potreb storilcev kaznivih dejanj.⁶⁰ Pravosodne agencije v ZDA uporabljajo COMPAS kot pomoč pri odločanju o razporejanju, nadzoru in upravljanju primerov storilcev kaznivih dejanj. COMPAS je bil razvit empirično, s poudarkom na dejavnikih, za katere je znano, da vplivajo

⁵⁷ Glej <https://www.ibm.com/think/topics/shedding-light-on-ai-bias-with-real-world-examples> (obiskano: 20. 1. 2025). Podrobneje o tem Sun et al., 2020, strani 1–39.

⁵⁸ Arbet et al., 2020, stran 1.

⁵⁹ Dastin, 2018.

⁶⁰ Orodje COMPAS vključuje dinamične dejavnike tveganja in zagotavlja informacije o različnih dobro preverjenih dejavnikih tveganja in potrebah, z namenom identificiranja ustreznih korektivnih ukrepov za zmanjšanje verjetnosti ponovitve kaznivih dejanj.

na ponovitev kaznivih dejanj. Dejavniki, ki tvorijo podlago za oceno tveganja,⁶¹ so sestavljeni iz statusa poklicnega izobraževanja, trenutne starosti, starosti ob prvi aretaciji, zgodovine nasilja, števila prejšnjih aretacij, zaposlitvenega statusa in prejšnje razveljavitve pogojnega izpusta.⁶² Na podlagi tega orodja so bili temnopolti obtoženci dvakrat pogosteje kot belopolti napačno ocenjeni kot osebe z višjim tveganjem za nasilno ponovitev kaznivega dejanja, medtem ko so bili belopolti povratniki napačno ocenjeni kot nizko tveganje 63,2 % pogosteje kot temnopolti obtoženci.⁶³ Ta primer ponazarja neprimernost pristranskosti učnih podatkov umetnointeligenčnega sistema, ki temeljijo na zgodovinskih kazenskih evidencah in vključujejo rasne razlike pri aretacijah in obsodbah. Orodju COMPAS je bilo očitano tudi pomanjkanje transparentnosti delovanja algoritma, saj ta ne omogoča preglednosti in sledljivosti pri odločanju v posameznih primerih. Lastniška narava algoritma COMPAS in njegova zapletenost sta oteževali razumevanje njegovih odločitev, kar je botrovalo k prikrivanju pristranskosti. Kljub temu je analiza ProPublice pokazala, da je algoritem pri ocenjevanju tveganja izkazoval rasno pristranskost – pogosto je precenjeval tveganje ponovitve kaznivega dejanja pri temnopoltih obtožencih, medtem ko ga je pri belopoltih podcenjeval.⁶⁴

5.3 Pristranskost, pravičnost in natančnost umetnointeligenčnih sistemov

Posebne značilnosti, ki opredeljujejo delovanje umetnointeligenčnih sistemov, vključno z netransparentnostjo (učinek črne skrinjice), kompleksnostjo, nepredvidljivostjo in delno avtonomnim vedenjem, lahko otežijo preverjanje skladnosti ter ovirajo učinkovito spoštovanje in uveljavljanje človekovih pravic.⁶⁵ Prisotnost podatkovne, algoritemske in kognitivne pristranskosti ter diskriminacije v umetnointeligenčnih sistemih ima globoke etične in ustavnopravne implikacije. Reševanje tovrstne problematike zahteva usklajena prizadevanja za razvoj pravičnih, preglednih in odgovornih sistemov umetne inteligence, ki spoštujejo vse človekove pravice.⁶⁶ Vendar pa je doseganje pravičnosti in natančnosti zahtevno, saj omejitve pravičnosti lahko okrnijo sposobnost umetnointeligenčnega sistema za natančno

⁶¹ Dejavniki, ki se upoštevajo, se razlikujejo glede na to, za kateri model ocenjevanja tveganj gre.

⁶² Glej <https://s3.documentcloud.org/documents/2840784/Practitioner-s-Guide-to-COMPAS-Core.pdf> (obiskano: 20. 1. 2025), strani 1, 28–29.

⁶³ Larson et al., 2016. Dejanski in konkretni primeri, ki ponazarjajo pristranskost ocene tveganja do temnopoltih oseb, so razvidni v delu Angwin et al., 2016.

⁶⁴ Min, 2023, stran 3812; Räs, 2022, strani 300–306.

⁶⁵ Evropska komisija, 2020, stran 12.

⁶⁶ Min, 2023, stran 3810.

napovedovanje in obratno.⁶⁷ Osredotočanje izključno na pravičnost lahko povzroči skupinske razlike, kjer določene skupine opravičeno prejemajo ugodno ali neugodno obravnavo, ne glede na njihove dejanske značilnosti.⁶⁸ To privede do enake obravnave različnih subjektov ter različnih pravnih in dejanskih okoliščin, kar povzroča kršitev pravice do enakopravnosti.⁶⁹ Na koncu je oblikovanje pravičnih in poštenih umetnointeligenčnih sistemov zapletena naloga, ki vključuje kompromis med pravičnostjo in natančnostjo.⁷⁰ Bistveno bo najti pravo ravnovesje, da bodo sistemi umetne inteligence zagotavljali pravične rezultate, ne da bi pri tem ogrozili svojo učinkovitost. Spoštovanje človekovih pravic, ki med drugim prepovedujejo pristransko delovanje umetnointeligenčnih sistemov, bo ključnega pomena za dosego algoritemske pravičnosti.⁷¹

6 Kršitev pravice do dela

6.1 Visokotvegani umetnointeligenčni sistemi

V Ustavi RS ni izrecno uporabljena besedna zveza »pravica do dela«, temveč je določba 49. člena Ustave RS poimenovana »svoboda dela«, ki sicer sestoji iz enakih elementov kot pravica do dela, določena v mednarodnih aktih.⁷² Uporaba umetnointeligenčnih sistemov v okviru pravice do dela lahko predstavlja veliko tveganje za posameznike, skupine, predstavnike delavcev (kot so sindikati), skupnosti in organizacije. Če je uporaba teh sistemov nepregledna, nepravilno uporabljena, napačno zasnovana ali neustrezno nadzorovana, lahko povzroči škodo ali krši človekove pravice in temeljne svoboščine. Uporaba pristranskih podatkov za usposabljanje umetnointeligenčnih orodij ali uporaba neustreznih ali nezakonitih dejavnikov oziroma kazalnikov v sistemih umetne inteligence lahko pomembno vpliva na osebni in poklicni razvoj delavca ter povzroči neenakost pri dostopu do zaposlitvenih priložnosti.⁷³

⁶⁷ Chouldechova, 2016; Min, 2023, stran 3814.

⁶⁸ Crawford, 2016; Min, 2023, stran 3814.

⁶⁹ Avbelj in Vatovec v Avbelj (ur.), 2019, stran 116.

⁷⁰ Pravičnosti ni mogoče in je morda niti ne bi smeli avtomatizirati. Umetna inteligenca namreč nima sposobnosti razumevanja kontekstualne enakosti, ne more zajeti in upoštevati lokalnih političnih, družbenih ter okoljskih dejavnikov posameznega primera. Tako Wachter et al., 2020, stran 29.

⁷¹ Min, 2023, stran 3814.

⁷² Korpič – Horvat, 2018, stran 25.

⁷³ Glej <https://www.edps.europa.eu/system/files/2023-10/1.-resolution-on-ai-and-employment-en.pdf> (obiskano: 2. 2. 2025), stran 2.

Umetnointeligenčni sistemi, ki negativno vplivajo na varnost ali temeljne pravice, so obravnavani kot visoko tvegani. Na področju delovnega prava so takšni sistemi prisotni zlasti pri zaposlovanju, upravljanju delavcev in dostopu do samozaposlitve.⁷⁴ Tako izhaja tudi iz Priloge III Akta o umetni inteligenci, ki kot visokotvegane sisteme umetne inteligence⁷⁵ opredeli: »(a) sisteme umetne inteligence za zaposlovanje ali izbor fizičnih oseb, zlasti za ciljno oglaševanje delovnih mest, analizo in filtriranje prijav za zaposlitev ter ocenjevanje kandidatov, in (b) sisteme umetne inteligence za odločanje o pogojih delovnih razmerij, napredovanju ali prenehanju delovnih pogodbenih razmerij, dodeljevanju nalog na podlagi vedenja posameznika oziroma osebnostnih lastnosti ali značilnosti ter spremljanju in ocenjevanju uspešnosti in vedenja oseb v takih razmerjih.«⁷⁶

Razvrstitev umetnointeligenčnega sistema med visokotvegane sisteme umetne inteligence prinaša posebne zahteve za te sisteme in obveznosti za operaterje takšnih sistemov.⁷⁷ V skladu s tem morajo visokotvegani sistemi umetne inteligence izpolnjevati zahteve iz oddelka 2 Akta o umetni inteligenci,⁷⁸ pri čemer je treba upoštevati njihov predvideni namen ter splošno priznane najsodobnejše dosežke na področju umetne inteligence.⁷⁹ Delodajalci, ki uporabljajo umetnointeligenčne sisteme, ki jih Akt o umetni inteligenci opredeli kot visokotvegane, morajo izpolnjevati stroge obveznosti v zvezi s preglednostjo, nadzorom, usposabljanjem in poročanjem. Akt o umetni inteligenci določa zahteve za ponudnike in uporabnike umetnointeligenčnih sistemov, če se uporabljajo za zaposlovanje, napredovanje, prenehanje pogodbenega delovnega razmerja, za dodeljevanje nalog in ocenjevanje uspešnosti.⁸⁰

Če gre z Aktom o umetni inteligenci za prepovedan umetnointeligenčni sistem, se morajo delodajalci izogibati njegovi uporabi. Akt o umetni inteligenci prepoveduje uporabo umetnointeligenčnih sistemov, ki veljajo za škodljive ali diskriminatorne. Kot prepovedani sistemi veljajo umetnointeligenčni sistemi,⁸¹ ki:

⁷⁴ Glej <https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence> (obiskano: 3. 2. 2025).

⁷⁵ Drugi odstavek 6. člena Akta o umetni inteligenci določa, da se za visokotvegane sisteme umetne inteligence štejejo tudi sistemi umetne inteligence iz Priloge III.

⁷⁶ Glej četrto točko Priloge III Akta o Umetni inteligenci.

⁷⁷ Glej točko c) drugega odstavka 1. člena Akta o umetni inteligenci.

⁷⁸ Oddelek 2, zahteve za visokotvegane sisteme UI, obsega člene od 8 do 15 Akta o umetni inteligenci.

⁷⁹ Določba 8. člena Akta o umetni inteligenci.

⁸⁰ Zahteve za visokotvegane umetnointeligenčne sisteme se začnejo uporabljati 2. 8. 2026 ali 2. 8. 2027, odvisno od opredelitve sistema (primerjaj 113. člen Akta o umetni inteligenci). Zimmermann et al., 2024.

⁸¹ Primerjaj prepovedane prakse umetnointeligenčnih sistemov, določene s 5. členom Akta o umetni inteligenci. Uvodna točka 179 Akta o umetni inteligenci določa, da se prepovedi iz te uredbe uporabljajo že od 2. 2. 2025.

- sklepajo o čustvih fizične osebe na delovnem mestu;
- iz biometričnih podatkov sklepajo občutljive osebne značilnosti;
- osebam dodeljujejo ocene na podlagi družbenega vedenja ali osebnostnih značilnosti.⁸²

Akt o umetni inteligenci ne velja le za ponudnike, ki dajejo na trg ali v uporabo umetnointeligenčne sisteme v območju EU, temveč se uporablja tudi za multinacionalne delodajalce, če njihovi umetnointeligenčni sistemi zunaj EU sprejemajo odločitve v zvezi z delovno silo v EU.⁸³ Na primer, delodajalec s sedežem v tretji državi, ki uporablja umetnointeligenčni sistem za merjenje uspešnosti zaposlenih pri dodeljevanju bonusov po vsem svetu, vključno z delavci v EU, bo zavezan z Aktom o umetni inteligenci.⁸⁴

6.2 Dejanski primeri kršitve pravice do dela

Sodišče v Amsterdamu je obravnavalo in delno zavrnilo vlogo, ki so jo vozniki Uberja vložili proti avtomatizirani prekinitvi njihovih pogodb zaradi domnevnih goljufij. Sodišče je ugotovilo, da deaktivizacija licence oziroma postopek prekinitve njihovih pogodb ne predstavlja avtomatiziranega sprejemanja posameznih odločitev v skladu z 22. členom Splošne uredbe o varstvu podatkov.⁸⁵

Italijanski nadzorni organ za varstvo podatkov je presojal, ali gre za dopustno uporabo umetnointeligenčnih sistemov, ki avtomatizirano sprejemajo posamezne odločitve, vključno z oblikovanjem profilov, na podlagi katerih je prišlo do izključitve nekaterih dostavljavcev iz delovnih priložnosti. Nadzorni organ za varstvo podatkov je ugotovil, da je pri tem prišlo do kršitve Splošne uredbe o varstvu podatkov, saj podjetje ni uvedlo ustreznih ukrepov za varovanje človekovih pravic in svoboščin svojih zaposlenih pred diskriminatornim avtomatiziranim odločanjem. Točkovalni sistem za dodeljevanje dostavnih terminov je namreč nekatere dostavljavce izključil iz zaposlitvenih priložnosti.⁸⁶

⁸² Zimmermann et al., 2024.

⁸³ Točka c) prvega odstavka 2. člena Akta o umetni inteligenci.

⁸⁴ Chance, 2024, stran 6.

⁸⁵ Rb. Amsterdam - C./13/692003/HA RK 20-302.

⁸⁶ Povzetek sklepa italijanskega nadzornega organa za varstvo podatkov, št. 9677611, 5. 7. 2021 in <https://www.edps.europa.eu/system/files/2023-10/1.-resolution-on-ai-and-employment-en.pdf> (obiskano: 2. 2. 2025), stran 7.

7 Kršitev svobode izražanja

Delovanje umetnointeligenčnih sistemov – zlasti generativne umetne inteligence – lahko posega tudi v pravico do svobode izražanja, in sicer v njen del, ki vključuje sprejemanje informacij.⁸⁷ Neresnične informacije, ki jih proizvajajo umetnointeligenčni sistemi, lahko predstavljajo nedopusten poseg v uporabnikovo pravico do svobode izražanja oziroma sprejemanja informacij, pri čemer pa ni vsako takšno dejanje že samo po sebi nedopustno. Pri ugotavljanju, ali obstaja pozitivna dolžnost ponudnika umetnointeligenčnega sistema glede pravilnega razširjanja informacij, je treba upoštevati pravično ravnovesje med splošnim interesom skupnosti in interesi posameznika. Obseg pozitivne dolžnosti se neizogibno razlikuje glede na raznolikost okoliščin v državah pogodbenicah, kompleksnost nadzora nad sodobnimi družbami ter potrebo po tehtanju med različnimi prioritetami in razpoložljivimi viri.⁸⁸ Nedopustno poseganje v pravico do sprejemanja informacij nastopi le v primerih, ko je posamezniku resneje omejen, izkrivljen ali usmerjen dostop do informacij v javnem interesu.

Vzrok za proizvajanje in navajanje neresničnih informacij izvira iz dveh razlogov. Prvi razlog odraža proizvod netočnih informacij zaradi nepravilnih vhodnih podatkov, na katerih je zgrajen velik jezikovni model. To lahko povzročijo že napačne informacije na spletu in drugih virih, ki so del podatkovnega nabora umetnointeligenčnega sistema.

Drugi – bolj zaskrbljujoč – razlog nastopi, ko umetnointeligenčni sistem »halucinira« oziroma ustvarja nove, neresnične informacije, kadar ne najde ustreznega odgovora na uporabnikovo vprašanje. V tem primeru umetnointeligenčni sistem »zavestno« proizvede netočne informacije in jih prikazuje kot resnične.⁸⁹ Mogoča je situacija, kjer si umetnointeligenčni sistem, če ne razpolaga s podatki za točen odgovor, nekritično izmisli zanj pravilen odgovor, ki ga označi kot resničnega. Pri tem lahko pride do izmišljevanja sodnih odločb, ki v konkretnem pravnem redu sploh ne

⁸⁷ Teršek v Avbelj (ur.), 2019, stran 374. Tako Ustava RS (39. člen) kot EKČP (10. člen) (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, Uradni list RS–MP, št. 7/94) vključujeta v pravico do svobode izražanja sprejemanje informacij. Eskens et al. 2017, stran 260.

⁸⁸ Glej 43. točko sodbe ESČP *Özgür Gündem v. Türkiye*, št. 23144/93 z dne 16. 3. 2000.

⁸⁹ Glej <https://www.thefire.org/research-learn/artificial-intelligence-free-speech-and-first-amendment> (obiskano: 3. 2. 2025).

obstajajo.⁹⁰ Izmišljevanje pravnih pravil ali sodne praske in zatrjevanje njihove resničnosti bi se lahko obravnavalo kot nedopustno okrnitev sprejemanja informacij, s čimer bi delovanje umetnointeligenčnih sistemov lahko posegalo v uporabnikovo pravico do svobode izražanja – predvsem v primerih obstoječe informacijske asimetrije med umetnointeligenčnim sistemom in uporabnikom. Umetnointeligenčni sistemi lahko na številne načine izboljšajo komunikacijo in dostop do informacij, tudi prek tradicionalnih medijev,⁹¹ vendar če je s tem omogočen dostop do večjega števila netočnih in neresničnih informacij, je takšna izboljšava zgolj navidezna, če ne celo ovirajoča in škodljiva.

8 Kršitev pravice do osebnega dostojanstva ter varstva pravic zasebnosti in osebnostnih pravic

Temelj in meja ustavnega varstva časti izhajata iz pravice do osebnega dostojanstva (34. člen Ustave RS) ter varstva pravic zasebnosti in osebnostnih pravic (35. člena Ustave RS).⁹² Osrednji vidik varstva pravic zasebnosti in osebnostnih pravic je zagotavljanje nedotakljivosti zasebnosti, vendar med osebnostne pravice, varovane s 35. členom Ustave RS, umeščamo tudi pravico do varstva časti in ugleda.⁹³

Sistemi generativne umetne inteligence so pogosto uporabljeni za kratkočasenje uporabnikov. V tej zvezi nastanejo številni zapisi, slike in video posnetki, ki na humorističen način prikazujejo osebe v neobičajnem, nerodnem ali zabavnem kontekstu. Takšni proizvodi, vsaj praviloma, ne bodo predstavljali protipravnega posega v pravico do osebnega dostojanstva, pravico do zasebnosti in osebnostne pravice v smislu 35. člena Ustave RS – zlasti, če gre za javne osebe.⁹⁴ Vendar pa se umetnointeligenčne sisteme lahko zlorabi tudi za oblikovanje žaljivih ali intimnih proizvodov. V Španiji je v javnost prišel primer zlorabe umetnointeligenčnih sistemov za namene ustvarjanja pornografskega gradiva. Uporabnik je v

⁹⁰ Primerjaj Beširević, Zahrstnik v Romih (ur.), 2023, strani 111–112 (avtorja opisujeta primer, kjer je klepetalni robot ChatGPT v pozivu na poznavanje slovenske sodne prakse odgovoril z neresnično in neobstoječo sodno odločbo) in zadevo »United States District Court Southern District OF New York«, Roberto Mata proti Avianca, Inc., 22-cv-1461, z dne 22. 6. 2023 (gre za zadevo, kjer je odvetnik predložil neobstoječe sodne odločbe z lažnimi navedki in citati, ki jih je ustvaril klepetalni robot ChatGPT).

⁹¹ Primerjaj Haas, 2020, stran 1.

⁹² Ustavno sodišče Republike Slovenije, U-I-226/95, ECLI:SI:USRS:1999:U.I.226.95, točka 10.

⁹³ Farmanj v Avbelj (ur.), 2019, strani 342–343.

⁹⁴ Tudi za absolutno javne osebe veljata pravica do osebnega varstva ter varstvo pravic zasebnosti in osebnostnih pravic, čeprav v omejenem obsegu, ki je običajno rezultat tehtanja med pravico do osebnega dostojanstva oziroma pravico do zasebnosti in pravico do svobode izražanja. V primeru žaljivih ali zlonamernih objav, katerih namen je zaničevanje osebe, pa varstvo pripada tudi (absolutno) javni osebi. Glej Toplak v Šturm (ur.), 2010, stran 370.

umetnointeligenčni sistem naložil fotografije mladoletnih deklet, katerih starost je bila med 11 in 17 leti. Fotografije je uporabnik pridobil iz družbenih omrežij in jih brez privolitve uporabil v programu umetne inteligence. Na tej podlagi je program ustvaril slike golih teles z obrazi, ki jih je prevzel iz naloženih fotografij.⁹⁵ Takšni primeri uporabe in zlorabe umetnointeligenčnih sistemov so eklatanten primer protipravnega posega v pravico do osebnega dostojanstva, pravico do zasebnosti in osebnostne pravice v smislu 35. člena Ustave RS.⁹⁶ Predvsem tehnologija globokih ponaredkov (ang. deep fake) zna zlahka omogoči platformo za zasledovanje nepristnih in škodoželjnih interesov, ki ogrožajo človekove pravice.

Uporabnikovo prikazovanje, objavljanje in razširjanje proizvodov umetnointeligenčnih sistemov spadajo med njegovo pravico do svobode izražanja, vendar je pri tem omejen s tujo pravico do zasebnosti, vključno s pravico do varstva časti in dobrega imena. Kolizija pravice do svobode izražanja ter pravice do varstva časti in dobrega imena je lahko dopustna oziroma neobstoječa, četudi gre za zelo ostre, surove in brezobzirne izjave, ki jih oseba dojema kot kritiko ravnanja ali stališča in ne kot napad na osebnost ali njeno sramotitev, poniževanje, prezir ali zasmehovanje. Zadevni pravici sta vendarle lahko kolidirajoči, če izjavitelj z izjavo ne zasleduje prispevka k razpravi v zadevah javnega pomena, temveč je izjava žaljiva za drugega – takrat protipravnost izjav ni izključena.⁹⁷

Pravica do lastnega glasu oziroma pravica na glasu velja za eno od osebnostnih pravic, varovanih na podlagi 35. člena Ustave.⁹⁸ V tej zvezi je bilo sporno oblikovanje glasu umetnointeligenčnega sistema, poimenovanega »Sky«, ki je po barvi in tonaliteti spominjal na glas znane igralka Scarlett Johansson.⁹⁹ OpenAI, ki je oblikoval in dal v javno uporabo sistem z možnostjo komuniciranja z umetnim ženskim glasom, poudarja, da program »Sky« ni imitacija igralkinega glasu. Navkljub temu je OpenAI kasneje z namenom izognitve morebitnem sodnem sporu to funkcijo umaknil iz uporabe.¹⁰⁰

⁹⁵ Brkan, 2023. Glej tudi Viejo, 2023.

⁹⁶ Ustavnopravno zagotovljeno varstvo pravic zasebnosti varuje pred razkritjem posameznikove osebne zadeve, ki jih slednji želi ohraniti skrite in ki se po naravi stvari ali glede na ustaljena pravila ravnanja v družbi štejejo za take. Ustavno sodišče Republike Slovenije, U-I-272/98-26, ECLI:SI:USRS:2003:U.I.272.98.

⁹⁷ Farmany v Avbelj (ur.), 2019, stran 347.

⁹⁸ Farmany v Avbelj (ur.), 2019, stran 344, in odločba Ustavnega sodišča Republike Slovenije, Up-472/02, ECLI:SI:USRS:2004:Up.472.02.

⁹⁹ Omenjena igralka je v filmu »Her« glasovno upodobila glas umetnointeligenčnega sistema.

¹⁰⁰ Robins-Early, 2024.

9 Zaključek

Umetnointeligenčni sistemi lahko vplivajo pozitivno na izboljšanje dostopa do informacij in poenostavitev procesov, vendar če proizvodi umetnointeligenčnih sistemov temeljijo na kršitvah in posegih v ustavno varovane dobrine, je treba utemeljeno podvomiti o stimuliranju teh sistemov in njihovi družbeni koristnosti.

Umetnointeligenčnim sistemom je na podlagi besedilnega in podatkovnega rudarjenja dovoljeno reproducirati avtorska dela, do katerih zakonito dostopajo. Avtor ima pri tem možnost prepovedati podatkovno in besedilno rudarjenje takšnih del. V tej zvezi so bile razvite tehnične rešitve (npr. Robots Exclusion Standard, Cloudflare), ki onemogočajo spletnim pajkom in botom umetnointeligenčnih sistemov dostop do javno dostopnih spletnih vsebin. Dopustnost besedilnega in podatkovnega rudarjenja je vsekakor ključnega pomena za funkcionalno in natančno delovanje umetnointeligenčnih sistemov, čeprav to pomeni vsebinsko omejitev avtorske pravice. Pobuda in odgovornost, da umetnointeligenčnim sistemom prepreči dostop do lastnih avtorskih del, je torej na avtorju. Poleg kršitve avtorskih pravic pri razvoju, usposabljanju in delovanju umetnointeligenčnih sistemov, so lahko avtorske pravice ogrožene tudi pri končnem proizvodu oziroma konkretnem izhodnem rezultatu umetnointeligenčnega sistema. To je pogosto zlasti pri modelih generativne umetne inteligence, ki večinoma ne navajajo uporabljenih virov ali si jih celo izmislijo. Dosledno navajanje virov izvira iz akademske poštenosti in korektnosti ter je namenjeno preverjanju kredibilnosti in natančnosti navedenih podatkov. Zanemarjanje obveznosti navedbe tujega avtorskega dela se lahko pri fizičnih osebah šteje za plagiatorstvo.

Informacijska zasebnost, ki zagotavlja varstvo osebnih podatkov, je na področju delovanja in uporabe umetnointeligenčnih sistemov podvržena številnim tveganjem, povezanim z upoštevanjem določb Splošne uredbe o varstvu podatkov. Če se modeli generativne umetne inteligence vključujejo v procese podjetij, bi moral biti ponudnik teh sistemov dejansko obravnavan kot obdelovalec podatkov v luči Splošne uredbe o varstvu podatkov. Upravitelj podatkov mora z obdelovalcem skleniti pogodbo o obdelavi podatkov, sicer gre za nezakonito obdelavo osebnih podatkov. V izogib temu so na voljo poslovne različice umetnointeligenčnih sistemov, ki svojim strankam zagotavljajo pogodbo o obdelavi podatkov. Nadalje Splošna uredba o varstvu podatkov določa posebna pravila za prenos osebnih podatkov, ki se obdelujejo ali so namenjeni obdelavi po prenosu v tretjo državo. Zato morajo

podjetja iz EU, ki želijo uporabljati umetnointeligenčni sistem ponudnika s sedežem v tretji državi, upoštevati pravne posledice prenosa osebnih podatkov v tretje države.¹⁰¹ Umetnointeligenčni sistemi morajo prav tako upoštevati in izvajati »pravico do izbrisa« oziroma »pravico do pozabe«. Preteča nevarnost se kaže v izgubi nadzora nad osebnimi podatki, ki so bili uporabljeni kot učni podatkovni nabor, zaradi česar je v takšnih primerih praktično nemogoče udejanjiti pravico do izbrisa, četudi se ta utemeljeno uveljavlja.

Razlog za pristranskost umetnointeligenčnih sistemov je mogoče identificirati v podatkovni pristranskosti (neprimeren in pristranski učni podatkovni nabor), algoritemski pristranskosti (algoritem je namerno ali nehote zasnovan pristransko) in kognitivni pristranskosti (pristranskost pri izbiri ali ovrednotenju podatkov).¹⁰² Pristranskost umetnointeligenčnih sistemov je mogoče odpraviti z oblikovanjem in zagotavljanjem pravičnega ter natančnega delovanja teh sistemov. Iskanje ustreznega ravnovesja med pravičnostjo in natančnostjo je zahtevno, saj lahko omejitve pravičnosti okrnijo sposobnost umetnointeligenčnega sistema za natančno napovedovanje.¹⁰³ Nasprotno, osredotočanje izključno na pravičnost lahko povzroči skupinske razlike, kjer določene skupine opravičeno prejemajo ugodno ali neugodno obravnavo, ne glede na njihove dejanske značilnosti.¹⁰⁴ Ključno bo najti pravo ravnovesje med natančnostjo in pravičnostjo, ne da bi prišlo do diskriminacije med osebami ali skupinami oseb.

Akt o umetni inteligenci navaja kot visokotvegane umetnointeligenčne sisteme tiste, ki se uporabljajo za zaposlovanje ali izbor fizičnih oseb, ciljno oglaševanje delovnih mest, analizo in filtriranje prijav za zaposlitev, ocenjevanje kandidatov, za odločanje o pogojih delovnih razmerij, napredovanju ali prenehanju delovnih pogodbenih razmerij, dodeljevanju nalog na podlagi vedenja posameznika oziroma osebnostnih lastnosti ter spremljanju in ocenjevanju uspešnosti ter vedenja. Kvalifikacija umetnointeligenčnega sistema kot visokotvegane prinaša posebne strožje zahteve, ki jih morajo ti sistemi upoštevati. Če gre za umetnointeligenčni sistem, ki vključuje prepovedane prakse v smislu 5. člena Akta o umetni inteligenci (npr. uporaba umetnointeligenčnega sistema za sklepanje o čustvih fizične osebe na delovnem mestu), je njegova uporaba prepovedana. Neustrezna uporaba umetnointeligenčnih

¹⁰¹ Primerjaj Paschou, 2024.

¹⁰² Glej <https://www.ibm.com/think/topics/shedding-light-on-ai-bias-with-real-world-examples> (obiskano: 20. 1. 2025).

¹⁰³ Chouldechova, 2016; Min, 2023, stran 3814.

¹⁰⁴ Prav tam.

sistemov lahko negativno vpliva na osebni in poklicni razvoj delavca ter povzroči neenakost pri dostopu do zaposlitvenih priložnosti.¹⁰⁵

Neresnične informacije, ki jih proizvajajo umetnointeligenčni sistemi, lahko okrnijo svobodo izražanja, in sicer njen del, ki vključuje sprejemanje informacij.¹⁰⁶ Razlog za proizvajanje in navajanje neresničnih informacij je predvsem odraz nepravilnih vhodnih podatkov oziroma podatkovnega učnega nabora ter haluciniranja umetnointeligenčnih sistemov, pri čemer lahko celo pride do izmišljevanja pravnih pravil in sodne prakse.

Uporaba umetnointeligenčnih sistemov za oblikovanje žaljivih in intimnih vsebin lahko pomeni protipraven poseg v pravico do osebnega dostojanstva, pravico do zasebnosti in osebnostne pravice v smislu 35. člena Ustave RS – predvsem kadar gre za javno razkazovanje takšnih proizvodov. Uporabnikovo prikazovanje, objavljane in razširjanje vsebin, ustvarjenih z umetnointeligenčnimi sistemi, sicer sodi v njegovo pravico do svobode izražanja, vendar je pri tem omejeno s pravico drugih do osebnega dostojanstva, pravico do zasebnosti, vključno s pravico do varstva časti in dobrega imena.

Slovensko nacionalno pravo in pravo EU skupaj tvorita pravno ogrodje, ki posamezniku zagotavlja zadovoljivo varstvo pravic iz ustvarjalnosti, varstva osebnih podatkov, enakosti pred zakonom, svobode dela, svobode izražanja, pravice do osebnega dostojanstva in varnosti ter pravic zasebnosti in osebnostnih pravic. Zgolj s spoštljivim odnosom do človekovih pravic je mogoč varen in ustavnopravno skladen razvoj umetnointeligenčnih sistemov. Namesto, da bi se stremelo k razvoju človeku prijaznih umetnointeligenčnih sistemov, ima trenutna regulacija dejansko odvračilne učinke. Trenutno imajo namreč le štiri od petdesetih največjih tehnoloških podjetij sedež v EU.¹⁰⁷ Tudi investicije v razvoj umetnointeligenčnih sistemov v EU so krepko v zaostanku v primerjavi z investicijami v ZDA.¹⁰⁸ Tehnološki sektor v EU naj bi »zaviral« pravni akti, ki posegajo na področje tehnološke regulacije, kot so Splošna uredba o varstvu podatkov, Akt o digitalnih

¹⁰⁵ Glej <https://www.edps.europa.eu/system/files/2023-10/1.-resolution-on-ai-and-employment-en.pdf> (obiskano: 2. 2. 2025), stran 2.

¹⁰⁶ Primerjaj Teršek v Avbelj (ur.), 2019, stran 374.

¹⁰⁷ Glej <https://companiesmarketcap.com/tech/largest-tech-companies-by-market-cap/> (obiskano: 4. 2. 2025).

¹⁰⁸ Benaich, 2024.

storitvah, Akt o digitalnih trgih¹⁰⁹ in Akt o umetni inteligenci. S svojo podrobno regulativno politiko naj bi EU v veliki meri posegala v tehnološke inovacije,¹¹⁰ kar ima odvrtačilni učinek na investicije in razvoj umetno-inteligenčnih sistemov v EU. Takšen pogled obravnava spoštovanje človekovih pravic kot žrtev delovanja umetno-inteligenčnih sistemov, čeravno bi moral biti njihov temeljni postulat. Razvijalci in uporabniki umetno-inteligenčnih sistemov so sicer že podvrženi podrobni evropski zakonodaji o človekovih pravicah, vendar lahko nekatere specifične značilnosti umetne inteligence, kot je netransparentnost, otežijo uporabo in izvrševanje teh pravnih aktov,¹¹¹ zaradi česar bo treba biti še posebej pozoren na skladnost umetno-inteligenčnih sistemov z varovanimi ustavnopravnimi pravicami.

Literatura

- Adamson, A. S., Smith, A. (2018) Machine Learning and Health Care Disparities in Dermatology. *JAMA Dermatol*, 154(11), strani 1247–1248, doi:10.1001/jamadermatol.2018.2348.
- Angwin, J., Larson, J., Mattu, S., Kirchner, L. (2016) Machine Bias, dostopno na: <https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing> (obiskano: 31. 1. 2025).
- Arbet, J., Brokamp, C., Meinzen-Derr, J., Trinkley, K. E., Spratt, H. M. (2020) Lessons and tips for designing a machine learning study using EHR data, *Journal of Clinical and Translational Science*, 21(5), strani 1–10, doi: 10.1017/cts.2020.513.
- Avbelj, M., Vatovec, K. v Avbelj, M. (2019) 14. člen, Komentar Ustave Republike Slovenije (Nova Gorica: Nova univerza, Evropska pravna fakulteta), strani 110–123.
- Benaich, N. (2024) State of AI report, dostopno na: https://docs.google.com/presentation/d/1GmZmoWOa2O92BPncRcTKa15xvQGhq7g4I4hjJSNIC0M/edit#slide=id.g2f75efebcb2_0_159 (obiskano: 4. 2. 2025).
- Beširević, I., Zahrastnik, K. v Romih, D. (2023) Uporabnost klepetalnega robota ChatGPT pri raziskovanju na področju prava, *Digitalna ekonomija in pravo 2023* (Društvo ekonomistov), strani 105–123.
- Bocharov, A., Vargas, S., Martinetti, A., Tatoris, R., Azevedo, C. (2024) Declare your AI independence: block AI bots, scrapers and crawlers with a single click, dostopno na: <https://blog.cloudflare.com/declaring-your-ai-independence-block-ai-bots-scrapers-and-crawlers-with-a-single-click/> (obiskano: 30. 1. 2025).
- Brkan, M. (2023) Pravni spori zaradi uporabe umetne inteligence, dostopno na: <https://www.iusinfo.si/medijsko-sredisce/kolumne/pravni-spори-zaradi-uporabe-umetne-inteligence-308425> (obiskano 3. 2. 2025).
- Chance, C. (2024) What does the EU AI act mean for employers?, dostopno na: <https://www.cliffordchance.com/content/dam/cliffordchance/briefings/2024/08/what-does-the-eu-ai-act-mean-for-employers.pdf> (obiskano: 3. 2. 2025).
- Chouldechova, A. (2016) Fair prediction with disparate impact: A study of bias in recidivism prediction instruments, dostopno na: <https://arxiv.org/pdf/1610.07524> (obiskano: 31. 1. 2025).

¹⁰⁹ Uredba (EU) 2022/1925 Evropskega parlamenta in Sveta z dne 14. septembra 2022 o tekmovalnih in pravičnih trgih v digitalnem sektorju in spremembi direktiv (EU) 2019/1937 in (EU) 2020/1828 (UL L 265, 12. 10. 2022, strani 1–66).

¹¹⁰ Thierier, 2022; Inserra, 2024.

¹¹¹ Evropska komisija, 2020, stran 10.

- Crawford, K., Whittaker, M., Elish, M. C., Barocas, S., Plasek, A., Ferryman, K. (2016) The AI Now Report: The Social and Economic Implications of Artificial Intelligence Technologies in the Near-Term, dostopno na: <https://www.slideshare.net/slideshow/the-ai-now-report-the-social-and-economic-implications-of-artificial-intelligence-technologies-in-the-nearterm/79866755> (obiskano: 31. 1. 2025).
- Čebulj, J. (2002) Opredelitev in razmerje do drugih ustavnih določb, 38. člen Komentarja Ustave Republike Slovenije, dostopno na: <https://e-kurs.si/komentar/opredelitev-in-razmerje-do-drugih-ustavnih-dolocb-17/> (obiskano: 10. 2. 2025).
- Dastin, J. (2018) Insight - Amazon scraps secret AI recruiting tool that showed bias against women, dostopno na: <https://www.reuters.com/article/world/insight-amazon-scraps-secret-ai-recruiting-tool-that-showed-bias-against-women-idUSKCN1MK0AG/> (obiskano: 30. 1. 2025).
- Day, T. (2023) A Preliminary Investigation of Fake Peer-Reviewed Citations and References Generated by ChatGPT, *The Professional Geographer*, 75(6), strani 1024–1027, dostopno na: <https://doi.org/10.1080/00330124.2023.2190373>.
- Eskens, S., Helberger, N., Moeller, J. (2017) Challenged by news personalisation: five perspectives on the right to receive information. *Journal of Media Law*, 9(2), strani 259–284, dostopno na: <https://doi.org/10.1080/17577632.2017.1387353>.
- Evropska komisija (2020) White paper On Artificial Intelligence - A European approach to excellence and trust, dostopno na: https://commission.europa.eu/document/download/d2ec4039-c5be-423a-81ef-b9e44e79825b_en?filename=commission-white-paper-artificial-intelligence-feb2020_en.pdf (obiskano: 4. 2. 2025).
- Evropska komisija (2023) Intellectual Property in ChatGPT, dostopno na: https://intellectual-property-helpdesk.ec.europa.eu/news-events/news/intellectual-property-chatgpt-2023-02-20_en (obiskano: 23. 1. 2025).
- Farman, P. v: Avbelj, M. (2019) 35. člen, Komentar Ustave Republike Slovenije (Nova Gorica: Nova univerza, Evropska pravna fakulteta), strani 339–349.
- Grynbaum, M. M., Mac, R. (2023) The Times Sues OpenAI and Microsoft Over A.I. Use of Copyrighted Work, dostopno na: <https://www.nytimes.com/2023/12/27/business/media/new-york-times-open-ai-microsoft-lawsuit.html> (obiskano: 29. 1. 2025).
- Haas, J. (2020) Freedom of the Media and Artificial Intelligence, dostopno na: <https://www.osce.org/files/f/documents/4/5/472488.pdf> (obiskano: 3. 2. 2025).
- Harris, Y. (2024) Where and how does a chatbot get its information?, dostopno na: <https://powell-software.com/resources/blog/where-does-chatbot-get-its-information/> (obiskano: 23. 1. 2025).
- Helms, S., Krieser, J. (2023) Copyrights, Professional Perspective - Copyright Chaos: Legal Implications of Generative AI, dostopno na: <https://www.bloomberglaw.com/external/document/XDDQ1PNK000000/copyrights-professional-perspective-copyright-chaos-legal-implic> (obiskano: 30. 1. 2025).
- Insera, D. (2024) Artificial Intelligence Regulation Threatens Free Expression, dostopno na: <https://www.cato.org/briefing-paper/artificial-intelligence-regulation-threatens-free-expression#legislative-approaches> (4. 2. 2025).
- Korpič – Horvat, E. (2018) Pravica do dela, *Anali PAZU HD*, 4(1–2), strani 25–36.
- Larson J., Mattu, S., Kirchner, L., Angwin, J. (2016) How We Analyzed the COMPAS Recidivism Algorithm, dostopno na: <https://www.propublica.org/article/how-we-analyzed-the-compas-recidivism-algorithm> (obiskano: 31. 1. 2025).
- Lucchi, N. (2024) ChatGPT: A Case Study on Copyright Challenges for Generative Artificial Intelligence Systems, *European Journal of Risk Regulation*, 15, strani 602–624.
- Min, A. (2023) Artificial Intelligence and Bias: Challenges, Implications, and Remedies, *Journal of Social Research*, 11(2), strani 3808–3817.
- Paschou, V. (2024) How to use ChatGPT in your company in compliance with the GDPR, dostopno na: <https://www.activemind.legal/guides/chatgpt/> (obiskano: 29. 1. 2025).

- Räz, T. (2022) COMPAS: zu einer wegweisenden Debatte über algorithmische Risikobeurteilung, *Forens Psychiatr Psychol Kriminol*, 16, strani 300–306.
- Robins-Early, N. (2024) ChatGPT suspends Scarlett Johansson-like voice as actor speaks out against OpenAI, dostopno na: <https://www.theguardian.com/technology/article/2024/may/20/chatgpt-scarlett-johansson-voice> (obiskano: 3. 2. 2025).
- Sahathullah, A. L. (2023) How does AI get data?, <https://ahamed-saha.medium.com/how-does-ai-get-data-ea09bee6caa8> (obiskano: 23. 1. 2025).
- Stone, E. F., Gueutal, H. G., Gardner, D. G., McClure, S. (1983) A field experiment comparing information-privacy values, beliefs, and attitudes across several types of organizations, *Journal of Applied Psychology* 68(3), strani 459–468, DOI: 10.1037/0021-9010.68.3.459.
- Sun, W., Nasraoui, O., Shafto, P. (2020) Evolution and impact of bias in human and machine learning algorithm interaction, *PLoS ONE*, 15(8), strani 1–39, dostopno na: <https://doi.org/10.1371/journal.pone.0235502>.
- Teršek, A., v: Avbelj, M. (2019) 39. člen, Komentar Ustave Republike Slovenije (Nova Gorica: Nova univerza, Evropska pravna fakulteta), strani 370–389.
- Thierer, A. (2022) Why the Future of AI Will Not Be Invented in Europe, dostopno na: <https://techliberation.com/2022/08/01/why-the-future-of-ai-will-not-be-invented-in-europe/> (obiskano: 4. 2. 2025).
- Toplak, L., v: Šturm, L. (2010) 35. člen, Uvodna opredelitev, Komentar Ustave Republike Slovenije (Ljubljana: Fakulteta za podiplomske državne in evropske študije), strani 367–370.
- Viejo, M. (2023) In Spain, dozens of girls are reporting AI-generated nude photos of them being circulated at school: 'My heart skipped a beat', dostopno na: <https://english.elpais.com/international/2023-09-18/in-spain-dozens-of-girls-are-reporting-ai-generated-nude-photos-of-them-being-circulated-at-school-my-heart-skipped-a-beat.html> (obiskano: 3. 2. 2025).
- Vokinger, K. N., Feuerriegel, S., Kesselheim, A. S. (2021) Mitigating bias in machine learning for medicine, *Commun Med*, 25(1), strani 1–3, dostopno na: <https://doi.org/10.1038/s43856-021-00028-w>.
- Wachter, S., Mittelstadt, B., Russell, C. (2020) Why Fairness Cannot Be Automated: Bridging the Gap Between EU Non-Discrimination Law and AI. *Computer Law & Security Review*, 41, strani 1–31.
- Zhang, D., Finckenberg-Broman, P., Hoang, T., Pan, S., Zhenchang, X., Mark, S., Xiwei, X. (2024) Right to be forgotten in the Era of large language models: implications, challenges, and solutions, *AI Ethics* (Springer), strani 1–10, <https://doi.org/10.1007/s43681-024-00573-9>.
- Zimmermann, A., Karapetyan, M., Banse, J. (2024) The EU AI Act: What Employers Should Know, dostopno na: <https://www.orricks.com/en/Insights/2024/09/The-EU-AI-Act-What-Employers-Should-Know> (obiskano: 3. 2. 2025).

Extended abstract

The chapter examines and critically analyses the operation and use of artificial intelligence systems from the perspective of constitutional law violations. Artificial intelligence systems are permitted to reproduce copyrighted works to which they have lawful access based on text and data mining. However, authors have the option to prohibit text and data mining of such works, placing the initiative and responsibility on them to prevent artificial intelligence systems from accessing their copyrighted materials. In addition to copyright infringements during the development, training, and operation of artificial intelligence systems, copyright protection may also be at risk in the final output or specific products generated by artificial intelligence. This is particularly evident in generative AI models, which often fail to cite the sources used or even fabricate them. Information privacy, which ensures the protection of personal data, is subject to numerous risks in the operation and use of artificial intelligence systems, particularly in relation to compliance with the General Data Protection Regulation. Key concerns include whether an artificial intelligence system provider should be classified as a data

processor under the General Data Protection Regulation, whether the legal consequences of transferring personal data to third countries should be considered when using artificial intelligence systems operated by providers based in third countries, and whether artificial intelligence systems can effectively respect and implement the “right to erasure” or the “right to be forgotten.” The causes of bias in artificial intelligence systems can be identified in data bias, algorithmic bias, and cognitive bias. Artificial intelligence bias can be mitigated by designing and ensuring fair and accurate artificial intelligence operations. Striking the right balance between accuracy and fairness—without resulting in discrimination against individuals or groups—will be of critical importance.

The Artificial Intelligence Act is particularly relevant to the right to work, as it defines high-risk artificial intelligence systems as those used for recruitment or selection of individuals, targeted job advertisements, analysis and filtering of job applications, candidate evaluations, decisions affecting terms of work-related relationships, promotions, or termination of work-related contractual relationships, task allocation based on individual behaviour or personality traits, and monitoring and evaluating employee performance and behaviour. False information generated by artificial intelligence systems may impair freedom of expression, particularly the right to receive information. The production and dissemination of false information primarily result from inaccurate input data or biased training datasets, as well as artificial intelligence hallucinations, where artificial intelligence systems even fabricate legal rules and judicial decisions. The use of artificial intelligence systems to generate offensive or intimate content may constitute an unlawful infringement of the right to personal dignity, the right to privacy, and personality rights under Article 35 of the Constitution of the Republic of Slovenia—especially when such content is publicly displayed. This often leads to a collision between freedom of expression and the aforementioned rights.

Slovenian national law and EU law together form a legal framework that provides individuals with adequate protection of their rights concerning copyright, personal data, equality before the law, freedom of work, freedom of expression, the right to personal dignity and security, as well as privacy and personality rights. Only through a respectful approach to fundamental human rights can artificial intelligence systems be developed safely and in accordance with constitutional law. However, considering the trends in technological investment and development, it is evident that extensive regulation of artificial intelligence systems in the EU may, regrettably, have a deterrent effect.

