

# Konferenca **PRAVO V INFORMACIJSKI DRUŽBI**

Ljubljana, 28. marec 2024

---

## ZBORNİK POVZETKOV

Uredil: dr. Matija Damjan

---

**ij** inštitut za primerjalno pravo

**IK** INŠTITUT ZA KRIMINOLOGIJO  
*pri Pravni fakulteti v Ljubljani*



Pravna fakulteta  
Univerza v Ljubljani



**CENTER ZA IT,  
PRAVO IN ETIKO**

# Program konference

Konferenca

## PRAVO V INFORMACIJSKI DRUŽBI

v četrtek, 28. marca 2024,  
na Pravni fakulteti Univerze v Ljubljani, v modri dvorani

09.00–09.15	<b>SPREJEM IN PRIJAVA UDELEŽENCEV</b>
09.15–09.30	<b>Uvodni pozdrav</b>
09.30–09.45	<b>Digitalizacija čezmejnega uveljavljanja pravice do socialne varnosti</b> prof. dr. Grega Strban, Pravna fakulteta Univerze v Ljubljani
09.45–10.00	<b>Uveljavljanje odgovornosti držav za kršitve človekovih pravic pri uporabi umetne inteligence na mednarodni ravni</b> prof. dr. Vasilka Sancin, Pravna fakulteta Univerze v Ljubljani
10.00–10.15	<b>Digitalizacija javnih naročil</b> doc. dr. Katja Štemberger Brizani, Pravna fakulteta Univerze v Ljubljani
10.15–10.30	<b>Izključitev odgovornosti posrednikov po Aktu o digitalnih storitvah</b> Maša Drofenik in Špela Jamnik, Register.si
10.30–10.45	<b>Akt o digitalnih storitvah in federirana družbena omrežja</b> doc. dr. Matija Damjan, Inštitut za primerjalno pravo pri Pravni fakulteti v Ljubljani
10.45–11.00	<b>Razprava</b>
11.00–11.15	<b>Odmor</b>
11.15–11.30	<b>Pravica do popravila kot sredstvo za doseganje trajnosti</b> as. Tjaša Kalin, Inštitut za primerjalno pravo pri Pravni fakulteti v Ljubljani
11.30–11.45	<b>Umetna inteligenca v delovnem pravu</b> as. Katarina Kogej, Pravna fakulteta Univerze v Ljubljani
11.45–12.00	<b>Deliktna odgovornost in umetna inteligenca</b> as. Jernej Renko, Pravna fakulteta Univerze v Ljubljani
12.00–12.15	<b>Predlog Akta o UI in umetnointeligenci sistemi z diskriminatornim potencialom</b> as. Lucija Strojjan, Inštitut za primerjalno pravo pri Pravni fakulteti v Ljubljani
12.15–12.30	<b>Razprava</b>
12.30–13.00	<b>Odmor</b>
13.00–13.15	<b>Umetna inteligenca v vesolju: priložnosti in izzivi</b> Iva Ramuš Cvetkovič, Inštitut za kriminologijo pri Pravni fakulteti v Ljubljani
13.15–13.30	<b>Kaj prinaša Uredba o preglednosti in ciljanem političnem oglaševanju glede obdelave osebnih podatkov?</b> dr. Pika Šarf, Informacijski pooblaščenec RS in Inštitut za kriminologijo pri Pravni fakulteti v Ljubljani
13.30–13.45	<b>Pravna izhodišča infrastrukture za odprto znanost na presečišču Slovenije in Evropskega oblaka odprte znanosti</b> Marko Drobňjak, Arnes in Inštitut za kriminologijo pri Pravni fakulteti v Ljubljani
13.45–14.00	<b>Temni vzorci in odločanje: pravne in etične zagate v digitalnem okolju</b> Manja Skočir, Inštitut za kriminologijo pri Pravni fakulteti v Ljubljani
14.00–14.30	<b>Razprava</b>
14.30	<b>ZAKLJUČEK KONFERENCE</b>

Izvedbo konference je podprla Javna agencija za znanstvenoraziskovalno in inovacijsko dejavnost Republike Slovenije v okviru raziskovalnega programa P5-0337 »Pravni izzivi informacijske družbe«.

---

# Povzetki

## Digitalizacija čezmejnega uveljavljanja pravice do socialne varnosti

Prof. dr. Grega Strban

Pravica do socialne varnosti je umeščena med temeljne človekove pravice, ki jo je treba zagotoviti tudi, ko se osebe gibljejo preko meja svoje države. To je še posebej pomembno v Evropski uniji (EU), ki spodbuja gibanje znotraj Unije. Zagotoviti ga je treba, tudi s povezovanjem različnih nacionalnih sistemov socialne varnosti. Čeprav države članice samostojno urejajo vsebino teh sistemov, enostranski ukrepi ne morejo biti učinkoviti pri čezmejnih dejanskih stanjih. Zato je v pristojnosti EU sisteme socialne varnosti med seboj tehnično, pravno in upravno povezati. V teh sistemih se zbirajo posebej občutljivi osebni podatki, ki so lahko povezani recimo s starostjo, invalidnostjo, zdravstvenim stanjem ali brezposelnostjo. Države članice morajo v skladu z načelom iskrenega sodelovanja in medsebojnega zaupanja izmenjevati številne podatke o osebah, ki se gibljejo v EU, da te ne bi izgubljale pravic zaradi gibanja v Uniji. Sodelovanju med nosilci socialnega zavarovanja je namenjena posebna platforma o elektronski izmenjavi podatkov o socialni varnosti (EESSI – *Electronic Exchange of Social Security Information*). Slovenija je sodelovala pri prvi elektronski izmenjavi podatkov, in sicer z Avstrijo leta 2019. Namen je pospešiti postopek odločanja in izplačevanja dajatev, omogočiti učinkovito preverjanje podatkov, zagotoviti bolj fleksibilno in uporabnikom prijazno elektronsko okolje in spremljanje statističnih podatkov o čezmejnem gibanju oseb. Poleg tega se vzpostavlja Elektronska izkaznica socialnega zavarovanja (ESSPASS - *European Social Security Pass*) kot del akcijskega načrta za Evropski steber socialnih pravic. Digitalizira se postopek zahtevanja in prejemanja dokazil o upravičenosti in njihovo preverjanje v realnem času. V pilot sta vključena obrazec o zakonodaji, ki naj se uporabi, recimo pri napotitvah ali sočasnih zaposlitvah (obrazec A1) in evropska kartica zdravstvenega zavarovanja (EKZZ). Digitalizacija čezmejnega uveljavljanja pravice do socialne varnosti je povezana z drugimi ukrepi na področju digitalizacije v EU.

## Uveljavljanje odgovornosti držav za kršitve človekovih pravic pri uporabi umetne inteligence na mednarodni ravni

Prof. dr. Vasilka Sancin

Prispevek naslavlja aktualno vprašanje uveljavljanja odgovornosti za kršitve človekovih pravic pri uporabi umetne inteligence (UI). Pri tem se omeji na dva načina: 1) preučuje le odgovornost držav (in ne posameznikov, fizičnih in pravnih oseb) in 2) ugotavlja možnosti za uveljavljanje odgovornosti za kršitve mednarodnega prava človekovih pravic na mednarodni ravni pred mehanizmi OZN. Negativni učinki UI na človekove pravice (npr. glede zasebnosti, drugačne obravnave) lahko vodijo tudi v kršitve mednarodnopravno varovanih človekovih pravic, čeprav so te v mednarodnih pogodbah s področja človekovih pravic opredeljene tehnološko nevtralnno. Pri ugotavljanju odgovornosti držav se zastavljajo številna dejanska in pravna vprašanja, od obstoja možnosti izogibanja kršitvam pri avtonomnem odločanju, kar je povezano s stopnjo avtonomije uporabljenih tehnologij, težav pri določanju nadzora zaradi razpršenosti akterjev, do zahtevnosti vzpostavljanja vzročne zveze. Za vzpostavitev odgovornosti države po mednarodnem pravu je namreč treba dokazati kumulativen obstoj pripisljivosti ravnanja državi in kršitev njene mednarodnopravne obveznosti, ter hkraten neobstoj katere od okoliščin, ki bi lahko izključila protipravnost ravnanja. V okviru mehanizmov OZN prispevek osvetli možnosti uveljavljanja odgovornosti zaradi kršitev človekovih pravic pri uporabi UI predvsem pred Meddržavnim sodiščem v Haagu, kadar bi šlo za postopke reševanja sporov med državami, na eni strani, in pred Odborom za človekove pravice, kot pogodbenim telesom, ustanovljenim z Mednarodnim paktom o državljanskih in političnih pravicah, na katerega se lahko, med drugim, obračajo z zatrjevano kršitvijo prizadeti posamezniki, na drugi strani.

---

## Digitalizacija javnih naročil

Doc. dr. Katja Štemberger Brizani

Tendence k digitalizaciji postopkov javnega naročanja so se pojavile že pred dobrimi dvajsetimi leti, s sprejemom Direktive 2004/18/ES. Vendar uporaba elektronskih komunikacijskih sredstev za države članice takratne Evropske skupnosti po tej direktivi ni bila obvezna, temveč je temeljila na prostovoljnem pristopu. Deset let kasneje pa je na podlagi Direktive 2014/24/EU tak način oddaje javnega naročila obvezen (razen predpisanih izjem). Države članice so bile na podlagi 22. člena te direktive zavezane, da digitalizirano poslovanje zagotovijo (vsaj) glede pošiljanja obvestil v zvezi z javnim naročilom, dostopnostjo razpisne dokumentacije in izmenjave informacij med naročniki in kandidati oziroma ponudniki, kar vključuje zlasti elektronsko oddajo ponudb. Te zahteve so bile v slovensko pravo implementirane<sup>1</sup> z ZJN-3, pri čemer se je prvi odstavek 37. člena ZJN-3 (pravila o sporočanju) pričel uporabljati 1. 4. 2018, določbe o zvezi z dinamičnim nabavnim sistemom, elektronsko dražbo, elektronskim katalogom in vrsto, obliko in načinom objave javnih obvestil pa so se začele uporabljati z dnem uveljavitve tega zakona, to je 1. 4. 2016, osrednji nabavni organ pa je začel prvič uporabljati elektronska komunikacijska sredstva za sporočanje in izmenjavo informacij 1. 1. 2017.<sup>2</sup> Elektronska izvedba javnega naročanja je namreč terjala ne samo pravne, pač pa tudi systemske prilagoditve. V ta namen je bil vzpostavljen portal e-JN, v okviru katerega delujejo informacijski sistemi e-Nabava (za naročnike), e-Oddaja (za ponudnike), e-Dosje (elektronsko preverjanje razlogov za izključitev ponudnika – od leta 2023 je digitaliziran v celoti), e-Katalog (elektronski katalog) in e-Dražbe (elektronske dražbe). 1. 1. 2021<sup>3</sup> je začel delovati tudi spletni informacijski portal e-Revizija, s čimer je bil digitalni pristop iz postopka oddaje javnih naročil razširjen tudi na pravno varstvo v teh postopkih. Kljub številnim prednostim, elektronsko javno naročanje prinaša tudi nekatera tveganja, zlasti z vidika varstva osebnih in drugih podatkov (npr. poslovnih skrivnosti), enake dostopnosti in pravice do izjave oz. do informacije (v zvezi z vročanjem odločitev naročnika).

## Izključitev odgovornosti posrednikov po aktu o digitalnih storitvah

Maša Drogenik, Špela Jamnik

"Nova pravila Uredbe (EU) 2022/2065 o enotnem trgu digitalnih storitev in spremembi Direktive 2000/31/ES (Uredba Akta o digitalnih storitvah, angleško Digital Services Act - DSA), ki je bila sprejeta 4. oktobra 2022, se v celoti uporabljajo od 17. februarja 2024. Pravila so sorazmerna z velikostjo spletnih akterjev, njihovo vlogo in vplivom v spletnem ekosistemu in na družbo. Ponudniki posredniških storitev so izvzeti iz večine obveznosti, ki jih Uredba nalaga.

Predlog slovenskega Zakona o izvajanju uredbe EU o enotnem trgu digitalnih storitev v prvem odstavku 17. člena za odstranjevanje nezakonitih vsebin s spleta določa sodno pristojnost. Zakonodajalec predlaga, da odločbo o odstranitvi nezakonite vsebine ponudniku posredniških storitev izda pristojno Okrožno sodišče v Ljubljani po zakonu, ki ureja nepravdni postopek. Skladno s 25. členom predlaganega zakona bodo določbe 8. do 11. člena Zakona o elektronskem poslovanju na trgu (Url. RS, št. 96/09 s spremembami) z uveljavitvijo tega zakona prenehale veljati."

---

<sup>1</sup> Že pred sprejemom ZJN-3 sta bila v Sloveniji dobro razvita in uveljavljena objava obvestil v elektronski obliki in dostopnost dokumentacije v zvezi z oddajo javnega naročila v elektronski obliki, bili pa so prisotni tudi prvi poskusi e-dražb, e-katalogov, uveljavljen pa je tudi sistem e-računov. Tako P. Ferk, Elektronsko javno naročanje - podarjena priložnost za korenite spremembe, Pravna praksa, št. 1, 2016, str. 21.

<sup>2</sup> Glej 118. člen ZJN-3.

<sup>3</sup> Glej 16. člen ZPVPJN-C.

---

## Akt o digitalnih storitvah in federirana družbena omrežja

Doc. dr. Matija Damjan

Akt o digitalnih storitvah (DSA) skuša zaščititi internet pred širjenjem nezakonitih in škodljivih vsebin ter varovati temeljne pravice spletnih uporabnikov. Ureditev spletnih posrednikov je asimetrična: za zelo velike spletne platforme veljajo strožja pravila za zaščito pred sistemskimi tveganji, povezanimi z njihovim (negativnim) družbenim vplivom. Federirana družbena omrežja, kot sta Mastodon in Bluesky, so se pojavila kot alternativa uveljavljenim centraliziranim družbenim omrežjem. Delujejo kot sistemi medsebojno povezanih strežnikov, ki komunicirajo prek decentraliziranega omrežnega protokola. To njihovim uporabnikom omogoča, da med seboj komunicirajo in si izmenjujejo podatke, kot bi bili na isti platformi. Ker federirano omrežje nima enega lastnika, skrbnik vsakega lokalnega strežnika določi pravila in jih uveljavlja v strežniku in ne v celotnem omrežju.

Prispevek preučuje, kako se pravila DSA uporabljajo za federirana družbena omrežja. Če se vsak strežnik obravnava kot ločena platforma, mora izpolnjevati le minimalne obveznosti za storitve gostovanja in ne pravil, ki so namenjena družbenim omrežjem. Kljub temu lahko celotno združeno omrežje preseže prag 45 milijonov mesečnih uporabnikov. Je to vrzel v okviru DSA in ali so potrebna posebna pravila za obravnavo posebnih tveganj, ki izhajajo iz povezanih omrežij? Bo regulativno breme DSA uničilo federirana omrežja, ki temeljijo na prostovoljnem delu, ali pa Fediverse omogoča obid zahtev DSA?

## Pravica do popravila kot sredstvo za doseganje trajnosti

As. Tjaša Kalin

Evropska unija se aktivno zavzema za bolj zeleno gospodarstvo. V okviru Evropskega zelenega dogovora je bila sprejeta usklajena strategija za podnebno nevtralnost, z viri gospodarno in konkurenčno gospodarstvo, ki vključuje razširitev krožnega gospodarstva. Evropska komisija si je znotraj Novega akcijskega načrta za krožno gospodarstvo prizadevala za krepitev vloge potrošnikov pri politiki za trajnostne izdelke, predvsem z določitvijo nove pravice do popravila. Popravilo je namreč bolj učinkovito in trajnostno kot recikliranje, saj se prihrani energija, material, voda, hkrati pa so nižji tudi transportni stroški. Pravica do popravila, kot namiguje že njeno ime, pomeni pravico posameznika, da kupljeno blago popravi bodisi sam bodisi pri neodvisnem serviserju oz. serviserju, ki ga izbere sam. Osnovna predpostavka je dejstvo, da je posameznik blago oz. napravo kupil, s tem postal lastnik in bi posledično moral imeti pravico uporabe, vzdrževanja in popravila blaga na način, ki ga smatra za najprimernejšega. Trenutno je v postopku sprejemanja predlog direktive o skupnih pravilih za spodbujanje popravila blaga, s katerim se uresničuje prednostna naloga Evropske komisije glede zelenega prehoda in cilja trajnostne potrošnje. Cilj direktive je spodbuditi popravilo in ponovno uporabo, kadar je blago z napako mogoče popraviti ali prenoviti. Predlog direktive potrošnikom zagotavlja orodja, ki povečujejo preglednost in izboljšujejo pogoje popravila ter proizvajalcem nalaga obveznost, da določeno blago popravijo tudi zunaj obveznega jamstva.

## Umetna inteligenca v delovnem pravu

as. Katarina Kogej

Umetna inteligenca (UI) ima pomemben vpliv na trg dela in delovno pravo. Njena uporaba je pospešila avtomatizacijo dela, kar je vodilo k ukinitvi določenih delovnih mest ter postopni opustitvi nekaterih poklicev. Največje posledice so (in bodo) vidne na delovnih mestih, na katerih so bili zaposleni nižje kvalificirani delavci. Hkrati proces avtomatizacije dela pripomore k zagotavljanju večje varnosti pri delu in povečuje produktivnost. Ob tem se je bistveno povečala potreba po delavcih z novimi digitalnimi znanji in kompetencami za uporabo umetne inteligence. Pomembna za uspešno prilagoditev novim spremembam

---

sta tako predvsem preusposabljanje in izpopolnjevanje, ki ju najdemo tudi med cilji *Evropskega leta spretnosti 2023*.

Razvoj UI je bistveno prispeval k razvoju novih oblik dela, predvsem razmahu platformnega dela. Preko platform se delavcem posredujejo navodila, omogočajo pa tudi izvajanje precej poglobljenega nadzora. To sproži vrsto vprašanj, vse od posega v zasebnost in dostojanstvo posameznikov, do vprašanj povezanih z omejenim delovnopравnim in socialnopравnim varstvom tovrstnih delavcev, ki delo pogosto opravljajo izven okvirjev delovnega razmerja. Nujnost naslavljanja vprašanj v zvezi z UI pri obravnavi platformnega dela je prepoznal tudi evropski zakonodajalec, ki je v predlog *Direktive o izboljšanju delovnih pogojev pri platformnem delu* vključil pravila o uporabi UI na delovnem mestu.

Nadalje UI omogoča digitalizacijo in avtomatizacijo vloge delodajalca, in to že pri samem zaposlovanju. Kljub temu, da je cilj pospešiti odločanje in zmanjšati subjektivnost pri izbiri, so lahko učinki pogosto ravno nasprotni, za netransparentnostjo pa se skriva diskriminacija. Delodajalec lahko UI uporabi pri razporejanju dela, dajanju navodil ter izvajanju nadzora nad delavci (t.i. algoritemsko upravljanje), pri čemer se pod vprašaj postavlja kriterij subordinacije kot eden izmed ključnih elementov za ugotovitev obstoja delovnega razmerja. UI se lahko uporabi tudi pri ocenjevanju dela delavcev, napredovanju ali odpuščanju, pri čemer delavcem v delovnem razmerju varstvo še zmeraj nudijo pravila *ZDR-1*, ki postopek prenehanja delovnega razmerja natančno urejajo.

Nenazadnje pa je UI vse pogosteje uporabljena kot orodje pri izvajanju javne politike zaposlovanja. Zavodi za zaposlovanje jo uporabljajo tako v postopku profiliranja (razvrščanja iskalcev zaposlitve glede na tveganje za dolgotrajno brezposelnost), targetiranja (ciljno usmerjanje iskalca v ustrezen program za usposabljanje ali zaposlovanje) kot za usklajevanje povpraševanja iskalcev zaposlitve s ponudbo na trgu dela.

Naslavljanje nekaterih izzivov UI je možno že v okviru obstoječe delovnopравne zakonodaje ter pravil na področju varstva osebnih podatkov in prepovedi diskriminacije, določeno varstvo pa bo po sprejetju prinesla tudi *Uredba Evropskega parlamenta in Sveta o določitvi harmoniziranih pravil o umetni inteligenci*. Pri oblikovanju novih pravil in naslavljanju izzivov je ključno rešitve oblikovati s pomočjo socialnega dialoga.

## **Deliktna odgovornost in umetna inteligenca**

As. Jernej Renko

Uvedba umetne inteligence na večini področij naših življenj obeta številne olajšave. Vendar pa kot vsaka disruptivna tehnologija prinaša tudi nova nepoznana tveganja, ki izhajajo iz avtonomije in globoke mrežne prepletenosti avtonomnih sistemov. Nadomestitev človeškega upravljavca tehnologije s samoučnim se algoritmom bo med drugim sprožila še neodgovorjena vprašanja deliktne prava, in sicer kdo je tisti, ki bi moral biti odgovoren za škodo, ki jo povzroči avtonomni sistem.

Prvi možen naslovník deliktne odgovornosti je proizvajalec avtonomnega sistema. Zastareli koncepti, na katerih temelji evropsko harmonizirano pravo proizvajalčeve odgovornosti, niso zmožni ponuditi ustrezne rešitve. Proizvajalec je edini subjekt, ki ima določeno mero nadzora nad avtonomnim sistemom, zato je ključnega pomena, da je postavljen v središče fokusa nove ureditve.

Uporabniku avtonomnega sistema bo odvzet nadzor na avtonomnim sistemom, zato ga z izjemo primerov, ko bi mu lahko očitali krivdno povzročitev škode, ni primerno pavšalno obremenjevati z odgovornostjo za škodo, ki jo povzroči avtonomni sistem.

Uvedba t.i. elektronske pravne subjektivitete in s tem deliktne odgovornosti avtonomnega sistema samega, kljub zanimivosti koncepta, prinaša preveč tveganj, ki jih njene prednosti zaenkrat še ne odtehtajo.

---

## **Predlog Akta o umetni inteligenci in umetnointeligenčni sistemi z diskriminatornim potencialom**

As. Lucija Strojan

Za videzom nevtralnosti, racionalnosti ter nepristranskosti, ki ga tipično pripisujemo umetni inteligenci in algoritemskemu odločanju, se lahko skrivajo učinki, ki škodljivo učinkujejo na temeljne pravice, vključno s prepovedjo diskriminacije. Gre za »novo« pojavno obliko družbenega tveganja, na katerega se opozarja praktično od samega začetka akademskega razpravljanja in širšega pisanja o negativnih posledicah uporabe umetne inteligence. Ob diskriminatornih aplikacijah umetne inteligence, se opozarja na širšo problematiko predsodkov in diferenciacije podatkov, ki je vpeta v samo delovanje umetnointeligenčnih sistemov. Pravni okvir EU je zasnovan na primerih t. i. človeške diskriminacije, ki se na več načinov razlikuje od oblik diskriminacije, ki jih ustvarjajo algoritemske aplikacije. Na tem mestu dobrodošlo in nujno dopolnitev pravnega okvira prinaša Predlog Akta o umetni inteligenci, ki obstoječe pravo EU o nediskriminaciji dopolnjuje s posebnimi zahtevami. Akt prinaša pristop, ki temelji na tveganju in (nekatero) sisteme, ki pomembneje vplivajo na temeljne pravice, izrecno uvršča na seznam umetnointeligenčnih sistemov velikega tveganja. Gre za umetnointeligenčne sisteme z različnih področij (npr. kritična infrastruktura, izobraževanje in poklicno usposabljanje, zaposlovanje, upravljanje delavcev in dostop do samozaposlitve, uživanje bistvenih zasebnih in javnih storitev in ugodnosti ter dostop do njih), ki lahko pripeljejo do diskriminacije oseb oz. skupin, ohranjajo diskriminatorne vzorce iz preteklosti ali celo ustvarijo nove oblike diskriminatornih vplivov. Zanje so predvidene zahteve v zvezi s podatki in njihovim upravljanjem, vodenjem dokumentacije in evidenc, preglednostjo in zagotavljanjem informacij, testiranjem, človeškim nadzorom, robustnostjo, točnostjo in varnostjo. Vprašanje, ali lahko ti mehanizmi ustrezno obvladujejo diskriminatoren potencial umetnointeligenčnih sistemov velikega tveganja, zaenkrat ostaja še odprto.

## **Umetna inteligenca v vesolju: priložnosti in izzivi**

Iva Ramuš Cvetkovič

Vesoljska tehnologija predstavlja izjemno pomemben del našega vsakdana, saj omogoča opravljanje številnih storitev in delovanje temeljne infrastrukture. Vendar pa so z njo povezana številna tveganja za življenje in zdravje ljudi. Tovrstna tveganja, kot so na primer možnost kolizije oz. trka dveh (ali več) vesoljskih objektov, kibernetiski (teroristični) napad na vesoljske objekte in eksponentno naraščanje količine vesoljskih smeti, bodo v prihodnosti postajala vse bolj verjetna. Kljub temu, da obstaja splošen mednarodni pravni okvir za vesoljske aktivnosti, in da vse več držav sprejema tudi nacionalno zakonodajo na tem področju, marsikatero vprašanje v zvezi z omenjenimi tveganji ostaja nenaslovljeno – med drugim vprašanje dokazovanja predpostavk za vzpostavitev odškodninske odgovornosti, konkretizacija nadzora zasebnih akterjev v vesolju in natančen obseg aplikacije pravil splošnega mednarodnega prava v vesolje. V zadnjem času se kot odgovor na tveganja vedno bolj izpostavlja umetno inteligenco, ki naj bi bila sposobna povečati varnost, učinkovitost in predvidljivost vesoljske tehnologije, a ta s seboj prinaša nove dileme in nevarnosti. V prispevku se zato osredotočam na primerjavo med priložnostmi in izzivi, ki jih bo ustvarila uporaba umetne inteligence v vesolju, na podlagi katere zagovarjam tezo, da se je tovrstne uporabe treba lotiti premišljeno in temu ustrezno prilagoditi tudi obstoječi (mednarodni in nacionalni) pravni okvir, saj lahko v nasprotnem primeru umetna inteligenca v vesolju prinese več tveganj, kolikor jih bo odpravila.

---

## Kaj prinaša nova Uredba o političnem oglaševanju glede obdelave osebnih podatkov v političnih kampanjah?

Dr. Pika Šarf

Obdelavo osebnih podatkov pri političnem oglaševanju trenutno na ravni EU ureja več pravnih aktov, v prvi vrsti je to Splošna uredba o varstvu podatkov, ki se uporablja kot *lex generalis* glede vseh obdelav osebnih podatkov, ne glede na uporabljeno tehnologijo in namen takšne obdelave, poleg Splošne uredbe pa so relevantne tudi nekatere določbe Akta o digitalnih storitvah ter potencialno tudi Uredbe (EU, Euratom) št. 1141/2014 Evropskega parlamenta in Sveta z dne 22. oktobra 2014 o statutu in financiranju evropskih političnih strank in evropskih političnih fundacij. Že sedaj razgibanemu zakonodajnemu okviru se je pred kratkim pridružila tudi Uredba (EU) 2024/900 Evropskega parlamenta in Sveta z dne 13. marca 2024 o preglednosti in ciljanju v političnem oglaševanju, ki je bila sprejeta 13. marca 2024, uporabljala pa se bo v večjem delu od 10. oktobra 2025. Uredba definira pojem političnega oglaševanja, kot tudi, kaj zajemajo tehnike ciljanja in tehnike prikazovanja oglasov, medtem ko se glede nekaterih drugih ključnih pojmov opira na zakonodajo s področja varstva osebnih podatkov in Akt o digitalnih storitvah. Glede spletnega političnega oglaševanja z uporabo tehnik ciljanja in tehnik prikazovanja oglasov, ki vključujejo obdelavo osebnih podatkov, določa strogo opredeljene pogoje, ki morajo biti kumulativno izpolnjeni za to, da je takšna obdelava podatkov dopustna, medtem ko je uporaba posebnih kategorij osebnih podatkov (tj. občutljivih podatkov) v ta namen prepovedana.

## Temni vzorci in odločanje: pravne in etične zagate v digitalnem okolju

Manja Skočir

Raziskave s področja vedenjske ekonomije, psihologije in nevroznanosti so v zadnjih petdesetih letih razkrile, da človeško odločanje pogosto ne sledi aksiomom racionalnosti in optimizacije koristi ter pokazale, kako dovzetni za manipulacijo so posamezniki. Etična spornost že tako problematičnih praks – zlasti uporabe dregljajev za vplivanje oz. usmerjanje vedenja – se je še dodatno poglobila s tem, ko so se te iz analognih preselile v digitalna okolja. Informacijska tehnologija je z uporabo vmesnikov ter z možnostjo natančnega prilagajanja vsebin uporabnikom, odprla nove možnosti za manipulacijo vedenja. V referenčni literaturi se je za poimenovanje nabora spletnih praks, ki z izkoriščanjem vedenjskih pristranskosti in psiholoških ranljivosti skozi subtilno oblikovane uporabniške vmesnike, uporabnike zavajajo k sprejemanju odločitev v nasprotju z njihovimi interesi, uveljavil izraz "temni vzorci" (ang. *dark patterns*). Članek analizira najpogostejše oblike temnih vzorcev, pojasni, da so spori zato, ker kratijo avtonomijo posameznikov in manipulirajo z njimi ter analizira zakonodajne odzive Evropske unije na področju prava varstva zasebnosti in prava varstva potrošnikov za regulacijo temnih vzorcev. Prispevek oriše tudi možnosti za ureditev teh praks v skladu s členom 5(1) akta EU o umetni inteligenci in poudari pomembnost varovanja avtonomije posameznikov ob vse hitrejšem tehnološkem napredku.