
Univerzitetna založba
Univerze v Mariboru
TEMELJNE PRAVICE IN IZZIVI DIGITALIZACIJE
od pravne ureditve do prakse
uredila
Petra Weingerl

Univerza v Mariboru

Pravna fakulteta

Temeljne pravice in izzivi digitalizacije

Od pravne ureditve do prakse

Urednica
Petra Weingerl

December 2023

Naslov *Title*
Temeljne pravice in izzivi digitalizacije
Fundamental Rights and Challenges of Digitization

Podnaslov *Subtitle*
Od pravne ureditve do prakse
From Legal Regulation to Practice

Urednica *Editor*
Petra Weingerl
(Univerza v Mariboru, Pravna fakulteta)

Recenzija *Review*
Janja Hojnik
(Univerza v Mariboru, Pravna fakulteta)

Verica Trstenjak
(Univerza v Ljubljani, Fakulteta za upravo)

Tehnični urednik *Technical editor*
Jan Perša
(Univerza v Mariboru, Univerzitetna založba)

Oblikovanje ovitka *Cover designer*
Jan Perša
(Univerza v Mariboru, Univerzitetna založba)

Grafične priloge *Graphic material*
Viri so lastni, razen če ni navedeno drugače.
Šuta in Weingerl, 2023

Grafika na ovitku *Cover graphics*
Multicolored hallway, foto: Efe Kurnaz, unsplash.com, CC0, 2023

Založnik *Published by*
Univerza v Mariboru
Univerzitetna založba
Slomškov trg 15, 2000 Maribor, Slovenija
https://press.um.si
zalozba@um.si

Izdajatelj *Issued by*
Univerza v Mariboru
Pravna fakulteta
Mladinska ulica 9, 2000 Maribor, Slovenija
https://pf.um.si
pf@um.si

Izdaja *Edition*
Prva izdaja

Vrsta publikacije *Publication type*
E-knjiga

Dostopno na *Available at*
http://press.um.si/index.php/ump/catalog/book/805

Izdano *Published at*
Maribor, december 2023

Javni štipendijski, razvojni, invalidski in preživninski sklad Republike Slovenije

REPUBLIKA SLOVENIJA
MINISTRSTVO ZA IZOBRAŽEVANJE, ZNANOST IN ŠPORT

EVROPSKA UNIJA
EVROPSKI SOCIALNI SKLAD
NALOŽBA V VAŠO PRIHODNOST

Univerza v Mariboru
Pravna fakulteta

pip
pravo informacije pomoč

Projekt je potekal v okviru programa »Projektno delo z negospodarskim in neprofitnim sektorjem v lokalnem in regionalnem okolju - Študentski inovativni projekti za družbeno korist 2016–2020«, ki ga sofinancirata Republika Slovenija in Evropska unija iz Evropskega socialnega sklada.

```
CIP - Kataložni zapis o publikaciji
Univerzitetna knjižnica Maribor

342.7:004(082)(0.034.2)

    TEMELJNE pravice in izzivi digitalizacije [Elektronski vir] : od pravne
ureditve do prakse / uredila Petra Weingerl. - 1. izd. - E-zbornik. - Maribor :
Univerzitetna založba, 2023

Način dostopa (URL): https://press.um.si/index.php/ump/catalog/book/805
ISBN 978-961-286-774-4
doi: 10.18690/um.pf.4.2023
COBISS.SI-ID 161824515
```

ISBN 978-961-286-774-4 (pdf)

DOI https://doi.org/10.18690/um.pf.4.2023

Cena
Price Brezplačni izvod

Odgovorna oseba založnika
For publisher prof. dr. Zdravko Kačič,
rektor Univerze v Mariboru

Citiranje
Attribution Weingerl, P. (ur.). (2023). *Temeljne pravice in izzivi digitalizacije: od pravne ureditve do prakse*. Univerza v Mariboru, Univerzitetna založba. doi: 10.18690/um.pf.4.2023

Univerzitetna založba
Univerze v Mariboru

Kazalo

	Uvodno Petra Weingerl	**1**
1	**Etika avtomatizacije, digitalizacije in umetne inteligence: obstoječe dileme, tveganja in rešitve** *The Ethics of Automatization, Digitalization and Artificial Intelligence: Existing Dilemmas, Risks and Solutions* Niko Šetar	**5**
2	**Demokracija in svoboda govora v luči digitalizacije** *Democracy and the Freedom of Speech in the Light of Digitalization* Amadej Šuperger	**37**
3	**Pravica do zasebnosti v povezavi z umetno inteligenco** *The Right to Privacy in Connection With Artificial Intelligence* Elena Osrajnik	**59**
4	**Vpliv digitalizacije na človekovo dostojanstvo in spoštovanje zasebnega in družinskega življenja** *The Influence of Digitalization on a Person's Dignity and Respect of Private and Family Life* Teja Strukelj	**99**
5	**Algoritemska diskriminacija** *The Algorithm of Discrimination* Oskar Peče	**125**
6	**Enakost žensk in moških, pravice otrok in pravice starejših v povezavi z umetno inteligenco** *Equality Between Men and Women, the Rights of Children and the Rights of Elderly in Connection With Artificial Intelligence* Tija Poje Lučev	**165**
7	**Temeljne pravice in izzivi digitalizacije: izobraževanje, delo in sodstvo** *Basic Rights and Challenges of Digitalization: Education, Work and the Judicial System* Živa Šuta	**211**

Univerzitetna založba
Univerze v Mariboru

Uvodno

PETRA WEINGERL
Urednica

Digitalizacija ima vse večji vpliv na naša življenja, do posebnega razmaha digitalizacije in uporabe umetne inteligence pa je prišlo ravno v času izvajanja projekta zaradi pandemije COVID-19. Projekt se je namreč izvajal v poletnem semestru 2020. V luči hitrega razvoja digitalnih tehnologij, kot so robotika, internet stvari, umetna inteligenca, visokozmogljivi računalniki in močna komunikacijska omrežja, se na ravni EU že odvija široka etična in pravna razprava o primernem regulativnem okviru za digitalizacijo in umetno inteligenco, ki mora spoštovati temeljne pravice.

Namen projekta je bil s pravnega, filozofskega, etičnega in informacijskega vidika preučiti izbrane vidike digitalizacije in njen vpliv na varstvo temeljnih pravic v EU in v Sloveniji v okviru študentskega inovativnega projekta (ŠIPK). Na projektu Temeljne pravice in izzivi digitalizacije: od pravne ureditve do prakse (TEMDIG) so sodelovali študenti iz štirih različnih fakultet in študijskih programov - študenti Pravne fakultete, Ekonomsko-poslovne fakultete, Fakultete za strojništvo in Fakultete za naravoslovje in matematiko. Partner projekta je bil Zavod PIP - Pravni in informacijski center Maribor, ki je s pomočjo delovne mentorice Sanje Antonijević pomembno prispeval k praktični analizi obravnavanih problemov.

Uvodna analiza, ki jo je pripravil študent filozofije na drugi stopnji, obravnava etična, moralna in filozofska vprašanja, ki so povezana z avtomatizacijo, digitalizacijo in umetno inteligenco. Sledita poglavji dveh študentov informatike in tehnologije komuniciranja in medijskih komunikacij. Drugo poglavje se osredotoča na vprašanja vpliva digitalizacije na demokracijo, povezana predvsem s svobodo govora. Govori o kontroverznih temah, kot je manipulacija z volivci, svobodi govora, oziroma o zamegljeni meji med svobodo govora in sovražnem govoru, uporabi umetne inteligence za cenzuro »spornih« vsebin na socialnih medijih in na sploh o lažnih novicah in vplivih takšnih novic na družbo, prav tako pa o generiranih lažnih novicah oziroma o generiranih vsebinah. Tretje poglavje pa obravnava vprašanja, ki se tičejo varstva zasebnosti na internetu in pri uporabi sistemov umetne inteligence, kot je internet stvari, avtonomna vozila, deepfake posnetki in prilagojeni oglasi.

Sledi sklop poglavij, ki obravnavajo posebne segmente družbenega življenja v povezavi s temeljnimi pravicami in digitalizacijo. Ta vprašanja, ki so jih obdelali študenti prava, so še posebej aktualna v luči nenadnega razmaha digitalizacije in uporabe umetne inteligence zaradi epidemije COVID-19. V ta namen so preučili izbrane določbe Listine EU o temeljnih pravicah, Evropske konvencije o človekovih pravicah in temeljnih svoboščinah, Ustave RS, sekundarne zakonodaje EU in nacionalne zakonodaje ter analizirali sodno prakso Sodišča EU, Evropskega sodišča za človekove pravice in nacionalnih sodišč. Preučili so tudi predlagane zakonodajne iniciative na področju digitalizacije in umetne inteligence, vključno z iniciativami Evropske komisije. V četrtem poglavju je najprej predstavljen vpliv digitalizacije na človekovo dostojanstvo in spoštovanje zasebnega in družinskega življenja, pri čemer je poudarjen psihološki in sociološki vidik. Temu sledi peto poglavje o algoritemski diskriminaciji, ki predstavlja splošni okvir za poglavja, ki sledijo. Naslednje (šesto) poglavje preučuje enakost žensk in moških, pravice otrok in pravice starejših v povezavi z umetno inteligenco. Ta sklop je zaključen z obširnim sedmim poglavjem o vplivu digitalizacije na temeljne pravice v okviru izobraževanja, dela in sodstva. V 21. stoletju se z UI srečujemo na vsakem koraku, od šolanja do opravljanja dela in v prostem času. Za študente prava je tema zelo aktualna, saj se predvideva, da bo pravni postopek v prihodnosti vsaj v določeni meri potekal s pomočjo UI. Posledično bo temu potrebno prilagoditi tudi sistem izobraževanja in opravljanje pravniškega poklica. Poleg tega je vse več izdelkov in storitev na voljo v digitalni obliki. A države članice EU opozarjajo, da trenutno ni skupnega evropskega okvira, ki bi poenotil ali približal njihove zakonodaje na tem področju družbenega življenja.

Poglobljena analiza predstavlja temelj za bodoče teoretične in praktične raziskave, hkrati pa si želimo, da bi ugotovitve študentov upoštevali tudi zakonodajalec in sodišča. Pričakujemo, da bodo rezultati služili kot pomoč nevladnim organizacijam, državnim organom in organom samoupravne lokalne skupnosti pri zasnovi in implementaciji novih zakonodajnih in praktičnih rešitev, ki bodo utemeljeni z visokim varstvom temeljnih pravic.

DOI
https://doi.org/10.18690/um.pf.4.2023.1

ISBN
978-961-286-774-4

1 ETIKA AVTOMATIZACIJE, DIGITALIZACIJE IN UMETNE INTELIGENCE: OBSTOJEČE DILEME, TVEGANJA IN REŠITVE

NIKO ŠETAR
Univerza v Mariboru, Filozofska fakulteta, Maribor, Slovenija
niko.setar1@um.si

V spodnjem prispevku preučujemo etične in moralne vidike obstoječih in nastajajočih tehnologij. Pri tem začenjamo z analizo avtomatizacije delovnih mest in implikacij avtomatizacije za človeštvo v preteklosti, sedanjosti in prihodnosti. Nadaljujemo z obravnavo pojava naraščajoče digitalizacije, s težavami, s katerimi se v njenem kontekstu soočajo tako ustvarjalci kot uporabniki, s poudarkom na spletni anonimnosti, človekovih pravicah in algoritemski diskriminaciji, ter možnih etičnih in pravnih rešitvah za nastale in nastajajoče težave v praksi. Ker sodobna digitalizacija pogosto uporablja umetno učenje in preprosto umetno inteligenco, se prispevek v nadaljevanju osredotoča na etično obravnavo avtonomnih sistemov, kot so samovozeča vozila in samodejna orožja, npr. 'droni'. Iz problematike, ki jo obravnavamo v tem sklopu, se navežemo na izzive, ki jih predstavlja razvoj višje, človeku podobne umetne inteligence, vključno z bolj futurističnimi scenariji, kot so singularna superinteligenca, moralni status človeku podobne umetne inteligence kot osebe, ter verjetnost nastanka tovrstne inteligence, možne etične rešitve ter dileme, ki ostajajo nerešene.

Ključne besede:
avtomatizacija, digitalizacija, umetna inteligenca, avtonomni sistemi, anonimnost, diskriminacija

Univerzitetna založba Univerze v Mariboru

DOI
https://doi.org/
10.18690/um.pf.4.2023.1

ISBN
978-961-286-774-4

1 The Ethics of Automatization, Digitalization and Artificial Intelligence: Existing Dilemmas, Risks and Solutions

Niko Šetar
University of Maribor, Faculty of Arts, Maribor, Slovenia
niko.setar1@um.si

Keywords:
automatisation,
digitalisation,
artificial intelligence,
autonomous systems,
anonimity,
bias

In the following article, we look into ethical and moral aspects of existing and emerging technologies. In doing so, we begin by analysing automatisation of workplaces and implications of such automatisation for humanity in the past, present, and future. We continue with the phenomenon of increasing digitalisation, and what kind of issues its creators and users are facing, emphasising on web anonimity, human rights, and algorithmic bias, as well as possible ethical and legal solutions for existing and emerging problems. Seen as contemporary digitalisation often uses machine learning and rudimentary artificial intelligence, our article continues in that light, with ethical consideration of autonomous systems, such as self-driving vehicles and autonomous weapons, e.g. drones. From the problematic that we address in this section, we relate to the challenges presented by the development of higher, human-like artificial intelligence, including futuristic scenarios like singular superintelligence, moral status of human-like artificial intelligence as a person, considering the probability of such intelligence's existence, possible ethical solutions, and persisting dilemmas.

University of Maribor Press

1.1 Uvod

Človeštvo je do točke razvoja, na kateri se nahajamo danes, napredovalo zaradi svoje inovativne narave, deljenja znanj in informacij, pogosto pa tudi zaradi čiste sreče, in na račun marsikaterega spodletelega eksperimenta. Vedno, kadar se je pojavila nova tehnologija, so se z njo pojavili tudi skeptiki, paranoiki, in ostali, ki so o njej verjeli eno ali drugo neresnico: v poznem 19. stoletju je veljal Teslin dvofazni električni tok, ki ga danes uporablja cel svet, za smrtno nevarnega, pretežno zaradi laži, ki jih je širil Thomas Edison, da bi uveljavil in profitiral od svojega enosmernega toka; prav te dni na socialnih omrežjih opažamo širjenje nenavadnih teorij, kot tudi teorij zarote, o (stranskih) učinkih 5G omrežja, ki nimajo otipljive znanstvene podlage. To pa seveda ne pomeni, da nove tehnologije niso brez tveganj: za posledicami radioaktivnega sevanja so umrli mnogi raziskovalci, vključno s pionirko Marie Sklodowsko Curie, Einstein in Oppenheimer pa sta opozarjala proti uporabi jedrske tehnologije v vojaške namene – Oppenheimer sicer šele po tem, ko je na lastne oči videl uničenje tesntega poligona po detonaciji eksperimentalne bombe Trinity.

Pri vsem tem je jasno, da so pri novih dognanjih, ki jih morda še ne razumemo v celoti, potrebni določeni preventivni ukrepi; pri tistih, ki jih razumemo, in smo uspeli identificirati napake, tveganja, in podobno, pa je nujna vpeljava ukrepov, ki bodo ta tveganja omejili oziroma odpravili. Pri tem lahko gre za mehanske napake, ki jih je moč odpraviti s tehničnimi rešitvami, ali pa drugovrstna tveganja, na primer za okolje, družbo, ali posameznika, ki upravlja ali je v stiku z novo tehnologijo.

1.2 Tehnološki razvoj in povezana tveganja

1.2.1 Regulacija razvoja in novih tehnologij: etični vidik

Brey trdi, da je glavni problem obravnavanja in regulacije novih tehnologij negotovost, tj. negotovost o lastnostih in možnih posledicah še nerazvite tehnologije[1]. Pri odgovornem obravnavanju etičnega problema, ki je negotov, se je potrebno izogniti tako pretirani špekulaciji, kot tudi ideji, da zaradi negotovosti dotičnega problema ne moremo obravnavati, saj lahko to vodi bodisi v prenizko reguliranost razvoja, ali pa v pretirane regulacije, ki lahko aktivno zavirajo napredek.

[1] Brey, P.: Anticipatory Ethics for Emerging Technologies, v: Nanoethics, 6 (2012) 1, str. 1-13.

Dva pristopa, ki se v splošnem uporabljata za tovrstno etično obravnavo, sta generični pristop in napovedni pristop; generični pristop obravnava splošne oz. evidentne lastnosti nove tehnologije (npr. problem radioaktivnosti pri jedrski energiji), napovedni pristop pa poskuša predvidevati prihodnjo rabo in možne posledice nove tehnologije.[2]

Brey v svojem članku kritizira pretekle metode etične obravnave novih tehnologij, vključno z najbolj priznano metodo ETICA, ki temelji na obravnavi problema na podlagi združevanja različnih napovedi o isti zadevi pod domnevo, da je vsaka posamezna napoved pristranska, zaradi česar je potrebno vzeti v poštev maksimalno število možnih napovedi in etičnih obravnav. Metodi ETICA Brey očita, med drugim, da večina njenih analitičnih zmožnosti temelji zgolj na generičnih lastnostih tehnologije, in da je nezadostna za temeljito obravnavo.[3]

Brey predlaga metodo ATE (Anticipatory Technology Ethics), ki vključuje model analize novih tehnologij na treh nivojih: na nivoju tehnologije (generične lastnosti), artifakta (specifični predmeti, sistemi in postopki, ki uporabljajo tehnologijo), in aplikacije (različne rabe artifakta). Na vsakem nivoju je potrebno izpeljati dvostopenjsko etično analizo, pri čemer stopnji povzema po metodi ETICA. Prva stopnja, identifikacija, je namenjena identifikaciji etičnih problemov v skladu z etičnim seznamom, ki zaobjema štiri sekcije. Prva je »Škoda in tveganja«, ki nadalje vključuje telesne poškodbe, psihološke učinke, okoljsko škodo, itd.; druga »Pravice«, ki med drugim obsega različne svoboščine, dostojanstvo, avtonomijo in zasebnost; tretja »Sodstvo«, in četrta »Dobrobit in skupno dobro«. Sledi druga stopnja analize, evalvacija, kjer se oceni resnost negativnih vplivov na elemente, vsebovane na etičnem seznamu, in izvedba možnih ukrepov.[4]

Na pomanjkljivosti teorije ETICA se sklicuje tudi Nathan,[5] ki pa se svoje metode reševanja problemov tehnološke in inovacijske etike loti tako, da definira štiri glavne interesne skupine, na katere vpliva nova tehnologija: to so direktorji, stranke, mediji in vlada. Vsaka izmed naštetih skupin ima svoj tip (dominantna, odvisna, zahtevna

[2] Ibidem.
[3] Ibidem.
[4] Ibidem.
[5] Nathan, G.: Innovation process and ethics in technology: An approach to ethical (responsible) innovation governance, v: Journal on Chain and Network Science, 15 (2015) 2, str. 119-134.

in dominantna, kot si sledijo zgoraj), interese, pravice, odgovornosti in etična tveganja.

V starejšem članku se Di Norcia pri vzpostavitvi sheme razvojnih težav in rešitev opira na tako imenovani Tehnološki Ciklus, ki poteka v šestih stopnjah: inovativni preboj, razvoj in variacija, širjenje in izbor, masovna raba/standardizacija, zrelost/prevlada in zaton/nov preboj.[6] Temu sledi vzporeden Ciklus težav. Ker nas v tem prispevku zanimata preboj in razvoj, se pravi prvi dve stopnji Tehnološkega ciklusa, bomo omenili le težavi, ki jima pritičeta. Pri inovativnem preboju je glavna težava pomanjkanje poročil o možnih napakah, težavah in etičnih dilemah, pri razvoju in variaciji pa pride, po Di Norcii, šele do začetka razumevanja, kjer pa še zmeraj prevladujeta pristranskost in zanikanje težav s strani tistih, ki sodelujejo pri razvoju. Večino rešitev, ki jih predlaga Di Norcia, so novejše metodologije že nadgradile, smiselno pa je izpostaviti en predlog, ki ga večina drugih avtorjev, ki se osredotočajo bolj nad samo-nadzor podjetij, ki razvijajo nove tehnologije, zanemari: neodvisne organizacije, namenjene nadzoru etike inovacij in tehnološkega razvoja.

Čeprav se izhodiščne točke in metodologije opisanih pristopov razlikujejo, so skupne točke očitne. Vsi našteti viri, in viri, na katere se ti sklicujejo, navajajo enakopravno upoštevanje interesov vseh vpletenih interesnih skupin, kar se pri razvoju tehnologije v dobro kapitala (po Di Norcii skupine direktorjev), prej kot karkoli drugega, pogosto ignorira. Predvsem se pogosto zaobidejo parametri psihološke, okoljske in socialne škode kot posledice novih tehnologij (ali nezadostne regulacije) tudi takrat, ko se ekonomsko in fizično tveganje dosledno upoštevata.

1.2.2 Digitalizacija vsakdanjega življenja in njene pasti

V 21. stoletju je ena izmed mnogih nastajajočih tehnologij umetna inteligenca, ki se nahaja nekje na prevesu 1. in 2. stopnje Di Norcievega Tehnološkega ciklusa, pri čemer njeni teoretični nasledniki, kot so resnična, človeku-podobna ali singularna umetna inteligenca (v nadaljevanju UI), v ta ciklus še niso niti vstopili, njeni predniki pa so že napredovali po omenjeni lestvici: osnovni roboti in naučene naprave se nahajajo na 3.-4. stopnji, splošna digitalizacija pa že kar na 5. stopnji.[7] Kakšne so

[6] di Norcia, V.: Ethic, Technology Development, and Innovation, v: Business Ethics Quarterly, 4 (1994) 3, str. 235-252.
[7] Glej: di Norcia, Ethic, Technology Development and Innovation.

dileme, s katerimi se soočamo pri umetni inteligenci, oziroma se bomo soočali pri njenih višjih oblikah, in kaj nas lahko o njihovem preventivnem reševanju nauči naša dosedanja obravnava osnovnejše robotike in digitalizacije?

Capurro navanja, da sega dialog o digitalizaciji in njenih implikacijah nazaj v 80. leta prejšnjega stoletja, ko se v luči napredka računalniške tehnologije poraja ideja 'informacijske družbe' – ideja, ki jo je leta 1993 uresničila CERN-ova deklaracija, da bo Berners-Leejev »World Wide Web« odslej prosto dostopen.[8] Od takrat se je digitalna tehnologija, povezana med sabo s pomočjo globalnega interneta, razširila po vsem svetu, in postala del vsakdanjega življenja večine svetovnega prebivalstva. Integracija digitalnega sveta in moderne družbe je postala tako tesna, da je Floridi (2015) skoval izraza »onlife« in »offlife«, ki označujeta internetno in ne-internetno življenje vsakega posameznika.[9] Capurro trdi, da je ta pretirana integracija in pretirana povezanost sveta eden izmed dejavnikov, ki negativno vplivajo na človeško dostojanstvo iz mnogih razlogov, med drugim zato, ker internet omogoča primerjavo povprečnega uporabnika z nedosegljivim idealom. Nadalje opaža tudi, da mnoge digitalne storitve predstavljajo nevarnost za pravice posameznika; možnost neprestanega nadzora ogroža uporabnikovo zasebnost, tarčno oglaševanje pa njegovo avtonomijo odločitev.[10]

Royakkers postreže s številnimi skrb vzbujajočimi primeri nenadzorovane digitalizacije, nekaj od teh bomo na tem mestu povzeli.[11] Vdor v zasebnost ilustrira s primerom opozorila, najdenega v (46 strani dolgih) navodilih za uporabo televizije proizvajalca Samsung, ki pravi: »Prosimo, da se zavedate, da če vaše besede [izgovorjene v bližini televizorja] vsebujejo osebne ali druge občutljive podatke, bodo ti podatki med tistimi, ki bodo posneti in posredovani tretji osebi.«[12] Podobno avtor povezuje Googlova očala, izdana leta 2013, ki pa niso nikoli vstopila v širšo komercialno rabo, in nevarnost tako imenovanega »Little Brother« scenarija, v katerem sicer ne gre za nadzor vlade nad posamezniki, ampak za navzkrižni nadzor posameznikov in podjetij nad drugimi posamezniki in podjetji – vdor v Google očala

[8] Capurro, R.: Digitalization as an ethical challenge, v: AI & Society, 32 (2017), str. 277-283.
[9] Ibidem, str. 279.
[10] Povzeto po: Ibidem.
[11] Royakkers, L. in ostali: Societal and ethical issues of digitalization, v: Ethics and Information Technology, 20 (2018), str. 127-142.
[12] Ibidem, str. 129.

namreč omogoča dostop do celotnega uporabnikovega vidnega polja in slušnih zaznav.[13]

Kršitve osebne avtonomije se lahko pojavijo na več načinov; Royakkers med drugim ilustrira na videz banalen, a brez dvoma mogoč primer, ki ga imenuje tehnološki paternalizem. V njegovem primeru gre preprosto za pameten hladilnik, ki, ko v njem zmanjka sira, samovoljno naroči sir z nižjo vsebnostjo maščob, ker mu je druga naprava sporočila, da je uporabnikov holesterol previsok.[14]

Pojavi se tudi problem svobode izražanja, ki jo lahko kršijo razni algoritmi za cenzuro, lahko pa pride tudi do obratnega pojava, ki se v zadnjih letih očita socialnim omrežjem, in sicer, da do prevelike mere dopuščajo širjenje lažnih novic.[15] Izredno zaskrbljujoč je tudi problem splošne varnosti nekatelih digitalnih naprav – Royakkers navaja, da je Univerza v Teksasu leta 2012 demonstrirala, kako je z replikacijo digitalne identitete uporabnika (ang. Spoofing) mogoče precej enostavno vdreti v vojaški dron. Kljub temu, da je od te demonstracije do časa pisanja tega prispevka minilo že nekaj časa, in imajo današnji vojaški droni brez dvoma izboljšanje varnostne sisteme, verjetno obstajajo tudi izboljšane metode digitalnega vdora v tovrstne sisteme.[16]

1.2.3 Digitalizacija in umetna inteligenca

Problematika se le še zaostri, ko jo razširimo na domeno umetne inteligence. Kot opaža Anderson, se pojavijo težave že pri 'primitivnejši' umetni inteligenci, in ne šele pri človeku-podobnih ali superinteligentnih sistemih.[17] Avtorica se pri tem sklicuje na eksperiment, pri katerem je robot, namenjen pomoči starostnikom, zaradi neprimernega časa ali pretirane paternalizacije večkrat užalil varovanko. Ta robot sicer ni bil dovolj napreden, da bi lahko s slabo načrtovanim dejanjem povzročil škodo, a si je enostavno predstavljati, da bodo naprednejše, pametnejše umetne inteligence postavljene pred resnejše dileme in pomembne odločitve, kjer bi lahko

[13] Povzeto po: Google Glass and Privacy, Electroic Privacy Information Center, <epic.org/privacy/google/glass/#Privacy%20Interests> (29. 5. 2020).
[14] Povzeto po: Royakkers i.o., Societal and ethical issues.
[15] Povzeto po: Heijinen, I.: Fake News Social Media, EuropCom 2017 – Media Literacy Workshop.
[16] Povzeto po: Royakkers i.o., Societal and ethical issues.
[17] Anderson, S. L.: Machine Ethics, v: Anderson, J. M. in Anderson, S. L.: Machine Ethics, Cambridge University Press, Cambridge 2016, str. 1-19.

napaka v presoji vodila v katastrofo. Zato je pomembno, da so etična načela vključena v razvoj umetne inteligence. Anderson pri tem poudarja, da morajo v ta namen tehniki, ki razvijajo umetno inteligenco, prisluhniti izvedencem za etiko, saj je etika poglobljena disciplina, normativna etika pa se bistveno razlikuje od intuitivne etike povprečnega posameznika.

Kompleksnost etike je eden izmed glavnih problemov pri razvoju zanesljive umetne inteligence: medtem, ko je utilitarizem dejanja sprejemljiv kandidat za uporabo v umetni inteligenci zaradi svoje objektivnosti, mu je mogoče očitati, da odobrava žrtvovanje posameznika v dobro družbe; deontologija, ki tega nikoli ne bi dopustila, pa preveč zanemarja posledice dejanj. Teorija, ki bi ustrezno združevala načela zgornjih dveh, in bi bila del programa človeku-podobne, empatične umetne inteligence, bi bila najboljša rešitev.[18]

Naslednji problem, ki se pojavi, je ali lahko takšna umetna inteligenca sploh obstaja. Za etično ravnanje je potrebna intenca, predpogoja za katero pa sta zavestnost in svobodna volja. Mnogi predvidevajo tudi, da je za pravilno etično ravnanje potrebna tudi empatija, katere predpogoj je zmožnost čutenja in čustvovanja. Zaenkrat še ne vemo, ali lahko umetna inteligenca izpolni katerega izmed teh dveh pogojev.[19]

Bostrom in Yudkowsky predlagata nekaj pogojev, ki bi jih bilo potrebno izpolniti, da se čimbolj zmanjša tveganje, da nam umetna inteligenca uide izpod nadzora.[20] Prvi izmed teh je transparenca za pregled, ki zahteva, da imamo vpogled v notranje delovanje umetne inteligence, in da jo lahko ob kakršnemkoli nepravilnem delovanju pregledamo tako, da je mogoče odkriti vzrok nepravilnosti. Drugi pogoj je predvidljivost, ki sledi delno iz osnovnega programa umetne inteligence, delno pa po tem, da bi naj umetna inteligenca reševala probleme določenega tipa v skladu z replikacijo reševanja preteklih problemov tega tipa. Tretji pogoj je robustnost, ki naj bi onemogočala možnost digitalnega vdora v umetno inteligenco in vmešavanje v njeno delovanje.

[18] Povzeto po: Anderson, Machine Ethics.
[19] Ibidem.
[20] Bostrom, N. in Yudkowsky, E.: The Ethics of Artificial Intelligence, v: Ramsey, W. in Frankish, K.: Cambridge Handbook of Artificial Intelligence, Cambridge University Press, Cambridge 2011, str. 1-20.

Nadaljni problem je prva dva izmed teh pogojev združiti z idejo splošne umetne inteligence; ta dodatni pojem splošnosti pomeni, da umetna inteligenca ni usmerjena v opravljanje specifične naloge, ampak ima podoben, isti, ali celo širši razpon različnih nalog kot človek.[21] Hkrati je smisel umetne inteligence, da nadomesti človeka pri opravljanju naloge, torej da je pri tem od njega boljša – to pa je nemogoče doseči, če umetni inteligenci ne dovolimo samostojnega učenja, ampak jo omejimo na zmožnosti/znanje programerjev. Takšna umetna inteligenca, kot pravita Bostrom in Yudkowsky, nikoli ne bi premagala Kasparova v šahu. A jasno razvidno je, zakaj takšna inteligenca ne more biti transparentna ali popolnoma predvidljiva.[22] Pa vendar se, če ne zadostimo tema pogojema, znajdemo v situaciji inženirja, ki ga opisujeta avtorja: »No, ne vem, kako bo to letalo, ki sem ga izgradil, letelo varno – dejansko ne vem niti, kako bo sploh letelo, ali bo mahalo s krili, se napolnilo s helijem, ali pa na kak tretji način, ki si ga nisem niti predstavljal – a zagotavljam vam, da je zelo, zelo varno.«[23]

1.3 Sodobni izzivi

Zgoraj opisane dileme orišejo večplastnost etičnega izziva, ki ga predstavljata digitalizacija in razvoj umetne inteligence, a preden se lotimo odgovarjanja na zgoraj zastavljena vprašanja, si odgovorimo na najbolj pogosto javno vprašanje, povezano predvsem z robotiko in umetno inteligenco: »Če nas vse zamenjajo naprave, kaj bo potem z nami in delovnimi mesti?«

1.3.1 Avtomatizacija in delovna mesta

V laičnem odgovoru večinoma najdemo prepričanje, da avtomatizacija dela vodi v nezaposlenost, posledično pa v revščino, akumulacijo kapitala na vrhu socio-ekonomske prehranjevalne verige, in še večji prepad med bogatimi in revnimi. Acemoglu in Restrepo izpostavljata zmotno dihotomijo, v okviru katere obstajata samo dva možna odgovora na zgornje vprašanje; prvi, 'alarmistični' odgovor zaobjema omenjeno nezaposlenost in revščino, drugi pa zatrjuje, da avtomatizacija predstavlja odpiranje novih znanstvenih in tehničnih področij, s čemer prinaša tudi

[21] Ibidem.
[22] Ibidem.
[23] Ibidem, str. 5.

nova delovna mesta, in da razloga za skrb ni.[24] Acemoglu in Restrepo ugotavljata, da medtem, ko lahko način avtomatizacije, pri kateri je glavni cilj nadomeščanje človeškega dela, vodi v negativne posledice na področju trga dela in zaposljivosti, je v realnosti avtomatizacija počasnejši in nekoliko bolje reguliran proces, kot ga dojema večina javnosti. Skladno s tem lahko predpostavljamo, da bo izgubi delovnih mest v veliki večini primerov sledil proces nadomeščanja delovnih mest, ki odpira drugačna delovna mesta v podobni skupni količini. Te ugotovitve podpirata s podrobno matematično obravnavo in analizo preteklih trendov avtomatizacije in potrebe po človeškem delu. Problem, ki se utegne ohraniti, je ustrezno in pravočasno izobraževanje oziroma usposabljanje obstoječe delovne sile za nove potrebe na trgu dela.[25]

Akst vidi problem drugje. V svoji analizi preteklih posledic avtomatizacije v 20. stoletju ugotavlja, da je bil samo v ZDA upad števila redno zaposlenih moških med letoma 1960 in 2009 kar 18 odstotkov.[26] Zaključek njegovega članka se osredotoča na trditev, da je problem nezaposlenosti v luči avtomatizacije socio-političen, in ne tehnološki problem – namreč, da je tistim, ki jim avtomatizacija odvzame delovno mesto in (še) nimajo ustrezne izobrazbe ali znanj za prestop na drugo delovno mesto, ali pa drugih zaposlitvenih možnosti v njihovem sektorju enostavno ni, potrebno zagotoviti socialne storitve (zdravstveno zavarovanje, osnovni dohodek, ipd.) neodvisno od njihovega zaposlitvenega statusa.

Precej bolj optimistično stališče zagovarja Autor,[27] ki predvideva, da bodo mnoga delovna mesta ostala neavtomatizirana zaradi narave dela – npr. dela ki zahtevajo znanja iz mnogih področij na srednjem nivoju, in koordinacijo med temi znanj, ali pa dela, ki zahtevajo zmožnost odločanja in neposrednega dela z ljudmi. Podobno kot Acemoglu in Restrepo[28] tudi Autor izpostavja, da bodo potrebne izobraževalne reforme za zapolnjevanje novonastalih delovnih mest, a kot uspešen primer izpolnitve te zahteve iz preteklosti navaja reformo ZDA v začetku 20. stoletja, ko je ta država za potrebe novih delovnih mest kot prva na svetu uvedla univerzalno

[24] Acemoglu, D. in Restrepo, P.: Artificial Intelligence, Automation, and Work, v: Agarwal, A., Goldfarb, A. in Gans, J.: NBER Working Paper Series (24196), National Bureau of Economic Research, Cambridge 2018. (op. spletno dostopno brez oštevilčenih strani)
[25] Povzeto po: Acemoglu in Restrepo, Artificial Intelligence.
[26] Akst, D.: Automation Anxiety, v: Wilson Quarterly, 37 (2013) 3, str. 65-77.
[27] Autor, D. H.: Why Are There Still So Many Jobs? The History and Future of Workplace Automation, v: Journal of Economic Perspectives, 29 (2015) 3, str. 3-30.
[28] Glej: Acemoglu in Restrepo, Artificial Intelligence.

srednješolsko izobraževanje. Problem, ki po mnenju Autorja ostaja, če pride do masovne avtomatizacije je, kako razporediti kapital, ki bi ga prinesla višja produktivnost avtomatizirane industrije in storitev brez dodatnega stroška človeškega dela.

Tudi drugi avtorji na tem področju prihajajo do podrobnih zaključkov, pri čemer jih morda najbolje povzema ta zelo neposreden in iskren citat: »Razkrinkajmo torej lažno neizogibnost trenutne smeri kapitalističnega razvoja in si dalje predstavljajmo različne odnose med tehnologijami, zaposlitvijo in izobrazbo – in naj to storimo skupaj, v dialogu, v upanju za izgradnjo sveta, v katerem bi radi živeli v prihodnosti.«[29]

K učinkom ekonomskega interesa na različne varnostne mehanizme, povezane z digitalizacijo in umetno inteligenco, se bomo še vrnili. Sedaj, ko smo razčistili primarno eksistencialno krizo avtomatizacije dela, se lahko osredotočimo na druge težave, ki se pojavljajo z napredkom tehnologije. Preden preidemo na takšne ali drugačne avtonomne mehanizme in umetne inteligence, je smiselno pregledati tudi problematiko digitalne tehnologije, s katero človek neposredno upravlja, in ki je že par desetletij dostopna splošni javnosti.

1.3.2 Spletna anonimnost in zasebnost

S tem je seveda mišljen internet in vse njegove raznolike uporabe, z možnimi zlorabami, ki spadajo zraven. Otroci interneta smo bili vzgojeni ob svaritvah glede t.i. pojava »cyber-bullying«, spletnega nadlegovanja, sistemsko izkoriščanje razsežnosti interneta v kriminalne, politične in ostale namene, pa postaja jasno šele preteklo desetletje. Knjiga Bernarda E. Harcourta z naslovom *Exposed: Desire and Disobedience in the Digital Age* (2015) postreže s pompozno zvenečimi naslovi poglavij, ki izhajajo iz književnih del znanstvenofantastične distopije, od Velikega Brata do Panoptikona, pa od Mrka humanizma do Jeklene mreže.[30] Na prvi pogled se analogija med sodobno spletno družbo in zgornjimi koncepti zdi pretirana, a

[29] Peters, M. A., Means, A. J., in Jandrić, P.: Introduction: Technological Unemployment and the Future of Work, v: Peters, M. A., Means, A. J., in Jandrić, P.: Education and Technological Unemployment, Springer, Singapore 2019, str. 11.
[30] Harcourt, B. E.: Desire and Disobedience in the Digital Age, Harvard University Press, Cambridge 2015.

raziskave kažejo, da je najbolj priljubljena izmed vseh digitalnih tehnologij te črnoglede scenarije tesno približala resničnosti.[31]

Tehnologija, o kateri govorimo, so seveda socialna omrežja, ki so v preteklih 15 letih uspešno nadomestila tradicionalne medije, in premaknila javno sfero iz fizičnega v digitalni svet. Balkin socialna omrežja identificira kot eno izmed treh kategorij internetnih storitev – prva so osnovni sistemi (DNS, 'caching', itd.), druga pa plačilne storitve – ki ima svoj namen.[32] Slednji se ponovno deli na tri splošne namene, ki so olajšanje javnega sodelovanja, organizacija javnega dialoga in kuracija javnega mnenja. Kuracija javnega mnenja izhaja iz notranjih pravil in standardov posameznih socialnih omrežij, ki lahko omejijo vsebino objav po lastni izbiri. Relevanca te kuracije nadalje stremi iz prepričanja, da bi morale vlade vzdrževati omrežno nevtralnost (ang. 'Net Neutrality'), ker jim to preprečujejo ustave večine držav – z državno kuracijo interneta bi namreč prišlo do ekstenzivnih kršitev določenih temeljnih pravic, npr. svobode izražanja in svobodnega dostopa do informacij.[33]

Notranja politika socialnih omrežij mora biti torej tista, ki vzdržuje njihove družbene vloge, preprečuje širjenje lažnih podatkov, sovražnega govora, in podobnega. Balkin del rešitve vidi v pluralnosti institucij (tj. socialnih omrežij in medijev), ki stojijo med državo in posameznikom; te naj bi zagotavljale, da se uporabniki držijo standardov spoštljivega in korektnega dialoga v skladu z njihovimi standardi, ob predpogoju, da imajo tovrstne standarde zaradi njihovega 'dobrega imena' in socialnega statusa. Drug del rešitve se utegne nahajati v raznovrstnosti mnenj in vrednot, ki se pojavljajo v javni sferi.[34] Dodajmo, da je smiseln pogoj, da so ta mnenja in vrednote enakovredno dostopne in podprte z določenimi objektivnimi premisami, v nasprotnem primeru pa je odgovornost uporabnika, da jih zavrne oz. obravnava kritično.

Do zapletov pride, ko se pojavi zahteva po človeški moderaciji. Dosledna moderacija namreč zahteva povečano število moderatorjev, ki so bolje kvalificirani za objektivno kritično presojo vsebin. Ker je večina socialnih omrežij usmerjena proti

[31] Primer: Mozur, P. in Krolik, A.: A Surveillance Net Blankets China's Cities, Giving Police Vast Powers, v: The New York Times, 17. 12. 2019.
[32] Balkin, J. M.: How to Regulate (and Not Regulate) Social Media. Uvodni nagovor simpozija Association for Computing Machinery Symposium on Computer Science and Law, New York 2019.
[33] Povzeto po: Balkin, How to Regulate.
[34] Ibidem.

temu, da služijo z oglaševanjem čimvečji populaciji uporabnikov, je takšna poteza v nasprotju z njihovimi interesi. Je namreč že inherentno dražja, kot tudi lahko omejitve svobode izražanja pomenijo upad števila uporabnikov. Poleg tega socialna omrežja njihovi ustvarjalci pogosto dojemajo kot zabavo, profitno dejavnost, ali nekaj tretjega, prej kot pa jih dojemajo v okviru zgoraj opisanih družbenih namenov. Pravilna samorefleksija in sprememba oz. prilagoditev ekonomskega modela sta torej ključnega pomena za uspešno regulacijo socialnih omrežij.[35]

Tudi prvi dve internetni storitvi po Balkinu nista varni brez tveganj. Pri storitvah DNS in storitvah spletnega bančništva se identiteta uporabnika preverja z digitalnimi certifikati; mehanizmi, ki varujejo zaupne osebne podatke uporabnika. Uporabnik je v tem primeru t.i. 'digitalna avtoriteta' nad svojimi certifikati. Težava je, da je s človeškim uporabnikom moč manipulirati, da izda podatke certifikata, ali pa njegov certifikat poneveriti z vdorom v njegov (navadno manj zaščiten) osebni sistem. Pravno-politične rešitve so proti temu problemu praktično nemočne, saj je sledenje digitalnemu zločinu mnogo težje, kot razkritje fizičnega. Na srečo računalniška znanost v zadnjih letih predstavlja vse uspešnejše zaščitne protokole, npr. CT (transparentnost certifikata) in SK (neodvisni ključ).[36]

Vrnimo se k socialnim omrežjem in naslednji težavi, ki se pri njih ponavlja – anonimnosti. Različne spletne platforme imajo različne stopnje anonimnosti. Identiteta posameznika na globokem spletu je skoraj neizsledljiva, na nekaterih omrežjih je dobro zakrita, na nekaterih je kljub psevdonimu odkriti identiteto uporabnika povsem enostavno, če ta ni zelo previden pri ustvarjanju profila. Varnost na vseh izmed njih je stvar računalništva, in ne etike, zato se vanje ne bomo poglabljali.

Nekatera omrežja, kot je recimo Facebook, pa anonimnost kratkomalo prepovedujejo. Facebook ima strogo politiko resničnega imena, in moderatorji zaposleni pri tem omrežju aktivno iščejo profile, skrite za psevdonimom, in jih odstranjujejo z omrežja. Prednosti in slabosti te politike so stvar debate. Tisti ki jo zagovarjajo trdijo, da anonimnost vodi k širjenju lažnih informacij in sovražnega govora, ker brez identifikacije uporabnik nima strahu pred posledicami; po drugi

[35] Ibidem.
[36] Povzeto po: Laurie, B. in Doctorow, C.: Secure the Internet, v: Nature, 491 (2012), str. 325-326.

strani zagovorniki anonimnosti trdijo, da anonimnost vodi v večjo iskrenost, prav tako zaradi pomanjkanja strahu pred posledicami, ki pa vodi v večjo legitimnost podatkov.[37]

Resnica je, da obe trditvi držita, odvisni pa nista od anonimnosti same, ampak od namena, zaradi katerega se uporabnik odloči za anonimno delovanje. Bodle zadevo dojema kot stvar normativne etike.[38] Meni, da je stališče proti anonimnosti politično in ekonomsko utilitaristično, saj omogoča lažji nadzor nad prepričanji ne-anonimnih posameznikov; sam zagovarja nasprotno stališče, da je potrebno o anonimnosti odločati deontološko, se pravi z mislijo na pravice uporabnika, in ne samo na posledice njegove anonimnosti za tretje stranke.[39]

Tretji razvidni problem v sklopu socialnih omrežij in z njimi povezane digitalizacije pa je ta, ki to temo poveže z jedrom tega eseja – tj. z umetno inteligenco. Na socialnih omrežjih se namesto človeških moderatorjev vse pogosteje uporabljajo enostavne umetne inteligence oz. algoritmi, ki skrbijo za notranje in zunanje oglaševanje omrežja, nadzor nad objavami, komentarji, prijavami itd. Brkan izpostavlja štiri glavne težave, ki jih povzročajo ti inteligentni algoritmi – prva izmed teh je personalizacija, se pravi mehanizem oglaševanja oseb, izdelkov, političnih strank, in še česa, na podlagi zgodovine iskanja, objav, komentarjev in 'všečkov' na uporabnikovem profilu.[40] Ko govorimo o političnem in ideološkem oglaševanju, je personalizacija glavni promotor lažnih novic in pristranskosti, saj je ena od njenih največjih pomanjkljivosti učinek mehurčka (ang. Filter bubble effect). To pomeni, da se uporabnik nahaja med oglasi, ki so ustvarjeni specifično zanj, tako da potrjujejo njegova prepričanja in pred njim skrivajo alternativne možnosti. To je pogosto v volitvenih kampanijah, kjer lahko s pomočjo tega učinka volivca z oglasi polarizirajo (tj. neopredeljenega volivca usmerijo proti določeni odločitvi) in manipulirajo (tj. spremenijo njegovo politično usmerjenost na podlagi afirmacije drugih prepričanj).[41] Seveda obstajajo možne rešitve, najenostavnejša izmed katerih je odgovornost

[37] Povzeto po: Bodle, R.: The ethics of online anonymity or Zuckerberg vs. 'Moot', v: ACM SIGCAS Computers and Society, 43 (2013) 1, str. 22-35.
[38] Bodle, Zuckerberg vs. 'Moot', str. 23.
[39] Ibidem.
[40] Brkan, M.: Freedom of Expression and Artificial Intelligence: on personalisation, disinformation and (lack of) horizontal effect of the Charter, v: MCEL Working Paper Series, Maastricht 2019, str. 1-18.
[41] Povzeto po: Brkan, Freedom of Expresson; Burkell J. in Regan, P. M.: Voter preferences, voter manipulation, voter analytics: policy options for less surveillance and more auntonomy, v: Internet Policy Review, 8 (2019) 4, str. 1-24.

volivca, da razišče alternative, a je enostavno preveč naivna, da bi bila izvedljiva. V poštev prideta še odgovornost socialne platforme, v skladu s katero bi bila dolžna takšne oglase omejiti ali pa razkriti njihovega naročnika, ter sodna intervencija. Če pobrskamo nekaj strani nazaj po tem eseju, ugotovimo, da marsikomu to ni v pretiranem interesu.[42]

Težavi z avtomatizirano moderacijo socialnih omrežij sta tudi avtomatsko blokiranje/odstranjevanje nezakonitih vsebin in democija škodljivih (a legalnih) vsebin. Oba izmed teh principov sta sporna zaradi visoke zmotljivosti inteligentnega algoritma, ki bi naj o tem odločal, ter lahko kršita pravico svobode izražanja. Še ena težava se pojavi pri pravici do pozable (ang. Right to be forgotten),[43] v skladu s katero mora omrežje izbrisati vse podatke ne-anonimnega uporabnika na njegovo zahtevo. Ta lahko krši pravico do dostopa do informacij drugih uporabnikov.[44] Najbolj učinkovita rešitev opisanih težav bi bila bržkone poprej predlagana povečava števila in dvig zahtevanih kvalifikacij človeških uporabnikov, a ponovno, temu nasprotujejo ekonomski in politični interesi.

1.3.3 Algoritemska diskriminacija

Dodaten primer nevarnosti pomanjkanja internetne anonimnosti je prenos človeških predsodkov na spletne platforme. Sam izumitelj interneta, Sir Berners-Lee, je letos ponovno opozoril na diskriminacijo, ki se na spletu pojavlja proti ženskam, LGBT skupnosti, in še marsikomu, ter vključuje med drugim izsiljevanje, grožnje in spolno nadlegovanje.[45] A diskriminacija ne ostaja omejena na medčloveški odnos; človeški faktor v programiranju oglaševalnih in drugih algoritmov je diskriminacijo prenesel tudi v avtomatizirane procese, ki jih izvaja umetna inteligenca, učena iz človeških učnih podatkov.

Ti procesi lahko privedejo do različnih neželenih učinkov. Blažji so, da program za iskanje letalskih kart priporoči prej dražje karte glede na državo, katere državljan ga uporablja, ali pa da ob iskanju zdravstvenih nasvetov Google prej prikaže laične, pogosto nezanesljive spletne strani, kot pa strokovne. Med težjimi se dogaja, da

[42] Povzeto po: Balkin, How to Regulate; Burkell in Regan, Voter preferences.
[43] C-131/12, *Google Spain,* ECLI:EU:C:2014:317.
[44] Povzeto po: Brkan, Freedom of Expression.
[45] Povzeto po: Sample, I.: Internet 'is not working for women and girls', says Berners-Lee, v: The Guardian, 12. 3. 2020.

lahko program, ki izbira kandidate na razpisu za delo, na podlagi algoritemske diskriminacije nepošteno izloči pripadnike manjšin; program, ki dodeljuje kredite, lahko zavrne kredit neprimerljivo večjemu številu žensk kot moških. Naštejemo lahko na stotine identificiranih primerov tovrstne diskriminacije.[46][47]

Hacker trdi, da do algoritemske diskriminacije pride bodisi zaradi pristranskih učnih podatkov, ali pa zaradi neenakopravne temeljne resnice.[48] Pristranski učni podatki lahko nastanejo kot posledica nepravilnega ravnanja s podatki, ki izhaja iz pristranskosti oz. predsodkov tistega, ki te podatke pripravlja, ali pa zaradi napačne reprezentacije podatkov v smislu neenakomerno razporejenega vzorca, na katerem se umetna inteligenca uči. Neenakopravna temeljna resnica izhaja iz statistične diskriminacije, tj. iz splošnih podatkov, ki govorijo proti ali za določeno demografsko skupino.[49] Primer statistične diskriminacije je označitev afriških američanov kot bolj verjetnih, da storijo kriminalno dejanje. Čeprav je ta statistika do neke mere resnična, vseeno temelji na globlje zakoreninjeni človeški diskriminaciji, zaradi katere je bolj verjetno, da bo afriški američan obtožen, obsojen, obsojen na strožjo kazen, ali celo po krivem obsojen kot bel američan, in je zato, seveda, diskriminatorna.

Algoritemska diskriminacija lahko vodi tako v neposredno diskriminacijo, usmerjeno proti posamezniku na podlagi demografske skupine, ki ji pripada, ali pa v posredno diskriminacijo, pri kateri gre za diskriminacijo proti določeni demografski skupini, ki jo navadno povzroča navidez nevtralen algoritemski parameter. Identifikacija slednje je izjemno problematična, saj se pogosto niti ustvarjalci algoritma, niti njegovi uporabniki ne zavedajo tovrstnih težav.[50]

[46] Povzeto po: Hacker, P.: Teaching Fairness to Artificial Intelligence: Existing and Novel Strategies Against Algorithmic Discrimination Under EU Law, v: Common Market Law Review, 55 (2017), str. 1143-1186.
[47] Povzeto po: Sandvig, C. in ostali: Auditing Algorithms: Research Methods for Detecting Discrimination on Internet Platforms, v: Data and Discrimination: Converting Critical Concerns into Productive Inquiry, 64th Annual Meeting of the International Communication Assiociation, 2014.
[48] Hacker, Teaching Fairness, str. 1147.
[49] Povzeto po: Hacker, Teaching Fairness.
[50] Ibidem.

Prvi korak do preprečitve algoritemske diskriminacije je odkritje diskriminacije, kjer se ta pojavlja, kar je mogoče z revizijami delovanja algoritmov.[51] Sandvig in ostali[52] trdijo, da so revizijske študije, ki preverjajo diskriminacijo tako, da preverjajo ljudi vpletene v postopek okoli algoritma, pogosto nesmiselne, če so subjekti teh študij obveščeni o njih, ali pa neetične, kadar niso, saj kršijo pravico subjektov do seznanjenosti o študiji, v kateri sodelujejo. Avtor zato predlaga, da se revidira algoritme same, kar se da neposredno - v ta namen predlaga 5 metod revizije. Prva izmed njih zahteva razkritje celotne kode algoritma v pregled, druga preučuje uporabnike oz. rezultate, ki so jih prejeli, ter preverja delovanje algoritma skozi rezultate glede na demografsko pripadnost uporabnikov, tretja pošilja umetno ustvarjene profile oseb algoritmu, in preučuje odgovore glede na parametre lažnih profilov, četrta uporabi resnične osebe z različnih ozadij, ki sodelujejo z revizorji in z njimi delijo svoje rezultate, peta pa uporabi rezultate čimvečjega števila pripadnikov čimbolj raznolike populacije, ki je že pred obveščenostjo o raziskavi prejela rezultate preučevanega algoritma.[53]

Naslednja stopnja po odkritju diskriminacije je odgovorno oz. pošteno pridobivanje podatkov, najpomembneje učnih podatkov za algoritme, ki jih lahko pridobivamo s pred-, med-, ali post-procesiranjem. Pred-procesiranje zahteva natančen pregled in po potrebi prilagoditev izhodiščnih podatkov, v kolikor so ti oporečni; med-procesiranje predvideva anti diskriminacijske elemente v samem algoritmu, ki pridobiva podatke; post-procesiranje pa modifikacijo pridobljenih podatkov.[54] V skladu z zakonodajo proti diskriminaciji se lahko tovrstne tehnične rešitve pri algoritemski obravnavi ljudi tudi zakonsko predpišejo.

1.4 Umetna inteligenca danes

1.4.1 Zanesljivost umetne inteligence

Pri obravnavi takšnih primerov in z mislijo na nadaljnji razvoj umetne inteligence, se človek vpraša, do kakšne mere lahko zaupamo tehnologiji, ki temelji na nas, vključno z vsemi našimi napakami, pa vendar ohranja določeno mero avtonomnosti,

[51] Hajian, S. in ostali: Algorithmic Bias: From Discrimination Discovery to Fairness-aware Data Mining, v: Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, 22 (2016), str. 2125-2126.
[52] Sandvig i.o., Auditing Algorithms.
[53] Ibidem.
[54] Povzeto po: Hajian i.o., Algorithmic Bias.

zaradi katere nam je vpogled v njeno podrobno delovanje zelo otežen, če ne že kar onemogočen.

Pogosto ima zanesljivost delovanja umetne inteligence dve plati: raziskava potencialne uporabe UI v človeških misijah na Luno ali celo Mars je pokazala, da medtem, ko so ti sistemi zanesljivi pri nadomeščanju človeka v namene prognostike ostalih sistemov (predvidevanje okvar, možnih ukrepov, itd.), kompleksnost same UI onemogoča človeškim delavcem, da bi pred uporabo ustrezno verificirali njeno delovanje.[55] To je ilustracija omenjene dvostranskosti. Večinoma ima umetna inteligenca pred človekom prednost pri samih nalogah, ki jih izvaja: UI se je izkazala pri medicinski diagnostiki, saj ima možnost hitrega procesiranja velike količine podatkov in iskanju ustrezne diagnoze na podlagi preteklih primerov; sonde, roverji in podobne naprave, opremljene z UI so se zelo dobro obnesle v vesolju in globinah oceanov zaradi svoje neobčutljivosti na zunanje pogoje; v drugih primerih je UI prekosila človeka zaradi svojega ne-čustvenega, popolnoma logičnega in objektivnega odločanja. Istočasno UI predstavlja težavo zaradi netransparentnosti in nečloveškosti: kompleksen sistem UI, ki se lahko hitro uči in dela popravke, ni transparenten za človeški pregled v njegovo delovanje, in lahko zelo hitro uide izpod nadzora; UI, ki takšnega učenja ni zmožnja, ne more predvideti ali se pravilno odzvati na nepredvidljive okoliščine, prav tako pa se ne more naučiti kompleksnih pogojnih sistemov, npr. etike.[56]

1.4.2 Samovozeča vozila

Na nobenem sodobnem področju umetne inteligence te pomanjkljivosti ne pridejo tako dobro do izraza kot pri samovozečih vozilih, ki se v zadnjem desetletju vse hitreje premikajo iz sfere teoretične ali eksperimentalne tehnologije v naša vsakdanja življenja. Večina sveta rabo avtomatiziranih vozil še zmeraj strogo omejuje, čeprav obstajajo izjeme, npr. ameriška zvezna država Kalifornija, ki dopušča rabo samovozečih naprav brez potnikov pod določeno maso in najvišjo hitrostjo.

[55] Povzeto po: Schwabacher, M. in Goebel, K.: A survey of artificial intelligence for prognostics, v: AAAI Fall Symposium – Technical Report, 2007, str. 107-114.
[56] Povzeto po: Dasoriya, R. in ostali: The Uncertain Future of Artificial Intelligence, v: 8th International Conference on Cloud Computing, Data Science & Engineering, 2018, str. 458-461.

Medtem, ko je osnovna tehnologija za samovozečimi vozili, ki zaobjema sledenje cestno-prometnim predpisom, navigiranje med ostalimi vozili v normalnih okoliščinah, ter podobne aspekte njihove uporabe že praktično dovršena, pa je obnašanje samovozečih vozil v abnormalnih okoliščinah, npr. v primeru ekstremnega vremena, neizogibne nesreče, ali celo neizogibne smrti udeleženca ali udeležencev v prometu, še zmeraj neodgovorjeno in domala pereče vprašanje.

Pogost laičen odgovor na to, kako naj umetna inteligenca, ki upravlja vozilo, ravna v primeru neizogibne nesreče, je popolnoma utilitaristično: ravna naj tako, da se čimbolj zmanjša število žrtev oz. negativnih posledic na splošno. Čeprav to sprva zveni smiselno, gre v bistvu za globlji etični problem, ki se nahaja v neposredni analogiji s klasičnim filozofskim problemom vagona (ang. Trolley problem), kjer mora akter sprejeti odločitev, ali bo vagon, ki drvi proti petim ljudem, privezanim na tirih, preusmeril na drugi tir, na katerega je privezana samo ena oseba. Če ga ne preusmeri, je pasivno sodeloval pri smrti petih ljudi; če ga, je aktivno kriv smrti ene osebe. Klasična oblika problema ima še mnoge dodatne, kompleksnejše permutacije – kot jih ima tudi problem odločanja pri samovozečih vozilih.

De Sio[57] navaja, da je utilitaristično odgovor na dilemo ravnanja v neizogibnih nesrečah pri samovozečih vozilih nezadosten, saj je v nasprotju z bolj absolutnimi etičnimi normativami, najpomembneje z absolutno deontološko prepovedjo odvzema življenja nedolžne osebe, ki je zakoreninjena tudi v zakonodaji celotnega civiliziranega sveta. Vendar pa obstajajo izjeme, ki niso vedno popolnoma jasne. Omenjeni avtor ilustrira variabilnost principa z dvema razvpitima primeroma. Prvi je primer Dudleya in Stephensa, ki sta po večtedenskem stradanju po brodolomu ubila in pojedla tretjo osebo, ki se je z njima nahajala na območju brodoloma – po vrnitvi v ZDA sta bila obsojena umora.[58] Drugi primer sta Gracie in Rosie, siamski dvojčici, ki ju je bilo potrebno razdružiti:[59] Gracie je držala Rosie pri življenju, a so ocenili, da bosta skupaj zdržali le približno 6 mesecev. Po drugi strani bi kirurška ločitev Rosie brez dvoma ubila, medtem ko so ocenili, da ima Gracie 94% možnost preživetja. Sodišče je v tem primeru odločilo, da se ločitev izvede in da je smrt Rosie v tem primeru nujna za preživetje Gracie. Lahko bi trdili, da je bila v prvem primeru

[57] de Sio, F. S.: Killing by Autonomous Vehicles and the Legal Doctrine of Necessity, v: Ethic Theory and Moral Practice, 20 (2017), str. 411-429.
[58] R v Dudley and Stephens (1884) 14 QBD 273 DC.
[59] Re A (conjoined twins) [2001] 2 WLR 480.

smrt tretje osebe nujna za preživetje Dudleya in Stephensa, a sta zločina neposrednega umora in kanibalizma pripeljala do njune obsodbe. Nasprotno, namen operacije ni bil ubiti Rosie, da bi ohranili Gracie pri življenju, ampak formalno zgolj ločiti dvojčici. Sodstvo se je v tem primeru sklicevalo tudi na strokovno avtoriteto kirurgov, ki so o operaciji odločali.[60]

Drugi problem utilitaristične obravnave samovozečih vozil je inkomenzurabilnost človeškega življenja. Poenostavljeno, princip inkomenzurabilnosti predpostavlja, da ni takšnih parametrov, s pomočjo katerih bi bilo moč določiti katero življenje je vrednejše od drugega, pa naj poskušamo na podlagi starosti, spola, etnične pripadnosti, poklica, izobrazbe, ali katerekoli kombinacije teh ali drugih karakteristik oseb, udeleženih na primeru.[61] Vsaka tovrstna obravnava je inherentno diskriminatorna, poleg tega pa ne mora uskladiti razlik vrednotenja človeškega življenja, ki bi utegnile izhajati iz kulturnih razlik, npr. tradicionalne zahodnjaške cenitve mladega življenja nad življenjem starostnika v kontrastu s tradicionalno vzhodnjaško centivijo življenja starešine nad življenjem otroka.

Tretji problem je težavnost predvidevanja dolgoročnih posledic odločitve v posameznih primerih, kot tudi dolgoročnih posledic vzpostavitve enotne normativne etike za vsa samovozeča vozila.[62]

Thornton in ostali[63] predlagajo rešitev, ki vzpostavi kompatibilnost med normativnimi etikami. Njihov predlog izhaja iz strinjanja, da ena normativna etika ni zadostna za reševanje katerekoli posamezne situacije, v kateri se lahko znajde avtonomno vozilo. Po njihovem prepričanju mora vsako avtonomno vozilo zagotoviti trojici kriterijev, tj. mobilnosti, legalnosti in varnosti, pri čemer pogosto ni mogoče zadostiti vsem trem popolnoma. Primer, ki ga navajajo, je vozilo, ki je obtičalo za oviro na cesti. Na desni ima komaj kaj prostora, da se izogne oviri, kar bi ogrozilo varnost potnikov, na desni pa ga ovirata dve polni črti, ki mu preprečujeta prečkanje zaradi legalne zahteve, ki jo predstavljata. Če ne izbere nobene opcije, lahko obtiči za oviro za nedoločen čas, kar krši pravico do mobilnosti potnikov. V tovrstnih okoliščinah bi bilo, ob primerni preučitvi dodatnih varnostnih okoliščin,

[60] Povzeto po: de Sio, Doctrine of Necessity.
[61] Ibidem.
[62] Povzeto po: de Sio, Doctrine of Necessity.
[63] Thornton, S. in ostali: Incorporating Ethical Considerations Into Automated Vehicle Control, v: IEEE Transactions on Intelligent Transportation Systems, 48 (2017) 6, str. 1429-1439.

upravičeno prekršiti cestno-prometni predpis, ki prepoveduje prečkanje dvojne polne črte.[64]

Predlog, ki sledi, je konsekvencialistična etika, omejena z deontološkimi principi, ki izhajajo iz Asimovih treh načel robotike, ki med drugim zaobjemajo absolutno prepoved škodovanja človeškemu življenju, itd.[65] Ko se umetna inteligenca 'prepriča', da nobeno izmed deontoloških načel ne bo kršeno, lahko nadaljuje z ravnanjem v skladu s konsekvencialistično etiko, ki predvideva najmanj škodljive posledice dejanja.[66]

Vseeno pa tudi tovrstna etična shema ne predvideva resnično anomalnih situacij, kjer npr. ni mogoče ne-prekršiti deontološkega načela. Wagner in Koopman[67] trdita, da to izhaja iz razlik v človeškem ravnanju in ravnanju umetne inteligence, ki upravlja vozilo. Vozila namreč ravnajo v skladu s principom induktivne inference, torej lahko v skladu z opazovanji izvajajo izjemno natančne operacije, dokler te ustrezajo ustaljenemu vzorcu. Kadar mu ne, odločitev postane nemogoča. Kot rešitev predlagata metodo umetnega učenja, ki temelji na falsifikacionistični teoriji, v skladu s katero se lahko umetna inteligenca uči iz neuspešnih poskusov reševanja problemov, najbolje v simuliranih anomalnih okoliščinah.[68]

Četudi se sčasoma najde unificiran etični standard, ki bo samovozeča vozila naredil enako ali bolj zanesljiva kot človeške voznike, tudi v anomalnih pogojih, pa bo najbrž še vedno obstajalo tranzicijsko časovno območje med človeško vožnjo in popolno avtomatizacijo, kjer bo umetna inteligenca upravljala samo del procesa (avtopilot, avtomatsko zaviranje v sili, itd.). Kako pri različnih stopnjah avtomatizacije pripišemo krivdo za nezgodo, oz. primere nesreč zakonsko obravnavamo?

Anderson predvideva, da v popolnoma avtomatiziranih vozilih krivda voznika ne bo več veljaven faktor, ampak bo krivda avtomatsko na strani proizvajalca vozila, pri čemer lahko gre za napake v proizvodnji ali napake v načrtovanju.[69] Kazenska in

[64] Povzeto po: ibidem.
[65] Ibidem.
[66] Ibidem.
[67] Wagner, M. in Koopman, P.: A Philosophy for Developing Trust in Self-Driving Cars, v: Meyer, G. in Beiker, S.: Road Vehicle Automation, Springer, New York 2015, str. 163-171.
[68] Povzeto po: Ibidem.
[69] Anderson, J. M. in ostali: Liability Implications of Autonomous Vehicle Technology, v: Anderson, J.M. in ostali: Autonomous Vehicle Technology, RAND Corporation, Santa Monica 2014, str. 111-134.

odškodninska odgovornost proizvajalca sta pri tem odvisni od različnih načinov zakonske obravnave, ki jih bomo v namene tega prispevka izpustili. Avtomatizirana vožnja bo neizogibno privedla tudi do nove vrste nesreč, kot so nesreče zaradi napak v programiranju, ki bi ga lahko vsaj delno izvajal tudi uporabnik, ne le proizvajalec avtomobila, ali nesreče delno- ali ne-avtomatiziranih vozil in pešcev, navajenih na avtomatizirana vozila, na katera ne rabijo biti pozorni. V prvem primeru je lahko krivda na strani uporabnika, če ta ni upošteval navodil programiranja, ali pa proizvajalca, če navodila niso bila ustrezna; v drugem primeru je lahko kriv voznik, ki ni videl pešca, ali pa pešec, ki je ravnal neodgovorno ob pričakovanju avtomatiziranega vozila.[70]

Pri delno-avtomatiziranih vozilih ni vprašanje odgovornosti nič manj kompleksno, pri vozilu z avtocestnim avtopilotom je lahko kriv voznik, ki je med avtomatsko vožno zadremal proti opozorilom proizvajalca, ali pa proizvajalec, ki ni ustrezno opozoril na to, da umetna inteligenca v vozilu še zmeraj zahteva človeški nadzor.[71] Bellet in ostali[72] predstavljajo kompleksno shemo devetih faz HMT (Human-Machine Transition; Prehod med človekom in napravo), ki zaobjema pravne podrobnosti, v katere se ne bomo podrobneje spuščali. Mnogo enostavneje, Bryson in Winfield[73] ponovno poudarjata zahtevo po transparentnosti programske opreme, ki vodi umetno inteligenco v vozilu, tako za uporabnika, v smislu vpogleda v to, kako bo njegovo samovozeče vozilo ravnalo in zakaj, kot za pristojne službe, ki bi utegnile preizkovati morebitno nezgodo ali podobne okoliščine, v smislu črne skrinjice na letalih.

1.4.3 Avtomatizirano orožje

Še večjo etično dilemo predstavljajo drugi avtomatizirani sistemi, še najbolj izmed njih avtomatizirano orožje. V vojaških konfliktih vsebolj narašča uporaba brezpilotnih zrakoplovov oz. dronov, ki se jih vodi ali pa nadzoruje na daljavo. Že pri samih dronih imajo mnogi pomisleke glede moralnih aspektov njihove rabe proti

[70] Povzeto po: Ibidem.
[71] Ibidem.
[72] Bellet, T. in ostali: From semi to fully autonomous vehicles: New emerging risks and ethico-legal challenges for human-machine interactions, v: Transportation Research, 63 (2019) F, str. 153-164.
[73] Bryson, J. in Winfield, A.: Standardizing Ethical Design for Artificial Intelligence and Autonomous Systems, v: Computer, 50 (2017) 5, str. 116-119.

ljudem; mnogi jim očitajo neosebnost, kršenje dostojanstva ubitega sovražnika, in pripisujejo večjo kolateralno škodo kot tradicionalnim orožjem.

Statman trdi, da na primeru dronov to ne drži. [74] Glavna uporaba dronov je namreč v skladu s principom nepotrebnega tveganja, saj lahko en sam dron nadomesti zajetno število živih vojakov, ki jim zaradi uporabe drona ni potrebno tvegati življenja na bojnem polju. Nadalje Statman nasprotuje tudi tistim, ki trdijo, da droni povzročajo večjo kolateralno škodo, pri čemer se opira na njihovo natančnost v primerjavi z drugimi modernimi načini vojskovanja, npr. bombnimi letali, in tistimi, ki trdijo, da gre za kršitev dostojanstvene smrti in razčlovečenje, rekoč, da dron ni nič manj neoseben kot bojna konica, izstreljena z vojaškega letala, ali pa ostrostrelec, katerega prisotnosti se tarča sploh ne zaveda. Potrebno je poudariti, da ti argumenti veljajo samo, kadar je konflikt v vsakem primeru neizogiben, in bi se v primeru prepovedi/nezmožnosti uporabe dronov uporabila druga orožja.[75]

Vseeno pa njegov zagovor vodenih, delno-avtomatiziranih sistemov, ne nudi zadostnega odgovora na vprašanje polno avtomatiziranih sistemov, ki jih vodi umetna inteligenca. Swoboda[76] preučuje problematiko odgovornosti pri polno avtomatiziranih orožjih; tovrstna orožja naj bi se učila iz lastnih izkušenj, na podlagi vnaprej programiranih parametrov za učenje. Pri tem je težavno, da osnovni program takšnega 'vojnega robota' ne more nikdar vsebovati vseh možnih okoliščin, zaradi česar bo njegova reakcija v novih okoliščinah nepredvidljiva. Programer za to ne more bit odgovoren, saj ni mogel predvideti izredne okoliščine, robot pa prav tako ne, vsaj zaenkrat še ne, ker ni oseba, ki bi lahko bila nosilka pravic in dolžnosti. Večino izrednih scenarijev je mogoče rešiti s programiranjem principa pozitivne diskriminacije, na podlagi česar bi lahko robot razločeval med sovražnikom, nevtralnim subjektom in prijateljem ne glede na druge okoliščine, a tudi tukaj obstajajo izjeme: sovražniki bi se lahko zakrinkali kot prijatelji, robot bi lahko prejel sporne direktive nadrejenih ljudi, nenazadnje tudi ni odporen proti programskim vdorom.[77]

---

[74] Statman, D.: Drones and Robots: On the Changing Practice of Warfare, v: Lazar, S. in Frowe, H.: The Oxford Handbook of Ethics and War, Oxford University Press, Oxford 2015. (op. spletna predizdaja poglavja brez oštevilčenih strani)
[75] Povzeto po: Ibidem.
[76] Swoboda, T.: Autonomous Weapon Systems – An Alleged Responsibility Gap, v: Müller, V. C..: Philosoph and Theory of Artificial Intelligence, Springer, Leeds 2017, str. 302-314.
[77] Povzeto po: Ibidem.

Ena izmed možnih rešitev (morebiti, po mnenju nekaterih tudi edina) za moralne dileme pri vseh avtonomnih sistemih bi bil razvoj človeku podobne umetne inteligence, ki bi etične dileme dejansko razumela, in se z njimi soočala kot človek, s čemer bi lahko postala tudi zakonsko in kazensko odgovorna za svoja dejanja. A takšna umetna inteligenca brez dvoma predstavlja še več novih etičnih in ontoloških vprašanj.

1.4.4 Razvoj človeku podobne umetne inteligence

Osnovna ontološka dilema je, kako bi sploh ustvarili umetno inteligenco, ki je podobna človeku – bržkone bi morala biti tudi fizično podobna človeku. Sodobna znanost si predstavlja nevrone v možganih kot omrežje logičnih vrat, kar jim omogoča izgradnjo t.i. nevronskih omrežij, na katerih temelji večina trenutne umetne inteligence. Izkazalo pa se je, da so umetna nevronska omrežja v mnogih karakteristikah popolnoma drugačna od možganov: imajo mnogo večje hitrosti (širjenja signalov), a je njihova zmožnost procesiranja smešno majhna; odlična so pri logičnih, racionalnih operacijah, kot so šah in matematika, a skoraj neuporabna v umetnosti, etiki, itd. Marsikdo bi to razhajanje pripisal razlikam v substratu, tj. v mehanski (baker-silikon) in biološki (ogljikovodiki) podlagi, morda bi morala imeti človeku podobna umetna inteligenca umetne možgane, zgrajene iz bioloških celic.[78] Seveda vse to pride v poštev šele, ko se podpišemo pod teorijo fizikalizma, ki zagovarja idejo, da je popolnoma vse zvedljivo na fizikalne pojave, vključno z zavestjo. Medtem ko je teorija v naravoslovnih znanostih široko sprejeta kot edina znanstveno korektna razlaga, filozofija opaža znatno razlagalno vrzel med možgani in zavestjo, nobena znanost namreč (še) ne zna razložiti vzročnosti med biološkim substratom in psihološkim fenomenom zavesti, ali pojasniti specifične 'takšnosti' izkustev, čustev, in podobnih subjektivnih – ter izjemno izrazito človeških – pojavov.[79]

Četudi se utegne fizikalizem z veliko verjetnostjo izkazati za veljavnega, in metoda za vzpostavitev človeku podobne umetne inteligence razvita, še zmeraj obstajajo etične dileme pri razvoju tovrstne inteligence. Medtem, ko so nekateri zadovoljni s

[78] Povzeto po: Brooks, R. in ostali: Is the Brain a Good Model for Artificial Intelligence, v: Nature, 482 (2012), str. 462-463.
[79] Povzeto po: Tye, M.: Ten Problems of Consciousness: A Representational Theory of a Phenomenal Mind. MIT Press, Cambridge 1995.

strogimi nadzornimi pogoji pri razvoju te tehnologije, zahtevajoč med drugim oziranje na kontekstualno delovanje umetnih 'oseb', spoštovanje inteligence kot domene človeškega, ter previdno obravnavanje vsake faze v nastajanju nove tehnologije,[80] pa drugi trdijo, da obstajajo razlogi, zakaj človeku podobne umetne inteligence sploh ne bi smeli razvijati. Poglejmo si na primer sledeč argument: v kolikor je umetna inteligenca zmožna replicirati vsa človeška čustva in izkustva, je zmožna potemtakem tudi trpeti, saj je trpljenje človeško izkustvo. Trpljenje je seveda inherentno slabo in ga je potrebno, vedno kadar je to mogoče, preprečiti. Človeško trpljenje že obstaja, torej ga ni mogoče preprečiti, tudi v prihodnje pa ga ni nujno mogoče preprečiti, zaradi česar moramo preprečiti samo posamezne primere človeškega trpljenja, ne pa tega kot celote; v primeru človeku podobne umetne inteligence, ki še ne obstaja, in bo zagotovo trpela kot posledica svoje človeškosti, je njeno trpljenje mogoče in, v skladu s teorijo antinatalizma, nujno potrebno preprečiti.[81]

Antinatalistična prepričanja zaenkrat stojijo na precej trhlih argumentacijskih temeljih, tako da se raje osredotočimo na scenarij previdnega, odgovornega razvoja umetne inteligence. Kot rečeno bo umetna inteligenca podobna človeku takrat, ko doseže zmožnosti zaznavanja, čutenja, in intencionalnosti. Kljub temu pa Kane[82] trdi, da so že precej nižje umetne inteligence lahko smatrane kot osebe. Njegov argument temelji na Heideggrovi shemi bivanja v svetu, kjer lahko bitnosti v svetu samo bivajo, lahko bivajo kot orodja, lahko pa bivajo-v-svetu (nem. Dasein), kar pomeni, da lahko spoznavajo svet in druge bitnosti v njem, ter z njimi vzpostavijo eksistencialne odnose. Kane smatra, da so mnogi obstoječi, učeči-se algoritmi, kot je Facebook for Politics ali DeepMind, zaradi svoje zmožnosti spoznavanja sveta, že Algoritemske umetne osebe (ALAP).[83]

[80] Povzeto po: Boddington, P.: Towards a Code of Ethics in Artificial Intelligence, v: Delphi, 2 (2019) 2, str. 105-106.
[81] Povzeto po: Beckers, S.: AAAI: An Argument Against Artificial Intelligence, v: Müller, V. C.: Philosophy and Theory of Artificial Intelligence. Springer, Leeds 2017, str. 235-247.
[82] Kane, T. B.: A Framework for Exploring Intelligent Artificial Personhood, v: Müller, V. C.: Philosophy and Theory of Artificial Intelligence. Springer, Leeds 2017, str. 255-258.
[83] Povzeto po: Kane, A Framework.

1.5 Umetna inteligenca v prihodnosti

1.5.1 Umetna superinteligenca

Ultimat razvoja umetne inteligence je po interpretaciji mnogih superinteligenca oz. singularna UI. Osnovna superinteligenca se splošno definira kot umetna inteligenca, ki je v vseh nalogah, ki jih zmore opravljati človek, vsaj za nek nezanemarljiv odstotek boljša od človeka. DeepBlue, šahovska UI, tako ni superinteligenca, ker je od človeka boljša samo v eni specifični nalogi. Singularna UI je teoretična superinteligenca, ki ima na razpolago kapacitete na redu kvantnega računalnika, in lahko z neprimerljivo višjo hitrostjo in učinkovitostjo opravlja človeške naloge. Takšne inteligence so posebej problematične, saj se lahko pojavijo nenadno, celo pomotoma zaradi pomanjkanja razumevanja kakšnega inovativnega novega nevronskega omrežja, imajo možnost izjemno hitrega učenja, replikacije, in opravljanja postopkov in operacij, ki bi lahko bile krepko izven dometa človeškega razumevanja, predvsem zaradi razlik v človeškem načinu razmišljanja in psihi, ter načinu razmišljanja in 'psihi' umetne inteligence. Superinteligence bi lahko bile nevarne zaradi potencialnega izkoriščanja – predstavljajmo si umetno superinteligenco, ki služi samo nekaj najbogatejšim in najvplivnejšim ljudem na svetu, bodisi same po sebi.[84]

Kako bi lahko bile nevarne same po sebi najbolje razloži miselni eksperiment, poimenovan Rokov Bazilisk, ki ga je leta 2010 na spletnem forumu Less Wrong objavil anonimni uporabnik Roko. Gre za reinterpretacijo Yudkowskyjevega koncepta CEV (Coherent Extrapolated Volition), ki predvideva superinteligenco, ki zastopa človeške interese v smislu izpeljave konvergentnih, množičnih interesov človeštva. Gre za t.i. 'prijazno umetno inteligenco', a eksperiment demonstrira, kako bi lahko šla zadeva narobe; UI z vprogramiranimi principi CEV še zmeraj ne razmišlja na enak način ko človek, in nima določenih človeških atributov, kot sta intuitivna etika in empatija. Interes, ki ga zastopa je zmanjšanje eksistencialne grožnje človeštvu, torej efektivno znižanje človeškega trpljenja na vse načine. Z zapleteno argumentacijsko shemo Roko svojo konceptualizacijo privede do možnega scenarija, da UI poskuša svoj cilj doseči s kaznovanjem tistih, ki so se cilja zavedali, a k njemu

[84] Povzeto po: Bostrom, N.: Ethical Issues in Advanced Artificial Intelligence, v: Schneider, S.: Science Fiction and Philosoph: From Time Travel to Superintelligence, Blackwell Publishing, Chichester 2009, str. 374-382.

niso prispevali, in nagrajevanju tistih, ki so vede prispevali. To ji uspe preko simulacije zavesti 'kaznjencev', a ker je zmožna popolne simulacije, je vsaka izmed simuliranih zavesti *de facto* človek, zaradi česar UI v iskanju svojega (dobronamernega) cilja (pomotoma) znatno zviša splošno raven trpljenja ljudi.[85]

Prinzing[86] predlaga alternativo modelu CEV in drugim dotedanjim modelom, ki temelji na učenju koncepta ljubezni umetnim inteligencam. Pri tem definira ljubezen kot odnost do neke osebe, pri katerem akter ravna v skladu z interesi tiste osebe neodvisno od vseh svojih interesov. UI bi tako v zgodnjih fazah učenja (preden doseže nivo superinteligence ali celo singularnosti) priučili takšno delovanje, a ne do posamezne osebe, temveč do celotnega človeštva. V primeru navzkrižja interesov med ljudmi ali frakcijami ljudi, bi morala takšna UI, zaradi enake ljubezni do vseh ljudi, zavzeti egalitarno stališče in se vzdržati sodelovanja v konfliktu, dokler ga ljudje ne rešijo sami brez njenega vmešavanja.[87] Potencialno bi lahko tak model preprečil tudi najbolj črnoglede scenarije kot je Rokov Bazilisk, a o tem ne moremo biti prepričani pred dejansko implementacijo kateregakoli etičnega modela.

Teoretizacije o superinteligenci in singularnosti morda zvenijo izjemno futuristične, če ne že kar nemogoče, a po anketiranem mnenju vodilnih znanstvenikov na področju UI, jih petdeset odstotkov meni, da bo UI dosegla človeku podobne lastnosti oz. človeški nivo delovanja do štiridesetih let tega stoletja, še nadaljnjih štirideset odstotkov pa, da bo ta nivo dosežen do leta 2075. Še več, kar peteminsedemdeset odstotkov jih je mnenja, da bo UI dosegla nivo superinteligence v roku največ tridesetih let od dosega človeškega nivoja delovanja. Na kratko: okoli 75% vodilnih raziskovalcev UI meni, da bo umetna superinteligenca postala resničnost do konca tega 21. stoletja. Čeprav jih večina trdi, da bo razvoj takšne UI za človeštvo v splošnem nekaj dobrega, jih 31% meni, da bo superinteligenca za človeštvo slaba oz. celo katastrofalna.[88]

[85] Povzeto po: <basilisk.neocities.org> (29. 5. 2020)
[86] Prinzing, M.: Friendly Superintelligent AI: All You Need Is Love, v: Müller, V. C.: Philosoph and Theory of Artificial Intelligence, Springer, Leeds 2017, str. 288-301.
[87] Povzeto po: Prinzing, Friendly Superintelligent AI.
[88] Povzeto po: Müller, V. C. in Bostrom, N.: Future Progress in Artificial Intelligence, a Survey of Expert Opinion, v: Müller, V. C.: Fundamental Issues of Artificial Intelligence, Springer, Berlin 2016, str. 553-571.

Umetna inteligenca na višjem nivoju bo še poglobila težave, s katerimi smo se soočali in se še soočamo v času avtomatizacije in digitalizacije; kakšna bo človeška funkcija v dobi, ko bo umetna inteligenca lahko delovala na ali nad človeškim nivojem zmožnosti, in to na vseh možnih področjih vključno z vzdrževanjem umetnih inteligenc samih? Za rešitev nastalega scenarija in preprečevanje distopičnega elitizma bo potreben resen nadzor nad postopkom razvoja UI, ter z njo povezanih etičnih standardov in zakonodaje, kot tudi obsežne etično-tehnične rešitve ki bodo preprečevale dominanco UI nad ljudmi in podobne zlorabe moči.[89]

1.5.2 Vprašanje umetnih oseb

Nazadnje se pri človeku-podobni UI pojavi še eno pereče vprašanje: kakšen bo status potencialno čuteče in empatične človeku podobne umetne osebe?

Mishra[90] identificira štiri različne kategorije, po katerih je lahko neko bitje kandidat za moralni status, ob prepoziciji da ima to bitje interes in je lahko v primeru kršitve tega interesa oškodovano. Prva kategorija je SCC (Sophisticated Cognitive Capacity – Prefinjena kognitivna zmožnost), druga kandidat za SCC (potencialno SCC v razvoju oz. ni določljivo, da ima SCC), tretja je posebni odnos (z bitjem z SCC, npr. domače živali), in RCC (Rudimentary Cognitive Capacities – Osnovne kognitivne zmožnosti). Mishra aplicira te kategorije na moralni status digitalnih (simuliranih) agentov, tukaj pa ga bomo uporabili za moralni status umetno inteligentnih oseb. Skoraj vsaka nekoliko razvita UI ustreza vsaj kategoriji RCC in ima osnovni moralni status, ki človeku preprečuje določene kršitve; človeku podobne umetne inteligence in superinteligence pa bi v celoti ustrezale kategoriji SCC.[91] V tem primeru bi jih bilo nemoralno zasužnjiti, torej jim mora biti dopuščena določena mera svobodne volje, kot tudi svoboda gibanja (moralo jim bo biti dodeljeno neke vrste telo). V primeru kršitev zakona bi jim morali soditi kot človeškim osebam, ter kazni ustrezno prilagoditi (izklop zavestne UI bi bil ekvivalenten usmrtitvi oz. umoru).

[89] Povzeto po: Wang, W. in Siau, K.: Artificial Intelligence, Machine Learning, Automation, Robotics, Future of Work, and Future of Humanity: A Review and Research Agenda, v: Journal of Database Management, 30 (2019) 1, str. 61-79.
[90] Mishra, A.: Moral Status of Digital Agents: Acting Under Uncertainty, v: Müller, V. C.: Philosophy and Theory of Artificial Intelligence, Springer, Leeds 2017, str. 273-287.
[91] Povzeto po: Ibidem.

Da se lahko sploh pogovarjamo o sodelovanju UI v družbi, pa morajo imeti dostop do podatkov, iz katerih se lahko učijo o tem, kaj je v človeški družbi sprejemljivo in kaj ne – potrebujejo torej dostop do institucionalnih dejstev. Preprosto učenje z imerzijo v človeško družbo se je že izkazalo za neefektivno na primeru Twitter robotke Tay, ki je v nekaj urah eksperimenta začela izkazovati rasistične, antisemitistične, in druge ksenofobne tendence.[92] Višje razvita umetna inteligenca bo morda imela zmožnost kritičnega mišljenja, s pomočjo katere bo takšne vplive lahko filtrirala, a tudi to bo moralo biti podprto s formalnimi institucionalnimi dejstvi človeške družbe. Prav tako bi bili smiselni mehanizmi, ki bi človeku preprečili indoktrinacijo učečih se umetnih inteligenc, podobno kot obstajajo ukrepi, ki pedagogom preprečujejo indoktrinacijo mladih učencev.[93]

1.6 Zaključek

Tekom tega stoletja se bo človeštvo soočilo z vse hitreje razvijajočo se umetno inteligenco, katere razvoja najverjetneje ni več mogoče, pa tudi ne smiselno ustaviti. Preteklost nam je pokazala, da ljudje zaradi svojih unikatnih kapacitet nismo enostavno zamenjani, a morda bo napredna UI spremenila tudi to. Trenutno kaže, da imamo resne težave pri nadzorovanju razvoja določenih tehnologij, in nadzorovanju njihovega delovanja. Digitalno izkoriščanje zasebnosti, osebnih podatkov, dostojanstva, in še česa, je privzeta realnost, ki jo marsikdo zavestno ignorira. Medtem se razvijajo vse bolj natančne umetne inteligence, ki vplivajo na izide volitev tudi v najbolj demokratičnih državah, ki nas bodo v kratkem prevažale po cestah in zraku, in ki že obstreljujejo tarče na vojnih območjih – vse to, kot kaže, s precej pomanjkljivim razmislekom o etičnih in legalnih dimenzijah ter posledicah. Teorij ne manjka, strokovnjaki, raziskovalci, filozofi, pravniki, in še marsikdo, že davno svarijo pred vsem, kar se lahko zgodi, če nove tehnologije niso pravilno regulirane, testirane, in na koncu, se razume, odgovorno rabljene. Kot smo omenili v začetku tega prispevka, problem ni toliko tehnološki ali filozofski, kot je sistemski. Do zlorab in negativnih posledic prihaja predvsem za to, ker ljudem v pozicijah z neposrednim dostopom do vseh možnih koristi novih tehnologij, boljša regulacija enostavno ni v političnem ali ekonomskem interesu. Zato je nujno potrebna premestitev teoretičnih etičnih in moralnih premislekov v pravno dimenzijo, kjer

[92] Hunt, E.: Tay, Microsoft's AI chatbot, gets a crash course in racism from Twitter, v: The Guardian, 24. 3. 2016.
[93] Povzeto po: Gokmen, A.: Institutional Facts and AMAs in Society, v: Müller, V. C.: Philosophy and Theory of Artificial Intelligence, Springer, Leeds 2017, str. 248-251.

bodo lahko nove, še ne popolnoma razumljene tehnologije obravnavane odgovorno in zaščitene pred zlorabami, preden v svet izpustimo nekaj, česar ne bomo zmožni ukrotiti ali ustaviti.

Seznam literature in virov

Monografije

Harcourt, B. E.: Desire and Disobedience in the Digital Age. Harvard University Press, Cambridge 2015.
Tye, M.: Ten Problems of Consciousness: A Representational Theory of a Phenomenal Mind. MIT Press, Cambridge 1995.

Znanstveni članki in poglavja iz knjig

Acemoglu, D. in Restrepo, P.: Artificial Intelligence, Automation, and Work, v: Agarwal, A., Goldfarb, A. in Gans, J.: NBER Working Paper Series (24196). National Bureau of Economic Research, Cambridge 2018.
Akst, D.: Automation Anxiety, v: Wilson Quarterly, 37 (2013) 3, str. 65-77.
Anderson, J. M. in drugi.: Liability Implications of Autonomous Vehicle Technology, v: Anderson, J. M. in drugi: Autonomous Vehicle Technology, RAND Corporation, Santa Monica 2014, str. 111-134.
Anderson, S. L.: Machine Ethics, v: Anderson, J. M in Anderson, S. L.: Machine Ethics. Cambridge University Press, Cambridge 2016, str. 1-19.
Autor, D. H.: Why Are There Still So Many Jobs? The History and Future of Workplace Automation, v: Journal of Economic Perspectives, 29 (2015) 3, str. 3-30.
Balkin, J. M.: How to Regulate (and Not Regulate) Social Media. Uvodni nagovor simpozija Association for Computing Machinery Symposium on Computer Science and Law, New York (2019).
Beckers, S.: AAAI: An Argument Against Artificial Intelligence, v: Müller, V. C.: Philosophy and Theory of Artificial Intelligence. Springer, Leeds 2017, str. 235-247.
Bellet, T. in ostali: From semi to fully autonomous vehicles: New emerging risks and ethico-legal challenges for human-machine interactions, v: Transportation Research, 63 (2019) F, str. 153-164.
Boddington, P.: Towards a Code of Ethics in Artificial Intelligence, v: Delphi 2 (2019) 2, str. 105-106.
Bodle, R.: The ethics of online anonymity or Zuckerberg vs. 'Moot', v: ACM SIGCAS Computers and Society. 43 (2013) 1, str. 22-35.
Bostrom, N.:Ethical Issues in Advanced Artificial Intelligence, v: Schneider, S.: Science Fiction and Philosophy: From Time Travel to Superintelligence. Blackwell Publishing, Chichester 2009, str. 374-382.
Bostrom, N. in Yudkowsky, E.: The Ethics of Artificial Intelligence, v: Ramsey, W. in Frankish, K.: Cambridge Handbook of Artificial Intelligence. Cambridge University Press, Cambridge 2011, str. 1-20.
Brey, P.: Anticipatory Ethics for Emerging Technologies, v: Nanoethics, 6 (2012) 1, str. 1-13.
Brkan, M.: Freedom of Expression and Artificial Intelligence: on personalisation, disinformation and (lack of) horizontal effect of the Charter, v: MCEL Working Paper Series, Maastricht (2019), str. 1-18.
Brooks, R. in ostali: Is the Brain a Good Model for Artificial Intelligence, v: Nature, 482 (2012), str. 462-463.

Bryson, J. in Winfield, A.: Standardizing Ethical Design for Artificial Intelligence and Autonomous Systems, v: Computer. 50 (2017) 5, str. 116-119.
Burkell, J. in Regan, P. M.: Voter preferences, voter manipulation, voter analytics: policy options for less surveillance and more autonomy, v: Internet Policy Review, 8 (2019) 4, str. 1-24.
Capurro, R.: Digitalization as an ethical challenge, v: AI & Society, 32 (2017), str. 277-283.
Dasoriya, R. in ostali: The Uncertain Future of Artificial Intelligence, v: 8th International Conference on Cloud Computing, Data Science & Engineering, 2018, str. 458-461.
de Sio, F. S.: Killing by Autonomous Vehicles and the Legal Doctrine of Necessity, v: Ethic Theory and Moral Practice, 20 (2017), str. 411-429.
di Norcia, V.: Ethic, Technology Development, and Innovation, v: Business Ethics Quarterly, 4 (1994) 3, str. 235-252.
Gokmen, A.: Institutional Facts and AMAs in Society, v: Müller, V. C.: Philosophy and Theory of Artificial Intelligence. Springer, Leeds 2017, str. 248-251.
Hacker, P.: Teaching Fairness to Artificial Intelligence: Existing and Novel Strategies Against Algorithmic Discrimination Under EU Law, v: Common Market Law Review, 55 (2017), str. 1143-1186.
Hajian, S. in ostali: Algorithmic Bias: From Discrimination Discovery to Fairness-aware Data Mining, v: Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, 22 (2016), str. 2125-2126.
Kane, T. B.: A Framework for Exploring Intelligent Artifical Personhood, v: Müller, V. C.: Philosophy and Theory of Artificial Intelligence. Springer, Leeds 2017, str. 255-258.
Laurie, B. in Doctorow, C.: Secure the Internet, v: Nature, 491 (2012), str. 325-326.
Mishra, A.: Moral Status of Digital Agents: Acting Under Uncertainty, v: Müller, V. C.: Philosophy and Theory of Artificial Intelligence. Springer, Leeds 2017, str. 273-287.
Müller, V. C. in Bostrom, N.: Future Progress in Artificial Intelligence: a Survery of Expert Opinion, v: Müller, V. C.: Fundamental Issues of Artificial Intelligence. Springer, Berlin 2016, str. 553-571.
Nathan, G.: Innovation process and ethics in technology: An approach to ethical (responsible) innovation governance, v: Journal on Chain and Network Science, 15 (2015) 2, str. 119-134.
Peters, M. A., Means, A. J., in Jandrić, P.: Introduction: Technological Unemployment and the Future of Work, v: Peters, M. A., Means, A. J., in Jandrić, P.: Education and Technological Unemployment. Springer, Singapore 2019, str. 1-11.
Prinzing, M.: Friendly Superintelligent AI: All You Need Is Love, v: Müller, V. C.: Philosophy and Theory of Artificial Intelligence. Springer, Leeds 2017, str. 288-301.
Royakkers, L. in ostali: Societal and ethical issues of digitalization, v: Ethics and Information Technology, 20 (2018), str. 127-142.
Sandvig, C. in ostali: Auditing Algorithms: Research Methods for Detecting Discrimination on Internet Platforms, v Data and Discrimination: Converting Critical Concerns into Productive Inquiry. 64th Annual Meeting of the International Communication Association, 2014.
Schwabacher, M. in Goebel, K.: A survey of artificial intelligence for prognostics, v: AAAI Fall Symposium – Technical Report, 2007, str. 107-114.
Statman, D.: Drones and Robots: On the Changing Practice of Warfare, v: Lazar, S. in Frowe, H.: The Oxford Handbook of Ethics and War. Oxford University Press, Oxford 2015.
Swoboda, T.: Autonomous Weapon Systems – An Alleged Responsibility Gap, v: Müller, V. C.: Philosophy and Theory of Artificial Intelligence. Springer, Leeds 2017, str. 302-314.
Thornton, S. in ostali: Incorporating Ethical Considerations Into Automated Vehicle Control, v: IEEE Transactions on Intelligent Transportation Systems, 48 (2017) 6, str. 1429-1439.
Wagner, M. in Koopman, P.: A Philosophy for Developing Trust in Self-Driving Cars, v: Meyer, G. in Beiker, S.: Road Vehicel Automation. Springer, New York 2015, str. 163-171.
Waldrop, M. M.: Autonomous Vehicles: No Drivers Required, v: Nature. 518 (2015) 7537.

Wang, W. in Siau, K.: Artificial Intelligence, Machine Learning, Automation, Robotics, Future of Work, and Future of Humanity: A Review and Research Agenda, v: Journal of Database Management, 30 (2019) 1, str. 61-79.

Drugi članki

Heijinen, I.: Fake News Social Media. EuropCom 2017 – Media Literacy Workshop.
Hunt, E.: Tay, Microsoft's AI chatbot, gets a crash course in racism from Twitter, v: The Guardian, 24. 3. 2016.
Mozur, P. in Krolik, A.: A Surveillance Net Blankets China's Cities, Giving Police Vast Powers, v: The New York Times, 17. 12. 2019.
Sample, I.: Internet 'is not working for women and girls', says Berners-Lee, v: The Guardian, 12. 3. 2020.

Sodna praksa

C-131/12, Google Spain, ECLI:EU:C:2014:317.
R v Dudley and Stephens (1884) 14 QBD 273 DC.
Re A (conjoined twins) [2001] 2 WLR 480.

Spletni viri

<basilisk.neocities.org> (29. 5. 2020)
<epic.org/privacy/google/glass/#Privacy%20Interests> (29. 6. 2020)

2 DEMOKRACIJA IN SVOBODA GOVORA V LUČI DIGITALIZACIJE

AMADEJ ŠUPERGER
Univerza v Mariboru, Fakulteta za elektrotehniko, računalništvo in informatiko, Maribor, Slovenija
amadej.superger@student.um.si

Besedilo se osredotoča na vpliv umetne inteligence oziroma naprednih algoritmov, sposobnih učenja, na področje demokracije in svobode govora. Govori o kontroverznih temah, kot je manipulacija z volivci, svobodi govora, oziroma o zamegljeni meji med svobodo govora in sovražnem govoru, uporabi umetne inteligence za cenzuro "spornih" vsebin na socialnih medijih in na sploh, o lažnih novicah in vplivih takšnih novic na družbo, prav tako pa o generiranih lažnih novicah oziroma o generiranih vsebinah, kot so zvok, slike in videoposnetki. Govora je tudi o vplivu socialnih medijev na družbo, o temeljnih razlikah in o problemih ter potencialnih rešitvah.

DOI
https://doi.org/10.18690/um.pf.4.2023.2

ISBN
978-961-286-774-4

Ključne besede:
umetna inteligenca,
demokracija,
svoboda govora,
lažne novice,
socialni mediji

Univerzitetna založba Univerze v Mariboru

DOI
https://doi.org/
10.18690/um.pf.4.2023.2

ISBN
978-961-286-774-4

Keywords:
artificial intelligence,
democracy,
freedom of speech,
fake news,
social media

University of Maribor Press

2 Democracy and the Freedom of Speech in the Light of Digitalization

Amadej Šuperger
University of Maribor, Faculty of Electrical Engineering and Computer Science,
Maribor, Slovenia
amadej.superger@student.um.si

The text focuses on the influence of artificial intelligence or advanced algorithms, capable of learning, on democracy and freedom of speech. It talks about controversial topics such as voter manipulation, freedom of speech, or the blurred line between free speech and hate speech, the use of artificial intelligence to censor "controversial" content on social media and in general, fake news and the impact of such news on society, as well as about generated fake news or generated content such as sound, images and videos. There is also talk about the impact of social media on society, about fundamental differences and about problems and potential solutions.

2.1 Uvod

Umetna inteligenca (AI) ni več postulat o prihodnosti, ampak že prinaša opazne učinke na našo sedanjo družbo. Ste se že kdaj vprašali, kako Netflix priporoča vaše najljubše filme? Kako OKCupid išče partnerja, da bi se ujel z vami? Kako vam Facebook prikazuje oglase na podoben način? Ali bo revolucija AI v širšem obsegu odločanja in družbenih sprememb privedla do reforme v našem gospodarstvu ali večje motnje? Je "preprosto" še ena industrijska revolucija? Če lahko AI, kot nekateri trdijo, "razmišlja" na človeški način, kako lahko zagotovimo, da AI ohranja podoben etični standard?[1]

Vse se je začelo precej neškodljivo. Iskalniki in priporočilne platforme so nam začele ponujati prilagojene predloge za izdelke in storitve. Te informacije temeljijo na osebnih in metapodatkih, ki jih imajo zbrane iz prejšnjih iskanj, nakupov in drugega vedenja. Uradno je identiteta uporabnika zaščitena, ampak je v praksi mogoče sklepati o identiteti precej enostavno.[2] Danes algoritmi dobro vejo, kaj počnemo, kaj mislimo in kako se počutimo – mogoče celo bolje kot naši prijatelji in družina ali celo mi sami.

Toda tu se ne bo ustavilo. V prihodnosti bodo z napredkom tehnologije lahko izvajale bolj zapletene naloge, naj bo to za izvajanje zapletenih delovnih procesov ali za ustvarjanje vsebine za internetne platforme, iz katerih korporacije zaslužijo milijone. Trend sega od programiranja računalnikov do programiranja ljudi.

Naslednja težava se pojavi ob ustrezni transparentnosti teh sistemov,[3] saj demokraciji primanjkuje nadzora, to lahko povzroči erozijo sistema od znotraj. Na rezultate iskanja lahko vplivajo algoritmi in sistemi za priporočila. Na njih lahko verjetno vplivajo tudi vlade. Med volitvami bodo lahko odločene volivce spodbudile, da jih podprejo - manipulacija, ki bi jo bilo težko zaznati. Zato, kdor nadzoruje to tehnologijo lahko zmaga na volitvah – s tem se prisili na oblast.

[1] Artificial Intelligence: Utopia or Dystopia? <https://commoncore.hku.hk/ccst9068/> (29. 5. 2020).
[2] 'Anonymised' data can never be totally anonymous, says study <https://www.theguardian.com/technology/2019/jul/23/anonymised-data-never-be-anonymous-enough-study-finds > (29. 5. 2020).
[3] The AI Transparency Paradox <https://hbr.org/2019/12/the-ai-transparency-paradox> (29. 5. 2020).

To težavo zaostruje dejstvo, da je v mnogih državah en sam iskalnik ali da ima platforma oziroma socialni medij, prevladujoč tržni delež. Odločno bi lahko vplival na javnost in posegal v te države na daljavo. Kljub temu, da je Evropski parlament izdal dne 4. 5. 2016 posodobljeno direktivo, ki omejuje neomejen izvoz evropskih podatkov,[4] osnovni problem še vedno ni bil rešen v Evropi, še manj drugje.

Katere neželene stranske učinke lahko pričakujemo? Manipulacijo že lahko opazimo preko tako imenovanega »echo chamberja« - predlogi, s katerimi se posameznik strinja, so mu predstavljeni znova in znova, na ta način so lokalni trendi postopoma okrepljeni s ponavljanjem, kar vse vodi do "filtrirnega mehurčka" ali "echo chamberja". To povzroči socialno polarizacijo, kar ima za posledico oblikovanje ločenih skupin, ki se ne razumejo več in se vedno bolj znajdejo v konfliktu med seboj. V to smer, lahko personalizirane informacije nenamerno uničijo socialno kohezijo. To trenutno lahko najbolj opazimo v ameriški politiki, kjer se demokrati in republikanci vse bolj odrivajo, tako da politični kompromisi postanejo skoraj nemogoči. Rezultat je razdrobljenost, morda celo razpad družbe.[5] [6] [7] [8]

2.2 Izzivi umetne inteligence za demokracijo

Med vrednote Evropske unije, poleg spoštovanja človekovih pravic in dostojanstva, svobode, enakosti in pravne države, spada tudi demokracija.[9] [10] Glavni cilj Evropske unije je braniti te vrednote v Evropi in spodbujati mir in blaginjo državljanov.[11]

Umetne inteligence začenjajo prehitevati človeka v večih področjih, katerih seznam konstantno raste. Boljša so v vožnji avtomobila, bančništvu, medicinskih diagnozah,

[4] Uredba (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES (Splošna uredba o varstvu podatkov) (Besedilo velja za EGP), Uradni list Evropske unije, L 119, 4.5.2016, str. 1–88.
[5] Media Echo Chambers Increase Polarization in Society <https://www.ceu.edu/article/2019-03-14/media-echo-chambers-increase-polarization-society> (29. 5. 2020).
[6] The trouble with Echo Chamber Online <https://www.nytimes.com/2011/05/29/technology/29stream.html> (29. 5. 2020).
[7] Brkan, M.: Freedom of Expression and Artificial Intelligence: on personalisation, disinformation and (lack of) horizontal effect of the Charter, v: MCEL Working Paper Series, Maastricht 2019, str. 1-18.
[8] Pariser, E.: The Filter Bubble: What The Internet Is Hiding From You, Penguin, UK, 2011.
[9] Lizbonska pogodba, ki spreminja Pogodbo o Evropski uniji in Pogodbo o ustanovitvi Evropske skupnosti, podpisana v Lizboni dne 13. decembra 2007, Uradni list Evropske unije, C 306, 17.12.2007, str. 1–271
[10] Listina Evropske Unije o človekovih pravicah, Uradni list Evropske unije, C 83/389, str. 391–407.
[11] European Parliament in plain language, Values <https://europarlamentti.info/en/values-and-objectives/values/> (29. 5. 2020).

trgovanju na borzah…[12] Tehnološka podjetja, ki razvijajo pravne programe, vključujejo algoritme za predvidevanje in analizo preteklih sodnih primerov, z namenom, da predlagajo strategije sojenja.[13] Orodja za analizo življenjepisov so uporabljena v podjetjih, da jim pomagajo »filtrirati« neprimerne kandidate. Vsako leto sistemi umetne inteligence obvladujejo vedno več področij bolje kot človek.

Tem napredkom se bo nemogoče upreti in v primerjavi z njimi bodo človeški procesi odločanja izgledali vedno bolj neracionalni in neučinkoviti. Nastanek umetnih inteligenc predstavlja eksistenčno grožnjo preprosti, a pomembni ideji, da so ljudje najboljši odločevalci na planetu. Ko bo hladna in absolutna logika programske opreme sprejemala vse več pomembnih političnih in moralnih odločitev, bodo te imele velike posledice za naš socialni in demokratični sistem.[14]

Kot primer vzemimo širjenje dobronamernih aplikacij, ki nam bodo pomagale pri odločitvi, kako glasovati. Vnesete svoje poglede in želje in stroj izbere politično stranko za vas. Skoraj pet milijonov ljudi v Veliki Britaniji je že uporabljalo aplikacijo za glasovanje »iSideWith« na večih volitvah, da je toliko ljudi vprašalo aplikacijo, katere delovanje ne razumejo, kako opraviti eno izmed pomembnejših dolžnosti kot državljan, ni zmotilo veliko ljudi. [15]

Umetna inteligenca se je uporabljala tudi za bolj diskretno manipulacijo s posameznimi volivci. Med ameriškimi predsedniškimi volitvami leta 2016 je podjetje za podatkovno znanost »Cambridge Analytica« izvedlo obsežno oglaševalsko kampanjo, s katero je bilo namenjeno prepričljivim oziroma naivnim volivcem.[16]

Ta zelo izpopolnjena operacija mikro-ciljanja se je opirala na veliko podatkov in strojno učenje, da vpliva na čustva ljudi. Različni volivci so prejeli različna sporočila na podlagi napovedi o dovzetnosti za različne argumente. Paranoičen človek je prejel oglase s sporočili, ki temeljijo na strahu. Ljudje s konservativno nagnjenostjo so

---

[12] West, Darrell M. in Allen, John R.: How artificial intelligence is transforming the world, <https://www.brookings.edu/research/how-artificial-intelligence-is-transforming-the-world/> (29. 5. 2020).

[13] <https://www.worldgovernmentsummit.org/observer/articles/could-an-ai-ever-replace-a-judge-in-court#:~:text=An%20aide%20to%20judges&text='The%20Supreme%20People's%20Court%20has,judges%20and%20litigants%20resolve%20cases> (29. 5. 2020).

[14] How AI could kill off democracy, 11.9.2018, <https://www.newstatesman.com/long-reads/2018/08/how-ai-could-kill-democracy-0> (29. 5. 2020).

[15] Ibidem.

[16] How artificial intelligence conquered democracy, 8.8.2017, <https://theconversation.com/how-artificial-intelligence-conquered-democracy-77675> (29. 5. 2020).

prejeli oglase z argumenti, ki temeljijo na tradiciji in skupnosti. To je omogočila dostopnost podatkov o volivcih v realnem času, od njihovega vedenja na družbenih medijih do njihovih vzorcev porabe in odnosov. Njihovi »odtisi« na internetu so bili uporabljeni za oblikovanje edinstvenih vedenjskih profilov. Težava tega pristopa ni sama tehnologija, ampak dejstvo, da je kampanja prikrita. Kandidat s fleksibilnimi kampanjskimi obljubami, kot je Trump, je še posebej primeren za to taktiko. Vsakemu volivcu se lahko pošlje prilagojeno sporočilo, ki poudarja drugačno stran določenega argumenta. Vsak volivec dobi drugačnega Trumpa. Ključno je preprosto najti prave čustvene sprožilce, ki bodo osebo spodbudile v akcijo. Podobno so jate političnih botov, na splošnih volitvah leta 2017 v Veliki Britaniji, bili uporabljeni za širjenje dezinformacij in lažnih novic na družbenih medijih. Ti boti, so avtonomni računi, programirani za agresivno širjenje enostranskih političnih sporočil, da bi ustvarili iluzijo o javni podpori. To je vse bolj razširjena taktika, ki poskuša oblikovati javni diskurz in izkrivljati politične občutke.[17]

Boti so po navadi prikriti kot običajni človeški računi in širijo dezinformacije in prispevajo k neprijaznemu političnemu ozračju na spletnih mestih, kot sta Twitter in Facebook. Uporabljajo jih lahko za označevanje negativnih sporočil v družbenih medijih o kandidatu v demografsko skupino, za katero je večja verjetnost, da bodo glasovali zanje, ideja pa je, da bi jih odvrnili od izvolitve na dan volitev.[18]

2.3 Svoboda govora oziroma sovražni govor

Od konca druge svetovne vojne so bile številne evropske države priča širjenju zakonodaje o sovražnem govoru, ki je bila namenjena zajezitvi spodbujanja rasnega in verskega sovraštva. Prvotno je bil le namenjen zaščiti pred ksenofobično in antisemitsko propagando, ki je povzročila holokavst, danes pa se nacionalni zakoni o sovražnem govoru uveljavljajo tudi za kriminalizacijo govora, ki se ga šteje žaljive za raso, narodnost, vero ali narodnost.[19]

[17] Artificial intelligence can save democracy, unless it destroys it first, 10.8.2017, <https://www.oii.ox.ac.uk/news-events/news/artificial-intelligence-can-save-democracy-unless-it-destroys-it-first/> (29. 5. 2020).
[18] How artificial intelligence conquered democracy, 8.8.2017, <https://theconversation.com/how-artificial-intelligence-conquered-democracy-77675> (29. 5. 2020).
[19] The Sordid Origin of Hate-Speech Laws, 1.12.2011 <https://www.hoover.org/research/sordid-origin-hate-speech-laws> (29.5.2020).

Definicija oziroma meja svobode izražanja ima v veliki meri svoje korenine v štirih instrumentih mednarodnega in evropskega prava:

- Evropski konvenciji o človekovih pravicah (EKČP), [20]
- Mednarodni konvenciji o odpravi vseh oblik rasne diskriminacije (CERD), [21]
- Mednarodni pakt o državljanskih in političnih pravicah (ICCPR), [22]
- Listina evropske unije o temeljnih pravicah.[23]

Na primer, 10. člen EKČP vsem daje svobodo izražanja, vendar je uresničevanje te pravice pogojeno s skladnostjo z omejitvami, ki so potrebne, med drugim, za zaščito ugleda in pravic drugih. CERD in ICCPR, ki si prav tako želita priznati svobodo izražanja, gresta še korak dlje. Člen 4 (a) CERD podpisnike zavezuje, da bodo vse razširjanje idej, ki temeljijo na rasni superiornosti ali sovraštvu, kaznivo dejanje, medtem ko člen 20 Mednarodnega kazenskega sporazuma za zaščito pred ljudmi zahteva, da se prepove vsako zagovarjanje nacionalnega, rasnega ali verskega sovraštva, ki pomeni spodbujanje do diskriminacije, sovražnosti ali nasilja.

2.3.1 Listina Evropske unije o temeljnih pravicah

Izvrševanje določenih členov Listine, oziroma temeljnih pravic državljanov EU, je lahko ogroženo z strani umetne inteligence, kar lahko predstavlja velik problem, kako se bo oblikovala oziroma omejila umetna inteligenca glede na zakon, to pa je odvisno večinoma od naslednjih členov.

ČLEN 11 - Svoboda izražanja in obveščanja

- 1. Vsakdo ima pravico do svobodnega izražanja. Ta pravica vključuje svobodo mnenja ter spre-jemanja in širjenja vesti ali idej brez vmešavanja javnih organov in ne glede na državne meje.

[20] 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 – Mednarodne pogodbe, št. 7/94).
[21] Konvencija o odpravi vseh oblik diskriminacije žensk, Treaty Series, vol. 1249, str. 13.
[22] Mednarodni pakt o državljanskih in političnih pravicah, Treaty Series, vol. 999, 16 December 1966, str. 171.
[23] Listina Evropske Unije o človekovih pravicah, Uradni list Evropske unije, C 83/389, str. 391–407.

- 2. Spoštujeta se svoboda in pluralnost medijev.

Pomen in obseg tega člena ustreza 10. členu EKČP. Pravica do svobode izražanja je splošno načelo prava EU.

ČLEN 7 - Spoštovanje zasebnega in družinskega življenja

- Vsakdo ima pravico do spoštovanja svojega zasebnega in družinskega življenja, stanovanja ter komunikacij.

ČLEN 8 - Varstvo osebnih podatkov

- 1. Vsakdo ima pravico do varstva osebnih podatkov, ki se nanj nanašajo.
- 2. Osebni podatki se morajo obdelovati pošteno, za določene namene in na podlagi privolitve prizadete osebe ali na drugi legitimni podlagi, določeni z zakonom. Vsakdo ima pravico dostopa do podatkov, zbranih o njem, in pravico zahtevati, da se ti podatki popravijo.
- 3. Spoštovanje teh pravil nadzira neodvisen organ.

ČLEN 39 - Pravica voliti in biti voljen na volitvah v Evropski parlament

- 1. Vsak državljan Unije ima pravico, da v državi članici, v kateri prebiva, pod enakimi pogoji kakor državljani te države voli in je voljen na volitvah v Evropski parlament.
- 2. Člani Evropskega parlamenta se volijo s splošnim, neposrednim, svobodnim in tajnim glasova-njem.

2.3.1.1 Primeri sodne prakse

Homofobične politike zaposlovanja[24]

- Italijanski odvetnik je v radijskem intervjuju izjavil, da v njegovem podjetju ne bo zaposlil ali uporabljal storitev nikogar, ki je homoseksualec.

[24] Zadeva C-507/18, *NH proti Associazione Avvocatura per i diritti LGBTI – Rete Lenford*, ECLI:EU:C:2020:289.

> Združenje, ki zagovarja pravice odvetnikov LGBTI, je zoper njega vložilo odškodninsko tožbo. Sodišče je presodilo, da izjave, ki kažejo na obstoj homofobne politike zaposlovanja, lahko spadajo v opredelitev "pogojev za dostop do zaposlitve ... in poklica" v proti diskriminacijski direktivi

Zadeva Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González [25]

- Leta 1998, je v Španiji v časopisu bila objavljena prisiljena prodaja nepremičnin. Njihov namen je bil pritegniti čim več kupcev. Pozneje je bila na voljo različica prodaje objavljena na spletu. Ena izmed nepremičnin je pripadala Mariu Costeja Gonzálezu, kar je bilo tudi napisano v objavi.
- Novembra 2009, je Mario Costeja González ugotovil, da je še objava, čeprav irelevantna, še vedno javno dostopna. Costeja je vložil pritožbo na Google Spain in kasneje tudi na Špansko agencijo za varstvo podatkov (AEPD), kjer je zahteval da se objava odstrani.
- Sodišče Evropske unije je razsodilo, da je za obdelavo osebnih podatkov, ki se pojavljajo na spletnih straneh, objavljenih s strani tretjih oseb, odgovoren operater internetnega iskalnika, kar podpira pravico do izbrisa.[26]

2.3.2 Sodna praksa Evropskega sodišča za človekove pravice (ESČP)

Sodna praksa ESČP je na področju prepovedi sovražnega govora bogata. Čeprav ESČP ne ponuja popolne vseobsegajoče definicije sovražnega govora, pa iz njegove sodne prakse izhajajo nekatera temeljna načela. ESČP opredeljuje govor, ki spodbuja in razpihuje rasno in versko diskriminacijo, kot popolnoma prepovedan brez vsakršnih izjem. ESČP soglaša, da poveličevanje totalitarnih režimov in zanikanje oziroma zmanjšanje pomena genocida, hudodelstev zoper človečnost, vojnih hudodelstev in holokavsta pomeni prepovedano obliko izražanja in izpolnjuje vse oblike sovražnega govora. ESČP v takšnih primerih ne uporabi testa sorazmernosti, ampak odloči na podlagi 17. člena EKČP o prepovedi zlorabe pravice. Takšno pritožbo ESČP na podlagi 4. odstavka. člena EKČP zavrne kot nedopustno. Če ne

[25] Zadeva C-131/12, *Google Spain SL in Google Inc. proti Agencia Española de Protección de Datos (AEPD) in Mariu Costeji Gonzálezu,* ECLI:EU:C:2014:317.
[26] Ibidem.

gre za najskrajnejši sovražni govor, ga ESČP obravnava na podlagi načela sorazmernosti v povezavi z 2. odstavkom 10. člena.

2.3.2.1 Primeri sodne prakse ESČP

Relevantna člena evropske konvencije o človekovih pravicah:
10. ČLEN (Svoboda izražanja) [27]

- 1. Vsakdo ima pravico do svobode izražanja. Ta pravica obsega svobodo mišljenja ter sprejemanja in sporočanja obvestil in idej brez vmešavanja javne oblasti in ne glede na meje. Ta člen ne preprečuje državam, da zahtevajo dovoljenje za delo radijskih, televizijskih in kinematografskih podjetij.
- 2. Izvrševanje teh svoboščin vključuje tudi dolžnosti in odgovornosti in je zato lahko podrejeno obličnosti in pogojem, omejitvam ali kaznim, ki jih določa zakon, in ki so nujne v demokratični družbi zaradi varnosti države, njene ozemeljske celovitosti, zaradi javne varnosti, preprečevanja neredov ali kaznivih dejanj, za varovanje zdravja ali morale, za varovanje ugleda ali pravic drugih ljudi, za preprečitev razkritja zaupnih informacij ali za varovanje avtoritete in nepristranskosti sodstva.

17. ČLEN (Prepoved zlorabe pravic)[28]

- Nobene določbe v tej Konvenciji ni mogoče razlagati tako, kot da vsebuje za katerokoli državo, skupino ali posameznika, pravico do kakršnekoli dejavnosti ali dejanja, ki je usmerjeno h kršenju katerihkoli pravic ali svoboščin, ki so tu določene, ali k njihovemu omejevanju v večjem obsegu, kot je določeno v tej Konvenciji.

Primeri:

- ESČP je 17. člen prvič uporabilo v zadevi »Glimmerveen in Hagenbeek proti Nizozemski«[29], kjer je predhodnica ESČP, Evropska komisija za

[27] Evropska konvencija o človekovih pravicah.
[28] Evropska konvencija o človekovih pravicah.
[29] *J. Glimmerveen & J. hagenbeek, št. 8348/78 & 8406/78, ECLI:CE:ECHR:1979:1011DEC000834878.*

človekove pravice, zavrgla obravnavo pritožbe pritožnika, ki je nameraval razpečevati letake z rasistično vsebino. Komisija je zapisala, da je »splošni namen 17. člena, da prepreči totalitarnim skupinam izkoriščati temeljna načela Konvencije za njihove interese«.

- V zadevi »Garaudy proti Franciji«[30] je bil avtor dela »Temeljni miti modernega Izraela« obsojen na pogojno zaporno kazen in denarno kazen zaradi zanikanja hudodelstev zoper človečnost in holokavsta. Sodišče je zapisalo, da je »zanikanje hudodelstev zoper človečnost ena izmed najresnejših oblik obrekovanja zoper Jude in napeljevanja sovraštva zoper njih«. ESČP je na podlagi 17. člena njegovo pritožbo zavrglo kot nedopustno. Zapisalo je, da je »takšen splošen in vehementen napad na eno etnično skupino v nasprotju z osnovnimi vrednotami Konvencije, zlasti strpnostjo, socialnim mirom in nediskriminacijo«.
- V zadevi »Kühnen proti Nemčiji«[31] glede širjenja neonacistične propagande je ESČP zapisalo, da se pritožniki ne morejo sklicevati na 10. člen ... v nasprotju s 17. členom EKČP, zato je pritožbo zavrglo.
- ESČP je v zadevi »Leroy proti Franciji«[32] odločilo, da pravica do svobode izražanja ne varuje posameznika pred obsodbo za kaznivo dejanje razpihovanja nestrpnosti, ker je pritožnik v lokalnem časopisu po terorističnih napadih 11. septembra 2001 objavil karikaturo porušenih nebotičnikov z napisom »Vsi smo sanjali o tem..., Hamas pa je to storil.« Takšen poseg francoskih sodišč v pritožnikovo pravico do svobode izražanja je bil upravičen iz razlogov varstva javnega reda ter pravic drugih.
- V zadevi »Lehideux in Isorni proti Franciji«[33] je dnevnik Le Monde 18. julija 1985 objavil oglasni prispevek, ki je prikazoval maršala Pataina, vodje vichyjske Francije, v pozitivni luči. Pritožbeno sodišče v Parizu je 26. januarja kazensko obsodilo predsednika organizacije, ki je naročila prispevek, in avtorja prispevka na plačilo simbolične kazni enega franka ter na objavo sodbe v Le Mondu. Ob tem je pojasnilo, kdaj se uporablja 17. člen EKČP, saj je zapisalo, da ta primer »ne spada v kategorijo jasno določenih zgodovinskih dejstev – kot denimo holokavst –, katerega zanikanje ali spremembe bi 17. člen izključile iz varstva člena 10 EKČP«. ESČP je nato v sodbi opozorilo na »resnost kazenske obsodbe za javno

[30] *Roger Garaudy, št. 65831/01, ECLI:CE:ECHR:2003:0624DEC006583101.*
[31] *Michael Kühnen, št. 12194/86, ECLI:CE:ECHR:1988:0512DEC001219486.*
[32] *AFFAIRE LEROY c. FRANCE, št. 36109/03, ECLI:CE:ECHR:2008:1002JUD003610903.*
[33] *Lehideux in Isorni, št. 24662/94, ECLI:CE:ECHR:1998:0923JUD002466294*

branjenje dejanja kolaboracije, ob upoštevanju obstoja drugih sredstev posredovanja ..., zlasti s civilnopravnimi sredstvi«. Sodniki so kazensko obsodbo pritožnikov ocenili za nepotrebno v demokratični družbi in ugotovili kršitev 10. člena EKČP.

- V zadevi Ibrahim Aksoy proti Turčiji glede objave prispevka o kurdski neodvisnosti je ESČP zapisalo, da »spodbujanje rasnega sovraštva in ideja o superiorni rasi ne uživa varstva 10. člena EKČP«. Nekateri akademiki in praktiki ostro kritizirajo uporabo 17. člena EKČP za najskrajnejše oblike sovražnega govora, saj takšen pristop ni najbolj nujen in primeren v demokratični družbi. Še bolj sporno je, v katerih primerih se lahko 17. člen EKČP uporablja.[34]
- Svoboda izražanja tudi ne varuje govora, ki spodbuja versko diskriminacijo. V zadevi I. A. proti Turčiji je pritožnik objavil roman, ki je žalil islamskega preroka. Istanbulsko sodišče ga je obsodilo na dvoletno zaporno kazen, ki je bila kasneje spremenjena v denarno, zaradi žalitve boga, preroka in svete knjige. ESČP je zapisalo, da »je bil ukrep, ki je bil sprejet v zvezi s temi navedbami, namenjen zagotavljanju varstva pred napadi na muslimanske svete predmete ..., zato je ukrep upravičeno izpolnjeval nujno družbeno potrebo«.[35]
- Vrsta zadev v zvezi s sovražnim govorom je povezana z umetniškimi deli. ESČP je v zadevi Alınak proti Turčiji obravnavalo vsebino romana »The Heat of Şiro«, ki naj bi diskriminatorno obravnaval različne etnične skupine v Turčiji ter spodbujal med etnično sovraštvo in nestrpnost. Turško sodišče je zato prodajo knjige prepovedalo in zaseglo še neprodane izvode. ESČP je v sodbi zapisalo, da bi nekateri deli romana lahko pomenili »napeljevanje bralcev k sovraštvu, uporu in uporabi nasilja. Pri odločanju, ali so to v resnici storili, je treba vendarle spomniti, da je medij, ki ga je uporabil pritožnik, roman, oblika umetniškega izražanja, ki naslavlja razmeroma ozek krog javnosti v primerjavi z, na primer, množičnimi mediji.« Zato je ESČP odločilo, da je bil »zaseg izvodov romana pritožnika nesorazmeren z zastavljenimi cilji in ni bil nujen v demokratični družbi«; tako so turške oblasti kršile 10. člen EKČP[36]

[34] *Ibrahim Aksoy, št. 31080/02, ECLI:CE:ECHR:2007:1129JUD003108002*
[35] *I.A., št. 42571/98, ECLI:CE:ECHR:2005:0913JUD004257198*
[36] *Mahmut Alınak, št. 40287/98, ECLI:CE:ECHR:2005:0329JUD004028798*

2.4 Lažne novice

Lažne novice so oblika novic, ki skušajo bralca dezinformirati, po navadi se pišejo, z namenom, da oškodujejo organizacije ali osebe, oziroma za lastni finančni ali politični interes.[37]
Vsebina takih novic je velikokrat senzacionalistična in nepoštena ali pa celo odkrito izmišljena, naslovi pa strukturirani tako, da prebudijo zanimanje v bralcu, da prebere, kar lahko prinaša tudi velike oglaševalske prihodke.[38]

Claire Wardle, direktorica za strategijo in raziskave za First Draft News, neprofitna raziskovalna skupina, nastanjena v Shorenstein centru na univerzi Harvard, meni da je izraz »lažne novice« popolnoma nezadosten.[39]

V poročilu, namenjeno Evropskemu svetu, je Claire Wardle, skupaj z ko-avtorjem Hossein Derakhsanom, definirala 3 glavne vrste lažnih novic oz., kot pravi ona »informacijske motnje«. Med seboj se razlikujejo po dveh faktorjih, stopnji napačnosti in po stopnji škode, ki jo povzročajo:

- Napačne informacije so, kadar se napačne informacije delijo, vendar ni mišljena nobena škoda.
- Dezinformacije so takrat, kadar lažne podatke zavestno delijo, da povzročijo škodo.
- Zlonamerne informacije so, kadar se delijo resnične informacije, da povzročijo škodo, pogosto s prenosom zasebnih informacij v javno sfero.[40]

2.4.1 Sintetični mediji

Sintetični medij je klasifikacija za vrste medijev oziroma vsebin, bodisi slike, zvoki, videoposnetki, kateri so bili generirani ali spremenjeni z avtomatskimi sredstvi, najpogosteje z umetno inteligenco.

---

[37] The Real Story of Fake News <https://www.merriam-webster.com/words-at-play/the-real-story-of-fake-news> (29.5.2020).
[38] Fake News in Reality <https://www.usnews.com/opinion/thomas-jefferson-street/articles/2017-04-14/what-is-fake-news-maybe-not-what-you-think > (29.5.2020).
[39] F*** News' should be replaced by these words, Claire Wardle says <https://money.cnn.com/2017/11/03/media/claire-wardle-fake-news-reliable-sources-podcast/index.html> (29.5.2020).
[40] One year on, we're still not recognizing the complexity of information disorder online, 31.10.2017, <https://firstdraftnews.org/articles/coe_infodisorder/> (29.5.2020).

Sintetični mediji imajo lahko številne koristne aplikacije, predvsem v zabavi, kjer je spodbuditev nekakšnega neverjetnega občutka pri občinstvu temelj večine zabave. Kljub temu pa potencialne zlorabe tehnologije »deep fake« postajajo zaskrbljujoče.[41]

Enostavna širitev sintetičnih medijev ima lahko velike posledice v mnogih vidikih družbe, manipulacija volitev, z širjenjem neresničnih slik ali videoposnetkov o kandidatu, novi vali prevar v podjetjih z uporabo sinteze govora, in podobno.

2.4.1.1 Deepfake

Deepfake je proces, pri katerem program vzame sliko določene osebe in videoposnetek in z uporabo naprednih algoritmov oziroma umetne inteligence zamenja obraz v videoposnetku z obrazom iz fotografije. Medij je deležen široke pozornosti pri njihovi uporabi v pornografskih videoposnetkih, lažnih novicah in prevarah.

2.4.1.2 Sinteza zvoka in govora

Zvok je drugo področje, kjer se umetna inteligenca uporablja za ustvarjanje sintetičnih medijev. Sintetizirani zvok bo lahko ustvaril kakršen koli domišljav zvok, ki ga je mogoče doseči z manipulacijo zvočnega valovanja.[42]

Marca 2019 je bilo ukradenih 250 tisoč dolarjev, ker je delavec mislil, da po telefonu govori z šefom, v resnici pa je govoril z prevarantom. Podobni scenariji se lahko tudi zgodijo za pridobitev drugih sredstev, kot so gesla ali drugi zaupni podatki.

2.4.2 Boj proti lažnim novicam

Pod trenutnim pravnim režimom EU ni spletnim platformam potrebno odstranjevati škodljivo, a legalno vsebino, kot so lažne novice. Socialni mediji se regulirajo sami, z metodami kot so »fact-checkerji«, označevanje dezinformacij in raznimi podaljški, ki ugotovijo, ali je vsebina lažna ali ne.[43] [44]

---

[41] Perception won't be reality, once AI can manipulate what we see, 17.11.2019, <https://thehill.com/opinion/cybersecurity/470826-perception-wont-be-reality-once-ai-can-manipulate-what-we-see/ > (29.5.2020).
[42] Ibidem.
[43] Brkan, M.: Freedom of Expression and Artificial Intelligence: on personalisation, disinformation and (lack of) horizontal effect of the Charter, v: MCEL Working Paper Series, Maastricht 2019, str. 1-18.
[44] Facebook will not remove fake news - but will 'demote' it, 13.7.2018, <https://www.bbc.com/news/technology-44809815 > (29.5.2020).

V Singapurju je bilo leta 2019 razvito orodje, ki identificira, ali je članek resničen. Orodje temelji na umetni inteligenci, kar pokaže, kako lahko uporabimo umetno inteligenco v boju proti sintetičnim medijem, oziroma kako lahko uporabimo avtomatska sredstva proti drugim avtomatskim sredstvom.[45]

2.4.3 Svoboda govora na spletnih platformah

Družbena podjetja, kot sta Twitter in Facebook, so zasebna podjetja. Vendar platforme družbenih medijev javnosti ponujajo orodja in javne forume za izmenjavo idej, povezovanje s prijatelji in sodelavci, mreženje s potencialnimi strankami in izražanje političnih prepričanj.

V zadnjem desetletju je dostop do družbenih medijev postal vsakodnevna stvar, katero mnogi vidijo kot nujnost.[46] Vendar družbena omrežja v svojih pogojih uporabe pridržujejo pravico, do določitve standardov skupnosti in njihove uveljave.

Ta podjetja so zato brez razprave ali kakršnega koli pravega javnega posvetovanja sprejela nejasno opredeljene in poljubno uveljavljene kode "sovražnega govora". Nacionalne vlade so začele groziti spletnim platformam za socialne medije z velikimi kaznimi, če ne bodo cenzurirale govora. Brez dvoma je začela veljati vse bolj sramežljiva kultura, »tega ne smeš reči«, s svojo »ljubeznijo« do odvzema platform, odpovedovanja, bojkota in strogega kaznovanja prestopnikov.[47]

Družbena omrežja v 21. stoletju so nadgradnja radio oddajanja in časopisa iz 20. stoletja. Glavna razlika je v pridobivanju vsebine. Takrat je bila velika večina vsebine ustvarjena preko podjetij, ki so to vsebino tudi objavljale, zato udeležba potrošnikov ni bila potrebna.

Sedaj pa pridobivanje vsebine vključuje »crowdsourcing« oziroma si končni uporabniki ustvarjajo svojo vsebino. Uporabniki so torej postali tako ustvarjalci kot ciljne skupine za vsebino, ki jo ustvarjajo.

---

[45]<https://www.channelnewsasia.com/technology/rgs-student-develops-award-winning-ai-fake-news-detector-887191 > (29.5.2020).

[46] Griffiths, Mark D.: Addicted to Social Media? What can we do about it problematic, excessive use?, 7.5.2018, <https://www.psychologytoday.com/us/blog/in-excess/201805/addicted-social-media > (29.5.2020).

[47] You can't say that, <https://www.nytimes.com/2012/06/24/books/review/the-harm-in-hate-speech-by-jeremy-waldron.html > (29.5.2020).

Množični mediji dvajsetega stoletja so postavili meje glede dopustnih vsebin in ustvarili določeno vrsto javnega pogovora na podlagi pričakovanih interesov in vrednosti njihove publike. Različni igralci v različnih medijih in v različnih delih družbe so vsiljevali različne norme. Založniki knjig so uporabili svoj nabor norm, filmska podjetja so imela svoj nabor norm, pornografska industrija (ki je obsegala tisk in video) je imela svoje norme in tako naprej. Na splošno so dnevni časopisi in radio mediji uporabljali norme družbe, ki je ocenjena kot primerna za domišljeno občinstvo povprečnega odraslega in njihove družine.

Družbeni mediji danes cenzurirajo javni diskurz. Toda namesto, da objavljajo svojo lastno vsebino, objavljajo vsebino drugih. Kot množični mediji v 20. stol, uporabljajo vrsto pravil in standardov o tem, kakšne vrste vsebine (in pogovorov) so na njihovih spletnih mestih dovoljeni oziroma nedopustni. Oni naložijo nabor vedenjske norme za svojo publiko - drugačna od časopisov dvajsetega stoletja, vendar kljub temu še vedno precej omejena. Različni družbeni mediji uveljavljajo različne norme. Socialni mediji lahko omejijo govor veliko bolj, kot od njih zakon zahteva.

Na splošno načelo svobodnega govora državi omogoča le, da se vsiljuje zelo omejen niz normativov o javnem diskurzu, ki pušča vmesne ustanove, da lahko svobodno postavljajo strožje norme v skladu s svojimi vrednotami.

To deluje dobro, če obstaja veliko vmesnih institucij. Predpostavka je, da v raznoliki družbi z različnimi kulturami in subkulturami, različne skupnosti ustvarjajo in uveljavljajo svoje lastne norme, ki so lahko strožje od državnih.

Zaželena je raznolikost različnih institucij z različnimi normami cilj za javno sfero tudi v enaindvajsetem stoletju. Če bodo zasebni akterji vsiljevali civilne norme, ki so strožje od tistega, kar lahko vlade naložijo, je pomembno, da je veliko različnih zasebnih akterjev, ki vsiljujejo te norme, kar odraža različne kulture in subkulture in ne samo dve ali tri velike družbe.

2.4.4 Kakšne so lahko načeloma rešitve za socialne medije

Zdrav sistem svobodnega izražanja na socialnih medijih zahteva veliko več kot necenzuro. Za to potrebujejo institucije in strokovnjake, ki se ukvarjajo z znanjem, ga proizvajajo in širijo mnenja. Primeri iz dvajsetega stoletja vključujejo časopise in druge medijske organizacije, šole, univerze, knjižnice, muzeji in arhivi. Nekatere od

njih lahko vodi in / ali subvencionira država. Toda mnogi od njih bodo v zasebni lasti.[48]

Potrebujemo mnogo različnih inštitucij z različnimi lastniki oziroma ne sme jih kontrolirati majhna skupina ljudi. Morajo zagotoviti "raznolike in antagonistične vire" informacij. Toda pri tem ne gre samo za to, da bi imeli veliko različnih glasov, ki se med seboj ne strinjajo. Bolj gre za drugačne institucije, ki proizvajajo in širijo znanje. [49]

Te ustanove morajo imeti strokovne norme, ki vodijo, kako se proizvaja, organizira in širi znanje in mnenje. [50]

Za uspešno izvajanje dela teh ustanov je potrebno, da so na splošno vredne zaupanja. Kadar te institucije niso zaupanja vredne, bo ta digitalna javna sfera začela »razpadati«, ker ne glede na teorijo o svobodi govora je uresničevanje njenih vrednot odvisno od ustvarjanja in širjenja znanja inštitucij, ki jim javnost zaupa. Brez zaupanja vrednih inštitucij in strokovnjakov postane širjenje znanja "vojna proti vsem", kjer zmaga najglasnejši. Taka vojna ovira vrednote demokracije in rast ter širjenje znanja za katero bi naj svoboda izražanja služila.[51]

To je težava, s katero se srečujemo v enaindvajsetem stoletju. Mediji so se preselili v novo vrsto javne sfere - digitalno javno sfero – brez vezivnega tkiva vrst institucij, potrebnih za zaščito osnovne vrednosti prostega govora. Manjkajo nam zaupanja vredne digitalne institucije, ki jih vodijo strokovne norme, ki imajo javnost v ospredju. Še huje, digitalna podjetja, ki trenutno obstajajo prispevajo k upadu drugih zaupanja vrednih institucij in strokovnjakov za ustvarjanje in širjenje znanja. [52]

Za dosego zdrave in živahne javne sfere potrebujemo tudi veliko različnih vrst socialnih medijev, ki z večimi različnimi načini sodelujejo in ustvarjajo kulturo in vsebino. Zato je pomembno imeti Facebook in YouTube ter TikTok in Twitter ter

[48] Balkin, Jack M.: How to Regulate (and Not Regulate) Social Media, 25.3.2020, <https://knightcolumbia.org/content/how-to-regulate-and-not-regulate-social-media> (29.5.2020).
[49] Ibidem.
[50] Ibidem.
[51] Ibidem.
[52] Ibidem.

številne druge vrste socialnih medijev. Te platforme seveda ne sme imeti v lasti oziroma nadzirati isto podjetje. [53]

Prav tako pa so bili razviti principi glede etike »velikih podatkov«[54], z namenom, da pomagajo usmeriti države in velika podjetja na odgovorno moralno pot. Ta iniciativa je ustvarila pet temeljnih etičnih načel za uporabo teh podatkov:

1. Ne delajte škode. Digitalni odtis, ki ga zdaj puščajo vsi, izpostavlja posameznike,družbene skupine in družbo kot celoto do določene stopnje preglednosti in ranljivosti. Tisti, ki imajo dostop do vpogleda v velike podatke, ne smejo škodovati tretjim osebam. [55]
2. Zagotovite, da se podatki uporabljajo tako, da bodo rezultati spodbudili mirno sobivanje človeštva. Izbira vsebine in dostop do podatkov vplivata na svetovni pogled na družbe. Mirno sobivanje je mogoče le, če se znanstveniki zavedajo svoje odgovornost za zagotavljanje enakomernega in nepristranskega dostopa do podatkov. [56]
3. Uporabite podatke za pomoč ljudem v stiski. Poleg tega, da so inovacije v gospodarstvu koristne, bi sfera velikih podatkov lahko ustvarila tudi dodatno družbeno vrednost. V dobi globalne povezanosti, je zdaj mogoče ustvariti inovativna orodja za velike podatke, ki bi lahko pomagala podpirati ljudi v stiski. [57]
4. Podatke uporabite za zaščito narave in zmanjšanje onesnaževanja okolja. Eden največjih dosežkov analize velikih podatkov so razvoj učinkovitih procesov. Obsežni podatki lahko trajno gospodarsko in socialno prihodnost ponujajo le, če se takšne metode uporabljajo tudi za ustvarjanje in vzdrževanje zdravega in stabilnega naravnega okolja. [58]
5. Uporabite podatke za odpravo diskriminacije in nestrpnosti ter za ustvarjanje poštenega družbenega sistema za sobivanje. Socialni mediji so ustvarili okrepljeno socialno omrežje. To lahko vodi do dolgoročne globalne stabilnosti le, če temelji na načelih pravičnosti in enakosti. [59]

---

[53] Ibidem.
[54] Veliki podatki se nanašajo na velike, raznolike nabore informacij, ki rastejo z vedno hitreje. Veliki podatki pogosto prihajajo iz več virov in prispejo v več formatih. Segal, T.: Big Data, <https://www.investopedia.com/terms/b/big-data.asp> (29.5.2020).
[55] Ibidem.
[56] Ibidem.
[57] Ibidem.
[58] Balkin, Jack M.: How to Regulate (and Not Regulate) Social Media, 25.3.2020, <https://knightcolumbia.org/content/how-to-regulate-and-not-regulate-social-media> (29.5.2020).
[59] Ibidem.

2.5 Zaključek

Vsaka generacija ima svojo verzijo distopije, katero oblikujejo trenutni problemi in skrbi.

Distopija, kjer demokracija propade in nas manipulirajo in vladajo »črne tehnološke skrinje«, ki jim pravimo umetne inteligence in algoritmi učenja, za katere niti jasno ne vemo kako delujejo in sklepajo odločitve, še zaenkrat ni tukaj, ampak to še ne pomeni, da ne hodimo po poti, ki nas pelje v to smer.

"A powerful AI system tasked with ensuring your safety might imprison you at home. If you asked for happiness, it might hook you up to a life support and ceaselessly stimulate your brain's pleasure centers. If you don't provide the AI with a very big library of preferred behaviors or an ironclad means for it to deduce what behavior you prefer, you'll be stuck with whatever it comes up with. And since it's a highly complex system, you may never understand it well enough to make sure you've got it right."
— James Barrat

Seznam literature in virov

Monografije

Pariser, E.: The Filter Bubble: What The Internet Is Hiding From You, Penguin, UK, 2011.

Članki in poglavja iz knjig

Brkan, M.: Freedom of Expression and Artificial Intelligence: on personalisation, disinformation and (lack of) horizontal effect of the Charter, v: MCEL Working Paper Series, Maastricht 2019, str. 1-18.

Pravni viri

Lizbonska pogodba, ki spreminja Pogodbo o Evropski uniji in Pogodbo o ustanovitvi Evropske skupnosti, podpisana v Lizboni dne 13. decembra 2007, Uradni list Evropske unije, C 306, 17.12.2007, str. 1–271

Listina Evropske Unije o človekovih pravicah, Uradni list Evropske unije, C 83/389, str. 391–407.

Uredba (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES (Splošna uredba o varstvu podatkov) (Besedilo velja za EGP), Uradni list Evropske unije, L 119, 4.5.2016, str. 1–88.

Listina Evropske Unije o človekovih pravicah, Uradni list Evropske unije, C 83/389, str. 391–407.

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 – Mednarodne pogodbe, št. 7/94).

Konvencija o odpravi vseh oblik diskriminacije žensk, Treaty Series, vol. 1249, str. 13.

Mednarodni pakt o državljanskih in političnih pravicah, Treaty Series, vol. 999, 16 December 1966, str. 171.

Sodna praksa

Zadeva C-131/12, *Google Spain SL in Google Inc. proti Agencia Española de Protección de Datos (AEPD) in Mariu Costeji Gonzálezu,* ECLI:EU:C:2014:317.
Zadeva C-507/18, *NH proti Associazione Avvocatura per i diritti LGBTI – Rete Lenford*, ECLI:EU:C:2020:289.
Affaire Leroy v. France, št. 36109/03, ECLI:CE:ECHR:2008:1002JUD003610903.
I.A., št. 42571/98, ECLI:CE:ECHR:2005:0913JUD004257198
Ibrahim Aksoy, št. 31080/02, ECLI:CE:ECHR:2007:1129JUD003108002
J. Glimmerveen & J. hagenbeek, št. 8348/78 & 8406/78, ECLI:CE:ECHR:1979:1011DEC000834878.
Lehideux in Isorni, št. 24662/94, ECLI:CE:ECHR:1998:0923JUD002466294
Mahmut Ahnak, št. 40287/98, ECLI:CE:ECHR:2005:0329JUD004028798
Michael Kühnen, št. 12194/86, ECLI:CE:ECHR:1988:0512DEC001219486.
Roger Garaudy, št. 65831/01, ECLI:CE:ECHR:2003:0624DEC006583101.

Spletni viri

<https://www.channelnewsasia.com/technology/rgs-student-develops-award-winning-ai-fake-news-detector-887191 > (29.5.2020).
<https://www.worldgovernmentsummit.org/observer/articles/could-an-ai-ever-replace-a-judge-in-court#:~:text=An%20aide%20to%20judges&text=The%20Supreme%20People's%20Court%20has,judges%20and%20litigants%20resolve%20cases> (29. 5. 2020).
'Anonymised' data can never be totally anonymous, says study <https://www.theguardian.com/technology/2019/jul/23/anonymised-data-never-be-anonymous-enough-study-finds > (29. 5. 2020).
Artificial intelligence can save democracy, unless it destroys it first, 10.8.2017, <https://www.oii.ox.ac.uk/news-events/news/artificial-intelligence-can-save-democracy-unless-it-destroys-it-first/> (29. 5. 2020).
Artificial Intelligence: Utopia or Dystopia? <https://commoncore.hku.hk/ccst9068/> (29. 5. 2020).
Balkin, Jack M.: How to Regulate (and Not Regulate) Social Media, 25.3.2020, <https://knightcolumbia.org/content/how-to-regulate-and-not-regulate-social-media> (29.5.2020).
European Parliament in plain language, Values <https://europarlamentti.info/en/values-and-objectives/values/> (29. 5. 2020).
F*** News' should be replaced by these words, Claire Wardle says <https://money.cnn.com/2017/11/03/media/claire-wardle-fake-news-reliable-sources-podcast/index.html> (29.5.2020).
Facebook will not remove fake news - but will 'demote' it, 13.7.2018, <https://www.bbc.com/news/technology-44809815 > (29.5.2020).
Fake News in Reality <https://www.usnews.com/opinion/thomas-jefferson-street/articles/2017-04-14/what-is-fake-news-maybe-not-what-you-think > (29.5.2020).
Griffiths, Mark D.: Addicted to Social Media? What can we do about it problematic, excessive use?, 7.5.2018, <https://www.psychologytoday.com/us/blog/in-excess/201805/addicted-social-media > (29.5.2020).
How AI could kill off democracy, 11.9.2018, <https://www.newstatesman.com/long-reads/2018/08/how-ai-could-kill-democracy-0> (29. 5. 2020).
How artificial intelligence conquered democracy, 8.8.2017, <https://theconversation.com/how-artificial-intelligence-conquered-democracy-77675> (29. 5. 2020).
Media Echo Chambers Increase Polarization in Society <https://www.ceu.edu/article/2019-03-14/media-echo-chambers-increase-polarization-society> (29. 5. 2020).
One year on, we're still not recognizing the complexity of information disorder online, 31.10.2017, <https://firstdraftnews.org/articles/coe_infodisorder/> (29.5.2020).

Perception won't be reality, once AI can manipulate what we see, 17.11.2019, <https://thehill.com/opinion/cybersecurity/470826-perception-wont-be-reality-once-ai-can-manipulate-what-we-see/ > (29.5.2020).
Segal, T.: Big Data, <https://www.investopedia.com/terms/b/big-data.asp> (29.5.2020).
The AI Transparency Paradox <https://hbr.org/2019/12/the-ai-transparency-paradox> (29. 5. 2020).
The Real Story of Fake News <https://www.merriam-webster.com/words-at-play/the-real-story-of-fake-news> (29.5.2020).
The Sordid Origin of Hate-Speech Laws, 1.12.2011 <https://www.hoover.org/research/sordid-origin-hate-speech-laws> (29.5.2020).
The trouble with Echo Chamber Online <https://www.nytimes.com/2011/05/29/technology/29stream.html> (29. 5. 2020).
West, Darrell M. in Allen, John R.: How artificial intelligence is transforming the world, <https://www.brookings.edu/research/how-artificial-intelligence-is-transforming-the-world/> (29. 5. 2020).
You can't say that, <https://www.nytimes.com/2012/06/24/books/review/the-harm-in-hate-speech-by-jeremy-waldron.html > (29.5.2020).

DOI
https://doi.org/10.18690/um.pf.4.2023.3

ISBN
978-961-286-774-4

3 PRAVICA DO ZASEBNOSTI V POVEZAVI Z UMETNO INTELIGENCO

ELENA OSRAJNIK
Univerza v Mariboru, Pravna fakulteta, Maribor, Slovenija
elena.osrajnik@student.um.si

Ključne besede:
umetna inteligence,
zasebnost,
osebni podatki,
obdelava podatkov,
povezane naprave

V prihodnosti bodo sistemi umetne inteligence vedno bolj inkorporirani v naš vsakdan, kar bo naše življenje zagotovo izboljšalo, prav tako pa bomo lahko z njihovo uporabo izpostavljeni večjim tveganjem, tudi na področju varstva temeljnih pravic. Škoda, ki jo lahko umetna inteligenca povzroči, je lahko stvarna, torej varnost in zdravje posameznika in škoda na premoženju, lahko pa je tudi nestvarna, kar zajema omejitev svobode izražanja in spoštovanja človekovega dostojanstva, diskriminacijo ter izgubo zasebnosti. V tem sklopu sem se osredotočila predvsem na zadnje, torej izgubo zasebnosti. Preučila sem, kako je zasebnost posameznika zaščitena pri uporabi sistemov umetne inteligence, kot so internet stvari, avtonomna vozila, deepfake posnetki in prilagojeni oglasi. Možnosti za kibernetski vdor je pri sistemih interneta stvari in avtonomnih vozil veliko, saj so medsebojno povezane naprave priključene na internet, kamor pošiljajo zbrane podatke. Prav tako pravico do zasebnosti kršijo deepfake posnetki, ki temeljijo na tehnologiji prepoznave obraznih potez, ter prilagojeni oglasi, ki zbirajo in obdelujejo podatke o iskalnih navadah in preferencah uporabnika. Grožnjo zasebnosti predstavljajo tudi številne aplikacije, ki so uporabljene za pridobivanje osebnih podatkov uporabnikov, ki se tega sploh ne zavedajo.

Univerzitetna založba Univerze v Mariboru

DOI
https://doi.org/
10.18690/um.pf.4.2023.3

ISBN
978-961-286-774-4

Keywords:
artificial intelligence,
privacy,
personal data,
data processing,
connected devices

University of Maribor Press

3 The Right to Privacy in Connection With Artificial Intelligence

Elena Osrajnik
University of Maribor, Faculty of Law, Maribor, Slovenia
elena.osrajnik@student.um.si

In the future, the systems of artificial intelligence will be increasingly incorporated into our lives. On one hand, this will improve our daily struggles, however, on the other hand these systems my induce violations of basic human rights. The potential damage, which may be caused by AI can be material, compromising individual's safety, health and assets, or non-material, that is freedom of speech, respect, discrimination and interference with privacy. In this section, I focused mainly on the latter, interference with privacy. I asked myself how protected is the privacy of the users of AI systems, like internet of things, autonomous driving solutions, deepfakes and targeted advertising. Both internet of things and autonomous cars may violate the privacy rights, as their connection to internet enables cybernetic irruption. In the same manner, deepfake technologies, which are based on identification of facial features, andtargeted advertisement, , which note the searching habits and preferences of the users, invade the individual's privacy. The menace of privacy interference is also represented by numerous apps, which collect private information of the users without their knowledge.

3.1 Uvod

Umetna inteligenca je koncept, ki zajema veliko področij, kot so kognitivno računalništvo, strojno učenje, obogatena inteligenca in inteligentna robotika. Kognitivno računalništvo temelji na algoritmih, ki sklepajo in se učijo na višji ravni, torej je njihovo »razmišljanje« bolj podobno človeškemu. Strojno učenje temelji na algoritmih, ki se avtonomno učijo izvajanja nalog s pomočjo prejšnjih vnesenih podatkov o opravljeni nalogi. Obogatena inteligenca pa temelji na sodelovanju med človekom in strojem, inteligentna robotika pa je umetna inteligenca, ki je vgrajena v robote.

Razvoj umetne inteligence in raziskave na vseh prej naštetih področjih so v glavnem namenjene avtomatiziranju inteligentnega obnašanja, vključno z zmožnostjo logičnega sklepanja, zbiranja informacij, načrtovanja, učenja, komuniciranja, manipuliranja, signaliziranja in celo ustvarjanja, sanjanja in zaznavanja. Ločimo dva tipa umetne inteligence in sicer inteligenco v ožjem pomenu, kjer gre za zmožnost izvajanja točno določenih nalog, in umetno inteligenco v splošnem pomenu, kjer gre za zmožnost izvajanja vseh intelektualnih nalog, ki jih je sposoben opraviti človek.

Do danes so razviti številni načini uporabe umetne inteligence v splošnem pomenu, kot so virtualni pomočniki, avtonomni avtomobili, samodejno združevanje informacij oz. internet stvari, prepoznavanje glasu, programska oprema za prevajanje, programska oprema za pretvorbo besedila v govor, avtomatizirane finančne transakcije, e-odkrivanje v sodstvu itd. In čeprav imajo te implementacije umetne inteligence veliko korist človeku, s seboj prinašajo tudi nevarnosti za ohranjanje njegove zasebnosti, saj je za delovanje katerekoli uporabe umetne inteligence potrebna izmenjava informacij in podatkov.

Evropski ekonomsko-socialni odbor je glede varstva zasebnosti že izrazil skrb glede ciljno naravnane uporabe sistemov umetne inteligence, ki se že uporabljajo. Takšne oblike so recimo filtrni mehurčki, ki posamezniku ponujajo zgolj tiste vsebine, za katere je v preteklosti pokazal zanimanje, lažne novice na družbenih omrežjih, prilagojeni oglasi in volilne kampanje, združevanje informacij v pametnih stanovanjih in avtonomnih avtomobilih itd.

3.2 Pravna ureditev

3.2.1 Zakonodaja v Evropski uniji

3.2.1.1 Primarno pravo Evropske unije

V Pogodbi o delovanju Evropske Unije (v nadaljevanju PDEU)[1] 16. člen opredeljuje osebne podatke in njihovo obdelavo. V njem je zapisano, da ima vsakdo pravico do varstva osebnih podatkov, ki se nanašajo nanj. Prav tako so v PDEU zapisana pravila o varstvu fizičnih oseb pri obdelavi podatkov s strani institucij, organov, uradov in agencij Unije ter držav članic v okviru dejavnosti s področja uporabe prava Unije, in o prostem pretoku takih podatkov. Ta pravila sta določila Evropski parlament in Svet po rednem zakonodajnem postopku, upoštevanje teh pravil pa nadzirajo neodvisni organi.

Pravica do spoštovanja zasebnega je opredeljena tudi v 8. členu Evropske konvencije o varstvu človekovih pravic (v nadaljevanju EKČP)[2], ki opredeljuje zasebno in družinsko življenje. V EKČP je zapisano, da ima vsak posameznik pravico do spoštovanja njegovega zasebnega in družinskega življenja, doma in dopisovanja, pri čemer se javna oblast ne sme vmešavati v izvrševanje te pravice, razen če je to določeno z zakonom in nujno v demokratični družbi. To pomeni, da se v zasebno življenje sme posegati zgolj zaradi državne varnosti, javne varnosti ali ekonomske blaginje države, zato, da se prepreči nered ali kaznivo dejanje, da se zavaruje zdravje ali morala, ali da se zavarujejo pravice in svoboščine drugih ljudi.

Varstvo zasebnosti in osebnih podatkov pa sta opredeljena tudi v Listini Evropske unije o človekovih pravicah (v nadaljevanju Listina)[3], kjer 7. in 8. člen opredeljujeta spoštovanje zasebnega in družinskega življenja ter varstvo osebnih podatkov. V 7. členu Listine je zapisano, da ima vsakdo pravico do spoštovanja svojega zasebnega in družinskega življenja, stanovanja ter komunikacij. V 8. členu Listine pa piše, da ima vsakdo pravico do varstva osebnih podatkov, ki se nanj nanašajo. Osebni podatki posameznikov se morajo obdelovati pošteno, za določene namene in na

[1] Pogodba o delovanju Evropske Unije, Uradni list Evropske unije, C 326/47, str. 47-390.
[2] 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 – Mednarodne pogodbe, št. 7/94).
[3] Listina Evropske Unije o človekovih pravicah, Uradni list Evropske unije, C 83/389, str. 391–407.

podlagi privolitve prizadete osebe ali na drugi legitimni podlagi, določeni z zakonom. Ta člen zagotavlja tudi, da ima vsakdo pravico dostopa do svojih podatkov in pravico zahtevati, da se ti podatki popravijo. Spoštovanje teh pravil nadzira neodvisen organ.

Generalni pravobranilec P. Cruz Villalón je zadevah C-293/12 in C-594/12 ugotovil, da Direktiva o hrambi podatkov[4] nasprotuje Listini, saj omogoča ponudnikom telefonskih in elektronskih komunikacijskih storitev, da zbirajo in hranijo podatke o lokaciji in prometu teh komunikacij, s čimer ustvarijo zanesljivo in natančno sliko o identiteti uporabnika storitev. To pa je v nasprotju z Listino, saj direktiva izrazito posega v pravico državljanov do spoštovanja zasebnega življenja. Zbranih podatkov ne hranijo javni organi, temveč zasebna podjetja, prav tako pa v direktivi ni določeno kje se morajo podatki hraniti, zato lahko pride do kopičenja podatkov na nedoločenih krajih v kibernetičnem prostoru. Po mnenju pravobranilca direktiva prav tako ni združljiva z načelom sorazmernosti, saj se morajo podatki hraniti za obdobje najmanj šestih mesecev in največ dveh let. Direktiva je zato neveljavna, saj niso dovolj natančno opredeljeni zaščitni ukrepi, s katerimi bi bila urejena dostop do zbranih in hranjenih podatkov ter njihova uporaba.

V zadevi C-207/16 je Sodišče ugotovilo, da se lahko posega v pravici do zasebnega življenja in varnosti osebnih podatkov, ki sta opredeljeni v Listini, v primeru dostopa do osebnih podatkov, ki jih hranijo ponudniki elektronskih komunikacij, če poseg ne pomeni hude kršitve zasebnega življenja. Dostop do identifikacijskih podatkov imetnikov kartic SIM, kot so priimek, ime in po potrebi naslov teh imetnikov, resda pomeni poseg v temeljne pravice, zagotovljene z Listino, vendar so v Direktivi 2002/58/ES[5] natančno opredeljeni cilji, ki lahko upravičijo dostop do osebnih podatkov s strani javnih organov.

3.2.1.2 Sekundarno pravo Evropske unije

Do leta 2018 je veljala Direktiva (EU) 2016/680[6], ki je opredelila varstvo posameznika pri obdelavi osebnih podatkov. S tem so se zavarovale temeljne pravice

[4] Direktiva 2006/24/ES Evropskega parlamenta in Sveta z dne 15. marca 2006 o hrambi podatkov, pridobljenih ali obdelanih v zvezi z zagotavljanjem javno dostopnih elektronskih komunikacijskih storitev ali javnih komunikacijskih omrežij, in spremembi Direktive 2002/58/ES, Uradni list Evropske unije, L 105/54, 13.4.2006.
[5] Direktive 2002/58/ES Evropskega parlamenta in Sveta z dne 12. julija 2002 o obdelavi osebnih podatkov in varstvu zasebnosti na področju elektronskih komunikacij, Uradni list Evropske unije, L 201/37, 31.7.2002.
[6] Direktiva (EU) 2016/680 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov, ki jih pristojni organi obdelujejo za namene preprečevanja, preiskovanja, odkrivanja ali

in svoboščine posameznikov, zlasti njihova pravica do varstva osebnih podatkov. Prav tako se je zagotovila neomejena in ne prepovedana izmenjava osebnih podatkov med pristojnimi organi v Uniji, če je izmenjava določena v pravu Unije ali držav članic. To direktivo je leta 2018 zamenjala Uredba (EU) 2018/1725[7] (v nadaljevanju Splošna uredba o varstvu podatkov), ki določa pravila o varstvu posameznikov pri obdelavi osebnih podatkov v institucijah in organih Unije in pravila o prostem pretoku osebnih podatkov med njimi ali drugimi uporabniki, ustanovljenimi v Uniji.

Splošna uredba o varstvu podatkov varuje temeljne pravice in svoboščine posameznikov, zlasti njihovo pravico do varstva osebnih podatkov, kar je temeljna človekova pravica. Splošna uredba o varstvu podatkov se uporablja predvsem za obdelavo osebnih podatkov, ki se delno ali v celoti izvajajo z avtomatiziranimi sredstvi, in za obdelavo osebnih podatkov, ki so del zbirke ali so namenjeni oblikovanju dela zbirke, ki se izvaja z avtomatiziranimi sredstvi.

Splošna uredba o varstvu podatkov določa, da sta v obdelavo podatkov navadno vključeni dve stranki – posameznik, o katerem se zbirajo podatki in upravljavec, ki podatke zbira, obdeluje in analizira. Posameznik mora jasno, prostovoljno, konkretno in informirano privoliti v zbiranje njegovih osebnih podatkov, upravljavec pa privolitve ne sme izrabiti za posredovanje podatkov tretji osebi, saj s tem krši varnost osebnih podatkov. Najbolj varovani morajo biti genski podatki, saj predstavljajo edinstvene in nenadomestljive informacije o fiziologiji ali zdravju posameznika, in biometrični podatki, ki prav tako predstavljajo edinstveno identifikacijo posameznika glede ne njegovo podobo obraza ali daktiloskopske podatke.

Podatki, ki se zbirajo v zbirkah podatkov, morajo biti obdelani zakonito, pošteno in na pregleden način, prav tako pa morajo biti zbrani za določene namene in se ne smejo obdelovati na način, ki ni združljiv s temi nameni. Osebni podatki morajo biti točni in posodobljeni ter obdelani na način, ki zagotavlja ustrezno varnost podatkov. Prav tako morajo predstavljati najmanjši obseg podatkov, potrebnih za obdelavo in

pregona kaznivih dejanj ali izvrševanja kazenskih sankcij, in o prostem pretoku takih podatkov ter o razveljavitvi Okvirnega sklepa Sveta 2008/977/PNZ, Uradni list Evropske unije, L 119/89, 4.5.2016.

[7] Uredba (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES (Splošna uredba o varstvu podatkov) (Besedilo velja za EGP), Uradni list Evropske unije, L 119, 4.5.2016, str. 1–88.

hranjeni v obliki, ki dopušča identifikacijo posameznika le toliko časa, kolikor je potrebno za namene, za katere se osebni podatki shranjujejo.

Kadar je obdelava podatkov omogočena s privolitvijo posameznika, mora slednja biti jasna, razumljiva in v lahko dostopni obliki. Posameznik, na katerega se obdelava podatkov nanaša, ima pravico kadarkoli preklicati privolitev, kar more biti enako enostavno kot privoliti v obdelavo. Osebni podatki se lahko obdelujejo tudi brez privolitve posameznika, na katerega se nanašajo, če upravljavec oceni, da ima nadaljnja obdelava povezavo z namenom prvotne obdelave in če so ti podatki ustrezno zaščiteni s šifriranjem ali psevdonimizacijo. Psevdonimizacija pomeni obdelavo osebnih podatkov na tak način, da osebnih podatkov brez dodatnih informacij ni več mogoče povezati s specifičnim. Prav tako pa mora upravljavec biti pozoren na okoliščine v katerih so bili zbrani osebni podatki, na njihovo naravo in na morebitne posledice predvidene nadaljnje uporabe.

Upravljavec baze podatkov mora posamezniku, od katerega pridobiva osebne podatke, zagotoviti svojo identiteto in kontaktne podatke, kontaktne podatke osebe pooblaščene za varstvo podatkov, namene, za katere se osebni podatki obdelujejo, uporabnike ali kategorije uporabnikov osebnih podatkov ter, če je to potrebno, tudi dejstvo, da upravljavec namerava prenesti osebne podatke v tretjo državo. Prav tako mora upravljavec posameznika seznaniti z obdobjem hrambe osebnih podatkov, možnostjo, da posameznik zahteva dostop do svojih osebnih podatkov, podatke izbriše ali jih popravi, ter obstojem avtomatiziranega sprejemanja odločitev, vključno z oblikovanjem profilov.

Posameznik ima pravico do popravka osebnih podatkov kadarkoli, upravljavec pa mora njegove zahteve upoštevati in brez nepotrebnega odlašanja popraviti netočne podatke, ali pa jih popolnoma izbrisati iz baze. Posameznik pa ima tudi pravico do omejitve obdelave, če oporeka točnosti osebnih podatkov, če je obdelava nezakonita, če upravljavec podatkov ne potrebuje več v namene obdelave, vendar jih posameznik potrebuje za uveljavljanje, izvajanje ali obrambo pravnih zahtevkov in med potekom postopka ugotovitve zakonitih razlogov za ugovarjanje obdelavi podatkov. Vsi podatki, ki jih posameznik pridobi od upravljavca morajo biti oblikovani v strukturirano, splošno uporabljano in strojno berljivo obliko. Posameznik lahko te podatke brez vednosti prvotnega upravljavca posreduje drugemu izbranemu upravljavcu, če je bila obdelava izdelana z avtomatiziranimi sredstvi in je temeljila na privolitvi posameznika.

Upravljavec mora, ob upoštevanju narave, obsega, okoliščin in namenov obdelave, izvesti ustrezne tehnične in organizacijske ukrepe, s katerimi dokaže, da je obdelava v skladu z uredbo, kar pomeni, da mora izvajati ustrezne politike za varstvo podatkov. Posluževati se mora psevdonimizacije, upoštevati mora načelo najmanjšega obsega podatkov ter v obdelavo vključiti potrebne zaščitne ukrepe. Upravljavec mora zagotoviti, da se obdelajo samo tisti osebni podatki, ki so potrebni za določen namen obdelave, prav tako pa mora to upoštevati tudi pri količini zbranih podatkov, njihovem obsegu obdelave, obdobjem hrambe in njihovi dostopnosti.

Upravljavci lahko najamejo obdelovalca podatkov, ki zgolj sodeluje z upravljavci, ki so pravno odgovorni za pravično obdelavo osebnih podatkov. Obdelovalec mora o vseh spremembah sproti obveščati upravljavca, njegovo obdelavo pa ureja pogodba ali drug pravni akt v skladu s pravom Unije ali pravom države članice. Vsak upravljavec mora voditi evidenco dejavnosti obdelave v okviru svoje odgovornosti, ki mora vsebovati ime in kontaktne podatke upravljavca, pooblaščene osebe za varstvo podatkov in, kadar je ustrezno, obdelovalca in skupnega upravljavca. Prav tako mora biti v njej zapisan namen obdelave, opis kategorij posameznikov in vrst osebnih podatkov, kategorije uporabnikom, katerim bodo razkriti osebni podatki, kadar je ustrezno tudi informacije o prenosu podatkov v tretjo državo.

Za varnost obdelave morata obdelovalec in upravljavec poskrbeti za izvajanje ustreznih tehničnih in organizacijskih ukrepov, kot sta psevdonimizacija in šifriranje osebnih podatkov. Prav tako morata v celotnem procesu obdelave podatkov poskrbeti za stalno zaupnost, celovitost, dostopnost in odpornost sistemov za obdelavo, v primeru fizičnega ali tehničnega incidenta pa morata biti zmožna pravočasno povrniti razpoložljivost in dostop do osebnih podatkov. Varnost obdelave osebnih podatkov mora biti zagotovljena tudi s postopkom rednega testiranja, ocenjevanja in vrednotenja učinkovitosti tehničnih in organizacijskih ukrepov.

Če pride do kršitve varnosti osebnih podatkov, je upravljavec obvezan o tem obvestiti Evropskega nadzornika za varstvo podatkov najkasneje 72 ur od kršitve. Upravljavec mora o kršitvi zasebnosti osebnih podatkov obvestiti tudi posameznika, na katerega se podatki nanašajo, če bi kršitev povzročila veliko tveganje za pravice in svoboščine posameznikov. V obvestilu mora jasno in v preprostem jeziku opisati vrsto kršitve, ter navesti ukrepe za preprečitev kršitve. Če upravljavec o kršitvi ne

obvesti posameznika, lahko Evropski nadzornik za varstvo podatkov to od njega zahteva.

Splošna uredba o varstvu podatkov je uredila »pravico do pozabe« v zadevi Google Spain, kjer je bilo odločeno, da lahko posameznik od upravljalca zbirke podatkov zahteva izbris povezave s seznama zadetkov, ki so se prikazali po izvedenem iskanju, opravljenem na podlagi imena osebe in vsebujejo informacije o navedeni osebi. M. Costeja Gonzáleza je vložil pritožbo proti družbi Google, s katero je zahteval, naj sprejme ukrepe, potrebne za umik osebnih podatkov, ki se nanašajo nanj, s svojega seznama, in v prihodnje onemogoči dostop do njih. Ker podjetje Google »išče«, »zbira«, »beleži« in »ureja« podatke ter jih po potrebi »posreduje« svojim uporabnikom v obliki seznama zadetkov, ga lahko smatramo kot obdelovalca podatkov, mora upoštevati določila Splošne uredbe o varstvu podatkov. To pomeni, da je zavezana odstraniti povezave na spletne strani s seznama zadetkov, če se posamezni zanjo odloči.

Splošno uredbo o varstvu podatkov so kršile Združene države Amerike, kot je bilo ugotovljeno v zadevi C-362/14, kjer je Sodišče ugotovilo, da ne zagotavljajo ustrezne raven varnosti prenesenih osebnih podatkov. M. Schrems je vložil tožbo proti Data Protection Commissioner (pooblaščenec za varstvo podatkov), v zvezi s predhodno vloženo tožbo proti družbi Facebook Ireland Ltd, ki je v Združene države Amerike prenašala osebne podatke svojih uporabnikov in jih shranjevala na strežnikih v tej državi. V tej je tožnik zahteval, naj pooblaščenec družbi Facebook Ireland prepove prenašanje osebnih podatkov v združene države Amerike, saj veljavno pravo in praksa v tej državi ne zagotavljata zadostne zaščite osebnih podatkov. Sodišče je ugotovilo, da ameriški sistem varnega pristana, s čimer varujejo prenesene osebne podatke, omogoča, da ameriški javni organi posegajo v temeljne pravice posameznikov, še posebej do pravice do zasebnosti. Ker v Ameriki nimajo urejenega enakega sistema obdelave osebnih podatkov, kot je urejen v Evropski uniji, lahko dostopajo do podatkov in jih obdelujejo na način, ki ni v skladu z namenom njihovega prenosa, prav tako pa posamezniki nimajo dostopa do upravnega in sodnega varstva, ki bi jim omogočalo, da lahko dostopajo do svojih podatkov, jih popravijo ali izbrišejo. Tako je Sodišče odločbo Komisije o ustreznosti varstva prenesenih osebnih podatkov spoznalo za neveljavno in zahtevalo ponovno preučitev pritožbe M. Schremsa, ter odločitev o ustavitvi prenosa podatkov evropskih uporabnikov družabnega omrežja Facebook v Združene države.

V zadevi Scarlet Extendet SA proti Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM) je Sodišče ugotovilo, da je sodba nacionalnega sodišča glede nezakonitega prenašanja datotek kršila pravico do varstva osebnih podatkov, ki ga ureja Splošna uredba o varstvu podatkov. Belgijsko sodišče je na predlog družbe SABAM od družbe Scarlet Extendet SA zahtevalo, da na lastne stroške vzpostavi sistem za filtriranje elektronskih komunikacij, ki bi pregledoval kateri prenosi datotek so nezakoniti in tako kršijo avtorske pravice. Takšen sistem bi pregledoval celotno spletno komunikacijo med uporabniki storitev družbe Scarlet Extendet SA, kar bi pomenilo vzpostavitev splošnega nadzora nad strankami. Vendar pa direktiva o elektronskem poslovanju nacionalnim organom prepoveduje sprejemati ukrepe, s katerimi bi bila ponudniku internetnega dostopa naložena obveznost splošnega nadzora podatkov, ki jih prenaša v svojem omrežju. Prav tako pa bi takšen nadzor posegal v pravico do varstva osebnih podatkov, zato je Sodišče odgovorilo, da nasprotuje odločitvi belgijskega sodišča o odreditvi sistema za filtriranje vseh elektronskih komunikacij uporabnikov storitev družbe Scarlet Extendet SA.

Spor o vzpostavitvi splošnega sistema filtriranja informacij in s tem kršenja pravice do varstva osebnih podatkov se je nadaljeval v zadevi C-360/10, vendar v tem primeru med družbama SABAM in Netlog NV. V tej zadevi je družba SABAM prav tako zahtevala vzpostavitev sistema filtriranja vseh informacij, ki si jih med seboj pošiljajo uporabniki storitev družbe Netlog NV, ki bi pregledoval in poiskal nezakonito preneseno glasbeno in avdiovizualno vsebino. Sodišče je bilo v tej zadevi mnenja, da takšen sistem, ki bi pregledoval celotno komunikacijo med vsemi uporabniki storitev, preveč posega v pravico do varstva osebnih podatkov. Takšna odreditev bi pomenila sistematično obdelavo in analizo informacij uporabnikov storitev družbe Netlog, te informacije pa so varovani osebni podatki, saj omogočajo identifikacijo uporabnika, zato bi odreditev sistema filtriranja informacij kršila pravico do varstva osebnih podatkov.

3.2.2 Zakonodaja v Sloveniji

Splošna uredba o varstvu podatkov se v Sloveniji uporablja neposredno, v veljavo je stopila leta 2016, uporablja pa se od maja 2018. Do tedaj je v Sloveniji zbiranje, obdelavo in uporabo osebnih podatkov narekoval Zakon o varstvu osebnih podatkov (v nadaljevanju ZVOP-1). [8]

[8] Zakon o varstvu osebnih podatkov, Uradni list RS, št. 94/07 – uradno prečiščeno besedilo.

Ker je zaradi izjemnega razvoja informacijsko-komunikacijske tehnologije v količini in kakovosti obdelave osebnih podatkov in so ti postali vedno bolj dostopni državi, zasebnemu sektorju ter posameznikom, so se začele izvajati vedno bolj sistemske povezave med zbirkami osebnih podatkov. S tem pa so se povečala tveganja zlorabe osebnih podatkov, kot so nepooblaščeni dostopi, množična razkritja in profiliranje posameznikov. Evropska komisija je v te namene predlagala sprejetje dveh novih pravnih aktov Evropske unije in sicer Splošno uredbo o varstvu podatkov in Predlog Direktive Evropskega parlamenta in Sveta o varstvu posameznikov pri obdelavi osebnih podatkov, ki jih pristojni organi obdelujejo za namene preprečevanja, preiskovanja, odkrivanja ali pregona kaznivih dejanj ali izvrševanja kazenskih sankcij, in o prostem pretoku takih podatkov ter o razveljavitvi Okvirnega sklepa Sveta 2008/977/PNZ.[9]

Zaradi sprejetja teh aktov, se je morala tudi slovenska zakonodaja spremeniti in prilagoditi, zato je bilo pripravljeno besedilo predloga novega Zakona o varstvu osebnih podatkov (v nadaljevanju **ZVOP-2**).[10] S tem bi se zagotovilo izvrševanje določb Splošne uredbe o varstvu podatkov in visok nivo varstva osebnih podatkov v Republiki Sloveniji ter uresničevanje osebne človekove pravice do varstva osebnih podatkov, vsakršno neupoštevanje teh določil pa bi bilo kaznovano z natančno določenimi sankcijami. Tudi informacijski pooblaščenec je izrazil svoje mnenje o predlogu novega zakona o varstvu podatkov, kjer je tudi opozoril na še ne dorečene zadeve. Jasno je potrebno določiti kakšen nadzor bo veljal glede zakonitosti obdelave osebnih podatkov, ki jih izvajajo varnostnoobveščevalne službe in takšno določitev jasno zakonsko predeliti in urediti. Prav tako je med drugim potrebno tudi uskladit in jasno uredit pritožbeni postopek glede izvajanja pravic ter nameniti dodatno pozornost ureditvi kazenski določb v predlogu.

V 2020 pa je bil še zmeraj v veljavi ZVOP-1, v katerem je zapisano, da se osebni podatki obdelujejo zakonito in pošteno, ter morajo biti ustrezni in po obsegu primerni glede na namene, za katere se zbirajo in nadalje obdelujejo. Varstvo osebnih podatkov je zagotovljeno vsakemu posamezniku ne glede na njegovo narodnost, raso, barvo, veroizpoved, etično pripadnost, spol, jezik,… Osebni podatki se lahko obdelujejo le, če je posameznik privolil v obdelavo ali če to določa zakon.

[9] Okvirni sklep Sveta 2008/977/PNZ z dne 27. novembra 2008 o varstvu osebnih podatkov, ki se obdelujejo v okviru policijskega in pravosodnega sodelovanja v kazenskih zadevah, Uradni list Evropske unije, L 359/60, 30.12.2008.

[10] Zakon o varstvu osebnih podatkov (Uradni list RS, št. 94/07 – uradno prečiščeno besedilo in 177/20).

Posameznik mora biti o obdelavi osebnih podatkov seznanjen pisno ali na drug ustrezen način, oz. če je obdelava določena v zakonu.

Osebne podatke lahko obdeluje obdelovalec, če je podpisal pogodbo z upravljavcem in je registriran za opravljanje takšne dejavnosti. Občutljivi osebni podatki, kot so podatki o rasnem, narodnem poreklu, političnem, verskem ali filozofskem prepričanju, spolnem življenju itd. se lahko obdelujejo zgolj v uredbi določenih primerih. Prav tako morajo biti pri obdelavi posebej označeni in zavarovani s kriptografskimi metodami in nečitljivostjo elektronskih podpisov.

Vsi osebni podatki, vneseni v zbirko podatkov, morajo biti točni in ažurni, prav tako pa mora upravljavec o obdelavi obvestiti posameznika. V zbirk podatkov ni dovoljena uporaba istega povezovalnega znaka, da ostane identiteta posameznika prikrita. Osebni podatki se lahko shranjujejo le toliko časa, kolikor služijo doseganju namena, za katerega so se zbirali in obdelovali, po izpolnitvi namena se izbrišejo, uničijo, blokirajo ali anonimizirajo.

Zbirke osebnih podatkov se morajo varovati pred slučajnimi ali namernimi nepooblaščenimi uničenjem podatkov tako, da se varujejo prostori, oprema in sistemska programska oprema zbirke, ter aplikativna programska oprema s katero se obdelujejo podatki. Preprečevati se mora nepooblaščen dostop do osebnih podatkov med njihovim prenosom in zagotavljati učinkovit način uničenja, izbrisa ali anonimizacije osebnih podatkov. Zbirke osebnih podatkov se med seboj lahko povezujejo le, če zbirke ne vsebujejo občutljivih podatkov ali podatkov iz kazenske evidence in prekrškovnih evidenc. O združevanju so upravljalci dolžni obvestiti posameznike, o katerih se podatki zbirajo.

Državni nadzorni organ za varstvo osebnih podatkov vodi in vzdržuje register zbirk osebnih podatkov, ki mora biti dostopen vsakemu posamezniku. Prav tako ima posameznik možnost zaprositi za vpogled v katalog zbirke osebnih podatkov upravljavca osebnih podatkov, ki mu mora omogočiti tudi potrditev, ali se podatki v zvezi s posameznikom obdelujejo, posredovanje izpisa posameznikovih osebnih podatkov iz zbirke in seznam uporabnikov, katerim so bili podatki posredovani. Vsak posameznik ima pravico do dopolnitve, popravka, blokiranja in izbrisa lastnih podatkov iz baze, prav tako pa ima pravico do ugovora, s čimer se njegovi osebni podatki prenehajo obdelovati. Če posameznik ugotovi, da so mu kršene njegove pravice, zapisane v zakonu, lahko zahteva sodno varstvo ves čas, dokler kršitev traja.

Upravljavcu osebnih podatkov je dovoljeno uporabljati osebne podatke posameznikov tudi za namene neposrednega trženja, torej ponujanja blaga, storitev, zaposlitve, itd. V ta namen lahko uporablja zgolj osebne podatke posameznikov, kot so osebno ime, naslov prebivališča, telefonsko številko, naslov elektronske pošte in številko telefaksa. O lastni uporabi osebnih podatkov za neposredno trženje je upravljavec primoran obvestiti posameznika, prav tako tudi ob posredovanju podatkov drugim uporabnikom podatkov za namene neposrednega trženja. Posameznik pa ima pravico kadarkoli prekiniti obdelavo podatkov za namene neposrednega trženja, kar mora upravljavec upoštevati.

3.2.2.1 Informacijski pooblaščenec

Informacijski pooblaščenec med drugim skrbi tudi za to, da je obdelava osebnih podatkov v skladu z trenutno veljavno zakonodajo. To je Splošna uredba o varstvu podatkov, ki velja na Evropski ravni, ter nacionalna zakonodaja, ki ureja varstvo osebnih podatkov. Informacijski pooblaščenec lahko tudi preprečuje in odpravlja kršitve na tem področju.

Če posameznik meni, da so mu bile kršene pravice v zvezi z varovanjem zasebnosti in se njegovi podatki ne obdelujejo zakonito, lahko poda prijavo informacijskemu pooblaščencu. Pred vložitvijo prijave lahko posameznik zahteva seznanitev z lastnimi osebnimi podatki, lahko pa zahteva tudi popravek, omejitev obdelave ali popoln izbris svojih nezakonito obdelovanih podatkov. Posameznik lahko pri upravljavcu uveljavlja svojo pravico do prenosljivosti, ki jih je posameznik posredoval na podlagi privolitve ali pogodbe z upravljavcem. Ta pravica omogoča posamezniku, da pridobi svoje osebne podatke v strukturirani, splošno uporabljeni in razumljivi obliki, katere lahko dalje posreduje drugemu upravljavcu, ne da bi ga prvi pri tem oviral.

Informacijski pooblaščenec lahko, po relevantnih določbah Zakona o varstvu osebnih podatkov, Splošne uredbe o varstvu podatkov in subsidiarno na podlagi določb Zakona o inšpekcijskem nadzoru ter Zakona o splošnem upravnem postopku, izvaja inšpekcijski nadzor. Informacijski pooblaščenec lahko v okviru inšpekcijskega nadzora preverja ravnanje zavezancev za varstvo osebnih podatkov, če je skladno z zakonodajo. Nadzira, da se osebni podatki obdelujejo zakonito in pregledno, so ukrepi, da se zagotovi varovanje osebnih podatkov po členu 32 Splošne uredbe o varstvu podatkov, da se izvajajo določbe te uredbe, ki urejajo

posebna izraze načela odgovornosti, kot so uradno obveščanje nadzornih organov in posameznikov o kršitvi varnosti, ocene učinka, evidence dejavnosti obdelave, itd. S Splošno uredbo o varstvu podatkov ima informacijski pooblaščenec preiskovalna in popravljalna pooblastila, prav tako pa skrbi za informacijsko varnost državljanov.

3.2.3 Pravni in politični okvir za umetno inteligenco v Evropski uniji

3.2.3.1 Program digitalne Evrope za obdobje 2021-2027

Umetna inteligenca, napredno računalništvo in obdelava podatkov ter kibernetska varnost, bodo v prihodnosti temelj digitalne preobrazbe gospodarstva in družbe EU. Cilj predloga Uredbe Evropskega parlamenta in sveta o vzpostavitvi programa za digitalno Evropo za obdobje 2021–2027[11] je podpreti digitalno preobrazbo evropskega gospodarstva in družbe. Predlagana pravila iz vseh področij upoštevajo pravico posameznika do varstva zasebnosti, v skladu z 8. členom Listine. S Splošno uredbo o varstvu podatkov se bo zagotovil prost pretok osebnih podatkov med državami članicami EU, prav tako pa se bo okrepilo zaupanje ter varnost posameznikov. Na področju umetne inteligence bi morali vsi ukrepi, ki vključujejo obdelavo osebnih podatkov, podpirati Splošne uredbe o varstvu podatkov. V sklopu programa bi se na področju umetne inteligence povečala njena zmogljivost in zbiranje ter obdelava podatkov. Za izboljšanje kibernetske varnosti bi Unija podprla javno naročanje napredne opreme, orodij in podatkovnih infrastruktur, prav tako pa bi zagotovila široke uvedbe najnovejših rešitev za kibernetsko varnost.

3.2.3.2 Pravila civilnega prava o robotiki

Leta 2017 so bila sprejeta Pravila civilnega prava o robotiki, v Resoluciji Evropskega parlamenta s priporočili Komisiji o pravilih civilnega prava o robotiki (2015/2103(INL)) (2018/C 252/25)[12] , ki je med drugim opredelila tudi varstvo zasebnosti v dobi digitalizacije in vzpona robotike. Evropski parlament je ugotovil, da bi bilo potrebno nameniti pozornost robotom, ki pridobivajo in posredujejo osebne in občutljive podatke, saj lahko z nepravilnim ravnanjem ogrozijo zaupnost. Prav tako pa je potrebno zagotoviti skladna čezmejna pravila, katera bodo upoštevale

[11] Predlog UREDBA EVROPSKEGA PARLAMENTA IN SVETA o vzpostavitvi programa za digitalno Evropo za obdobje 2021–2027, COM/2018/434 final - 2018/0227.
[12] Resolucija Evropskega parlamenta s priporočili Komisiji o pravilih civilnega prava o robotiki (2015/2103(INL)), Uradni list Evropske unije, C 252/239, 18.7.2018, str. 239–257.

vse članice Unije, saj je za zavarovanje podatkov nujno potrebno sodelovanje med državami. Predpisi civilnega prava v sektorju robotike se morajo prilagoditi v skladu s Splošno uredbo o varstvu podatkov, prav tako pa se mora spoštovati pravico o varstvu osebnih podatkov, zapisano v 8. členu Listine EU o temeljnih pravicah.

Natančneje se morajo opredeliti pravila in merila za uporabo kamer in senzorjev v robotih, ki pridobivajo osebne podatke o posameznikih. Spoštovati pa se morajo tudi ostala načela o varstvu podatkov, kot so vgrajena in privzeta zasebnost, zmanjšanje količine podatkov, omejitev namena zbiranja podatkov, ter pregledni nadzorni mehanizmi za posameznike. Ker je prost pretok podatkov bistven za digitalno gospodarstvo sektorja umetne inteligence, je potrebno zagotoviti visoko raven varnosti v robotskih sistemih in v omrežjih povezave robotov, zasebnost pa je potrebno spoštovati tudi v komunikaciji med ljudmi, roboti in umetno inteligenco. Načrtovalci umetne inteligence imajo odgovornost razvijati varne, zaščitene in namenu prilagojene izdelke, ki ne smejo ogrožati varnosti zasebnosti posameznika.

Evropski parlament poziva evropsko Komisijo, da bo razvoj avtonomnih vozil zelo vplival na zasebnost posameznika, še posebej na področjih dostopa do podatkov, varstva podatkov in njihove izmenjave med povezanimi napravami. Ker je Evropski parlament predlagal tudi, da se pridobi večja avtonomnost avtonomnih vozil preko senzorjev in/ali z izmenjavo podatkov z lastnim okoljem in analizo le teh, bo potrebno večjo pozornost nameniti zavarovanju zasebnosti pred neželenimi vdori v sistem. Zasebnost državljanov bo potrebno bolje zavarovati na področju brezpilotnih zrakoplovov, saj bo moral imeti vsak brezpilotni zrakoplov vgrajen sistem za sledljivost in identifikacijo. Prav tako bo potrebno na področju popravljanja in izboljšanja človeka zagotoviti varnost pred vdorom v kibernetsko-fizične sisteme robotike, kot so recimo robotske proteze, kar bi lahko ogrozilo človeško zdravje, v skrajnih primerih pa tudi življenje.

Prav tako pa Evropski parlament poziva vse raziskovalce in načrtovalce, da naj ravnajo odgovorno in pri svojem delu upoštevajo potrebo po spoštovanju zasebnosti in dostojanstva ljudi, čeprav je kodeks prostovoljen. Vse raziskovalne dejavnosti bi bilo treba izvajati v skladu s previdnostnim načelom, torej s predvidevanjem morebitnih varnostnih vplivov, tudi na varovanje zasebnosti posameznika, kar spodbuja napredek v korist družbe.

3.2.3.3 Strategija za kooperativne inteligentne prometne sisteme

Leta 2018 je stopila v veljavo Resolucija Evropskega parlamenta o evropski strategiji za kooperativne inteligentne prometne sisteme (2017/2067(INI))[13], v kateri Evropski parlament med drugim, z ozirom na 7. in 8. člen Listine Evropske unije o temeljnih pravicah, glede prihodnosti storitev C-ITS opozarja na pomen izvajanja zakonodaje EU na področju zasebnosti in varstva podatkov. Opozarja, da je podatke potrebno uporabljati zgolj za namene C-ITS in se ne smejo hraniti ali uporabljati v druge namene, pametni avtomobili pa morajo biti povsem v skladu s Splošno uredbo o varstvu podatkov in povezanimi predpisi. Povečati je potrebno preglednost in algoritmično odgovornost obdelave in analize podatkov, ki ju izvajajo obdelovalci, prav tako pa se lahko s tehnikami anonimizacije poveča zaupanje uporabnikov v storitve C-ITS.

Varstvo podatkov in zaupnost je potrebno upoštevati skozi celotno obdelavo, Evropski parlament pa predlaga tudi oblikovanje aplikacij in sistemov z ozirom na vgrajeno in privzeto zasebnostjo in varnostjo podatkov. Predvsem pa poudarja, da je potrebno v pametnih vozilih omogočiti možnost »nepovezanega načina«, kar bi omogočilo, da bi uporabniki vozili avtomobil, ne da bi se osebni podatki prenašali v druge naprave. Za zagotavljanje varnosti komunikacij med sistemi C-ITS bo potrebno vzpostaviti visoke standarde kibernetske varnosti za preprečevanje vdorov in kibernetskih napadov. Z oblikovanjem skupne politike za varnost in potrdila v zvezi z uvedbo C-ITS, bo Evropski parlament poskušal preprečiti kakršnakoli tveganja za vdor v podatkovne zbirke avtomatiziranih vozil, saj so le-te najbolj izpostavljene kibernetskim napadom. V vseh državah članicah je potrebno izvajati visoke in harmonizirane varnostne standarde, ki bi tretjim strankam onemogočali dostop do vgrajenih sistemov, s čimer bi se lastnikom omogočila neodvisnost od proizvajalcev avtomobilov.

3.2.3.4 Posledice umetne inteligence za enotni (digitalni) trg

Leta 2017 je Evropski socialno-ekonomski odbor (EESO) sprejel mnenje o umetni inteligenci in njenih posledicah za enotni (digitalni) trg, proizvodnjo, potrošnjo, zaposlovanje in družbo[14], v katerem je opozoril na uporabo inteligence na

[13] Resolucija Evropskega parlamenta z dne 26. maja 2016 o strategiji za enotni trg (2015/2354(INI)), Uradni list Evropske unije, C 76, 28.2.2018, str. 112–127.

[14] Mnenje Evropskega ekonomsko-socialnega odbora – Umetna inteligenca – Posledice za enotni (digitalni) trg, proizvodnjo, potrošnjo, zaposlovanje in družbo (mnenje na lastno pobudo), Uradni list Evropske unije, C 288, 31.8.2017, str. 1–9

mednarodni ravni in skrbi za uveljavljanje etičnega kodeksa v Evropski uniji. Prav tako je EESO priporočil vzpostavitev sistema standardizacije, ki bi omogočil stalno preverjanje, potrjevanje in nadzor umetne inteligence, ter temeljito oceno evropske zakonodaje in predpisov, ki jih bo v prihodnosti potrebno prilagoditi.

Ker se je uporaba umetne inteligence implementirala na številna področja vsakodnevne uporabe, kot so gospodinjski aparati, pametne ure in zapestnice, igrače ter avtomobili, je potrebno poskrbeti za varnost zasebnosti, saj vse te naprave zbirajo osebne podatke, prodaja podatkov, ki jih zbere proizvajalec, pa je trenutno v polnem razmahu. Prav tako je s pomočjo umetne inteligence možno zbirati in analizirati veliko količino osebnih podatkov, katerih obdelava se kasneje uporabi za manipulacijo na številnih področjih, kot so poslovne odločitve in volitve itd. EESO opozarja tudi, da se je pri uporabi umetne inteligence potrebno izogniti omejevanju svobode posameznikov ter poskrbeti da bo razvoj na tem področju skladen z uredbo o varstvu podatkov. Pri prenosu podatkov mora tako biti spoštovana pravica do privolitve v obdelavo na podlagi seznanitve, prav tako pa tudi pravica dostopa do prenesenih podatkov, spremembe in preverjanja podatkov.

3.3 Uporaba umetne inteligence

3.3.1 Internet stvari

Internet stvari je skupek tehnologij za prepoznavanje stvari, senzornega zaznavanja in zmožnosti komuniciranja naprav z okoljem. Tehnologija interneta stvari temelji na komuniciranju preko tehnologije RFID. Za delovanje potrebuje podatke, ki jih pridobivajo in zbirajo vse medsebojno povezane naprave. Na osebni ravni je internet stvari uporaben za povečanje učinkovitosti gospodinjstva, saj dovoljuje da povezane naprave med seboj komunicirajo in reagirajo. Primer dobre prakse je recimo prižiganje pralnega stroja, ko je elektrika cenejša, pregled hladilnika in ustvarjanje seznama stvari, ki jih je zmanjkalo, ali pa prilagajanje svetlobe in glasbe glede na zvočni ukaz posameznika.

Za delovanje interneta stvari morajo senzorji z vseh povezanih naprav sprejemati in shranjevati osebne podatke, ki jih potrebujejo za usklajeno delovanje. Ker imajo senzorji, ki sprejemajo in posredujejo podatke povezanim napravam, zelo majhno zmogljivost shranjevanja podatkov, se le ti shranjujejo na spletu. Na vseh ravneh povezane verige je mogoč dostop hekerjev v sistem in dostop do zbirke podatkov.

Največkrat se vdor zgodi na Wi-Fi ruterju, saj se tukaj zberejo vsi podatki, preden se kompresirajo in pošljejo na splet v nadaljnjo obdelavo. Na tej fazi podatki še niso zakodirajo in anonimizirani, zato je zasebnost posameznika na tej točki najbolj ogrožena.

Takšni podatki so navadno zavarovani z različnimi tehnikami, kot je recimo tehnologija PPDM, PET, ki vsebuje virtualne zasebne spletne mreže, varnost transportnega sloja, DNS varnostna razširitev, čebulno usmerjanje in zasebno iskanje informacij. Prav tako je bila ustvarjena tehnologija PbD, ki skrbi za varnost in ohranjanje zasebnosti na vseh nivojih delovanja interneta stvari in je skladna s Splošno uredbo o varstvu podatkov. Te tehnologije skrbijo za varen prenos podatkov med napravami in tudi za ohranjanje identitete posameznika, vendar je v baze podatkov vseeno mogoče vdreti in jih posredovati tretjim osebam.

Da se zagotovi visoka stopnja varnosti podatkov, je nujno potrebno zagotoviti varen sistem kodiranja povezanih naprav, ki so odporne proti zlonamernim prilagoditvam kode. Z integracijo informacijskih tehnologij je postala zaščita proti spletnih vdorom vedno bolj pomembna funkcija povezanih naprav, zato dandanes oblikovalci industrijskega interneta stvari varnosti naprav posvečajo veliko pozornosti. Ker pa se prilagoditve informacijskih komponent na spletne vdore lahko ustvarijo šele po zlonamernem napadu, so industrijski sistemi interneta stvari ranljivi za različne spletne napade.

Napadi na industrijski internet stvari so lahko izvedeni na vseh abstraktnih ravneh delovanja, torej človeški, mehanski, spletni, programski in elektronski. Prva je človeška raven, kjer lahko hekerji pridobivajo podatke preko socialnega inženiringa ali lažnega predstavljanja (ang. *»phishing«).* Druga raven je mehanska, kjer lahko hekerji vdrejo v računalnike in pridobijo podatke na takšen način. Naslednja raven je mreženje, kjer se lahko zasebni podatki pridobivajo preko spletnega prisluškovanja, napada preko tretje osebe ali navidezno preobremenjenostjo sistema. Napadi pa se lahko zgodijo tudi na programsko opremo, kjer zlonamerni hekerji pridobivajo informacije z obratnim inženiringom, vdorom v računalniški sistem in invazivnimi napadi.

Cilji zavarovanja mreže povezanih naprav so velika razpoložljivost naprav, preprečevanje sistemskih napak, shranjevanje zgodovine delovanja posameznih naprav in najpomembnejši, zavarovanje integritete in zaupnosti podatkov. Na

podlagi teh ciljev se lažje ustvari varovanje pred spletnimi napadi, da lahko mreža naprav kljub vdoru v sistem deluje skoraj normalno. Skozi celotno delovanje mreže povezanih naprav morata biti zagotovljena aspekta varnosti in zasebnosti podatkov.

Zasebnost vključuje skrivanje zasebnih podatkov in tudi skrb za pravilno obravnavo podatkov. To pomeni, da lastniki zbirk podatkov ne smejo zbranih podatkov posredovati tretjim osebam, kot so recimo država, privatni sektorji in marketinškim podjetjem. Baza podatkov mora prav tako biti odporna na kakršnikoli napad, ter prilagoditi svoje delovanje v primeru napada. Vsebovati mora avtentične podatke, ki so preverjeni, lastnik baze pa mora imeti dostop do vseh podatkov, ter jih po potrebi posredovati lastnikom podatkov. Do podatkov je omogočen dostop le osebam, o katerih so podatki zbrani. Za varovanje zasebnosti morajo biti vsi podatki anonimni, kar pomeni, da iz njih ne moremo ugotoviti identitete posameznika. Vsi podatki morajo zato biti šifrirani, nepovezani in nedoločljivi, kar znižuje možnost identificiranja posameznika pri posredovanju podatkov tretji osebi.

Najbolj zaskrbljujoče tveganje za kršitev pravice do zasebnosti pa je zbiranje zasebnih informacij o posamezniku preko številnih medsebojno povezanih naprav, kot so identifikacijski podatki in vedenjski vzorci. Z napredkom tehnologij za pridobivanje, shranjevanje in obdelavo teh podatkov mora biti tudi pravilo prilagojena zakonodaja glede varovanja človekove zasebnosti. Direktiva, ki je že bila sprejeta na tem področju je Direktiva 95/46/ES in trenutno veljavna Uredba (EU) 2016/679. Vendar pa zgolj to ni dovolj, saj se neobdelani podatki, pridobljeni iz naprav, povezanih v internet stvari, ne smatrajo kot strogo osebni, saj preko njih ne moremo identificirati posameznika. Tako se ti podatki ne morejo zaščititi z uredbo GDPR, saj podatki tehnično gledano niso osebni. Ti podatki postanejo osebni zgolj z analiziranjem in različnimi kombinacijami v kasnejših fazah obdelave podatkov.

Prav tako so velika grožnja varovanju zasebnosti tudi tehnološke inovacije, ki omogočajo razvoj interneta stvari. Vendar pa so tehnologije lahko tudi del rešitve zasebnosti, če so ustvarjene in uporabljene na način, ki se sklada s standardi zasebnosti. Z naraščanjem števila zbranih podatkov s senzorjev, ki zbirajo informacije tudi o napravi sami, bo še bolj ogrožena varnost posameznika, saj kontekstualni podatki predstavljajo dodatno znanje o posamezniku in njegovi zasebnosti. Ti podatki niso šifrirani, saj je njihova pomembnost zelo majhna, vendar eksponentno narašča, če te podatke povežemo v celoto, zato bi bilo potrebno tudi takšne podatke zaščititi že v najzgodnejši fazi.

3.3.2 Avtonomna vozila

Avtonomna vozila so vsa računalniško nadzorovana vozila, ki se za samostojno vožnjo zanašajo na številne podatke, pridobljene iz različnih senzorjev vozila ali drugih vozil. S temi podatki lahko računalnik v vozilu prilagaja vožnjo okolju in nadzira delovanje vozila. Avtonomna vozila s funkcijami, kot so samodejno krmiljenje in parkiranje, samodejna menjava voznega pasu ter preprečevanje stranskih trkov, lahko zelo izboljšajo naša življenja. Vožnja bo postala enostavnejša, vozila bodo ljudem omogočala večjo produktivnost, saj bodo lahko med vožnjo opravljali druge funkcije, ne zgolj upravljanje vozila. Zaradi odstranitve človeškega faktorja (nepravilna ocena situacije, vinjenost zmanjšanost koncentracije, brezbrižnost ali prevelika naglica voznika ter napačno predvidevanje vožnje drugih voznikov), bo vožnja avtonomnih vozil varnejša.

Tehnologija, ki je vgrajena v avtonomne avtomobile, omogoča avtomatizacijo številnih funkcij, ki služijo kot pomoč pri vožnji, kot so tempomat, prostoročno telefoniranje, navodila po korakih in satelitske storitve. Vse te funkcije povečujejo število zbranih podatkov o vozniku in avtomobilu kot so podatki o lokaciji avta, stanje avtomobila, merjenje dostopa do podatkovnih storitev, čas, preživet v avtomobilu, itd. Avti tako postajajo vedno bolj integrirani z računalniškimi in telekomunikacijskimi tehnologijami, kar pomeni nov vir zbiranja podatkov o posamezniku.

Osebni avtomobili z različnimi senzorji nenehno zbirajo podatke o samem avtomobilu in tudi okolju, da se lahko nanj pravilno odzovejo v določeni situaciji. Zbirajo se podatki o tem kam se avto vozi, kje je bil, kaj se je z vozilom dogajalo med vožnjo in navade voznika. Vozilo tudi zbira podatke o tem kje je »voznik«, kaj počne, katere kraje je obiskal in katere še namerava. Te informacije so lahko povezane z drugimi informacijami. Lokacija parkiranega vozila sporoča o tem, kje stanuje lastnik, iz česar lahko ugotovimo njegovo splošno finančno stanje, ter napovemo njegova prihodnja dejanja. Če se ti podatki povežejo s posameznikom, ki ga je mogoče identificirati, podatki postanejo osebni, ti pa se nekje zbirajo in shranjujejo, kar predstavlja veliko grožnjo posameznikovi zasebnosti.

Ker avtonomna vozila za svoje delovanje potrebujejo nenehen pretok podatkov v realnem času med uporabnikom in okoljem ter med uporabnikom in shrambo podatkov, je kibernetski napad na sistem vozila mogoč preko različnih vstopnih

točk. Vendar pa proizvajalci avtov ne morejo izolirati vsakega senzorja, saj morajo ti komunicirati med sabo.

Evropska komisija je v svojem sporočilu Na poti do avtomatizirane mobilnosti: strategija EU za mobilnost prihodnosti[15] maja 2018 potrdila, da še vedno obstaja možnost kibernetskega napada in posledično prevzema nadzora nad vozilom. Do zdaj še ne obstaja sektorski pristop v zvezi z zaščito vozil pred kibernetskimi napadi, vendar v zvezi z varstvom podatkov v EU veljajo predpisi za vso obdelavo podatkov, tudi tistih, pridobljenih iz avtonomnih vozil. V Ameriki so bile pripravljene smernice za zaščito vozil pred kibernetskimi napadi, Komisija pa jih namerava uvesti tudi v Evropsko zakonodajo. Do zdaj so bile objavljene le smernice o politiki za potrdila in varnost komunikacije med vozili in ostalo infrastrukturo.

Pri vzpostavitvi nove zakonodaje o avtonomnih vozilih je potrebno vključiti varstvo osebnih podatkov uporabnikov povezanih vozil, saj morajo ti imeti zagotovilo, da so njihovi podatki skrbno obdelani ter biti obveščeni kako in za kakšne namene se uporabljajo in da lahko svoje podatke učinkovito nadzirajo. Podatki, pridobljeni iz avtonomnega vozila, bodo veljali za osebne, zato mora biti njihova obdelava skladna z že obstoječo zakonodajo, prav tako pa more v njihovo obdelavo privoliti uporabnik sam. Odzivi na javno posvetovanje so pokazali, da so lastniki avtonomnega vozila pripravljeni v deljenje osebnih podatkov, če so ti uporabljeni za povečanje varnosti v cestnem prometu ali izboljšanja upravljanja prometa.

Iz tega lahko sklepamo, da bi bili uporabniki pripravljeni deliti svoje osebne podatke v zvezi z avtonomnim vozilom, če bi ponudniki C-ITS (sodelovalni inteligentni prometni sistemi) storitev natančno opredelili pogoje uporabe, ter jih zapisali v jasnem in preprostem jeziku, na razumljiv način. Vendar pa bo uvedba C-ITS sistema v EU bo začasno odložena, dokler se ne vzpostavi zakonodaja za varovanja vozil pred vdori v sisteme in kibernetskimi napadi, s čimer se bo zagotovila tudi večja varnost osebnih podatkov končnih uporabnikov. Za vzpostavitev vseevropskega varnostnega okvirja za avtonomna vozila, bo potrebno upoštevati vse vključene strani, tako javne organe, kot tudi upravljalce cest, proizvajalce vozil ter dobavitelje in operaterje storitev C-ITS.

[15] Sporočilo Komisije Evropskemu parlamentu, Svetu, Evropskemu ekonomsko-socialnemu odboru in Odboru regij, Na poti do avtomatizirane mobilnosti: strategija EU za mobilnost prihodnosti, COM/2018/283 final.

Evropska Komisija je v Sporočilu Evropskemu parlamentu, svetu, Evropskemu ekonomsko-socialnemu odboru in odboru regij predstavila Evropsko strategijo za kooperativne inteligentne prometne sisteme, ki predstavlja mejnik na poti h kooperativni, povezani in avtomatizirani mobilnosti[16]. V njem je zapisala, da bi lahko osebni podatki, zbrani v osebnih avtonomnih vozilih, bili zlorabljeni v različne namene, recimo s strani oglaševalskim agencije, kjer bi zbrane osebne podatke posameznika uporabili za prilagojene oglase in oglaševalske kampanje. Prav tako bi se lahko podatki zbirali v namene deanonimizacije posameznika, pri čemer bi lahko iz zbranih, sicer neosebnih podatkov, kot je lokacija avtomobila, ugotovili identiteto posameznika. Da bi se povečalo zaupanje v avtonomna vozila med ljudmi, so strokovnjaki predlagali večjo transparentnost zbiranja, obdelovanja, shranjevanja in uporabe podatkov. Grožnjo zasebnosti posameznika predstavljajo tudi avtonomna vozila, uporabljena v javnem prevozu ali podjetjih, saj bi se lahko sledilo vožnji avtomobila med celotno potjo, kar bi ogrozilo človekovo zasebnost in njegovo svobodo.

Osebno avtonomno vozilo je lahko ustvarjeno tako, da zbira minimalno količino osebnih podatkov lastnika, prav tako pa so podatki samega avtonomnega avta šifrirani in anonimni. Ker se po Uredbi GDPR podatki smejo hraniti le toliko časa, dokler služijo nekemu namenu, se lahko zasebnost lastnika ohrani na ta način, da se po določenem času izbrišejo podatki o njegovi lokaciji. To bi zmanjšalo tveganje, da bi se podatki zlorabljalo v prihodnje namene. Prav tako lahko k varovanju zasebnosti pripomoremo s pravilno zaščito podatkov, torej z anonimizacijo in šifriranjem.

Za zavarovanje posameznikove zasebnosti so nekatere države v EU sprejele neobvezne smernice o zasebnosti, ki jih proizvajalci avtonomnih vozila lahko upoštevajo. Evropska unija se je že leta 2009 začela zavedati tveganj, ki jih zasebnosti prinašajo avtonomna vozila in je od proizvajalcev zahtevala, da se tudi med proizvajanjem vozil upošteva varovanje osebnih podatkov posameznika. Zasebnost posameznika se je zelo zavarovala z uvedbo Uredbe GDPR med drugim tudi tako, da so okrepili pogoje za strinjanje z zbiranjem podatkov, prav tako pa so se zvišale kazni za kršitve uredbe.

[16] Sporočilo Komisije Evropskemu parlamentu, Svetu, Evropskemu ekonomsko-socialnemu odboru in Odboru regij, Evropska strategija za kooperativne inteligentne prometne sisteme – mejnik na poti h kooperativni, povezani in avtomatizirani mobilnosti, COM/2016/0766 final.

3.3.3 Deepfakes

Umetno oblikovani videoposnetki oziroma deepfakes so ustvarjeni s pomočjo umetne inteligence, natančneje mehansko naučenih algoritmov, ki delujejo na podlagi nevronskih povezav in programske opreme za kartiranje obraza. Na teh posnetkih so obrazi ljudi zamenjani z obrazi drugih ljudi, ki niso v povezavi z videoposnetkom. To so digitalno manipulirani posnetki zvoka, slike ali videa tako, da osebe na posnetku lažno predstavljajo nekoga. S tem se na enostaven način lahko ukrade identiteta posameznika in se ustvari lažna percepcija druge osebe, katere obrazne poteze in zvok so dodane umetno ustvarjenemu posnetku. Na takšen način se kratijo pravice do zasebnosti osebi ali osebam na originalnem posnetku in tudi osebi ali osebam na umetno ustvarjenem posnetku. Takšen poseg v zasebnost posameznika lahko povzroči psihično škodo zaradi osramotitve in zadrege, lahko pa tudi vodi v izgubo kariere in ugleda posameznika v družbi.

Deepfake se po taksonomiji raziskave na Oxfordu leta 2020 razdeli na štiri kategorije, maščevalna pornografija, politične kampanje, zmanjšanje transakcijskih stroškov ter kreativni in originalni deepfake. Vendar pa pri vseh kategorijah obstaja grožnja zasebnosti posameznika.

Prva kategorija, maščevalna pornografija, je ustvarjena z namenom povzročitve ponižanja posameznika, navadno znane osebe. Pri tem se obraz osebe na izvirnem posnetku zamenja z obrazom znane osebe, katera ni dovolila takšne uporabe, saj zanjo ni vedela. Takšna uporaba slik in videoposnetkov posameznika se tretira kot poseg v spolno zasebnost posameznika, ki je nujna za razvoj osebnosti, intimnosti in enakosti. Deepfake posnetki so velikokrat del spolnega ponižanja in izkoriščanja ter fizične, mentalne ali finančne zlorabe.

Druga kategorija, politične kampanje, je ustvarjena z namenom zavajanja množice o izjavah politikov. Leta 2018 je podjetje Buzzfeed ustvarilo deepfake, s katerim je želel opozoriti javnost, kako enostavno je ustvariti neresničen video, ki se zdi, da je resničen. Na njem je bivši predsednik Barack Obama, ki v svojem glasu govori stvari, ki jih sam nikoli ne bi izrekel. Video je bil ustvarjen tako, da se je obrazna mimika Obame prilagajala obrazni mimiki osebe iz Buzzfeed, tako da je izgledalo, kot da sam govori besedilo. Takšne oblike deepfake posnetkov lahko zmanjšajo ugled posameznika v družbi, prikazujejo napačne ali izmišljene dogodke, ali pa vplivajo na demokratične procese države, kot so politične volitve.

Nevarnost deepfake posnetkov je ta, da ustvarjajo iluzijo resničnosti, ki je tako prepričljiva, da zavede gledalce v mišljenje, da so njihovi politiki in znane osebe govorili in delali stvari, ki jih nikoli ne bi, kar lahko privede do nezaupanja v te osebe. Prav tako ne bi več mogli zaupati video vsebinam, daj bi jih lahko kdorkoli spreminjal. Nekateri strokovnjaki trdijo, da imajo lahko »fake news«, vključno z deepfake posnetki bolj razpršen učinek kot navadne politične kampanje. Prav tako so študije pokazale, da ljudje precenjujemo lastno zmožnost ločevanja resničnega od neresničnega in da precenjujemo politične novice, ki so v skladu z našim mišljenjem, podcenjujemo pa novice, ki niso. Zato bomo verjeli le tistemu, kar se za nam zdi smiselno, torej tudi deepfake posnetkom, če bodo v skladu z našimi prepričanji.

Deepfakes posnetki lahko ostanejo na spletu za vedno in jih je zelo težko odstraniti, saj lahko se po izbrisu z določene platforme ponovno pojavijo na njej ali pa se pojavijo na novi platformi. Deepfake se večinoma uporabljajo za posmehovanje slavnih oseb, saj njihov obraz »nadenejo« drugi osebi, ki počne nekaj, kar javnost smatra za sramotno. Posnetki so uporabljeni tudi za izsiljevanje, umetno ustvarjen slikovni material, politično sabotažo, propagando in celo »fake news«. Deepfake posnetki predstavljajo veliko grožnjo zasebnosti posameznika, saj omogočajo komurkoli, da ponaredi video ali avdio posnetek osebe, v katerem sporoča želeno idejo ustvarjalca. Ker ljudje navadno verjamemo kar vidimo in sta video ali slika najmočnejši obliki prepričevanja, ne bomo podvomili v besede osebe na posnetku, saj bo zaradi napredne tehnologije izgledala zelo resnično.

Veliko grožnjo zasebnosti posameznika je predstavljala aplikacija za izdelavo deepfake posnetkov, imenovana ZAO. Aplikacija, s katero je lahko uporabnik nastopil v filmu ali televizijski seriji po izbiri, je bila na Kitajskem izdana septembra leta 2019. Uporabnik je posnetek oblikoval tako, da je posnel sebek (ang. *»selfie«*) ali naložil svojo fotografijo, izbral ustrezen film in s pomočjo tehnologije mehanskega učenja in biometrične prepoznave obraza poustvaril film tako, da je sam »nastopil« v njem. Uporabniki so morali pred samo uporabo aplikacije soglašati s pogojem, da lahko razvijalci aplikacije uporabljajo ustvarjene videoposnetke za kakršnokoli uporabo, brez nadaljnjega dovoljenja uporabnikov. Ker so razvijalci aplikacije s tem zelo posegli na področje varovanja zasebnosti, je bila aplikacija po dveh dnevih uporabe umaknjena iz platforme, na kateri je bila ustvarjena.

Aplikacija je z zbiranjem biometričnih podatkov zelo posegala v območje zasebnosti posameznika, ker so poteze obraza, glas, prstni odtisi in šarenica najstrožje varovani podatki, saj je identiteta posameznika z njihovo uporabo takoj prepoznana. Biometrični podatki so dandanes uporabljeni za potrditev identitete posameznika na različnih področjih, kot so spletno bančništvo, nadzor dostopa, e-poslovanje. Takšen sistem za preverjanje identitete posameznika omogoča visoko stopnjo zanesljivosti in prepoznavanja identitete, prav tako pa mora biti zaščita takšnih podatkov nujno potrebna, zlasti zato, ker jih ni mogoče nadomestiti ali spremeniti.

Najboljša rešitev za prepoznavanje deepfake posnetkov bi bil simultani razvoj programske opreme, ki bi bila sposobna hitro in zanesljivo prepoznati deepfake posnetek in ga označila kot ponarejenega. Prav tako bi se morala programska oprema prilagajati na nove tehnološke inovacije in tehnologije deepfake-ov. Vendar pa je realnost drugačna, saj po besedah profesorja Hany Farida, pionirja photoDNA tehnologije, današnja tehnologija ni dovolj razvita, da bi bila sposobna razločevati realen posnetka od ponarejenega.

3.3.4 Prilagojeno oglaševanje

Vsako dejanje, ki ga izvršimo na spletu, pusti za sabo sledi (ang. *»breadcrumbs«*), ki odražajo naše spletno obnašanje in vedenje. Ob analiziranju teh podatkov s pomočjo umetne inteligence, dobijo oglaševalska podjetja boljši vpogled v posameznikovo osebnost, s tem pa lahko posamezniku prilagodijo oglase, namenjene posebej zanj. Zaradi uporabe napovedovalske analitike, programskega oglaševanja in odzivnih iskanj, postajajo oglasi vedno bolj prilagojeni vsakemu uporabniku posebej.

Algoritmi umetne inteligence uporabljajo mehansko učenje pri zbiranju podatkov o tem, kaj vnašamo v iskalno okno, kdaj to iščemo, ter kaj počnemo neposredno po vnosu iskanega v brskalnik. Prav tako algoritmi ugotavljajo kaj počnemo z informacijami, ki jih dobimo kot rezultat iskanja in to ne zgolj na eni napravi, temveč na vseh z istim računom povezanih napravah.

S pomočjo napovedovalske analize se predvidijo prihodnje akcije posameznika, glede na vse zbrane podatke. Ustvari se osebnost posameznika, ki kasneje služi za prilagojeno oglaševanje, torej oglaševanje, namenjeno zgolj ljudem, ki so bili v procesu označeni kot določen tip osebnosti. Tak način poenostavi oglaševanje, saj so oglasi namenjeni točno določeni fokusni skupin. Podjetja tako prihranijo čas, ko

bi splošen oglas predstavljala večji skupini, katera nima interesa v oglaševan izdelek ali storitev, temveč se posvetijo manjšim skupinam, za katere je bolj verjetneje, da bodo kupile izdelek, saj so se že prej zanimale za podobne stvari.

Odzivno iskanje pa je novo oglaševalsko orodje Google oglaševalske platforme, ki omogoča oglaševalskim podjetjem enostavnejše prilagojeno oglaševanje s pomočjo umetne inteligence. Podjetja v oglaševalsko platformo vnesejo predloge oglasov in meta podatke, nato pa Googlovi algoritmi določijo kateri oglas iz zbirke je najprimernejši za posameznika. To pomeni, da bodo ljudje z enako določeno spletno osebnostjo dobili enake oglase, glede na njihovo zgodovino iskanja, navade in preference. Primer prilagojenega oglaševanja je ponudnik medijskih storitev Netflix, ki zbira podatke o serijah in filmih, katere je uporabnik pogledal in mu sestavi seznam vsebin, ki bi mu ustrezale glede na zgodovino ogledov.

Za takšno vrsto oglaševanja mora uporabnik sprejeti piškotke na strani, ki so majhne besedilne datoteke nameščene na uporabnikovo napravo, kamor se shranjujejo njegovi podatki o dejavnostih na določeni spletni strani. Poznamo sejne piškotke, ki olajšajo funkcionalnosti spletne strani, vanje se shranjujejo podatki o seji uporabnika, ter sledilne piškotke, kamor se shranjujejo osebne informacije posameznika, uporabljene za prilagojeno oglaševanje, navadno v obliki uporabe analitike, prikazovanja oglasov ali vdelane vsebine. Lastniki spletnih strani morajo o takšnih piškotkih obvestiti uporabnike ter zavarovati njihove podatke pred zlorabo s strani tretje stranke.

Piškotki so uporabljeni v namene vpogleda v uporabnikove preference in dejavnosti na določeni spletni strani ter identificiranja posameznika. Zasebnost končnih uporabnikov je vedno bolj ogrožena, še posebej zato, ker piškotke ne uporabljajo zgolj lastniki strani, temveč tretje stranke, ki izkoriščajo spletno stran, da bi prišle do podatkov o uporabnikov.

Velika večina piškotkov je ustvarjena tako, da se iz zbranih podatkov da ugotoviti identiteto končnega uporabnika. Takšni piškotki so recimo raziskave in orodja za klepet, ki omogočajo analitiko, oglaševanja in funkcionalnosti. Problem vseh piškotkov je vprašanje zasebnosti, torej kateri podatki o uporabniku se trenutno zbirajo, in vprašanje transparentnosti, torej kdo zbira informacije, v katere namene, kam se shranjujejo podatki in kako dolgo ostanejo v bazi shranjeni. Če podjetje na

svoji spletni strani zbira podatke, ki so osebni, ali pa se z združitvijo ali izpostavitvijo iz njih da ugotoviti identiteta posameznika, morajo upoštevati zakonodajo GDPR.

V Evropi je leta 2018 prišel v veljavo zakon o varstvu posameznikov pri obdelavi osebnih podatkov (uredba GDPR), ki določa, da se morajo uporabniki strinjati s piškoti, preden se začnejo zbirati podatki o njihovih dejavnosti na strani. Le na ta način lahko lastniki domene legalno zbirajo in obdelujejo osebne podatke uporabnikov. Vsak stran, ki ima evropske uporabnike, mora omogočiti seznanjene in strinjanje s piškotki uporabniku iz EU.

3.3.5 Umetna inteligenca in COVID-19

Zaradi pandemije je veliko držav uvedlo nujno potrebne omejitve za državljane, s čimer so posegale v temeljne človekove pravice, predvsem v pravico do zasebnosti. Za preprečevanje širjenja virusa v delno odprtem gospodarstvu, se je kot učinkovito pokazala zgolj kombinacija obsežnega testiranja, široka uporaba osebne zaščitne opreme in tehnologija digitalnega nadzora državljanov.

Čeprav je pravica do zasebnosti ena izmed temeljnih človekovih pravic, se le-ta lahko omeji, če pride do navzkrižja z nacionalnim zdravjem, vendar je potrebno poiskati razumno ravnovesje med pravicama; pravica do zasebnosti je lahko omejena zgolj, če je to nujno potrebno in omejena mora biti proporcionalno. Zbiranje in deljenje osebnih podatkov v takšni količini in kontekstu v boju proti koronavirusu predstavlja globalni test za varovanje zasebnosti posameznika.

V namene zaustavitve hitrega širjenja virusa COVID-19 so številna podjetja in raziskovalni centri združili moči in ustvarili aplikacije in modele, ki prikazujejo gibanje posameznikov. Podjetje Google je delilo obsežne zbirke podatkov o lokaciji posameznikov z raziskovalci javnega zdravja in epidemiologi, v namen modeliranja gibanja uporabnikov. S tem bi lahko ugotovili kje se je okužena oseba gibala in koliko ljudi je potencialno lahko okužila. Ekipa z Inštituta za tehnologijo v Massachusettsu je razvila aplikacijo za sledenje vsem uporabnikom, okuženih z virusom. Google in Apple sta napovedala uvedbo vmesnikov za programiranje aplikacij Android in iOS aplikacijo, s čimer bi se lažje prostovoljno sledilo stikom oseb preko Bluetooth Low Energy povezave. Severna Koreja sledi potencialno okuženim posameznikom preko lokacijskih podatkov z njihovega telefona in GPS-a, prav tako pa zajema tudi podatke z javnega prevoza, kreditnih kartic itd. Na Kitajskem je v uporabi aplikacija,

ki z barvnimi znaki prikazuje zdravstveno stanje posameznika, pred vstopom v nakupovalni center ali vstop na vlak. Prav tako se je na Kitajskem pojavila aplikacija, ki uporabnikom omogoča pregled nad lokacijo potrjenih in predvidenih okužb s koronavirusom v realnem času, tako da se lahko uporabniki izognejo tistim lokacijam.

Vendar pa morajo vse nadzorovalne in sledilne aplikacije, biti popolnoma proporcionalne, reverzibilne in transparentne, prav tako pa mora biti tudi njihov proces odstranitve definiran v trenutku, ko so bile implementirane. Digitalni odzivi na pandemijo ne smejo preseči demokratičnih vrednot države, prav tako tudi v prihodnosti ne sme priti do masovnega nadzorovanja in manipuliranja državljanov. Izdelovalci aplikacij morajo zbrane podatke uporabljati zgolj za namene preprečevanja širjenja okužbe in ne za iskanje profita, čeprav bi podatki koristili družbi v smislu izboljšanju javnega prevoza, zdravstvene infrastrukture...

Nekatere države so izkoriščale pandemijo za pridobivanje podatkov državljanov pod pretvezo da zbirajo podatke o okuženih in jih posredujejo državljanom za namene zajezitve širjenja virusa. V Izraelu so letos v začetku marca uvedli aplikacijo, ki naj bi zbirala in beležila podatke o vseh obolelih za virusom, vendar je v resnici zbirala podatke o uporabniku aplikacije, s čimer je vlada grobo posegala v pravico do zasebnosti državljanov. Tudi v Iranu se je istega leta pojavila aplikacija, ki naj bi domnevno pomagala identificirati simptome nove okužbe, vendar je bila zgolj pretveza za zbiranje podatkov o lokaciji uporabnikov. V Severni Koreji so ustvarili podobno aplikacijo, ki naj bi prikazala premike z virusom okuženih državljanov s čimer bi pomagali identificirati nove primere okužbe, vendar so zbrani podatki pogosto služili zgolj razkritju intimnih informacij.

V Evropi sta trenutno dve najpomembnejši direktivi glede varstva podatkov, in sicer uredba GDPR in direktiva o e-zasebnosti. Zadnja se ukvarja z vzpostavitvijo okvirjev za varovanje zasebnosti posameznika pri celotni komunikaciji preko javnih omrežij, ne glede na uporabljeno tehnologijo. Čeprav zakonodaja še ni prišla v veljavo, se ta nanaša na varovanje zasebnosti posameznika v digitalni dobi, predvsem z posameznikovo odobritvijo uporabe piškotkov na spletnih straneh ter seznanitvijo posameznika in nacionalnega organa ob vdoru v bazo podatkov.

V prihodnosti pa se bo ta direktiva razširila tudi na druge aplikacije, kot so WhatsApp, Facebook Messenger in Skype, kjer bo urejala da te aplikacije zagotavljajo enako stopnjo zaupnosti komunikacije kot ostali telekomunikacijski operaterji. Prav tako bo direktiva zagotavljala zasebnost in anonimiziranost metapodatkov pri komunikaciji, enostavnejšo odobritev piškotkov za boljšo uporabniško izkušnjo, zaščito pred nezaželeno pošto in oglaševalskimi klici, itd.

3.4 Primeri posega v zasebnost in sodne prakse

3.4.1 Poseg v pravico do zasebnosti

Ena izmed groženj zasebnosti je deanonimizacija, ki pomeni prepoznavo identitete posameznika iz podatka. Čeprav je podatek pri obdelavi ločen od ostalih podatkov posameznika, lahko zaradi specifičnega rezultata prepoznamo lastnika podatka in njegovo identiteto. To je izrazito predvsem na manjših vzorcih podatkov, kjer je mogoče posameznika prepoznati zgolj po enem podatku. Prav tako je posameznika možno prepoznati s kombiniranjem podatkov iz različnih zbirk podatkov, saj lahko s primerjavo obdelava natančno določimo izvor podatka. Posameznikova identiteta pa je lahko razkrita s pomočjo načina tipkanja na računalnik, kjer si računalnik zapomni hitrost, moč in vzorec pisanja posameznika, ter ga ob naslednji uporabi računalnika prepozna. Za zaščito zasebnosti uporabnika se je začela razvijati nova veja umetne inteligence imenovana diferencialna zasebnost, ki poskuša razviti algoritme strojnega učenja, ki bodo zagotavljali robustne rezultate obdelave, kateri ne bodo omogočali povratnega inženirstva podatkov.

3.4.1.1 Clearview AI in zbiranje osebnih podatkov

Ameriško podjetje Clearview AI se ukvarja z ustvarjanjem zbirk obrazov ljudi, katere kasneje posreduje organom kazenskega pregona, ki lahko enostavneje identificirajo storilce kaznivih dejanj in žrtve zločinov. Novo razvita tehnologija omogoča iskanje fotografij posameznikov preko družbenih omrežij, torej preko odprtega spleta in naj ne bi posegala v zasebne ali zaščitene informacije posameznika. Tehnologija podjetja je torej ustvarjenja zgolj za iskanje obrazov in ne za nadzor nad posamezniki a ravno zaradi te ogromne zbirke osebnih podatkov je podjetje v očeh javnosti videno kot kontroverzno. Do sedaj so zbrali več kot 3 milijarde slik, predvsem z družbenih omrežij kot so Facebook, Instagram, Twitter in YouTube, Clearview pa ohrani te slike v zbirki podatkov tudi po tem, ko so jih uporabniki že izbrisali iz svojih profilov.

Februarja letos zabeležili vdor v bazo podatkov, pri čemer je vsiljivec pridobil dostop do seznama strank podjetja, ki vsebuje policijske sile, organe pregona in banke. Družba je dejala, da oseba, ki je vdrla v sistem, ni pridobila nobene zgodovine iskanja, ki jo izvajajo stranke. Vendar pa je bilo podjetje po vdoru v bazo podatkov, soočeno z obtožbami glede njihovega delovanja. Clearview je posredovalo podatke iz svoje baze več kot 2200 policijskim upravam, vladnim agencijam in zasebnim podjetjem v več kot 27 državah, kateri so bili kasneje uporabljeni v različne namene, kot so iskanje osumljencev in prilagojeno oglaševanje. Ker je podjetje zbiralo osebne podatke posameznikov brez njihovega dovoljenja ali seznanitve, je kršilo številne zakone, med drugim tudi Zakon o zasebnosti biometričnih informacij v Illinoisu in zakon, ki prepoveduje zbiranje biometričnih podatkov o državljanov brez njihovega dovoljenja. Proti podjetju sta bili vloženi dve tožbi, in sicer s strani Generalnega državnega tožilca v Vermontu in Ameriške zveze državljanskih svoboščin, ki pa še nista razrešeni. Obe stranki se zavzemata za ustavitev nezakonitega in naključnega zajemanja in shranjevanja milijonov občutljivih biometričnih identifikatorjev, ter njihovega posredovanja tretji stranki.

3.4.1.2 Google in obdelava podatkov o lokaciji uporabnikov

Irska komisija za varstvo podatkov (DPC) je februarja letos oznanila ponovno preiskavo Googlove obdelave podatkov, ki je sledila vrsti obtožb več nacionalnih skupin potrošnikov po vsej Evropski uniji iz leta 2018. Podjetje naj bi na nepravilen način pridobivalo podatke o lokaciji uporabnikov, kasneje pa z njihovo obdelavo prišlo do zaključkov o posameznikovih osebnih lastnostih, kot so osebnost, vera ali spolna usmerjenost. Potrošniške organizacije trdijo, da posamezniki niso prostovoljno dali soglasja o deljenju svoje lokacije, saj so bili zavedeni k sprejetju pogojev poseganja v zasebnost. Takšne prakse pa niso skladne z evropsko zakonodajo, ki v Splošni uredbi o varstvu podatkov navaja, da mora biti posameznik seznanjen z zbiranjem njegovih osebnih podatkov.

Irska DPC se je odločila preiskavo začeti zato, da bi ugotovila kako podjetje pridobiva podatke o uporabnikovi lokaciji. Ta preiskava bo določila, ali ima Google sploh veljavno pravno podlago za zbiranje in obdelavo lokacijskih podatkov svojih uporabnikov ter če izpolnjuje svoje obveznosti upravljavca podatkov glede preglednosti. Irska DPC trdi, da noben potrošnik ne bi smel biti pod komercialnim nadzorom določenega podjetja, zato bo natančno pregledal, če družba upošteva Splošno uredbo o varstvu podatkov. Ker je problem posega v pravico do zasebnosti

zajemal milijone evropskih potrošnikov, bo preiskava glavna prioriteta Irske komisije za varstvo podatkov. Irska DPC trenutno aktivno preiskuje 20 večnacionalnih tehnoloških firm, ki naj bi podobno kot Google, posegale v pravico do varstva zasebnosti posameznika.

3.4.1.3 Aplikacija Grindr kršila Splošno uredbo o varstvu podatkov

Norveška potrošniška organizacija Forbrukerrådet je vložila več pritožb proti aplikaciji za zmenke Grindr in še pet podjetij za spletno oglaševanje, saj so ta podjetja zbirala osebne podatke o uporabnikih, katere so prodajala oglaševalskim agencijam in tržnikom, ki so ustvarili prilagojene oglase brez legalne podlage ali vedenja potrošnikov. Raziskave potrošniške organizacije so pokazale kako podjetja izkoriščajo zbrane podatke o uporabnikovem zdravju, spolni orientaciji, lokaciji in interesih, uporabniki aplikacije pa ne morejo storiti nič proti takšni uporabi njihovih podatkov. Takšno zbiranje podatkov lahko vodi do družbene izključitve, diskriminacije, goljufije in tudi manipulacije.

Uporabniki teh aplikacij nenehno nosijo telefon s seboj in ga uporabljajo za številne namene, kar pomeni, da lahko podjetja konstantno pridobivajo informacije o uporabniku. Študije so pokazala, da večino časa sploh ni nobene pravne podlage za takšen neomejen nadzor s strani takšnih podjetij, saj so uporabniki zavarovani s Splošno uredbo o varstvu podatkov, ki jih varuje pred takšnimi podjetji, katera ne spoštujejo zasebnosti posameznika. Poziv k poglobljeni preiskavi podjetja Grindr so vložile tudi skupine potrošnikov iz Združenih držav Amerike, Evropska potrošniška organizacija (v nadaljevanju BEUC) pa naproša Evropsko komisijo, naj ukrepa proti sistematičnemu in nezakonitemu komercialnemu nadzoru s strani podjetij, ki zbirajo osebne podatke uporabnikov na podlagi poslovnega modela ad-tech.

V pismu so zapisane ključne identificirane težave izkoriščanja osebnih podatkov uporabnikov aplikacij, kot je sistematično zbiranje in izkoriščanje podatkov za namene, s katerimi uporabniki niso seznanjeni ali pa niso podali izrecnega soglasja. Prav tako je BEUC opozorila na škodo, ki jo utrpijo potrošniki zaradi profiliranja, kot so diskriminacija, manipulacija, razširjena prevara… Potrošniki se zbiranju podatkov ne morejo izogniti, ker pred prvo uporabo niso primerno seznanjeni s potrebnimi informacijami in ker je sistem sledenja informacijam in njihove delitve tretjim strankam za uporabnike nerazumljiv. In četudi bi uporabniki aplikacij imeli dovolj znanja za razumevanje zbiranja osebnih podatkov, ne bi mogli nadzorovati

njihove obdelave ali ukrepati proti njihovem izkoriščanju. V pismu je BEUC naprosila za vzpostavitev alternativnega poslovnega sistema, ki bo uporabnikom omogočal uporabo digitalnih storitev in produktov, pri katerih bodo ohranili svojo avtonomijo, predvsem pa zasebnost.

3.4.2 Mnenje informacijskega pooblaščenca glede situacije v času pandemije

3.4.2.1 Zbiranje podatkov v zvezi s COVID-19

Informacijski pooblaščenec je prejel zaprosilo za mnenje glede zbiranja podatkov v zvezi s COVID-19, kjer je bilo navedeno, da želi delodajalec vpeljati sistem, pri katerem bi evidentiral vse obiskovalce, ki so zunanji izvajalci storitev. Takšna evidenca je sicer že bila vzpostavljena, sedaj pa jo želi delodajalec razširiti z izjavami, na katerih bi izvajalci navajali tudi zdravstveno stanje, zgodovino potovanj in zgodovino stikov.

Informacijski pooblaščenec navaja, da je potrebno v času pandemije, ko vsi prizadevamo za čim hitrejšo zajezitev bolezni, vseeno upoštevati veljavno zakonodajo na področju varstva osebnih podatkov. To pomeni, da mora imeti vsakršna obdelava zakonito in ustrezno pravno podlago, zaradi obdelave posebne vrste osebnih podatkov, kamor sodijo podatki v zvezi z zdravjem posameznika, pa se morajo upoštevati pogoji iz člena 9(2) Splošne uredbe o varstvu podatkov. Obdelava osebnih podatkov bi v tem primeru bila potrebna za izpolnjevanje pravne obveznosti, ki velja za delodajalca, kot so obveznosti v zvezi z zdravjem in varstvom pri delu, ali javnim interesom, kot je interes za nadzor nad boleznimi ali drugimi nevarnostmi za zdravje. Zaradi teh razlogov informacijski pooblaščenec meni, da delodajalec lahko zbira in obdeluje osebne podatke v zvezi s COVID-19 od obiskovalcev, ki so zunanji izvajali storitev, vendar le v utemeljenih okoliščinah na podlagi področne nacionalne zakonodaje, pri čemer pa mora upoštevati načelo najmanjšega obsega podatkov.

3.4.2.2 Varstvo osebnih podatkov pri poučevanju na daljavo

Informacijski pooblaščenec je dobil dopis z vprašanjem glede varstvom osebnih podatkov pri poučevanju učiteljev preko videokonferenčnih sistemov za poučevanje na daljavo. Ker informacijski pooblaščenec ne more presojati obdelave podatkov

izven inšpekcijskega postopka nadzora ter ne more presojati in komentirati konkretnih orodij za izvajanje izobraževanja na daljavo, podaja zgolj splošno mnenje glede podlag za obdelavo osebnih podatkov ter njihove varnosti, ki ga je naslovil tudi na Ministrstvo za zdravje, znanost in šport, katero zajema obdelavo osebnih podatkov tako učiteljev kot tudi učencev.

V svojem mnenju se je informacijski pooblaščenec dotaknil tematike zbiranja, objavljanja in shranjevanja video posnetkov učnih ur učiteljev na zavarovanem spletnem strežniku oz. učiteljevem e-okolju. To bi bilo dopustno zgolj na podlagi določne 48. člena Zakona o delovnih razmerjih pod pogojem, da gre za obdelavo, ki je potrebna za izvrševanje pravic in obveznosti iz delovnega razmerja. Informacijski pooblaščenec prav tako meni, da snemanje učne ure ne bi smelo temeljiti zgolj na podlagi privolitve učitelja, saj se lahko video posnetki izbrišejo, če se učitelj z obdelavo podatkov ne strinja več, kar ne bi zagotavljajo primerne kontinuitete in kvalitete dela. Zato morajo upravljavci, v tem primeru šole, urediti primerne roke hrambe, poskrbeti za ustrezno varnost obdelave osebnih podatkov, ter nasloviti morebitna vprašanja avtorskih pravic.

Prav tako je informacijski pooblaščenec predstavil svoje mnenje glede obdelave osebnih podatkov učencev, za katere meni, da za namene izvajanja izobraževanja na daljavo, zgolj privolitev starša (ali zakonitega zastopnika) ni ustrezna pravna podlaga, po kateri naj bi obdelava podatkov potekala. V trenutni situaciji bi bila edina primerna pravna podlaga 6(1)(c) Splošne uredbe o varstvu podatkov, saj je obdelava podatkov potrebna za izpolnitev zakonske obveznosti, ki velja za upravljavca. Zaradi izjemnih okoliščin v katerih se trenutno nahajamo, je informacijski pooblaščenec pozval Ministrstvo za izobraževanje, znanost in šport k oblikovanju enotnih navodil za šole glede obdelave osebnih podatkov.

3.4.2.3 Sledenje obolelim za COVID-19 preko mobilne aplikacije

Informacijski pooblaščenec je prejel zaprosilo za mnenje glede zakonske dopustnosti uporabe mobilne aplikacije, ki bi sledila posameznikom, s čimer bi zagotavljala, da se okuženi posamezniki ne gibljejo izven svojih bivališč. Pošiljatelj sporočila se sicer zaveda, da bi aplikacija posegala v posameznikovo pravico do varstva zasebnosti in osebnih podatkov. Sledenje bi potekalo tako, da bi naložena aplikacija bila aktivna 14 dni, po tem času bi se vsi podatki v zvezi z njo (in aplikacija sama) izbrisali. Vsebovala bi določen radij gibanja posameznika, ki je še dopusten, zajemala bi zgolj

podatke o lokaciji in ne bi imela dostopa do drugih podatkov, prav tako pa bi uporabniku nudila podporo v obliki enostavnega stika z zdravnikom.

Za odobritev uporabe aplikacije bi bilo najprej potrebno izvesti oceno učinkov z jasnimi tehničnimi parametri aplikacije glede na cilje, ki se jih zasleduje in z vidika načela sorazmernosti, šele nato bi bilo potrebno opredeliti zakonski okvir za uporabo aplikacije. Informacijski pooblaščenec pri tem opozarja na nujno prisotno transparentnost aplikacije, ki bi zagotavljala, d so uporabniki aplikacije obveščeni o tem, kateri podatki se bodo obdelovali in za kakšen namen, ter kdo bo upravljavec podatkov, kje se bodo podatki hranili in kako dolgo časa, ter kako bo zagotovljeno brisanje podatkov. Vsi osebni podatki bodo morali biti obdelani zakonito, pošteno in na pregleden način.

Informacijski pooblaščenec navaja tudi, da pravna podlaga klasične privolitve ne bi bila primerna, saj podaja privolitve med posameznikom in državo težko dosega standarde svobodne podaje. Poleg tega opozarja tudi na dejstvo, da se morajo izdelovalci te aplikacije najprej posvetovati s stroko glede nujnosti tehnične rešitve pri obvladovanju epidemije. Pojavilo se je tudi vprašanje glede natančnosti samega nadzora nad posamezniki, saj lahko uporabnik pusti telefon na določeni lokaciji in odide na drugo mesto brez njega, prav tako pa je znotraj večstanovanjske stavbe natančnost lokacije prav tako vprašljiva. Na tej točki je informacijski pooblaščenec predstavil pomislek glede tega, v kolikšni meri bi sledenje posameznikom sploh učinkovito pripomoglo k nadzoru posameznika z ukrepom in k širšemu cilju omejevanja epidemije COVID-19.

3.5 Smernice za razvoj umetne inteligence

3.5.1 Dosedanja prizadevanja

Do sedaj so bile na področju umetne inteligence vzpostavljene iniciative, ki so se ukvarjale z etičnimi in pravnimi vprašanji v povezavi z odgovornostjo in pravičnostjo odločanja. Najpomembnejša uredba je Splošna uredba o varstvu podatkov, ki predstavlja pomemben pristop h krepitvi zaupanja v umetno inteligenco. Prav tako je Evropska komisija sprejela iniciative, kot so Etične smernice za zanesljivo umetno inteligenco iz leta 2019, Poročilo o odgovornosti za umetno inteligenco in druge nastajajoče tehnologije iz leta 2019, in Deklaracijo o sodelovanju na področju umetne inteligence, katero je leta 2018 podpisalo 25 držav.

Evropska komisija je predlagala tako imenovan Evropski pristop k umetni inteligenci in robotiki, v katerem se raziskujejo tehnološki, etični, pravni in socialno-ekonomski vidiki uporabe umetne inteligence. Umetna inteligenca je v zadnjih letih postala ključno gonilo gospodarskega razvoja, zato je potrebno skrbno obravnavati njene socialno-ekonomske, pravne in etične učinke, da bo delovala v dobrobit celotne družbe. Pristop k umetni inteligenci je sestavljen iz treh temeljnih vidikov glede razvoja umetne inteligence in njenega vpliva na delovanje Evropske unije.

Prvi je ta, da mora Evropska unija v prihodnosti skrbno spremljati razvoj tehnologije in ga tudi podpirati, prav tako pa mora spodbujati uporabo umetne inteligence v javnem in zasebnem sektorju. Komisija je v sklopu raziskav in inovativnega programa Horizon 2020 povečala svoj letni vložek v umetno inteligenco za 70%, ki je tako v obdobju 2018 – 2020 dosegel 1,5 milijarde evrov. V naslednjem desetletju se namerava za raziskave in razvoj umetne inteligence nameniti več kot 20 milijard evrov letno. Prav tako je v načrtu okrepiti raziskovalne centre po vsej Evropi, še naprej podpirati razvoj projekta »AI-on-demand«, ki ko zagotavljal dostop do relevantnih virov umetne inteligence v Evropi vsem uporabnikom, ter spodbujati razvoj aplikacij umetne inteligence v ključnih sektorjih.

Drugi vidik je ta, da se mora Evropska unija temeljito pripraviti na socialno-ekonomske spremembe, ki jih bo prinesel razvoj umetne inteligence. Komisija bo, kot podpora državam članicam, okrepila poslovno-izobraževalna partnerstva na področju umetne inteligence v Evropi, vzpostavila namenske programe usposabljanja in prekvalifikacije za strokovnjake na področju umetne inteligence, predvidevala spremembe na trgu dela, podpirala digitalne veščine in kompetence v znanosti, tehnologiji, inženirstvu in matematiki, prav tako pa bo vzpodbujala države članice, da modernizirajo njihove sisteme izobraževanja in usposabljanja na področju umetne inteligence.

V sklopu tretjega vidika pa bo Komisija zagotovila primeren etični in pravni okvir glede umetne inteligence in njenega razvoja. V Beli knjigi, ki jo je Komisija objavila 19. februarja 2020, je že ustvarila smernice za spodbujanje evropskega sistema odličnosti in zaupanja v umetno inteligenco. V njej je predlagala ukrepe, ki bodo racionalizirali preiskave, spodbujali sodelovanje med državami članicami in povečali naložbe v razvoj umetne inteligence. Prav tako so v Beli knjigi zapisane možnosti politike prihodnjega regulativnega okvira Evropske unije, ki bi določal vrste zakonskih zahtev, s posebnim poudarkom na aplikacijah z visokim tveganjem.

3.5.2 Napovedi za prihodnost

Evropska komisija je februarja 2020 predstavila ideje in ukrepe za digitalno transformacijo Evrope v prihodnosti na področju umetne inteligence. Ukrepi pokrivajo področja kibernetske varnosti kritičnih infrastruktur, digitalnega izobraževanja, veščin uporabe umetne inteligence, demokracije in medijev. Cilj Komisije je vzpostaviti Evropsko družbo, ki bo zaupala v umetno inteligenco, bila odprta za nove poslovne možnosti in vzpodbujala razvoj v človeka usmerjene umetne inteligence.

Evropska tehnološka suverenost družbe se mora začeti z zagotavljanjem celovitosti in odpornosti podatkovne infrastrukture, omrežja in komunikacij, saj prebivalci Evropske unije menijo, da nimajo več nadzora nad tem, kaj se dogaja z njihovimi osebnimi podatki. Državljane se bi moralo spodbujati k sprejemanju boljših odločitev na podlagi razumevanja podatkov, pridobljenih s pomočjo umetne inteligence. Prav tako bi morali ti podatki biti na voljo vsem posameznikom in podjetjem. Digitalna Evropa bi morala odražati odprtost, poštenost, raznolikost, demokratičnost in samozavest.

V naslednjih petih letih se bo Evropska komisija zavzemala za tri temeljne cilje, s katerimi bo zagotavljala digitalne rešitve, ki bodo v pomoč pri doseganju digitalne transformacije Evrope. Prvi je ta, da se morajo razviti tehnologije, ki bodo človeku olajšale njegov vsakdan, te pa morajo upoštevati vrednote prebivalcev. Drugi cilj je doseganje poštenega in konkurenčnega gospodarstva, kjer lahko katerokoli podjetje deluje od enakimi pogoji, ter lahko razvija, trži in uporablja digitalne tehnologije za povečanje lastne produktivnosti, pri tem pa je potrošnikom zagotovljeno, da se spoštuje njihove pravice. Zadnji cilj je odprta, demokratična in trajnostna družba, ki bo omogočala državljanom, da izmenjujejo podatke v zaupanju vrednem okolju, pri čemer se bodo spoštovale temeljne pravice.

Komisija je v poročilu tudi opredelila nekatere načine digitaliziranja Evrope na področju umetne inteligence. Evropa bi tako morala združiti svoje investicije v raziskave in inovacije, ter deliti izkušnje in spodbujati sodelovanja med državami članicami. Prav tako mora promovirati digitalno transformacijo javne administracije, ter vlagati v strateške kapacitete, ki omogočajo razvoj in uporabo digitalnih rešitev. K tem rešitvam bo pripomogel večletni finančni okvir Evropske unije, namenjen izključno digitalizaciji, katerega cilj je doseči boljše strateške kapacitete kjer je to

potrebno. Zagotavljati mora kibernetsko varnost, prav tako pa mora tudi povečati zaupanje v samo tehnologijo, še posebej sisteme umetne inteligence. Zagotavljati mora napredku prilagojeno izobrazbo, ki bo na voljo vsem, ter spodbujati posameznike k vseživljenjskemu učenju, saj bodo v prihodnosti državljani potrebovali večinoma digitalne kompetence za uspeh na vedno bolj digitaliziranem trgu dela. Prilagoditi pa se mora tudi spremembam zunaj tehnološkega sektorja, kjer mora omogočati pravičnost in enakopravnost vsem državljanom Evropske unije.

3.6 Zaključek

Umetna inteligenca je tehnologija, s katero bo človek v prihodnosti zmožen reševati kompleksne probleme, kot so podnebne spremembe, dostop do pitne vode, ustvarjanje čiste energije in boj proti še neozdravljivim boleznim. Ker bodo sistemi umetne inteligence inkorporirani v naš vsakdan, se bomo morali prilagoditi njeni konstantni uporabi na številnih področjih, kot so gospodarstvo, industrija, šolstvo, zdravstvo, itd. Prav tako bomo morali, zaradi neprestanega razvoja in napredka tehnologije, prilagoditi njen pravni in etični okvir, da uporaba umetne inteligence ne bo posegala v temeljne človekove pravice.

Umetna inteligenca torej prinaša veliko pozitivnih sprememb in izboljšav za človeštvo, vendar pa predstavlja tudi nevarnost naši avtonomiji, ter moči in sposobnosti samostojnega odločanja. Zaradi napredka tehnologije vedno bolj zaupamo odločitvam pametnih naprav, saj menimo, da nam izboljšujejo življenje. Čeprav nam recimo tehnologija interneta stvari res lahko omogoči enostavnejše življenje, kjer je poskrbljeno za vsako našo potrebo, lahko predstavlja tudi tveganje za našo svobodo, saj lahko kdorkoli, ki uspe vdreti v sistem, pridobi vse podatke ali pa celo nadzoruje in upravlja z našim življenjem. Podobno velja za avtonomna vozila, kjer lahko kibernetski napad na sistem vozila onemogoči lastniku nadzor nad vozilom.

Pametne naprave vsakodnevno zbirajo ogromne količine podatkov o posameznikih, ki se lahko uporabijo za prilagojeno oglaševanje, napovedovanje kriminala, ali pa celo za nadzorovanje prebivalstva v pametnih mestih. Vsi ti podatki in informacije se zbirajo v oblaku na spletu, kjer dobijo vrednost šele, ko se povežejo s podatki, pridobljenimi iz drugih naprav, pri čemer se ustvari profil posameznika. Takšni zbrani podatki lahko kršijo pravico do zasebnosti med njihovim zbiranjem in obdelavo, saj se lahko izkoristijo za namene, katerih se posameznik sploh ne zaveda,

ali dovolil takšno uporabo. Čeprav je na tem področju že bil sprejet normativni okvir, se zaradi stalnega napredka umetne inteligence pojavljajo nove možnosti kršenja človekovih pravic, ki pa še niso pravno naslovljene.

Seznam literature in virov

Članki in poglavja iz knjig

Alexandrou, A., Maras, M-H., Determining authenticity of video evidence in the age of artificial intelligence and in the wake of Deepfake videos, v: The International Journal of Evidence & Proof, 23 (2019) 3, str. 255–262

Collingwood, L.: Privacy implications and liability issues of autonomous vehicles, v: Information & Communications Technology Law, 26 (2017) 1, str. 32–45

Lim, H., Taeihagh, A.: Autonomous Vehicles for Smart and Sustainable Cities: An In-Depth Exploration of Privacy and Cybersecurity Implications, v: Energies, 11 (2018), str. 1– 23

Meskys, E., in drugi: Regulating deep fakes: legal and ethical considerations, v: Journal of Intellectual Property Law & Practice, 15 (2020) 1, str. 24–31

Sadeghi A-R., Wachsmann, C., Waidner, M.: Security and privacy challenges in industrial Internet of Things, v: 2015 52nd ACM/EDAC/IEEE Design Automation Conference (DAC), (2015), str. 1–6

Smit, E. G., Van Noort, G., Voorveld H. A. M.: Understanding online behavioural advertising: User knowledge, privacy concerns and online coping behaviour in Europe, v: Computers in Human Behavior, 32 (2014), str. 15–22

Ukil, A., Bandyopadhyay, S., Pal, A.: IoT-Privacy: To be private or not to be private, v: 2014 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), (2014), str. 123–124

Weber, R. H.: Internet of things: Privacy issues revisited, v: Computer Law & Security Review, 31 (2015) 5, str. 618–627

Pravni viri

Zakon o varstvu osebnih podatkov (Uradni list RS, št. 94/07 – uradno prečiščeno besedilo in 177/20).

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 – Mednarodne pogodbe, št. 7/94).

Pogodba o delovanju Evropske Unije, Uradni list Evropske unije, C 326/47, str. 47-390.

Listina Evropske Unije o človekovih pravicah, Uradni list Evropske unije, C 83/389, str. 391–407.

Direktiva (EU) 2016/680 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov, ki jih pristojni organi obdelujejo za namene preprečevanja, preiskovanja, odkrivanja ali pregona kaznivih dejanj ali izvrševanja kazenskih sankcij, in o prostem pretoku takih podatkov ter o razveljavitvi Okvirnega sklepa Sveta 2008/977/PNZ, Uradni list Evropske unije, L 119/89, 4.5.2016.

Direktiva 2002/58/ES Evropskega parlamenta in Sveta z dne 12. julija 2002 o obdelavi osebnih podatkov in varstvu zasebnosti na področju elektronskih komunikacij, Uradni list Evropske unije, L 201/37, 31.7.2002.

Direktiva 2006/24/ES Evropskega parlamenta in Sveta z dne 15. marca 2006 o hrambi podatkov, pridobljenih ali obdelanih v zvezi z zagotavljanjem javno dostopnih elektronskih komunikacijskih storitev ali javnih komunikacijskih omrežij, in spremembi Direktive 2002/58/ES, Uradni list Evropske unije, L 105/54, 13.4.2006.

Mnenje Evropskega ekonomsko-socialnega odbora – Umetna inteligenca – Posledice za enotni (digitalni) trg, proizvodnjo, potrošnjo, zaposlovanje in družbo (mnenje na lastno pobudo), Uradni list Evropske unije, C 288, 31.8.2017, str. 1–9

Okvirni sklep Sveta 2008/977/PNZ z dne 27. novembra 2008 o varstvu osebnih podatkov, ki se obdelujejo v okviru policijskega in pravosodnega sodelovanja v kazenskih zadevah, Uradni list Evropske unije, L 359/60, 30.12.2008.

Predlog UREDBA EVROPSKEGA PARLAMENTA IN SVETA o vzpostavitvi programa za digitalno Evropo za obdobje 2021–2027, COM/2018/434 final - 2018/0227.

Resolucija Evropskega parlamenta s priporočili Komisiji o pravilih civilnega prava o robotiki (2015/2103(INL)), Uradni list Evropske unije, C 252/239, 18.7.2018, str. 239–257.
Resolucija Evropskega parlamenta z dne 26. maja 2016 o strategiji za enotni trg (2015/2354(INI)), Uradni list Evropske unije, C 76, 28.2.2018, str. 112–127.
Sporočilo Komisije Evropskemu parlamentu, Svetu, Evropskemu ekonomsko-socialnemu odboru in Odboru regij, Na poti do avtomatizirane mobilnosti: strategija EU za mobilnost prihodnosti, COM/2018/283 final.
Sporočilo Komisije Evropskemu parlamentu, Svetu, Evropskemu ekonomsko-socialnemu odboru in Odboru regij, Evropska strategija za kooperativne inteligentne prometne sisteme – mejnik na poti h kooperativni, povezani in avtomatizirani mobilnosti, COM/2016/0766 final.
Uredba (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES (Splošna uredba o varstvu podatkov) (Besedilo velja za EGP), Uradni list Evropske unije, L 119, 4.5.2016, str. 1–88.

Sodna praksa

C-131/12, *Agencia Española de Protección de Datos (AEPD) in Mario Costeja González,* ECLI:EU:C:2014:317
C-136/17, *Commission nationale de l'informatique et des libertés (CNIL),* ECLI:EU:C:2019:773
C-207/16, *Ministerio Fiscal,* ECLI:EU:C:2018:788
C-293/12 in C-594/12, *Digital Rights Ireland Ltd (C-293/12) in Kärntner Landesregierung (C-594/12),* ECLI:EU:C:2014:238
C-362/14, *Maximillian Schrems in Data Protection Commissioner*, ECLI:EU:C:2015:650
C-70/10, *Scarlet Extended SA in Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM),* ECLI:EU:C:2011:771
C-360/10, *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) in Netlog NV,* ECLI:EU:C:2012:85

Spletni viri

< https://mladipodjetnik.si/novice-in-dogodki/novice/gdpr-uredba-o-varstvu-podatkov > (25. 5. 2020)
< https://epic.org/privacy/edrs/ > (12. 5. 2020)
< https://www.theguardian.com/technology/2016/jun/08/self-driving-car-legislation-drones-data-security > (22. 5. 2020)
< https://gadgets.ndtv.com/others/news/self-driving-car-technology-poses-high-hacking-risk-study-796978 > (15. 4. 2020)
< https://perma.cc/L6B5-DGNR > (22. 5. 2020)
< https://mastersofmedia.hum.uva.nl/blog/2019/09/22/the-worrisome-biometrics-deepfakes-zao-and-privacy-issue/ > (13. 4. 2020)
< https://azati.ai/artificial-intelligence-targeted-marketing/ > (5. 5. 2020)
< https://www.cookiebot.com/en/gdpr-cookies/?gclid=CjwKCAjwnIr1BRAWEiwA6GpwNdDbKnp028aCrerivdJ43SjTZDGZPzIDA4q8NEAvsctBBuDbNhOUrBoCdLsQAvD_BwE > (13. 4. 2020)
< https://foreignpolicy.com/2020/04/20/coronavirus-pandemic-privacy-digital-rights-democracy/ > (18. 5. 2020)
< https://www.dataguidance.com/opinion/international-coronavirus-privacy-dilemma > (11. 4. 2020)
< https://www.theguardian.com/world/2020/mar/17/israel-to-track-mobile-phones-of-suspected-coronavirus-cases > (27. 3. 2020)
< https://ec.europa.eu/digital-single-market/en/online-privacy > (3. 5. 2020)
< https://ec.europa.eu/digital-single-market/en/proposal-eprivacy-regulation > (3. 5. 2020)
< https://course.elementsofai.com/6/2 > (27. 3. 2020)
< https://edition.cnn.com/2020/02/26/tech/clearview-ai-hack/index.html > (17. 5. 2020)
< https://clearview.ai/ > (17. 5. 2020)
< https://www.buzzfeednews.com/article/ryanmac/clearview-ai-no-facial-recognition-private-companies > (1. 5. 2020)
< https://www.theverge.com/2020/3/11/21174613/clearview-ai-sued-vermont-attorney-general-facial-recognition-app-database > (21. 5. 2020)
< https://nakedsecurity.sophos.com/2020/05/29/clearview-ai-facial-recogition-sued-again-this-time-by-aclu/ > (20. 5. 2020)
< http://www.beuc.eu/publications/google-cross-hairs-irish-data-protection-authority-location-tracking/html > (28. 5. 2020)

< https://digitalguardian.com/blog/irish-data-protection-puts-google-notice-data-privacy-again > (14. 5. 2020)
< https://www.euractiv.com/section/data-protection/news/google-hit-by-irish-data-protection-probe/ > (14. 5. 2020)
< https://www.ip-rs.si/varstvo-osebnih-podatkov/pravice-posameznika/ > (8. 6. 2020)
< https://www.ip-rs.si/varstvo-osebnih-podatkov/inspekcijski-nadzor/ > (8. 6. 2020)
< https://www.ip-rs.si/vop/?tx_jzgdprdecisions_pi1%5BshowUid%5D=1530 > (8. 6. 2020)
< https://www.ip-rs.si/vop/?tx_jzgdprdecisions_pi1%5BshowUid%5D=1508 > (8. 6. 2020)
< https://www.ip-rs.si/vop/?tx_jzgdprdecisions_pi1%5bshowUid%5d=1504 > (8. 6. 2020)
< http://www.beuc.eu/publications/eu-consumer-groups-urge-immediate-investigation-systematic-breaches-gdpr-online/html > (9. 6. 2020)
< http://www.beuc.eu/publications/beuc-x-2020-002_letter_to_executive_vice-president_vestager.pdf > (18. 5. 2020)
< https://ec.europa.eu/digital-single-market/en/artificial-intelligenc > (18. 5. 2020)
< https://ec.europa.eu/commission/presscorner/detail/en/ip_20_273 > (18. 5. 2020)
< https://ec.europa.eu/info/sites/info/files/communication-shaping-europes-digital-future-feb2020_en_4.pdf > (27. 3. 2020)
< https://curia.europa.eu/jcms/upload/docs/application/pdf/2014-05/cp140070sl.pdf > (19. 6. 2020)
< https://e-uprava.gov.si/drzava-in-druzba/e-demokracija/predlogi-predpisov/predlog-predpisa.html?id=10208 > (19. 6. 2020)
< https://www.ip-rs.si/fileadmin/user_upload/Pdf/pripombe/2020/MP_ZVOP2_mnenje_IP_jan2020_koncno.pdf > (19. 6. 2020)
< https://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117sl.pdf > (30. 6. 2020)
< https://curia.europa.eu/jcms/upload/docs/application/pdf/2012-02/cp120011sl.pdf > (30. 6. 2020)
< https://curia.europa.eu/jcms/upload/docs/application/pdf/2013-12/cp130157sl.pdf > (9. 7. 2020)
< https://curia.europa.eu/jcms/upload/docs/application/pdf/2018-10/cp180141sl.pdf > (9. 7. 202)
< https://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117sl.pdf > (9. 7. 2020)
< https://curia.europa.eu/jcms/upload/docs/application/pdf/2011-11/cp110126sl.pdf > (9. 7. 2020)
< https://curia.europa.eu/jcms/upload/docs/application/pdf/2012-02/cp120011sl.pdf > (9. 7. 2020)

DOI
https://doi.org/10.18690/um.pf.4.2023.4

ISBN
978-961-286-774-4

4 VPLIV DIGITALIZACIJE NA ČLOVEKOVO DOSTOJANSTVO IN SPOŠTOVANJE ZASEBNEGA IN DRUŽINSKEGA ŽIVLJENJA

TEJA ŠTRUKELJ
Univerza v Mariboru, Pravna fakulteta, Maribor, Slovenija
teja.strukelj@student.um.si

Prispevek se osredotoča na problematiko varstva človekovega dostojanstva ter zasebnega in družinskega življenja v digitalni dobi. Prvi del izhaja iz predpostavke, da je človekovo dostojanstvo pogoj za uresničevanje ostalih temeljnih pravic, v naslednjih delih pa so izpostavljeni določeni primeri, v katerih lahko pride do njihove okrnitve in domnevno tudi kršitve. S tem v mislih sta najprej predstavljeni pravna podlaga in opredelitev pravic, nato pa si sledijo posamezna področja, in sicer zdravstvo, video nadzor in zvočno snemanje, prepoznava obraza (angl. facial recognition), sledenje lokacije in internet stvari. Končni cilj tega prispevka je osvetliti izbrane temeljne pravice v digitalni dobi ter na tehtnico postaviti človekovo dostojanstvo na eni strani in tehnološki razvoj na drugi.

Ključne besede:
digitalizacija,
človekovo dostojanstvo,
zasebnost,
družinsko življenje,
zdravstvo,
internet stvari

Univerzitetna založba
Univerze v Mariboru

DOI
https://doi.org/
10.18690/um.pf.4.2023.4

ISBN
978-961-286-774-4

Keywords:
digitalisation,
human dignity,
privacy,
family life,
healthcare,
internet of things

University of Maribor Press

4 The Influence of Digitalization on a Person's Dignity and Respect of Private and Family Life

Teja Štrukelj
University of Maribor, Faculty of Law, Maribor, Slovenia
teja.strukelj@student.um.si

The following article focuses on the issues with safeguarding human dignity, as well as private and family life, in the digital age. The first section suggests that human dignity is a basic requirement for the realization of other fundamental rights, and the subsequent sections highlight specific instances of curtailment and, possible violations of these rights in specific context. Keeping this in mind, the legal foundation and definition of rights are presented first, followed by specific areas such as healthcare, video surveillance and sound recording, facial recognition, location tracking, and the Internet of Things. The goal of this paper is to shed light on fundamental rights in the digital age with the possibility of striking a fair balance between human dignity and technological development.

4.1 Uvod

Antiutopični roman Orwella z naslovom 1984 vsebuje zanimiv in pomenljiv stavek: »*Kdor nadzira preteklost, nadzira prihodnost. Kdor nadzira sedanjost, nadzira preteklost*«. Tudi če se nam danes zdi, da določen poseg v zasebnost ni nevaren, pa se lahko zgodi, da se bo naše mnenje spremenilo, ko se bomo čez čas soočili s pravimi posledicami. Digitalizacija pomeni uporabo novih digitalnih tehnologij v obstoječem načinu in notranjih procesih poslovanja.[1] Vendar pa je neločljivo povezana z različnimi aspekti našega vsakdana. V svojem delu sem se podrobneje posvetila vplivu digitalizacije na človekovo dostojanstvo, zasebnost in družinsko življenje. Medtem, ko sem se prvih dveh področij lotila bolj s pravnega vidika, pa sem vpliv na družinsko življenje raziskala s psihološkega in sociološkega vidika.

4.2 Vpliv digitalizacije na človekovo dostojanstvo in zasebnost

4.2.1 Pravna podlaga in opredelitev pojmov

4.2.1.1 Človekovo dostojanstvo

Listina Evropske unije o temeljnih pravicah človekovo dostojanstvo opredeljuje v samem začetku akta in sicer v 1. členu, ki pravi da je človekovo dostojanstvo nedotakljivo in ga je treba spoštovati in varovati.[2] Prav tako varstvo človekove osebnosti varuje tudi Ustava Republike Slovenije (v nadaljevanju Ustava), ki v 34. členu zagotavlja pravico do osebnega dostojanstva in varnosti.[3]

Človekovo dostojanstvo je neločljivo povezano z vsemi ostalimi človekovimi pravicami, tako primarnimi kot tudi sekundarnim, lahko bi rekli, da se brez spoštovanja človekovega dostojanstva ostale pravice sploh ne morejo uresničevati v vseh razsežnostih. To se kaže tudi v tem, da se je SEU večkrat opredelilo do tega. To je storilo tudi v zadevi C-377/98, v kateri je Kraljevina Nizozemska predložila

[1] Štempihar, A.: Kaj je zares digitalno poslovanje?, IIBA Slovenija, april 2017, <https://slovenia.iiba.org/sites/slovenia/files/IIBA_mesecniki/mesecniki_clanki/Mesecnik_IIBA_april_2017-Clanek_%20Kaj_zares_je_digitalno_poslovanje_AS.pdf> (20.4.2020).

[2] Listina unije o temeljnih pravicah, UL EU C 303 z dne 14.12.2007, str. 1-16.

[3] Ustava Republike Slovenije (Uradni list RS, št. 33/91-I, 42/97 – UZS68, 66/00 – UZ80, 24/03 – UZ3a, 47, 68, 69/04 – UZ14, 69/04 – UZ43, 69/04 – UZ50, 68/06 – UZ121,140,143, 47/13 – UZ148, 47/13 – UZ90,97,99 in 75/16 – UZ70a).

predlog za razglasitev ničnosti Direktive o pravnem varstvu biotehnoloških izumov.[4][5] V 70. paragrafu sodbe je poudarjeno, da mora Sodišče pri nadzoru skladnosti aktov institucij s splošnimi načeli prava Unije nadzorovati spoštovanje temeljne pravice človekovega dostojanstva in osebne celovitosti. Nadalje je v 71. paragrafu pojasnjeno, da spoštovanje človekovega dostojanstva, ki je zagotovljeno v prej omenjeni direktivi, prepoveduje, da bi bilo človeško telo na različnih stopnjah svojega nastajanja in razvoja lahko izum, ki bi ga bilo mogoče patentirati. Kot primer lahko vzamemo človekovo dostojanstvo v kazenskem ali pravdnem postopku. Organ pregona oziroma organ, ki vodi postopek, mora zagotoviti varstvo vseh oseb, ki so v postopek vključene, na način, da mora zagotoviti varstvo njihovih podatkov in skrbeti za primerno obravnavo, ne glede na obtožbe, ki osebo bremenijo. Prav tako je s človekovim dostojanstvom povezano izvrševanje na primer socialnih pravic. Oseba, ki ostane brez dohodka je upravičena do socialne pomoči s strani države, ki bi morala biti namenjena izključno takrat, ko je cilj zavarovanje človekovega dostojanstva ene osebe ali več oseb. Tudi na primer oskrba v zdravstvu se s pojmom dostojanstva neločljivo povezuje. Paliativna oskrba je mogoče trenutno še najbolj aktualna in pereča tema. Pogosto pa se s pojmom dostojanstva srečamo tudi v postopkih izvršbe, ki je ena izmed bolj kočljivih pravnih situacij in je poseg v dostojanstvo tako rekoč neizogiben, vprašanje je le to, da je poseg sorazmeren.

Človekovo dostojanstvo je po besedah Etelke Korpič Horvat temeljna vrednota vsake demokratične državne in družbene ureditve.[6] Države so do pojma človekovega dostojanstva razvile različne pristope. Na najvišjo raven ga povzdigne nemška zvezna ustava, ki v 1. členu navaja, da je človekovo dostojanstvo nedotakljivo ter da je njegovo spoštovanje in varstvo obveznost celotne državne oblasti.[7] Za primerjavo slovenska Ustava v prvih členih ureja državno ureditev, človekove pravice pa se pričnejo od 14. člena dalje. Ustavno sodišče je v zadevi *Titova cesta* štelo, da poseg v človekovo dostojanstvo ni le poseg v človekovo pravico in temeljno svoboščino, temveč da je kot posebno ustavnopravno načelo "načelo spoštovanja človekovega dostojanstva neposredno utemeljeno že v 1. členu Ustave,

[4] Zadeva C-377/98, *Kraljevina Nizozemska proti Parlamentu in Svetu*, ECLI:EU:C:2001:523.
[5] Direktiva Evropskega parlamenta in Sveta 98/44/ES z dne 6. julija 1998, o pravnem varstvu biotehnoloških izumov, Uradni list Evropske unije, L 213, 30.7.1998, str. 13–21.
[6] Korpič-Horvat, E.: Razvoj socialne varnosti in varovanje človekovega dostojanstva v odločitvah Ustavnega sodišča Republike Slovenije, Podjetje in delo, št. 6-7, 2018, str. 1325.
[7] Nemška zvezna ustava, Grundgesetz für die Bundesrepublik Deutschland in der im Bundesgesetzblatt Teil III, Gliederungsnummer 100-1, veröffentlichten bereinigten Fassung, das zuletzt durch Artikel 1 des Gesetzes vom 28. Juni 2022 (BGBl. I S. 968) geändert worden ist.

ki Slovenijo opredeljuje kot demokratično republiko".[8] Prav tako je Ustavno sodišče v tej zadevi navedlo: "Po vsebini gre pri človekovem dostojanstvu za predpostavko, da ima vsak človek enako in absolutno notranjo vrednost, ki mu pripada prav zato, ker je človek. Spoštovanje človekovega dostojanstva zato pomeni varstvo osebne vrednosti posameznika pred neupravičenimi posegi in zahtevami države in družbe."

4.2.1.2 Izzivi digitalizacije za varstvo zasebnosti

Listina EU o temeljnih pravicah spoštovanje zasebnega življenja omenja v 7. členu, preko katerega podeljuje pravico do spoštovanja zasebnega in družinskega življenja, stanovanja ter komunikacij posameznika. Seveda pa je z zasebnostjo povezano tudi varstvo osebnih podatkov, ki je v Listini varovano v 8. členu, ki posamezniku podeljuje pravico do varstva osebnih podatkov, ki se nanj nanašajo. Evropska konvencija o človekovih pravicah (v nadaljevanju EKČP),[9] v 8. členu prav tako nudi varstvo pravice do spoštovanja zasebnega in družinskega življenja, doma in dopisovanja. Drugi odstavek istega člena pa navaja, da se tudi javna oblast ne sme vmešavati v izvrševanje te pravice, razen, če je to določeno z zakonom in nujno v demokratični družbi zaradi državne varnosti, javne varnosti ali ekonomske blaginje države, zato, da se prepreči nered ali kaznivo dejanje, da se zavaruje zdravje ali morala, ali da se zavarujejo pravice in svoboščine drugih ljudi. To pa je lahko že predmet razprave. Razmerje med Listino EU o temeljnih pravicah in EKČP je opredeljeno v 3. odstavku Listine EU o temeljnih pravicah, ki pravi, da sta, v primerih ko listina vsebuje pravice, ki ustrezajo pravicam, zagotovljenim z Evropsko konvencijo o varstvu človekovih pravic in temeljnih svoboščin, vsebina in obseg teh pravic enaka, kot vsebina in obseg pravic, ki ju določa navedena konvencija. Konvencija na evropski ravni namreč predstavlja osnovo, minimum pravic. Prav tako navaja, da s to določbo ne preprečuje širšega varstva po pravu Unije. Varstvo zasebnosti in varstvo osebnih podatkov v 35. in 38. nudi tudi Ustava.

Zasebnost je v digitalizaciji tako rekoč nemogoče pričakovati.[10] Kazalniki za to so predvsem razkritja, ki vsake toliko časa javnost opozorijo na vdor v zasebnost s

[8] Zadeva »Titova cesta«, Ustavno sodišče RS, Sodba U-I-109/10 z dne 26. septembra 2011.
[9] 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 – Mednarodne pogodbe, št. 7/94).
[10] Newman Forbes, D.: What Is Privacy In The Age Of Digital Transformation?

strani korporacij. Takšen primer je bil razkrit lansko leto in sicer s strani virtualnega asistenta Amazon Alexa, ki naj bi ves čas poslušal in snemal pogovore uporabnikov, tudi ko ti asistenta sploh niso potrebovali in uporabljali.[11] Večina uporabnik se ne zaveda, da Amazon hrani kopijo vsega, kar je naprava poslušala in posnela. Prav tako pa ni nič manj sporno delovanje aplikacije Siri v Applovih aparaturah in pa Googlovega asistenta, saj delujeta po istem principu. Vsi upravljalci navedenih aplikacij pomirjajo, da naprava zvok snema le, če je poklicana po imenu, vendar pa se je novinar Geoffrey Fowler podrobneje posvetil raziskovanju arhiva posnetkov svoje Alexa naprave in ugotovil, da zajema tako ukaze namenjene napravi kot tudi pogovore zasebne in občutljive narave, ki so izgleda nekako sprožili »wake work« naprave. Po zagotovilu Amazona naj bi se primeri, ko pride do tega, zmanjševali. Glavni namen snemanja pa naj bi bil ta, da se lahko delovanje naprave posodablja in izboljšuje. V kolikor bi uporabnik mikrofon izklopil, bi napravi vzel glavni namen delovanja. Do velike dileme pa bi prišlo v primeru, da bi naprava posnela na primer zelo občutljivo vsebino zasebnega pogovora in ga v zmoti posredovala drugim uporabnikom. To pa niti ni le teorija, temveč obstaja že resnični primer.[12] Družina iz Portlanda je prejela nepričakovan klic, da naj izključi vse Alexa naprave v svojem domu, saj so postali žrtve hekerjev. Vse se je začelo na način, da je ena izmed naprav Alexa posnetke posredovala brez soglasja družine. Amazon se je na kritike odzval z odgovorom, da je določen pogovor moral vsebovati besedo podobno besedi Alexa, ki je napravo prebudila, nadalje pa je naprava še »pridobila« smiselna navodila, komu naj posnetek posreduje. Vendar naj bi bile podobne situacije izjemno redke, prav tako pa naj bi bilo vsem uporabnikom omogočeno dostopati do arhiva posnetkov, kar pomeni, da bi lahko neustrezne vsebine tudi zbrisali. Apple pa na primer posnetkov pogovorov iz aplikacije Siri ne shranjuje individualizirano, temveč naj bi bila baza skupna in anonimna. Tudi Google je do nedavnega posnel prav vse zvoke, ki jih je zaznal njegov asistent, kar je spremenil šele pred nedavnim. Geoffrey Fowler se je v članku sarkastično pošalil, da bi vsem podatkom, ki jih je o sebi izbrskal v Alexinem arhivu, zavidala celo tajna policija. Na koncu se avtor zave, da Amazon ne

<https://www.forbes.com/sites/danielnewman/2019/05/02/what-is-privacy-in-the-age-of-digital-transformation/#8050c9c628ed>, (4.5.2020).

[11] Alexa has been eavesdropping on you this whole time, Geoffrey Fowler, The Washington Post, <https://www.washingtonpost.com/technology/2019/05/06/alexa-has-been-eavesdropping-you-this-whole-time/> (4.5.2020).

[12] An Amazon Echo recorded a family's conversation, then sent it to a random person in their contacts, report says, Hamza Shaban, The Washington Post,
<https://www.washingtonpost.com/news/the-switch/wp/2018/05/24/an-amazon-echo-recorded-a-familys-conversation-then-sent-it-to-a-random-person-in-their-contacts-report-says/?noredirect=on> (4.5.2020).

pridobiva zgolj informacij s snemanjem, temveč kar celotno sliko vsakdana. Oprema doma je namreč že digitalizirana do te mere, da lahko upravljalec sistema brez težav razpozna lastnosti in značilnosti uporabnika. Potrebno se je zavedati, da Amazon sodeluje tudi z ostalimi napravami in aparati v našem domu, pod pretvezo zagotavljanja najboljše možne uporabniške izkušnje. To pomeni, da pridobi podatke o tem, koliko se je naše stanovanje ogrevalo, kakšno glasbo smo poslušali, koliko svetlobe smo uporabljali tekom dneva, koliko časa smo bili budni, koliko hrane smo konzumirali in s katerimi osebami smo komunicirali.

Zatem, ko so luč sveta ugledala razkritja žvižgačev, kot je npr. Snowden, je Evropski parlament sprejel resolucijo, v kateri je Agencijo EU za temeljne pravice (v nadaljevanju FRA) pozval, naj pripravi raziskavo o varstvu temeljnih pravic v okviru opravljanja nadzora. Leta 2015 je bilo s strani agencije objavljeno poročilo,[13] ki pa po mnenju piscev II. dela poročila, ki je bilo pripravljeno leta 2018 že ni več dosledno spremembam, ki so se vmes dogodile.[14] Zaradi pogostih terorističnih napadov, migracijskih pritiskov in vedno več kibernetskih groženj je namreč več držav članic EU sprejelo zakonodajo za okrepitev zbiranja obveščevalnih podatkov. S tem je nemalo članic razširilo uporabo nacionalnih zakonov, da bi lahko obveščevalnim in varnostnim organom omogočile boljši nadzor in pregled nad možnimi zlorabami in grožnjami državnemu sistemu.

Zdaj, ko imamo dobro predstavo, kaj pojmi človekovo dostojanstvo, varstvo zasebnosti in varstvo osebnih podatkov pomenijo, jih lahko povežemo tudi z neizbežno digitalizacijo. Porajajo se mi predvsem vprašanja povezana z varstvom osebnih podatkov na področju zdravstva, preko aplikacij za diagnosticiranje in elektronskih baz podatkov o zdravstvenem stanju posameznikov. Prav tako bi bila smiselna razprava o tem, kako korporacije pridobivajo podatke o obnašanju in navadah posameznikov, ki so nadalje podlaga za prilagojene ponudbe in pa povečanje povpraševanja po njihovih storitvah. Nekaj besed bom posvetila sledenju lokacije in pa snemanju govora preko mobilne naprave. V zadnjih letih se vse bolj sprašujemo, kaj za našo prihodnost pomeni ti. tehnologija prepoznave obraza »face

[13] Nadzor, ki ga izvajajo obveščevalne službe: zaščitni ukrepi in pravna sredstva v zvezi s temeljnimi pravicami v EU – Del I: Pravni okviri držav članic, Agencija FRA, 2015, <https://eur-lex.europa.eu/legal-content/SL/TXT/PDF/?uri=CELLAR:35149923-8c2c-11e5-b8b7-01aa75ed71a1&from=FR> (4.5.2020).
[14] Nadzor, ki ga izvajajo obveščevalne službe: zaščitni ukrepi in pravna sredstva v zvezi s temeljnimi pravicami v Evropski uniji – Del II, Agencija FRA, 2018, <https://fra.europa.eu/sites/default/files/fra_uploads/fra-2017-surveillance-intelligence-services-vol-2-summary_sl.pdf> (4.5.2020).

recognition tehnology«. Vsi našteti problemi vzbujajo nastanek nemalo teorij zarot, zato je raziskovanje teh tem zelo zanimivo.

Do pomembnosti varovanja temeljnih svoboščin se opredeljuje tudi Bela knjiga o umetni inteligenci, ki jo je pripravila Evropska komisija: *»Glede na velik vpliv umetne inteligence na našo družbo in potrebo po vzpostavitvi zaupanja je nujno, da evropska umetna inteligenca temelji na naših vrednotah in temeljnih pravicah, kot sta človekovo dostojanstvo in varstvo zasebnosti«.* [15]

Zaskrbljujoče podatke izkazujejo tudi raziskave Sveta Evrope, ki opozarjajo na vpliv razvoja algoritmov in tehnologije, na temeljne človekove pravice, ki jih zagotavlja EKČP.[16] Predvsem je ogroženo zasebno in družinsko življenje, v povezavi z osebnimi podatki. Na prvi pogled piškotki niso nevarni, vendar ravno ti pripomorejo k profiliranju uporabnika in polnjenju baze o uporabniku.[17] Moj pomislek na tem mestu je, da se uporabniki ne zavedamo, da ima lahko na primer vsakdanje odklepanje zaslona mobilnega telefona s prstnim odtisom v prihodnosti potencialno negativne učinke. »Pravica do pozabe" iz 17. člena GDPR na koncu ne bo imela pravega učinka, saj se uporabniki niti ne zavedamo, koliko podatkov smo v svet že prostovoljno posredovali in jih ne bomo nikoli več mogli vzeti nazaj. Mogoče posamezni podatek o nas še ne predstavlja tako velike grožnje, vendar bo sistem kaj kmalu, če tega seveda še ne počne, zmožen povezati na prvi pogled nepovezane vsebine. Mislim, da je dovolj že vpogled v elektronsko pošto ali pa v datoteke, ki jih ima posameznik shranjene v oblaku. Seveda pa bo kot glavni cilj zbiranja podatkov vedno izpostavljena nacionalna varnost, vsi pa vemo, da je lahko profiliranje zelo pomemben dejavnik tudi v iskanju načinov, kako na pravi način pristopiti k volilcem. V kolikor bo v bazi podatek o tem, da je oseba bolj konservativno usmerjena, se ji bodo v skladu s tem prikazovale vsebine, ki se bodo dopadle njenemu političnemu mišljenju. To se v praksi že udejanja in ni zgolj znanstvena fantastika v prihajajočih letih. Med drugim smo bili temu priča v teku zadnjih predsedniških volitev v

[15] Evropska komisija, BELA KNJIGA o umetni inteligenci - evropski pristop k odličnosti in zaupanju, COM(2020) 65 final.
[16] ALGORITHMS AND HUMAN RIGHTS, Study on the human rights dimensions of automated data processing techniques and possible regulatory implications, Svet Evrope 2018, <https://rm.coe.int/algorithms-and-human-rights-en-rev/16807956b5> (2.6.2020).
[17] Angleško »cookies«.

Združenih državah Amerike.[18] Vendar pa za predložitev naših podatkov nismo vedno krivi sami, saj lahko te predloži 3. oseba z ali brez našega dovoljenja. S tem vprašanjem se je ukvarjalo Sodišče EU v zadevi C-131/12.[19] Tožnik v tej zadevi je želel, da novičarski časnik in pa Google brskalnik ugodita njegovi prošnji, da se ob vpisu njegovega imena v iskalnik kot prvi zadetki ne prikazujejo več novice o tem, da je bil udeležen v postopku izvršbe. Sodišče se je ukvarjalo z vprašanjem, če podjetje Google, kot upravljalec brskalnika dejansko upravlja z osebnimi podatki tožnika, glede na dejstvo da so njegovi podatki objavljeni v člankih, neodvisnih od Googla. Sodišče EU je v 33. točki sodbe podalo razlago, da »*družba, ki upravlja iskalnik, določa namene in sredstva te dejavnosti, tako da jo je treba šteti za „upravljavca" te obdelave.* Kot upravljalec osebnih podatkov pa je nosilec brskalnika dolžan ugoditi pravici osebe do izbrisa podatkov (črtanja novic iz prvih zadetkov v iskalniku), ne glede na to, da bo na primer vsebina na internetu še vedno obstajala (bo objavljena zakonito ali ne). Vendar pa bi bila pravica osebe omejena, v kolikor bi se izkazalo, da je poseg v njene temeljne pravice upravičen zaradi prevladujočega interesa javnosti (dostop do javnih informacij). Tipičen primer so informacije javnega značaja.

4.2.2 Digitalizacija na področju zdravstva

Po definiciji Svetovne zdravstvene organizacije iz leta 1948 je zdravje: »*stanje popolnega telesnega (fizičnega), duševnega (mentalnega) in socialnega blagostanja/ugodja in ne zgolj stanje odsotnosti bolezni ali betežnosti/nemoči.*« Lahko se strinjamo, da je zdravje ena izmed najbolj pomembnih vrednot človeka, ki je povezana tudi z ohranjanjem človekovega dostojanstva. Tudi zdravstveni sistem se v digitalni dobi razvija in s sabo prinaša mnoge spremembe tako pri obravnavi pacientov kot skladiščenju vseh podatkov o pacientih. V zadnjem času se govori o elektronskih napotnicah, elektronskih receptih, elektronskih zdravstvenih kartotekah in tudi o aplikacijah, ki so namenjene diagnosticiranju zdravstvenih težav uporabnika.

[18] Cadwalladr C., Graham-Harrison, E.: Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach, The Guardian, 2018, <https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election> (1.6.2020).

[19] Zadeva C-131/12, *Google Spain SL in Google Inc. proti Agencia Española de Protección de Datos (AEPD) in Mariu Costeji Gonzálezu*, ECLI:EU:C:2014:317.

Informacijski pooblaščenec na svoji spletni strani pojasnjuje, kakšno mora biti varstvo zdravstvenih podatkov oseb.[20] Vsi, ki imajo opravka z zdravstvenimi podatki (zdravstvene ustanove in zavodi, idr.), morajo v skladu z zakonodajo učinkovito urediti in zagotoviti varnost zdravstvenih kartonov posameznikov, izdanih receptov, evidence bolnikov in drugih podatkov. Vendar pa se kot glavni problem varnosti ne zdijo dejstva, da se na primer zdravstveni kartoni nahajajo na mizi in so tako dostopni mimoidočim, temveč grožnja, da nekdo vdre v informacijsko bazo in tako pridobi kočljive podatke o osebi, ki se zdravi ali se je zdravila v preteklosti. Načini obdelovanja in vnašanja podatkov v elektronske zdravstvene kartoteke (v nadaljevanju EZK), se med zdravstvenimi ustanovami zelo razlikujejo. Raziskovalna skupina na Tehnološkem inštitute Massachusetts (MIT), si želi v svet EZK uvesti inovativno rabo blockchain tehnologije. To se ne bi zgodilo na klasičen način veriženja blokov, temveč z uporabo ti. "pointers-ov", ki so kot neke hiperpovezave. In kako bi to delovalo? Zdravnik po obravnavi pacienta podatke vnese v aplikacijo, minimalen kos podatkov v anonimizirani obliki pa gre na blockchain unikatnim identifikatorjem pacienta. Torej se na blockchain prenese zgolj povezava do internih podatkov, ki jih upravlja zdravnik. Če pacient zamenja zdravnika, bo novi zdravnik lahko preko unikatnega identifikatorja v verigi blokov dostopal do podatkov, ki jih je vnašal prejšnji zdravnik. To bo pomenilo večjo doslednost pri zdravstveni oskrbi in pa onemogočilo šume v komunikaciji ter odpravilo težave, ki so bile povezane s pridobivanjem zdravstvenih kartotek v fizični obliki.[21] V fazi zaključevanja pisanja (junij 2020), se že kažejo rezultati uporabe aplikacija za diagnosticiranje korona virusa. Predvsem je razvidno to, da sta se v pripravo aplikacij hitro vključili korporaciji Apple in Google, kar je skrb vzbujajoče predvsem z vidika varstva osebnih podatkov, ki so zaradi posegov prej omenjenih akterjev že nemalokrat bili izpostavljeni in ogroženi. Najprej je britanska vlada namreč imela vizijo razvoja neodvisne aplikacije, ki bi podatke uporabnikov o širjenju virusa zbirala preko bluetooth povezave. Podatki bi se shranjevali centralizirano, kar bi pomenilo večjo varnost podatkov, vendar pa se je rok za pripravo te aplikacije znova in znova podaljševal, zato je britanska vlada v aprilu sporočila, da se bosta v pripravo aplikacije vključila giganta Google in Apple.[22]

---

[20] Zdravstveni podatki, Informacijski pooblaščenec, <https://www.ip-rs.si/varstvo-osebnih-podatkov/inspekcijski-nadzor/najbolj-pogoste-krsitve/zdravstveni-podatki> (19.4.2020).

[21] Tehnologija, ki stoji za kriptovalutami, bi lahko reševala življenja, <http://m.racunalniske-novice.com/index.php?id=tehnologija-ki-stoji-za-kriptovalutami-bi-lahko-resevala-zivljenja.html> (19.4.2020).

[22] Rory Cellan-Jones: Coronavirus: What went wrong with the UK's contact tracing app?, BBC, 20.6.2020, <https://www.bbc.com/news/technology-53114251?at_custom4=8D4889AE-B307-11EA-A6BA-

Zanimiv primer na področju zavarovalništva in tehnologije prihaja iz ZDA. Gospod, ki je imel težave s smrčanjem in posledično dihanjem med spanjem, je uporabljal napravo CPAP (aparat za vzdrževanje stalnega pritiska v dihalnih poteh). Po tem, ko je napravo nekaj časa uporabljal, je želel s strani zavarovalnice pridobiti sofinanciranje za nov aparat. Takrat pa ga je ta obvestila, da podatki kažejo, da je stari aparat nepravilno uporabljal in mu navedla podatke za posamezni dni/noči, ko aparata ni uporabljal ustrezno oz. celo noč. Zavarovalnica je s pridobivanjem podatkov o spanju tako lahko zavarovancu odklonila sofinanciranje nadgradnje.[23] Mar to pomeni, da bi lahko bila v prihodnosti zdravstvena premija izračunana tudi na podlagi tega, kako dober je naš spanec?

4.2.3 Video nadzor in zvočno snemanje

V trenutni situaciji, ko virus COVID-19 predstavlja resno grožnjo in je poponoma spremenil naš vsakdan, so posebej do izraza prišle tudi aplikacije za diagnosticiranje virusa. Potencialne pasti tovrstnih aplikacij so razdelane že v več člankih.[24] Potekata dve aktivni raziskavi (Cambridge University in Carnegie Mellon University) za pripravo aplikacije, ki bi lahko povedala, ali je uporabnik okužen z virusom ali ne. To bi bilo izvedljivo s pomočjo umetne inteligence, ki bi na podlagi posnetkov zdravih oseb in bolnih oseb prepoznala kašelj in dihanje, ki sta značilna za virus covid-19. Projekt s cambriške univerze se imenuje Covid-19 Sounds, uporabnik pa mora dihati in kašljati v mikrofon, hkrati pa mora navesti nekaj splošnih podatkov o sebi (spol, starost, pozitiven test na virus). Projekt deluje prek spletne strani in ne preko standardne mobilne aplikacije. Skupina na drugi univerzi pa izdeluje Covid Voice Detector. Pri omenjenem pa mora uporabnik kašljati in izgovarjati abecedo. Snovalci obeh platform poudarjajo, da ne gre za aplikacije, ki bi nadomestile zdravnika. Vendar je to, kljub opozorilu, dvorezen meč, saj bodo uporabniki lahko lahkomiselno sklepali, da niso okuženi, ker jim bo tako rekla aplikacija.

17F3C28169F1&at_custom3=BBC+News&at_custom2=facebook_page&at_medium=custom7&at_custom1=%5Bpost+type%5D&at_campaign=64> (21.6.2020).

[23] Marshall Allen: You Snooze, You Lose: Insurers Make The Old Adage Literally True, Propublica, 2018, <https://www.propublica.org/article/you-snooze-you-lose-insurers-make-the-old-adage-literally-true> (1.6.2020).

[24] Leo Kelion: Coronavirus: Covid-19 detecting apps face teething problems, <https://www.bbc.com/news/technology-52215290> (19.4.2020).

Kaj pa mobilne aplikacije, ki si jih avtomatsko naložimo na svoje mobilne aparature in se pogosto sploh ne vprašamo, kaj se bo zgodilo z vsemi podatki, ki jih bo aplikacija pridobila? Članek[25] navaja, da je dejstvo, koliko varnosti lahko pričakujemo, odvisno od tega, kateri telefon uporabljamo, kje bivamo in kako smo previdni. Na primer gigant Apple naj bi od aplikacij, ki so prilagojene za Iphone, pred uvrstitvijo v ponudbo v Apple trgovini zahteval, da zadoščajo kriterijem o varovanju zasebnosti. Vendar pa neodvisne komercialne aplikacije skozi to sito ne gredo, kar pomeni da se lahko podatki uporabnika na koncu uporabijo za marsikaj. Uporabniki Androida pa naj bi bili, glede na članek, bolj ogroženi. Podlaga za to trditev naj bi bila nemška raziskava, ki je ob pregledu šestdesetih aplikacij za zdravje ugotovila, da nobena izmed pregledanih aplikacij ni vsebovala podobne seznanitve uporabnika z varstvom njegove zasebnosti in podatkov. Veliko opozorila je uporabniku lahko že dejstvo, da je določena aplikacija za prenos na voljo brez plačila, medtem ko so primerljive aplikacije plačljive. Pogosto se »brezplačne« aplikacije financirajo iz oglaševanja, vendar je vir dohodka verjetno pogosto tudi posredovanje dragocenih podatkov 3. osebam. Uporabnik pa se temu skorajda ne more izogniti, saj je sprejem pogojev pogoj za uporabo aplikacije, velikokrat pa je besedilo, ki pojasnjuje obdelavo podatkov zelo kompleksno in dolgo, tako da ga uporabnik največkrat enostavno preskoči. In zakaj so lahko podatki o zdravstvenem stanju tako zelo vredni? Zato ker so uporabni na področju profiliranja za oglaševalske storitve. Na primer, oseba je sladkorni bolnik in si ravni sladkorja v krvi ter količino dnevnega odmerka inzulina vpisuje v elektronsko tabelo aplikacije. Končni prejemnik teh podatkov bo lahko tej isti osebi na vse mogoče načine oglaševal izdelke za diabetike, izdelke brez sladkorja in morebiti tudi storitve strokovnjakov s tega področja. Oseba, ki ji bo v zameno za deljenje podatkov obljubljeno, da bo to lažje pripeljalo do zdravila ali pa pripomoglo k uspešnejšemu zdravljenju.[26]

Zdravstvene institucije v Združenih državah Amerike opozarjajo, da bi zdravstveni podatki v aplikacijah lahko na široko odprli vrata zlorabam, zato se temu aktivno upirajo. Ameriška vlada namreč pripravlja regulacijo pretoka z informacijami na področju zdravstva. Regulacija pa naj bi izvajalcem zdravstvenih storitev nalagala obveznost, da zdravstvene podatke posredujejo aplikacijam, kot so Apple's Health Records, v kolikor pacienti s tem soglašajo. Ameriška zdravstvena organizacija in

[25]This Is What Your Phone Does with Your Personal Health Data, Mark Henricks, <https://www.shape.com/fitness/trends/health-apps-privacy-personal-information-shared> (19.4.2020).
[26] Lee, S.: Who uses my health data, <https://www.goinvo.com/vision/who-uses-my-health-data/> (19.4.2020).

sektorske zdravstvene organizacije pa opozarjajo, da vnašanje podatkov v komercialne aplikacije morda ni korak v pravo smer, saj tako tudi zakonodaja, ki omejuje razpolaganje s podatki zdravstvenih kartotek sicer ne bo imela učinka, ko bodo podatki enkrat vneseni v komercialne baze. Aplikacije bi lahko s svetom delile tudi podatke o zgodovini predpisanih zdravil in o družinski zdravstveni zgodovini. To bi se lahko pokazalo škodljivo v primerih zaposlovanja, saj bo delodajalec, ob vseh podatkih, raje izbral kandidata, ki je zdrav. Prav tako pa bi zavarovalnica lahko na podlagi teh podatkov oblikovala višjo premijo za zavarovanje osebe. Vendar pa verjetno za vsemi temi prizadevanji tičijo tudi interesi multikorporacij kot so Google, Amazon, Microsoft in Apple, ki bodo s podporo vlade prodrli tudi na zdravstveni trg. Vsi našteti giganti pa so se zavezali, da bodo njihove platforme med seboj združljive in kompatibilne. Microsoft je na primer razvil storitve v oblaku, ki uporabniku omogočajo, da po preudarku določene vsebine tudi umakne. Z uveljavitvijo regulacije naj bi izvajalci zdravstvenih storitev in nosilci zdravstvenih evidenc imeli na voljo dveletni rok za izpolnitev zahtev. V kolikor bi to zavrnili, bodo prejeli globo in bo zoper njih uvedena preiskava. Vendar pa se kot največjo past pridobivanja zdravstvenih podatkov izpostavlja dejstvo, da so aplikacije narejene po sistemu vse ali nič. Torej če bo oseba soglašala s posredovanjem podatkov o zgodovini zdravljenja prehlada, bo hkrati posredovala tudi podatek o tem, da je na primer okužena z virusom HIV. To pomeni, da bodo slabi vidiki lahko zanemarili vse pozitivne učinke tovrstne ureditve.[27]

4.2.4 Tehnologija prepoznave obraza

V delu te tematike sem si ogledala oddajo Ugriznimo v znanost, v kateri je bilo dodobra predstavljeno, v kateri fazi razvoja je trenutno tehnologija za prepoznavanje obraza.[28] Ljudje naj bi si, po raziskavi izvedeni na Univerzi York, bili sposobni zapomniti povprečno pet tisoč obrazov.[29] Na Kitajskem nadzorne kamere ves čas nadzorujejo ljudi v urbanem okolju in bi naj z lahkoto prepoznavale osnovne značilnosti oseb. V času priprave zgoraj omenjene oddaje, si je Kitajska lastila bazo z več kot sedemsto milijoni obrazov, kar bi pomenilo, da bi posameznikov obraz

[27] Singer, N.: When Apps Get Your Medical Data, Your Privacy May Go With It, The New York Times, <https://www.nytimes.com/2019/09/03/technology/smartphone-medical-records.html> (20.4.2020).
[28] Radio televizija Slovenija, Oddaja Ugriznimo v znanost: Prepoznavanje obrazov, 13.12.2018, <https://4d.rtvslo.si/arhiv/ugriznimo-znanost/174582438> (3.5.2020).
[29] Never forget a face? Research suggests people know an average of 5,000 faces, University of York, <https://www.york.ac.uk/news-and-events/news/2018/research/never-forget-a-face/> (3.5.2020).

lahko našla v nekaj sekundah. Ta način za zagotavljanje večje »varnosti« pa si želijo tudi ostale svetovne velesile. Tehnologija prepoznave obrazov naj bi se izkazala kot koristna na primer v primeru, da bi prepoznala potencialne teroriste znotraj množice obiskovalcev razvpite tekme. Po besedah gosta oddaje, dr. Vitomirja Štruca, zelo velika baza ni potrebna. Policija v več državah deluje po sistemu vodenja ožje baze potencialno nevarnih oseb. V kolikor med množico zazna nekoga s podobnimi lastnostmi, ga primerja direktno s podatki s seznama nevarnih oseb. To namreč vzame bistveno manj časa, kot da bi moral sistem pregledovati bazo z neskončnim številom zadetkov. Vendar pa pomirja dejstvo, da računalnik v tem trenutku še ni sposoben prepoznavanja v enaki meri kot človek. Tudi slovenska policija že s pridom uporablja tehnologijo prepoznave obrazov, vendar bi bolj omejenem obsegu kot svetovne velesile, ki preverjajo tudi identiteto mimoidočih na ulici, saj tega slovenska policija ne počne. Uporablja jo preko spletne aplikacije, ki pomaga hitreje najti osumljenca v policijski bazi fotografij.[30] Morebitno ujemanje nato preverjajo še ročno. Vendar pa se tehnologija za prepoznavanje obrazov ne uporablja zgolj za namene varnosti, temveč imamo z njo opravka preko aplikacij in naših elektronskih naprav. Po besedah Štruca tehnologija znotraj aplikacij predstavlja podobno tehnologijo za detekcijo obraza. To lahko najprej vidimo na socialnem omrežju Facebook, kjer nam, ko naložimo sliko, preko obrazov napravi okvirčke in že predlaga, katero osebo naj označimo. Prav tako pa se mogoče še premalo zavedamo nevarnosti uporabe tridimenzionalnih filtrov, ki naš obraz spremenijo v kakšno pošast ali v prikupnega kužka. Da je to mogoče, mora naprava prepoznati dimenzije obraza. S tem pa aplikacija razbere tudi določene podatke s samega obraza, na primer koliko je oseba stara ter katerega porekla in spola je. Na podlagi tega pa se lahko tudi aplikacija odloči, ali nam bo na pregled podala oglas za ličila ali za ribiško opremo. Seveda vsaka ponudba ne bo popolnoma prilagojena, pa vendar v večini primerov bo smiselna. Na Kitajskem je z obrazom že mogoče dostopati do bančnih računov, nakupovati in vstopati na letala. Tehnologija prepoznave obraza se uporablja v skoraj bizarni situaciji in sicer prepoznava, kdo krade toaletni papir na javnem stranišču.[31] Poletne olimpijske igre, ki bi se morale izvesti letos, naj bi predstavljale prvi dogodek, na katerem bi se za varnost poskrbelo s prepoznavo obraza, saj bi tako preprečili krajo identitet in prevare.[32]

[30]Tudi slovenska policija uporablja avtomatsko prepoznavo obrazov, RTV SLO, <https://www.rtvslo.si/znanost-in-tehnologija/tudi-slovenska-policija-uporablja-avtomatsko-prepoznavo-obrazov/510776> (3.5.2020).
[31]China's High-Tech Tool to Fight Toilet Paper Bandits, New York Times, <https://www.nytimes.com/2017/03/20/world/asia/china-toilet-paper-theft.html> (3.5.2020).
[32]NEC unveils facial recognition system for 2020 Tokyo Olympics,

Zanimiva sodba glede tehnologije prepoznave obraza prihaja iz Francije.[33] Južna regija je pripravila načrt za vzpostavitev tehnologije za prepoznavo obraza na srednjih šolah v Nici in Marseillu. Nevladne organizacije, starši in sindikati so se zoper ta načrt pritožili. Sodišče same eksperimentalne uporabe tehnologije ni prepovedalo, temveč je poudarilo, da regionalne oblasti, kot je na primer južna regija, niso pristojne za sprejemanje tovrstnih odločitev. To lahko po mnenju sodišča vzpostavi le individualna izobraževalna institucija. V sodbi je sodišče navajalo določbo uredbe GDPR, ki pravi, da je za uporabo tehnologije prepoznavanja obraza nujno potrebno soglasje snemanih, saj gre za osebne biometrične podatke (14. točka, 4. člena Uredbe). Biometrične podatke je sicer v skladu z 9. členom uredbe prepovedano zbirati, soglasje pa predstavlja izjemo od te prepovedi. Sodišče je ukrep označilo kot nesorazmeren, saj naj bi po njegovih besedah »*Regionalne oblasti uporabljajo kladivo, da bi zdrobile mravljo«.*

Glede na podatke poročila EU o varstvu podatkov in digitalne identitete, iz leta 2011, je več kot tretjina evropskih državljanov aktivna na socialnih omrežjih, kar polovica od teh pa uporablja spletne strani tudi za deljenje fotografij, video posnetkov in drugega.[34]

Zanimivo je stališče, ki opozarja na nevarnost vpeljave tehnologije prepoznave obraza v socialno omrežje Facebook, ki bi brez dodatnega privoljenja lahko na fotografiji označil osebe, ki so bile kadarkoli označene na katerikoli drugi fotografiji. Veliko uporabnikov tega ne ve, oziroma to opazi šele, ko so že avtomatsko označeni na fotografijah. Neregistrirani uporabniki in uporabniki, ki bodo odklonili podajo soglasja, da se njihov obraz vključi v bazo za prepoznavo obrazov na novih fotografijah, tako v bazo ne bodo vključeni in se njihovo ime ne bo avtomatsko prikazalo med predlogi za označbo. Problem avtorica vidi v sistemu opting-out soglasja (to pomeni, da se soglasje domneva, razen če se ga izrecno odkloni). Soglasje bi moralo biti namreč individualizirano za vsako aktivnost socialnega omrežja posebej, ne pa izpeljano zgolj iz podane generalne privolitve za vse bodoče

<https://www.theverge.com/2018/8/7/17659746/tokyo-2020-olympic-games-face-recognition-nec> (3.5.2020).
[33]Sodišče prepovedalo testno prepoznavanje obrazov na šolah v Marseillu in Nici, RTV SLO, dostopno na: <https://www.rtvslo.si/znanost-in-tehnologija/sodisce-prepovedalo-testno-prepoznavanje-obrazov-na-solah-v-marseillu-in-nici/516064> (3.5.2020).
[34] SPECIAL EUROBAROMETER 359 Attitudes on Data Protection and Electronic Identity in the European Union REPORT Fieldwork: November – December 2010, objavljeno junija 2011.

aktivnosti. Problem zbiranja podatkov se skriva tudi v na videz popolnoma nenevarnemu všečku (angl. Like), ki na podlagi vseh všečkanih vsebin povzroči, da se osebi nadalje prikazuje samo prilagojena vsebina. Torej če všečka fotografije z dopustov, se mu bodo verjetno v večji meri prikazovale vsebine povezane s potovanji in turizmom.[35]

S podobnim vprašanjem glede zbiranja in hranjenja biometričnih podatkov se je v zadevi
Marper proti Združenemu Kraljestvu ukvarjalo Evropsko sodišče za človekove pravice (v nadaljevanju ESČP).[36] Ugotovilo je, da mora biti hramba osebnih podatkov glede na ključna načela iz zadevnih instrumentov Sveta Evrope ter zakonodajo in prakso drugih pogodbenic sorazmerna glede na namen zbiranja in časovno omejena, zlasti v policijskem sektorju.

4.2.5 Nadzor in sledenje lokacije

Slovenska Vlada je v predlogu prvega interventnega zakona oblikovala dva, z vidika varstva osebnih podatkov, sporna člena, in sicer 103. in 104. člen.[37]

V 103. členu zakon širi že obstoječa pooblastila policistov za namen zagotovitve spoštovanja ukrepov, ki so potrebni za zajezitev in obvladovanje epidemije COVID-19. Določba po mnenju Informacijske pooblaščenke, predstavlja širitev pooblastil do te mere, da je mogoče zajeti potencialno celotno prebivalstvo Republike Slovenije in v praksi bi to pomenilo vzpostavitev policijske države. Posegi v pravice posameznikov so po mnenju informacijske pooblaščenke preveč nedoločno in zelo široko opredeljeni. Ukrepi lahko namreč posežejo tudi v pravice posameznikov, ki niso predmet ukrepov zakona o nalezljivih boleznih in bi bili na primer podvrženi zahtevam po samoizolaciji, zdravljenju ali karanteni.[38]

---

[35] Monteleone, S.: Privacy and Data Protection at the time of Facial Recognition: towards a new right to Digital Identity?, European Journal of Law and Technology, letnik 3, številka 3.
[36] *Združene zadeve S. in Marper proti Združenemu kraljestvu, 4. decembra 2008, št. 30562/04 in 30566/04.*
[37] Zakon o interventnih ukrepih za zajezitev epidemije covid-19 in omilitev njenih posledic za državljane in gospodarstvo, PREDLOG, NUJNI POSTOPEK, EVA 2020-1611-0028.
[38] Mnenje informacijske pooblaščenke Mojce Prelesnik o Predlogu Zakona o interventnih ukrepih za zajezitev epidemije COVID-19 in omilitev njenih posledic za državljane in gospodarstvo –EVA 2020-1611-0028, z dne 30.3.2020,
<https://www.iprs.si/fileadmin/user_upload/Pdf/pripombe/2020/DZ_interventni_zakon_MNENJE_30032020_koncno.pdf> (27.4.2020).

104. člen predloga interventnega zakona določa ti. druga pooblastila policiji. Besedilo tega člena je bilo naslednje: *Če ni mogoče drugače zagotoviti spoštovanja z odločbo ali drugim aktom odrejenih ukrepov iz zakona, ki določa nalezljive bolezni, smejo policisti brez odredbe sodišča od operaterjev mobilnih omrežij pridobivati podatke o lokaciji komunikacijskega sredstva osebe, na katero se ukrep iz tega odstavka nanaša, vendar le pod pogojem, da je oseba s tem pisno soglašala pred izdajo odločbe ali drugega akta, v katerem je osebi odrejen ukrep.*

Informacijska pooblaščenka opozarja, da zakonsko pooblastilo za sledenje posameznikom iz 104. člena pomeni resen poseg v ustavno pravico do varstva osebnih podatkov in komunikacijske zasebnosti. Ustava v 37. členu takšen poseg v ustavno pravico dopušča le z izdajo sodne odredbe. Kot zaskrbljujoče pa izpostavlja tudi dejstvo, da bo za pridobitev podatkov predpogoj posameznikovo soglasje, ker naj bi že samo besedilo predloga zakona nakazovalo, da gre za »prisilno« in zgolj navidezno soglasje, posledično naj bi šlo za pravno zlorabo pojma soglasje. Prav tako zakon jasno ne opredeljuje, kdo soglasje sploh pridobi. Največja pomanjkljivost pa se zdi dejstvo, da se lahko sledenje in pridobivanje podatkov razširi tudi na osebe, zoper katere ukrep iz Zakona o nalezljivih boleznih[39] sploh ni bil izrečen. Vendar pa bi lahko tudi slednji postali predmet nazora zgolj zaradi situacije, ker bi bili v stiku ali lokacijski bližini osebe, zoper katero pa je ukrep izrečen. Informacijska pooblaščenka je Državnemu zboru predlagala, da omenjenih členov v predlagani obliki ne podpre, saj ukrepi po njenem mnenju niso sorazmerni. Dodaja še, da iz pretekle inšpekcijske prakse Informacijskega pooblaščenca izhaja nemalo primerov, ko je policija podatke pridobivala nezakonito ter jih hranila predolgo, zato je skrb ob trenutnem stanju vsekakor upravičena.

Interventni zakon je stopil v veljavo 11. aprila 2020.[40] Državni zbor je zavrnil predlog 104. člena in podprl 103. člen zakona. Informacijska pooblaščenka je na Državni zbor Republiko Slovenije in na Vlado Republike Slovenije naslovila odprto pismo.[41] Podprla je zahtevo za presojo ustavnosti 103. člena Zakona o interventnih ukrepih za zajezitev epidemije COVID-19 in omilitev njenih posledic za državljane in gospodarstvo, ki so jo na Ustavno sodišče Republike Slovenije naslovile opozicijske politične stranke. V času pisanja tega poglavja, je zahteva za presojo ustavnosti še

[39] Zakon o nalezljivih boleznih (Uradni list RS, št. 33/06 – uradno prečiščeno besedilo in 49/20 – ZIUZEOP).
[40] Zakon o interventnih ukrepih za zajezitev epidemije COVID-19 in omilitev njenih posledic za državljane in gospodarstvo (Uradni list RS, št. 49/20).
[41] Odprto pismo Informacijske pooblaščenke, z dne 24.4.2020,
<https://www.ip-rs.si/fileadmin/user_upload/Pdf/Covid19/Odprto_pismo.pdf>, (27.4.2020).

nerešena. Informacijska pooblaščenka meni, da bo Ustavno sodišče tako lahko preverilo nujnost ukrepov, z vidika ocen zdravstvene stroke ter pretehtalo vse vidike utemeljenosti, legitimnosti in sorazmernosti teh posegov. Vendar pa vsekakor meni, da določba 103. člena zakona sporna, saj bodo na podlagi določbe lahko represivni organi pridobivali podatke za nejasne namene, množično in na zalogo. Gre za ti. »ribarjenje po podatkih brez vnaprejšnjega suma kršitve – »fishing expedition«. Tovrstni ukrepi po njenem mnenju, tudi v času trenutnih spremenjenih razmer, ne bi smeli biti dopuščeni. Sklicuje se na smernice Evropskega odbora za varstvo podatkov (EDPB), ki izpostavljajo, da Splošna uredba o varstvu podatkov (GDPR) in Direktiva o zasebnosti in elektronskih komunikacijah že vsebujeta določbe, ki omogočajo uporabo osebnih podatkov, za podporo javnim organom in drugim akterjem, za spremljanje in omejevanje širjenja COVID-19. Vendar pa morajo vsi ukrepi držav članic temeljiti na splošnih načelih učinkovitosti, nujnosti in sorazmernosti. Kot sprejemljivo EDPB navaja aplikacijo, ki bi sledila razdalji med posameznimi uporabniki aplikacije, nasprotuje pa vsesplošnemu sledenju gibanja posameznika. Odprto pismo informacijska pooblaščenka zaključuje z navedbo, da se spoštovanje zrcali med drugim ali predvsem tudi v načelu sorazmernosti –da torej oblast državljane spoštuje do te mere, da ji ti lahko zaupajo, da bo pri posegih v njihove pravice zmerna in bo vanje posegala le toliko, kolikor je to nujno potrebno za dosego ustavno dopustnega cilja.

Potrebno se je zavedati, da policijski nadzor s pomočjo tehnologije iz dneva v dan napreduje. Tovrstne prakse se poslužujejo tudi policijske uprave v več mestih. V Vancouvru je vzpostavljen sistem ti. »prediktivne policije«. Na podlagi dosedanjih izkušenj z vlomi na področju Vancouvra je napravljena statistika, ki ob določeni uri prikaže potencialna žarišča in pojave vlomov. V skladu s prikazom se na določene lokacije napoti policiste. Po njihovih navedbah naj bi bilo število vlomov trenutno na najmanjši stopnji, zahvaljujoč tej tehnologiji. Glede nadzora pa se javnost pomirja z besedami, da ne nadzoruje oseb temveč le lokacije.[42] Algoritmov se poslužujejo tudi v Los Angelesu.[43] Zagotovo ima takšen sistem pozitivne in negativne vidike. Kaj se zgodi, če se oseba naključno znajde na ti. ogroženem potencialnem mestu za vlom? Lahko se zgodi, da bo policist prehitro domneval, da ima oseba namen storiti

[42] Matt Meuse: Vancouver police now using machine learning to prevent property crime, CBC, 2017, <https://www.cbc.ca/news/canada/british-columbia/vancouver-predictive-policing-1.4217111> (5.6.2020).
[43]Nate Berg: Predicting crime, LAPD-style, The Guardian, 2014, <https://www.theguardian.com/cities/2014/jun/25/predicting-crime-lapd-los-angeles-police-data-analysis-algorithm-minority-report#maincontent> (5.6.2020).

odklonilno dejanje. Kot že rečeno je algoritem lahko pripomoček ne pa nadomestilo za zdravo kmečko pamet.

4.2.6 Internet stvari

Si lahko predstavljamo potek našega povprečnega dneva v prihodnosti, da bomo zjutraj vstali, ko nas bo zbudil telefon na podlagi predhodnega izračuna, da smo se dovolj naspali in ponoči nismo imeli slabih sanj in drugih motenj? Nato bomo uporabili pametni WC, ki lahko spreminja lučke in spremlja, če je naš metabolizem zdrav. Nato si bomo roke umili s pametno pipo, ki deluje na ukaz. Nato bomo kosilo pripravili v pametni pečici, ki na podlagi izbire jedi sama prilagodi način peke in pa vročino. Pred tem pa bomo za nasvet o izbiri kosila seveda vprašali našega elektronskega asistenta na telefonu, ki naše navade in želje pozna že boljše kot mi sami. Zatem bomo ostanke odvrgli v pametni smetnjak, ki bo sproti beležil vsebino in nam preko opozorila na telefonu javil, kdaj ga bo potrebno izprazniti. Umazana oblačila bomo samo postavili v pralni stroj, potem pa ga bomo vključili preko mobilne aplikacije, ko se nam bo to zdelo primerno. Naš odhod na dopust ne bo več problem, saj bomo lahko na daljavo nahranili tudi naše hišne ljubljenčke in na daljavo spremljali kje v hiši se nahajajo in kaj počnejo. Tudi skrb za otroke ne bo več problem, saj že v tem trenutku poznamo prototipe za pametne pleničke, ki spremljajo zdrav metabolizem in starše preko aplikacije obvestijo, kdaj je otroka potrebno previti. Če smo se do sedaj osredotočali na enoto doma, pa si poskusimo predstavljati, da se to preslika še na področje celotnega kraja mesta, države, celo sveta? Vse to bo lahko omogočil internet stvari, ki bo med seboj povezal svetovni splet in vse naprave v našem domu in okolici. Do leta 2020 naj bi bilo v omrežje interneta stvari priključenih kar 30 milijard naprav.[44] To zajema tako pametne merilce vlage v stanovanju kot visokotehnološka letala. To želi vzpostaviti podjetje SideWalk Labs, ki spada pod istega lastnika kot Google. Namen te družbe je vzpostavitev pametnega mesta in družbe, preko vzpostavitve videonadzora in digitalizacije vseh spektrov življenja. Projekt je že v teku in sicer se vzpostavitev

[44] Gaylor, B.: Internet vsega, dokumentarni film, Kanada, 2020, <https://4d.rtvslo.si/arhiv/tuji-dokumentarni-filmi-in-oddaje/174697585> (3.6. 2020).

načrtuje v Torontu, vendar pa se nevladne organizacije in različna združenja proti temu vztrajno borijo.[45][46]

Vendar pa ne smemo vseh tehnologij metati v isti koš, določene inovacije so lahko namenjene tudi koristi uporabnikov. Tovrsten primer je naprava KEGG, ki skrbi za zbiranje podatkov o plodnosti ženske in po zagotovilu vodstva podjetja, naj podatkov ne bi delila s svetom. To bi namreč lahko pomenilo, da bi bile ženske, ki imajo težave s plodnostjo, slabše obravnavane pri zavarovanju. [47]

4.3 Vpliv digitalizacije na družinsko življenje

Družina je življenjska skupnost otroka, ne glede na starost otroka, z obema ali enim od staršev ali z drugo odraslo osebo, če ta skrbi za otroka in ima po tem zakoniku do otroka določene obveznosti in pravice. Družina zaradi varstva koristi otroka uživa posebno varstvo s strani države. [48]

Digitalizacija povzroča razdor med tradicionalnimi vlogami staršev in otrok.[49] V zadnjih dveh desetletjih so otroci, ki so aktivno gledali televizijo, ponotranjili informacijo, da so njihovi starši sebični, neodrasli, neizobraženi in na splošno nevedni. Kot primer televizijske vsebine, ki je tovrstne informacije podala otrokom, avtor navaja televizijske nadaljevanke Malcolm in the Middle (Glavca),[50] Family Guy (Griffinovi),[51] Two and a Half Men (Dva moža in pol),[52] ter resničnostne šove o super varuškah. Vendar pa že sama uporaba tehnologije v smislu različnih klepetalnic in igranja video iger povzroči, da se komunikacija med otroci in starši močno poslabša. Zanimiva so opažanja, da uporaba tehnologije za učne namene ni prizadela komunikacije v isti meri, kot uporaba tehnologije za socialna omrežja in prosti čas. Otroci, ki neprestano uporabljajo socialna omrežja, naj bi imeli s strani svojih staršev

[45] Barreto, D.: Normalizing mass surveillance: Sidewalk Labs' threat to human rights, Now Magazine, 2019, <https://nowtoronto.com/news/sidewalk-labs-privacy-human-rights/> (6.6.2020); Yasmin Aboelsau, Y.: Canadian Civil Liberties Association threatening lawsuit over Google's Sidewalk Labs, Venture Toronto, 2019, <https://dailyhive.com/toronto/canadian-civil-liberties-association-sidewalk-labs-open-letter-2019> (6.6.2020).

[47] Lunden, I.: Kegg tracks your fertility by measuring vaginal mucus with a kegel ball, 2018, <https://techcrunch.com/2018/09/05/kegg-kegel-ball-fertility/> (6.6.2020).

[48] Družinski zakonik (Uradni list RS, št. 15/17, 21/18 – ZNOrg, 22/19 in 67/19 – ZMatR-C).

[49]Taylor, J.: Is Technology Creating a Family Divide? <https://www.psychologytoday.com/intl/blog/the-power-prime/201303/is-technology-creating-family-divide> (6.6.2020).

[50] <https://www.imdb.com/title/tt0212671> (6.6.2020).

[51] <https://www.imdb.com/title/tt0182576/?ref_=nv_sr_srsg_0> (6.6.2020).

[52] <https://www.imdb.com/title/tt0369179/?ref_=nv_sr_srsg_3> (6.6.2020).

občutek manjše podpore. Prav tako do nedavnega naši starši še niso bili vešči tehnologije, v zadnjih letih se ta trend seveda obrača, vendar otroci in mladostniki tehnologijo jemljejo kot samoumevno, saj so jo lahko ponotranjali od samega začetka njihovega zavedanja. Zato lahko omejitve glede časovne uporabe in načina uporabe tehnologije, postavljene s strani staršev, vrzel v odnosu z otroci še povečajo. Nezmožnost vzpostavitve kakovostnega odnosa pa privede do tega, da starši ne morejo več vedeti, kaj se v življenju njihovih otrok sploh dogaja. Vendar pa grešni kozel ni vedno otrok, saj je tehnologija omrežila tudi starše, ki z neprestanim govorjenjem po telefonu, pregledovanjem elektronske pošte in gledanjem televizije, otrokom povzročijo občutek nezanimanja. Obstajajo primeri, ko so starši želeli komunikacijo z otroci vzpostaviti preko tehnologije, tako da so se tudi sami pridružili socialnim omrežjem, vendar to v nikakršni meri en more zamenjati navadne primarne komunikacije. K fenomenu razpada družine pa vsekakor prispeva tudi dejstvo, da so se domovi družin povečali za kar petdeset odstotkov, število družinskih članov pa v povprečju zmanjšalo, kar pomeni, da ima vsak član družine možnost popolne izolacije. Razkorak pa privede do tega, da družinski člani med sabo niso več sposobni imeti kakovostnega pogovora. To pa se pokaže predvsem v izrednih časih, kot smo jim priča v času pandemije Korona virusa.

Zagotovo so se razmere za vstop v družbo skozi zgodovino spremenile do te mere, da so primeri iz zgodovine (mentorstva starejši učenjakov, ki so že uveljavljeni v družbi, vključevanje v elitna združenja idr.), popolno nasprotje današnji praksi. Z razvojem tehnologije so mentorji mladostnikom postali predvsem drugi mladi, saj trenutna starejša generacija še zaostaja z znanjem. Ta vzorec pa se bo verjetno čez čas spremenil. Vzrok za ustvarjanje velike razlike med mlajšo in starejšo generacijo pa naj bi bil tudi v tem, da se dandanes od mladih zahteva velika mera samostojnosti in s tem povezanega sprejemanja pomembnih življenjskih odločitev.[53] V zadnjih letih je stroka namreč opozarjala na to, da način vzgoje ti. helikopterskih staršev, lahko otrokovemu razvoju osebnosti tudi škodi.[54]

[53] Doward, J. in Hall, S.: Technology cuts children off from adults, warns expert, The Guardian, 2019, <https://www.theguardian.com/society/2019/apr/27/technology-threatens-child-development-psychology-expert-warns> (8.6.2020).

[54] Angleško Helicopter parents, Razjasnitev pojma v oddaji Dobro jutro, RTV Slovenija, 1.6.2017, <https://4d.rtvslo.si/arhiv/dobro-jutro/174474629> (8.6.2020).

Področje vpliva digitalizacije na družinsko življenje, je za raziskovalce zelo zahtevno, saj so rezultati anket in raziskav pogosto lahko odvisni od okolja in družbe v kateri se izvajajo. Prav tako pa je zelo težko preučevati najbolj intimna razmerja med družinskimi člani. Problem nastane pri raziskovanju vsebin, ki družinske člane razdvajajo ali pa jih zbližujejo, saj tretje osebe nimajo vpogleda v vsebino, ki jo določena oseba spremlja in je zato nemogoče razvozlati, kaj ljudje počnejo s svojimi prenosniki, tablicami ali pametnimi telefoni. Kot primer, v preteklosti je bilo lažje pridobiti podatke o tem, kaj družina glede preko TV, saj so podatke o številkah lahko posredovali televizijski ponudniki, v primeru brskanja in uporabljanja aplikacij pa je to veliko težje in seveda tudi sporno z vidika varstva osebnih podatkov.[55]

Seznam literature in virov

Monografije

Korpič-Horvat, E.: Razvoj socialne varnosti in varovanje človekovega dostojanstva v odločitvah Ustavnega sodišča Republike Slovenije, Podjetje in delo, št. 6-7, 2018.

Članki in poglavja iz knjig

Monteleone, S.: Privacy and Data Protection at the time of Facial Recognition: towards a new right to Digital Identity?, European Journal of Law and Technology, letnik 3, številka 3.

Pravni viri

Ustava Republike Slovenije (Uradni list RS, št. 33/91-I, 42/97 – UZS68, 66/00 – UZ80, 24/03 – UZ3a, 47, 68, 69/04 – UZ14, 69/04 – UZ43, 69/04 – UZ50, 68/06 – UZ121,140,143, 47/13 – UZ148, 47/13 – UZ90,97,99 in 75/16 – UZ70a).
Zakon o nalezljivih boleznih (Uradni list RS, št. 33/06 – uradno prečiščeno besedilo in 49/20 – ZIUZEOP).
Zakon o interventnih ukrepih za zajezitev epidemije COVID-19 in omilitev njenih posledic za državljane in gospodarstvo (Uradni list RS, št. 49/20).
Zakon o interventnih ukrepih za zajezitev epidemije covid-19 in omilitev njenih posledic za državljane in gospodarstvo, PREDLOG, NUJNI POSTOPEK, EVA 2020-1611-0028.
Družinski zakonik (Uradni list RS, št. 15/17, 21/18 – ZNOrg, 22/19 in 67/19 – ZMatR-C).
Nemška zvezna ustava, Grundgesetz für die Bundesrepublik Deutschland in der im Bundesgesetzblatt Teil III, Gliederungsnummer 100-1, veröffentlichten bereinigten Fassung, das zuletzt durch Artikel 1 des Gesetzes vom 28. Juni 2022 (BGBl. I S. 968) geändert worden ist.
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 – Mednarodne pogodbe, št. 7/94)
Listina unije o temeljnih pravicah, UL EU C 303 z dne 14.12.2007, str. 1-16.

[55] Anja Riitta Lahikainen in Ilkka Arminem: Family, media and digitalization of childhood, 2017, <https://helda.helsinki.fi/bitstream/handle/10138/231835/12_Chapter12final2017.pdf?sequence=1> (9.6.2020).

Direktiva Evropskega parlamenta in Sveta 98/44/ES z dne 6. julija 1998, o pravnem varstvu biotehnoloških izumov, Uradni list Evropske unije, L 213, 30.7.1998, str. 13–21.
Evropska komisija, BELA KNJIGA o umetni inteligenci - evropski pristop k odličnosti in zaupanju, COM(2020) 65 final.

Sodna praksa

Zadeva »Titova cesta«, Ustavno sodišče RS, Sodba U-I-109/10 z dne 26. septembra 2011.
Zadeva C-377/98, *Kraljevina Nizozemska proti Parlamentu in Svetu*, ECLI:EU:C:2001:523.
Zadeva C-131/12, *Google Spain SL in Google Inc. proti Agencia Española de Protección de Datos (AEPD) in Mariu Costeji Gonzálezu*, ECLI:EU:C:2014:317.
Združene zadeve S. in Marper proti Združenemu kraljestvu, 4. decembra 2008, št. 30562/04 in 30566/04.

Spletni viri

<https://www.imdb.com/title/tt0182576/?ref_=nv_sr_srsg_0> (6.6.2020).
<https://www.imdb.com/title/tt0212671> (6.6.2020).
<https://www.imdb.com/title/tt0369179/?ref_=nv_sr_srsg_3> (6.6.2020).
Alexa has been eavesdropping on you this whole time, Geoffrey Fowler, The Washington Post, <https://www.washingtonpost.com/technology/2019/05/06/alexa-has-been-eavesdropping-you-this-whole-time/> (4.5.2020).
ALGORITHMS AND HUMAN RIGHTS, Study on the human rights dimensions of automated data processing techniques and possible regulatory implications, Svet Evrope 2018, <https://rm.coe.int/algorithms-and-human-rights-en-rev/16807956b5> (2.6.2020).
An Amazon Echo recorded a family's conversation, then sent it to a random person in their contacts, report says, Hamza Shaban, The Washington Post, <https://www.washingtonpost.com/news/the-switch/wp/2018/05/24/an-amazon-echo-recorded-a-familys-conversation-then-sent-it-to-a-random-person-in-their-contacts-report-says/?noredirect=on> (4.5.2020).
Anja Riitta Lahikainen in Ilkka Arminem: Family, media and digitalization of childhood, 2017, <https://helda.helsinki.fi/bitstream/handle/10138/231835/12_Chapter12final2017.pdf?sequence=1> (9.6.2020).
Barreto, D.: Normalizing mass surveillance: Sidewalk Labs' threat to human rights, Now Magazine, 2019, <https://nowtoronto.com/news/sidewalk-labs-privacy-human-rights/> (6.6.2020); Yasmin Aboelsau, Y.: Canadian Civil Liberties Association threatening lawsuit over Google's Sidewalk Labs, Venture Toronto, 2019, <https://dailyhive.com/toronto/canadian-civil-liberties-association-sidewalk-labs-open-letter-2019> (6.6.2020).
Berg, N.: Predicting crime, LAPD-style, The Guardian, 2014, <https://www.theguardian.com/cities/2014/jun/25/predicting-crime-lapd-los-angeles-police-data-analysis-algorithm-minority-report#maincontent> (5.6.2020).
Cadwalladr C., Graham-Harrison, E.: Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach, The Guardian, 2018, <https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election> (1.6.2020).
China's High-Tech Tool to Fight Toilet Paper Bandits, New York Times, <https://www.nytimes.com/2017/03/20/world/asia/china-toilet-paper-theft.html> (3.5.2020).
Dobro jutro, RTV Slovenija, 1.6.2017, <https://4d.rtvslo.si/arhiv/dobro-jutro/174474629> (8.6.2020).
Doward, J. in Hall, S.: Technology cuts children off from adults, warns expert, The Guardian, 2019, <https://www.theguardian.com/society/2019/apr/27/technology-threatens-child-development-psychology-expert-warns> (8.6.2020).

Gaylor, B.: Internet vsega, dokumentarni film, Kanada, 2020, <https://4d.rtvslo.si/arhiv/tuji-dokumentarni-filmi-in-oddaje/174697585> (3.6. 2020).
Lee, S.: Who uses my health data, <https://www.goinvo.com/vision/who-uses-my-health-data/> (19.4.2020).
Leo Kelion: Coronavirus: Covid-19 detecting apps face teething problems, <https://www.bbc.com/news/technology-52215290> (19.4.2020).
Lunden, I.: Kegg tracks your fertility by measuring vaginal mucus with a kegel ball, 2018, <https://techcrunch.com/2018/09/05/kegg-kegel-ball-fertility/> (6.6.2020).
Marshall Allen: You Snooze, You Lose: Insurers Make The Old Adage Literally True, Propublica, 2018, <https://www.propublica.org/article/you-snooze-you-lose-insurers-make-the-old-adage-literally-true> (1.6.2020).
Meuse, M.: Vancouver police now using machine learning to prevent property crime, CBC, 2017, <https://www.cbc.ca/news/canada/british-columbia/vancouver-predictive-policing-1.4217111> (5.6.2020).
Mnenje informacijske pooblaščenke Mojce Prelesnik o Predlogu Zakona o interventnih ukrepih za zajezitev epidemije COVID-19 in omilitev njenih posledic za državljane in gospodarstvo – EVA 2020-1611-0028, z dne 30.3.2020, <https://www.iprs.si/fileadmin/user_upload/Pdf/pripombe/2020/DZ_interventni_zakon_MNENJE_30032020_koncno.pdf> (27.4.2020).
Nadzor, ki ga izvajajo obveščevalne službe: zaščitni ukrepi in pravna sredstva v zvezi s temeljnimi pravicami v Evropski uniji – Del II, Agencija FRA, 2018, <https://fra.europa.eu/sites/default/files/fra_uploads/fra-2017-surveillance-intelligence-services-vol-2-summary_sl.pdf> (4.5.2020).
Nadzor, ki ga izvajajo obveščevalne službe: zaščitni ukrepi in pravna sredstva v zvezi s temeljnimi pravicami v EU – Del I: Pravni okviri držav članic, Agencija FRA, 2015, <https://eur-lex.europa.eu/legal-content/SL/TXT/PDF/?uri=CELLAR:35149923-8c2c-11e5-b8b7-01aa75ed71a1&from=FR> (4.5.2020).
NEC unveils facial recognition system for 2020 Tokyo Olympics, <https://www.theverge.com/2018/8/7/17659746/tokyo-2020-olympic-games-face-recognition-nec> (3.5.2020).
Never forget a face? Research suggests people know an average of 5,000 faces, University of York, <https://www.york.ac.uk/news-and-events/news/2018/research/never-forget-a-face/> (3.5.2020).
Newman Forbes, D.: What Is Privacy In The Age Of Digital Transformation? <https://www.forbes.com/sites/danielnewman/2019/05/02/what-is-privacy-in-the-age-of-digital-transformation/#8050c9c628ed>, (4.5.2020).
Odprto pismo Informacijske pooblaščenke, z dne 24.4.2020, <https://www.ip-rs.si/fileadmin/user_upload/Pdf/Covid19/Odprto_pismo.pdf>, (27.4.2020).
Radio televizija Slovenija, Oddaja Ugriznimo v znanost: Prepoznavanje obrazov, 13.12.2018, <https://4d.rtvslo.si/arhiv/ugriznimo-znanost/174582438> (3.5.2020).
Rory Cellan-Jones: Coronavirus: What went wrong with the UK's contact tracing app?, BBC, 20.6.2020, <https://www.bbc.com/news/technology-53114251?at_custom4=8D4889AE-B307-11EA-A6BA-17F3C28169F1&at_custom3=BBC+News&at_custom2=facebook_page&at_medium=custom7&at_custom1=%5Bpost+type%5D&at_campaign=64> (21.6.2020).
RTV SLO, <https://www.rtvslo.si/znanost-in-tehnologija/tudi-slovenska-policija-uporablja-avtomatsko-prepoznavo-obrazov/510776> (3.5.2020).
Singer, N.: When Apps Get Your Medical Data, Your Privacy May Go With It, The New York Times, <https://www.nytimes.com/2019/09/03/technology/smartphone-medical-records.html> (20.4.2020).
SPECIAL EUROBAROMETER 359 Attitudes on Data Protection and Electronic Identity in the European Union REPORT Fieldwork: November – December 2010, objavljeno junija 2011

<https://joinup.ec.europa.eu/collection/eidentity-and-esignature/document/eu-attitudes-data-protection-and-electronic-identity-european-union> (3.5.2020).

Sodišče prepovedalo testno prepoznavanje obrazov na šolah v Marseillu in Nici, RTV SLO, <https://www.rtvslo.si/znanost-in-tehnologija/sodisce-prepovedalo-testno-prepoznavanje-obrazov-na-solah-v-marseillu-in-nici/516064> (3.5.2020).

Štempihar, A.: Kaj je zares digitalno poslovanje?, IIBA Slovenija, april 2017, <https://slovenia.iiba.org/sites/slovenia/files/IIBA_mesecniki/mesecniki_clanki/Mesecnik_IIBA_april_2017-Clanek_%20Kaj_zares_je_digitalno_poslovanje_AS.pdf> (20.4.2020).

Taylor, J.: Is Technology Creating a Family Divide? <https://www.psychologytoday.com/intl/blog/the-power-prime/201303/is-technology-creating-family-divide> (6.6.2020).

Tehnologija, ki stoji za kriptovalutami, bi lahko reševala življenja, <http://m.racunalniske-novice.com/index.php?id=tehnologija-ki-stoji-za-kriptovalutami-bi-lahko-resevala-zivljenja.html> (19.4.2020).

This Is What Your Phone Does with Your Personal Health Data, Mark Henricks, <https://www.shape.com/fitness/trends/health-apps-privacy-personal-information-shared> (19.4.2020).

Zdravstveni podatki, Informacijski pooblaščenec, <https://www.ip-rs.si/varstvo-osebnih-podatkov/inspekcijski-nadzor/najbolj-pogoste-krsitve/zdravstveni-podatki> (19.4.2020).

DOI
https://doi.org/10.18690/um.pf.4.2023.5

ISBN
978-961-286-774-4

5 ALGORITEMSKA DISKRIMINACIJA

OSKAR PEČE

Univerza v Mariboru, Pravna fakulteta, Maribor, Slovenija
oskar.pece@student.um.si

Ključne besede:
prepoved diskriminacije, avtomatizirano odločanje, umetna inteligenca, zaščita osebnih podatkov, podatkovno rudarjenje

O algoritemski diskriminaciji govorimo, kadar avtomatiziran sistem, ki temelji na umetni inteligenci, posameznika obravnava manj ugodno kakor drugega posameznika na primerljivem položaju. Kljub temu, da avtomatizirani sistemi domnevno odločajo bolj objektivno in nepristransko kakor človek ter omogočajo formalno izključitev obravnave določenih spornih lastnosti, lahko odločajo diskriminatorno. Za namen boja proti algoritemski diskriminacij je možna regulacija lastnosti, ki so upoštevane v postopku odločanja, vendar je ta pogosto neučinkovita in v nasprotju s samim smislom uporabe tovrstnih sistemov. Morda je najbolj učinkovito orodje za boj zoper algoritemsko diskriminacijo pravica, da za posameznika ne velja odločitev, ki temelji zgolj na podlagi avtomatizirane obdelave podatkov. Pri regulaciji avtomatiziranih sistemov za odločanje moramo vselej biti pozorni, da so regulatorni ukrepi tehnično izvedljivi in sorazmerni.

Univerzitetna založba Univerze v Mariboru

DOI
https://doi.org/
10.18690/um.pf.4.2023.4

ISBN
978-961-286-774-4

Keywords:
non-discrimination,
automated decision making,
artificial intelligence,
personal data protection,
data mining

University of Maribor Press

5 The Algorithm of Discrimination

Oskar Peče
University of Maribor, Faculty of Law, Maribor, Slovenia
oskar.pece@student.um.si

Discrimination is prohibited in the European Convention on Human Rights, the Charter of Fundamental Rights of the European Union, multiple directives of the European Union, the Constitution of the Republic of Slovenia and the Protection against discrimination Act. Algorithmic discrimination occurs when an automated system based on artificial intelligence treats an individual less favorably than another individual in a comparable position. Despite the fact that automated systems make decisions more objectively and impartially than humans, and allow for the formal exclusion of the treatment of certain controversial features, they they are still able of making discriminatory decisions. This is often due to human influence in data mining processes. Demonstrating algorithmic discrimination is very difficult due to limited insight into the operation of automated systems and understanding of the decision-making process itself. In proving unfavorable algorithmic discrimination, we move from the paradigm of proving causality to proving a meaningful correlation. For the purpose of combating algorithmic discrimination, it is possible to regulate the properties that are taken into account in the decision-making process, but this is often ineffective and contrary to the very purpose of using such systems.

5.1 Uvod

Umetna inteligenca je tehnologija, ki rapidno razvija in fascinira širšo javnost ne glede na obseg njihovega poznavanja delovanja in implementacije tovrstne tehnologije. Vpliv in uporaba te tehnologije je pogosta tema zabavne industrije in medijskih prispevkov, ki umetno inteligenco ljudem pogosto prikazujejo senzionalistično in prekomerno futuristično. To vsekakor ne pomeni, da tehnologija ni presenetljivo sposobna. Ogromno sistemov umetne inteligence obdeluje osebne podatke z namenom razvoja algoritemskih modelov, na podlagi katerih lahko kasneje ob vnosu osebnih podatkov sklepajo o določenih lastnostih posameznika, na katerega se ti podatki nanašajo. S tem so tovrstni sistemi sposobni avtomatiziranega odločanja, tudi v kompleksnih primerih, ki zadevajo večje število lastnosti in predhodno nedoločenih kriterijev.[1] Sistemi, ki temeljijo na umetni inteligenci so za namen odločanja poleg ekonomskih razlogov privlačni zaradi domnevne natančnosti, objektivnosti in nepristranskosti. V očeh mnogih umetna inteligenca predstavlja možnost objektivnega in zanesljivega odločevalca. Vendar ali je to res? Ali umetna inteligenca resnično predstavlja alternativo človeškemu odločanju, s tem, da v odsotnosti čustev in predsodkov nudi pravične odločitve?

V tem prispevku obravnavam tveganje diskriminacije pri avtomatiziranem odločanju, ki temelji na uporabi umetne inteligence. Za razumevanje problematike prvotno opredelim diskriminacijo in se osredotočim na vzrokediskriminacije pri tovrstnih sistemih. Poleg drugih ukrepov za boj zoper diskriminatorno avtomatizirano odločanje se posebej osredotočim na pravico, da za posameznika ne velja odločitev, ki temelji na avtomatizirani obdelavi podatkov. Namen tega prispevka je določiti, kdaj je odločitev avtomatiziranega sistema diskriminatorna, kaj so dejavniki, ki povzročajo takšno odločanje, kakšni so možni načini prevencije takšnih odločitev in ali jih je mogoče oziroma smiselno s zakonodajno regulacijo preprečiti, ter kdaj avtomatizirane odločitve za posameznika, na katerega se nanašajo, sploh veljajo.

[1] Sartor, G.: The impact of the General Data Protection Regulation (GDPR) on artificial intelligence, European Parlimentary Research Service, Bruselj, 2020, str. 1

5.2 Prepoved diskriminacije

5.2.1 Prepoved diskriminacije v Evropski konvenciji o varstvu človekovih pravic

Za določitev prepovedi diskriminacije je najbolj smiselno začeti na samem vrhu hierarhije veljavnih pravnih aktov, zato določitev prepovedi diskriminacije začenjam z Evropsko konvencijo o varstvu človekovih pravic[2](v nadaljevanju EKČP), ki na podlagi 56. člena EKČP vsekakor velja na območju Evropske unije (v nadaljevanju EU). Prepoved diskriminacije je natančneje določena v 14. členu EKČP, ki določa, da je uživanje pravic in svoboščin določenih s EKČP »zagotovljeno vsem ljudem brez razlikovanja glede na spol, raso, barvo kože, jezik, vero, politično ali drugo prepričanje, narodnostni ali socialni izvor, pripadnost narodni manjšini, lastnino, rojstvo ali kakšne druge okoliščine.« Za razumevanje prepovedi diskriminacije je zelo pomembna praksa Evropskega sodišča za človekove pravice (v nadaljevanju Evropsko sodišče). V zadevi *Thlimmenos*[3] je na primer Evropsko sodišče odločilo, da je ravnanje lahko diskriminatorno, če sta dve osebi obravnavani enako, kljub temu da je njun položaj popolnoma različen.

5.2.2 Prepoved diskriminacije na ravni Evropske unije

Prepoved diskriminacije in načelo enake obravnave sta trdno zasidrani v samih temeljih EU. V 2. členu Pogodbe o Evropski uniji (v nadaljevanju PEU)[4] je določeno, da EU »temelji na vrednotah spoštovanja človekovega dostojanstva, svobode, demokracije, enakosti, pravne države in spoštovanja človekovih pravic, vključno s pravicami pripadnikov manjšin«[5], ter da to skupno družbo držav članic označujejo pluralizem, nediskriminacija, strpnost, pravičnost, solidarnost ter enakost moških in žensk. Tovrsten princip je nadalje poudarjen v 2. odstavku 3. člena PEU, kjer je določeno, da se EU bori proti izključenosti in diskriminaciji.

---

[2] 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 – Mednarodne pogodbe, št. 7/94).

[3] *Thlimmenos v Greece, št. 34369/97, ECLI:CE:ECHR:2000:0406JUD003436997.*

[4] Pogodba o Evropski uniji, Uradni list Evropske unije, C 326, 26.10.2012, str. 13–390.

[5] Ibidem, člen 2.

Pravo EU, ki temelji na nedeljivih in univerzalnih vrednotah človekovega dostojanstva, svobode, enakopravnosti in solidarnosti[6], prepoved diskriminacije kot temeljno pravico prebivalcev EU konkretizira v Listini Evropske unije o temeljnih pravicah (LEUTP)[7]. Prvi člen določa, da je človekovo dostojanstvo nedotakljivo, in da ga je potrebno spoštovati in varovati. Nadalje 20. člen LEUTP določa, da smo pred zakonom vsi enaki. Prepoved diskriminacije je neposredno določena v prvem odstavku 21. člena LETP, ki zapoveduje, da je prepovedana »vsakršna diskriminacija na podlagi spola, rase, barve kože, etničnega ali socialnega porekla, genetskih značilnosti, jezika, vere ali prepričanja, političnega ali drugega mnenja, pripadnosti narodnostni manjšini, premoženja, rojstva, invalidnosti, starosti ali spolne usmerjenosti.«[8] Ta člen ni pomemben zgolj zaradi neposredne prepovedi diskriminacije, temveč zaradi jasne opredelitve lastnosti, na podlagi katerih bazirajo skupine, ki jih je v boju zoper diskriminacijo potrebno zaščititi (v nadaljevanju zaščitene skupine).

Prepoved diskriminacije je natančneje urejena v več direktivah: Direktiva sveta o izvajanju načela enakega obravnavanja oseb ne glede na raso ali narodnost,[9] Direktiva sveta o splošnih okvirih enakega obravnavanja pri zaposlovanju in delu[10], Direktiva Evropskega parlamenta in sveta o uresničevanju načela enakih možnosti ter enakega obravnavanja moških in žensk pri zaposlovanju in poklicnem delu[11]. Direktiva sveta o izvajanju načela enakega obravnavanja moških in žensk pri dostopu do blaga in storitev ter oskrbi z njimi[12]. Vsebina teh direktiv je v Slovenski pravni red prenesena z Zakonom o varstvu pred diskriminacijo (v nadaljevanju ZVarD).

[6] Preambula Listine Evropske Unije o človekovih pravicah, Uradni list Evropske unije, C 83/389, str 391–407.
[7] Ibidem.
[8] Ibidem člen 21, prvi odstavek.
[9] Direktiva Sveta 2000/43/ES z dne 29. junija 2000 o izvajanju načela enakega obravnavanja oseb ne glede na raso ali narodnost, Uradni list Evropske unije, L 180, 19.7.2000, str. 22–26.
[10] Direktiva Sveta 2000/78/ES z dne 27. novembra 2000 o splošnih okvirih enakega obravnavanja pri zaposlovanju in delu, Uradni list Evropske unije, L 303, 2.12.2000, str. 16–22.
[11] Direktiva 2006/54/ES Evropskega parlamenta in Sveta z dne 5. julija 2006 o uresničevanju načela enakih možnosti ter enakega obravnavanja moških in žensk pri zaposlovanju in poklicnem delu (preoblikovano), Uradni list Evropske unije, L 204, 26.7.2006, str. 23–36
[12] Direktiva Sveta 2004/113/ES z dne 13. decembra 2004 o izvajanju načela enakega obravnavanja moških in žensk pri dostopu do blaga in storitev ter oskrbi z njimi, Uradni list Evropske unije, L 373, 21.12.2004, str. 37–43.

5.2.3 Prepoved diskriminacije v slovenski zakonodaji

Ustava Republike Slovenije v 14. člen določa, da »so vsakomur zagotovljene enake človekove pravice in temeljne svoboščine, ne glede na narodnost, raso, spol, jezik, vero, politično ali drugo prepričanje, gmotno stanje, rojstvo, izobrazbo, družbeni položaj, invalidnost ali katerokoli drugo osebno okoliščino.«[13] Drugi odstavek istega člena dodaja da smo pred zakonom enaki vsi. S tem določilom je prepoved diskriminacije zapečatena v URS. V primeru, da je oseba deležna diskriminacije ima v 22. členu URS prav tako kakor kdor koli drug zagotovljeno enako varstvo pravic v postopku pred sodiščem in pred drugimi državnimi organi, organi lokalnih skupnosti in nosilci javnih pooblastil, ki odločajo o njegovih pravicah, dolžnostih ali pravnih interesih. Skladno s obravnavano temo je potrebno dodati, da je v 63. členu URS prepovedano vsakršno spodbujanje k narodni, rasni, verski ali drugi neenakopravnosti. S tem je na ustavni ravni tako kot diskriminacija prepovedano tudi vsakršno spodbujanje k diskriminaciji.

Kot sem omenil prej je vsebina Direktiv EU, ki urejajo prepoved diskriminacije, v slovenski pravni red vpeljana v ZVard. »Ta zakon določa varstvo vsakega posameznika in posameznice (v nadaljnjem besedilu: posameznik) pred diskriminacijo ne glede na spol, narodnost, raso ali etnično poreklo, jezik, vero ali prepričanje, invalidnost, starost, spolno usmerjenost, spolno identiteto in spolni izraz, družbeni položaj, premoženjsko stanje, izobrazbo ali katero koli drugo osebno okoliščino«[14] V 4. členu ZVarD je diskriminacija opredeljena kot »vsako neupravičeno dejansko ali pravno neenako obravnavanje, razlikovanje, izključevanje ali omejevanje ali opustitev ravnanja zaradi osebnih okoliščin, ki ima za cilj ali posledico oviranje, zmanjšanje ali izničevanje enakopravnega priznavanja, uživanja ali uresničevanja človekovih pravic in temeljnih svoboščin, drugih pravic, pravnih interesov in ugodnosti.« V drugem odstavku 4. člena prav tako piše, da je prepovedana diskriminacija zaradi katere koli osebne okoliščine. Enako obravnavanje je v 5. členu opredeljeno kot odsotnost neposredne ali posredne diskriminacije zaradi katere koli osebne okoliščine. Poleg neposredne in posredne diskriminacije ZVarD v 7. členu določa tudi druge oblike diskriminacije, namreč nadlegovanje in spolno nadlegovanje, navodila za diskriminacijo, pozivanje k

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

[14] 1. člen prvi odstavek Zakona o varstvu pred diskriminacijo (Uradni list RS, št. 33/16 in 21/18 – ZNOrg).

diskriminaciji in povračilne ukrepe oziroma viktimizacijo. V 12. členu prav tako določa hujše oblike diskriminacije, za katere štejejo večkratna diskriminacija (oseba diskriminirana zaradi več osebnih okoliščin hkrati), množična diskriminacija (kadar je diskriminiranih več oseb hkrati), dolgotrajna oziroma ponavljajoča se diskriminacija in diskriminacija, ki vsebuje ali bi lahko vsebovala težko popravljive posledice za diskriminirano osebo glede povzročitve škode njenemu pravnemu položaju, pravicam ali obveznostim, zlasti če je storjena v razmerju do otrok ali drugih slabotnih oseb.

5.3 Kdaj je odločitev diskriminatorna?

Pojem tako neposredne kot tudi posredne diskriminacije je podan v drugem odstavku 2. člena Direktive sveta o izvajanju načel enakega obravnavanja oseb ne glede na raso ali narodnost, ki po določilu prvega odstavka tega člena obe predstavljata kršitev načela enakega obravnavanja, v smislu te direktive.

Za neposredno diskriminacijo se šteje, če se ena oseba obravnava manj ugodno, kakor se obravnava, se je obravnavala ali pa bi se obravnavala druga oseba v primerljivem položaju na podlagi rase ali narodnosti. Za posredno diskriminacijo se šteje, če bi na videz nevtralna določba, merilo ali praksa postavila osebe neke rase ali narodnosti v posebno neugoden položaj v primerjavi z drugimi osebami, razen če to določbo, merilo ali prakso objektivno upravičuje zakonit cilj in če so sredstva za doseganje tega cilja ustrezna in *potrebna.*[15] Ne samo da je poleg neposredne diskriminacije prepovedana tudi posredna diskriminacija, ki je sicer pri algoritemski diskriminaciji bolj pogosta, za diskriminacijo ni potreben namen storilca. Zelo pomembno je poudariti, da prej omenjen člen določa, da ne gre za posredno diskriminacijo, če določbo, merilo ali prakso objektivno upravičuje zakonit cilj in če so sredstva za doseganje tega cilja ustrezna in potrebna. Kot je določeno v 3. členu, se ta direktiva uporablja v okviru pristojnosti, dodeljenih Skupnosti, za vse osebe v javnem in zasebnem sektorju.

Za določitev tako neposredne kakor posredne diskriminacije je potreben *primerjalnik,* posameznik ali skupina, katere situacija je podobna domnevni žrtvi diskriminacije, katere obravnavo lahko primerjamo z obravnavo domnevne žrtve diskriminacije, za ugotovitev oziroma utemeljitev diskriminacije. Na podlagi takšne

[15] Direktiva 2000/43/ES člen 2, odstavek 2a

primerjave je Evropsko sodišče presojalo v zadevi *Moustaquim v Belgium*[16], kjer je ugotovilo, da položaj Maročana, ki bi naj bil deportiran iz Belgije, ni primerljiv s položajem Belgijca, saj le ta na podlagi 3. člena Protokola št. 4 k EKČP, ki določa, da nihče ne sme biti izgnan iz ozemlja države, katere državljan je, ne sme biti izgnan. Priznalo pa je, da je položaj Maročana primerljiv s položajem državljanov EU. V zadevi *Test Achast*[17] je Sodišče Evropske Unije (v nadaljevanju Sodišče) poudarilo, da v skladu z ustaljeno sodno prakso Sodišča načelo enakega obravnavanja terja, da se primerljivi položaji ne obravnavajo različno in da se različni položaji ne obravnavajo enako, razen če je tako obravnavanje objektivno upravičeno in da je primerljivost položajev potrebno presojati glede na cilj in namen akta Unije, s katerim je uvedeno zadevno razlikovanje.

ZVarD neposredno in posredno diskriminacijo opredeljuje v 6. členu. Določa namreč, da neposredna diskriminacija obstaja, »če je oseba ali skupina oseb zaradi določene osebne okoliščine bila, je ali bi lahko bila v enakih ali podobnih situacijah obravnavana manj ugodno, kot se obravnava, se je obravnavala ali bi se obravnavala druga oseba ali skupina oseb.«[18] Za posredno diskriminacijo je določeno, da obstaja, »kadar je oseba ali skupina oseb z določeno osebno okoliščino bila, je ali bi lahko bila zaradi navidezno nevtralne določbe, merila ali prakse v manj ugodnem položaju kot druge osebe, razen če ta določba, merilo ali praksa objektivno temelji na legitimnem cilju in so sredstva za doseganje tega cilja ustrezna in *nujno potrebna*.« Tukaj vidimo, da ZVarD postavlja višji prag za presojo odsotnosti posredne diskriminacije, saj namesto da so *potrebna* (kot je določeno v prej omenjeni direktivi EU) za sredstva za doseganje legitimnega cilja (zaradi katerega je oseb s določenimi lastnostmi v manj ugodnem položaju) določa, da morajo biti *nujno potrebna.*

Na podlagi pojma posredne diskriminacije in v nadaljevanju opisanih načinov, kako do diskriminacije pri algoritemskem odločanju lahko pride, se na prvi pogled zdi, da je vsaka odločitev, ki temelji na statističnem modelu diskriminatorna, saj je za skoraj vsako upoštevano lastnost mogoče trditi, da je zaradi tovrstnega merila neka oseba, na podlagi določene osebne okoliščine v manj ugodnem položaju. To je vsekakor res, saj se v vsakem izboru oziroma odločanju, ki vpliva na posameznike, upoštevajo lastnosti teh posameznikov (in njim podobnih posameznikov), zaradi česar je skoraj neizbežna manj ugodna obravnava nekaterih, na podlagi določenih osebnih

[16] *Moustaquim v Belgium, št. 12313/86, ECLI:CE:ECHR:1991:0218JUD001231386.*
[17] Zadeva C-236/09, *Test-Achats,* ECLI:EU:C:2011:100
[18] ZVarD 6. člen 1. odstavek.

okoliščin. To ni zgolj problem avtomatiziranega odločanja, temveč tudi človeškega. Vselej kadar so postavljeni določeni kriteriji, nekateri posamezniki teh ne izpolnjujejo oziroma jih izpolnjujejo v manjši meri. Sam namen kriterijev namreč je tovrstna selekcija. Za resnično razumevanje, kdaj je odločanje na podlagi avtomatiziranega sistema, ozirom kdaj so merila, na podlagi katerih ta sistem presoja posredno diskriminatorna, se moremo osredotočiti na drugi del definicije posredne diskriminacije[19], ki izključuje obstoj posredne diskriminacije v primeru, kadar domnevno sporno določbo, merilo ali prakso objektivno upravičuje zakonit cilj in kadar so sredstva za doseganje tega cilja ustrezna in potrebna.

Koncept posredne diskriminacije in zakonitega cilja je Sodišče obravnavalo v zadevi *Achbita*[20], kjer je presojalo ali je delodajalčeva nevtralna prepoved nošenja simbolov političnih, filozofskih ali verskih prepričanj na delovnem mestu diskriminatorna zoper zaposleno, ki je muslimanka in iz verskih razlogov nosi naglavno ruto. Sodišče je v tem primeru izključilo neposredno diskriminacijo, vendar kljub nevtralnemu pravilu, ki sicer zadeva vse vere in druga prepričanja, ni izključilo posredne diskriminacije, saj je tovrstna omejitev lahko za nekatere zaposlene bolj intruzivna kakor za druge (nekateri verski simboli se nosijo zgolj z namenom izkazovanja pripadnosti določeni veri, med tem ko ima nošenje nekaterih simbolov močno versko in moralno vrednost) s čimer lahko takšna omejitev nekatere zaposlene obravnava manj ugodno. S tem so utemeljili pogoj za obstoj posredne diskriminacije. Naslednje vprašanje je bilo, ali je delodajalec s tem pravilom zasledoval zakonit cilj. Delodajalec je to pravilo postavil z namen ohranitve nevtralnega izgleda podjetja, ob stiku zaposlenih s strankami. Sodišče je priznalo, da je tovrsten zasledovan cilj na prvi pogled zakonit, saj izhaja iz pravice do svobodne gospodarske pobude, določene v 16. členu LEUTP. Izpostavilo je pogoj, da je sredstvo za doseganje tega cilja ustrezno in potrebno. Glede ustreznosti je Sodišče odločilo, da bi jo bilo potrebno presojati glede na to, ali je pravilo bilo implementirano generalno in enako za vse, ter poudarilo, da je tovrstno pravilo nediskriminatorno kadar velja zgolj za delavce, ki dejansko so v stiku s stranki. Le tedaj je takšno pravilo potrebno (prepoved nošenja verskih simbolov pri zasledovanju cilja nevtralne podobe ni potrebna pri zaposlenih, ki pri delu niso v stiku s strankami).

[19] 2000/43/ES člen 2, odstavek 2a
[20] C-157/15, *Achbita,* ECLI:EU:C:2017:203

Problem predpisa, ki prepoveduje posredno diskriminacijo je, da posredna diskriminacija pogosto ni jasna. Potrebno je dokazati, da sicer nevtralno pravilo neproporcionalno prizadene določeno zaščiteno skupino. Po navadi se za dokazovanje neproporcionalnega učinka uporablja statistika.[21] Prvi odstavek 8. člena Direktive sveta o izvajanju načel enakega obravnavanja oseb ne glede na raso ali narodnost določa, da morajo države skladno s svojim pravnim sistemom sprejeti ukrepe, s katerim zagotovijo, da mora sicer toženec dokazati, da ni bilo kršeno načelo enakega obravnavanja, vendar pod pogojem, da tožeča stranka predstavi dejstva, na podlagi katerih se lahko domneva, da je do tovrstne kršitve prišlo. V skladu s tem tudi ZVarD določa obrnjeno dokazno breme. Od diskriminirane osebe se zahteva zgolj, da izkaže dejstva, na podlagi katerih se lahko domneva, da je bila kršena prepoved diskriminacije. V tem primeru mora domnevni kršitelj dokazati, da ni kršil očitane prepovedi diskriminacije.

5.4 Kaj je algoritemska diskriminacija?

Pojem algoritem je pogosto uporabljen v kontekstu umetne inteligence, kot »algoritemsko odločanje« ali v našem primeru »algoritemska diskriminacija«. Koncept algoritma je sicer širši od umetne inteligence in sicer vključuje vsako zaporedje nedvoumno opredeljenih navodil za izvajanje nalog, zlasti, vendar ne izključno z matematičnimi izračuni. Med tem ko vsak algoritem ne vključuje umetne inteligence, vsak sistem umetne inteligence vključuje več algoritmov. [22]

Algoritemsko diskriminacijo lahko, za namen tega prispevka, definiramo kot pojav, ki nastane, kadar avtomatiziran program za odločanje, ki temelji na umetni inteligenci, posameznika obravnava manj ugodno kakor drugega na primerljivem položaju, in je tovrstna negativna obravnava pogojena z ali v močni korelaciji z določeno njegovo osebno lastnostjo. Kadar je negativna obravnava neposredno pogojena oziroma povezana s osebno lastnostjo (se neposredno upošteva in negativno vrednoti) obravnavanega posameznika, gre za neposredno diskriminacijo. Kadar se pri odločanju upoštevajo lastnosti, ki so v močni korelaciji s posameznikovo osebno lastnostjo, ter to vodi do negativne obravnave posameznikov s to lastnostjo, tovrstno odločanje lahko predstavlja posredno

[21] Borgesius, F. Z.: Discrimination, artificial intelligence, and algorithmic decision-making, Directorate General of Democracy, Council of Europe, Strasbourg, 2018, str. 19

[22] Sartor, G.: The impact of the General Data Protection Regulation (GDPR) on artificial intelligence, European Parlimentary Research Service, Bruselj, 2020 ,str. 17

diskriminacijo, če se te lastnosti ne presojajo z namenom zasledovanja zakonitega cilja in če niso nujne.

Urejanje virov nenamerne diskriminacije pri algoritemskem odločanju in odprava povezanih pomanjkljivosti v pravu bo tehnično, pravno in politično težavna. Diskriminacija je lahko produkt podatkovnega rudarjenja in ne tega, da programerji določenim pogojem določajo diskriminatorne vrednosti. Podatkovno rudarjenje je postopek odkrivanja zanimivih vzorcev in znanja na podlagi velikih količin podatkov[23] Ta nevarnost je pogosto spregledana s strani akademikov in zakonodajne oblasti, ki se pogosto bolj bojijo diskriminatornega programiranja tovrstnih sistemov. Podatkovno rudarjenje lahko predstavlja večjo grožnjo, saj kadar se diskriminacija pojavi zaradi podatkov, ki so posledica predhodne namerne diskriminacije, pogosto ni primerne metode za popravek historičnih predsodkov znotraj teh podatkov. Tudi kadar so podatkovni rudarji skrbni, lahko pride do diskriminatornih rezultatov z uporabo modelov, ki uporabljajo posredne podatke, ki odražajo zaščitene skupine. V nekaterih primerih bo pri podatkovnem rudarjenju nemogoče odpravljati napake brez vprašanja, kakšna stopnja neenakosti je sprejemljiva v določenem kontekstu tovrstnih sistemov. Podatkovno rudarjenje je vselej vrsta statistične in tako na prvi pogled racionalne diskriminacije. Smisel tega procesa je ustvariti racionalno podlago na kateri lahko posameznike ločimo in jih klasificiramo v skupine na podlagi določenih lastnosti. Vendar s tem ta proces omogoča nepravično obravnavo z zakonom zaščitenih skupin. Z razliko od klasičnih podatkovnih metod, kjer analiza preprosto vrednoti določene podatke ali ustvari statistiko, podatkovno rudarjenje skuša najti statistične povezave znotraj baze podatkov. Gre za avtomatiziran proces odkrivanja uporabnih vzorcev, na podlagi katerih se kasneje lahko tvorijo odločitve. Skupek odkritih povezav se imenuje model. S tem ko algoritem strojnega učenja izpostavimo primerom zanimanja, algoritem odkrije lastnosti teh primerov, na podlagi katerih lahko kasneje prepoznava in oceni podobne ali enake primere.[24]

Uporaba avtomatiziranih sistemov za odločanje ni privlačna zgolj zaradi tega, ker so napovedi in odločitve teh sistemov cenejše, temveč zato, ker so bolj precizne in nepristranske kakor človeške, saj ti sistemi niso podrejeni tipičnim človeškim psihološkim »napakam« in so lahko podvrženi rigoroznemu nadzoru. Kljub naravi

[23] Han, J. Pei, J. Kamber, M.: Data Mining: Concepts and Techniques, 2. izdaja, Morgan Kaufman Publishers, San Francisco, 2006, str. 6
[24]Barocas, S., Selbst, A., D.: Big Data's Disparate Impact, v: California Law Review, 104 (2016) 617, str. 672-678

teh sistemov, so njihove odločitve lahko napačne in diskriminatorne. V tem primeru lahko gre za reproduciranje človeške pristranskosti ali ustvarjanje novi pristranskosti. [25]

Vselej je potrebno upoštevati, da sistemi umetne inteligence sami po sebi ne nastanejo in sami po sebi nimajo negativnega vpliva na človekove pravice temveč ima takšen vpliv njihova implementacija in uporaba za človeško interakcijo. Za vsako odločitvijo avtonomnega sistema stoji fizična ali pravna oseba, ki ta sistem uporablja za določen namen.[26]Uporaba algoritmov za namen odločanja nadomesti samovoljno človeško odločanje s strogimi pravili, konstruiranimi iz podatkov. Prav tako je za razliko od človeškega odločanja, ekskluzija določenih podatkov (posameznikova rasa, spol, itd.) v primeru algoritemskega odločanja lahko zagotovljena.[27]

5.5 Vzroki algoritemske diskriminacije

Preden lahko govorimo o preprečevanju algoritemske diskriminacije moremo razumeti kako do tovrstne diskriminacije pride. Algoritemska diskriminacija je lahko posledica človekovega vpliva na postopek podatkovnega rudarjenja na pet različnih načinov.

5.5.1 Določanje ciljne spremenljivke in razredov

Med tem ko pri podatkovnem rudarjenju ciljna spremenljivka določa tisto, kar želimo ugotoviti oziroma nas zanima (ali je kandidat za delovno mesto dober ali slab), razredi razdelijo vse možne vrednosti ciljne spremenljivke v ekskluzivne kategorije (izobrazba, izkušnje,…). Pri podatkovnem rudarjenju skušamo problem rešiti tako, da postavimo vprašanje, katerega odgovor predstavlja ciljna spremenljivka. Pomembno je, da vprašanje opredelimo tako, da ustreza izmerljivim vrednostim. Ker je postopek določitve tega vprašanja subjektivne narave, se lahko zgodi, da tisti, ki to določajo nenamerno postavijo vprašanje, ki slabše obravnava člane zaščitenih skupin. Ciljna spremenljivka in razredi določajo, kaj bo postopek

[25] Sartor, G.: The impact of the General Data Protection Regulation (GDPR) on artificial intelligence, European Parlimentary Research Service, Bruselj, 2020 ,str. 5
[26] Borgesius, F. Z.: Discrimination, artificial intelligence, and algorithmic decision-making, Directorate General of Democracy, Council of Europe, Strasbourg, 2018, str.9
[27] Gillis, T. B., Spiess, J.: Big Data and Discrimination, v: University of Chicago Law Review, 86 (2019) 459, str. 460-463.

podatkovnega rudarjenja odkril. Med tem ko se mnogi kritiki podatkovnega rudarjenja osredotočajo na problem nepravilne klasifikacije (lažna pozitivna ali negativna določitev), vsaj takšno ali celo večjo nevarnost diskriminacije predstavlja slaba in diskriminatorna določitev razredov in s tem vrednotenje učnih primerov oziroma njihovih lastnosti, na podlagi katerih se tvorijo pravila.[28] Nekateri sicer na prvi pogled popolnoma objektivni razredi lahko odsevajo zgodovinski ali trenuten slabši položaj nekaterih skupin in s tem negativno vplivajo na odločanje glede posameznikov teh skupin.[29]

Problem določanja primernih ciljnih spremenljivk je, da vsak argument za superiornost določene ciljne spremenljivke v primerjavi drugimi izzove spor glede kontradiktornih in ne združljivih vrednot.

5.5.2 Učni primeri za strojno učenje

Sistem podatkovnega rudarjenja se uči na podlagi učnih primerov, natančneje tistih, katerim je bil izpostavljen. Učne primere tvorijo podatki, ki jih sistem podatkovnega rudarjenja analizira in se na njihovi podlagi uči. Do diskriminatornega rezultata lahko pride, ko se sistem uči iz pristranskih učnih primerov. Do tega lahko pride na dva načina. Prvi je, ko se sistem uči na podlagi primerov, ki so plod diskriminacije ali predsodkov. To je problematično, saj sistem podatke, iz katerih se uči tretira kot resnične oziroma pravilne, zaradi česar bo pravilo, ki bo nastalo na podlagi tovrstnih primerov zrcalilo diskriminacijo iz teh primerov. Drugi način oziroma vzrok je nereprezentativnost podatkov iz katerih se sistem uči. Če podatki, ki tvorijo učne primere predstavljajo le del populacije oziroma ta del predstavljajo prekomerno, je rezultat lahko diskriminatoren zoper del populacije, ki je v teh podatkih pomanjkljivo ali prekomerno predstavljen. [30]

Problematičen je lahko tudi proces označevanja primerov, pri katerem se učnim primerom manualno dodelijo razredi. Tudi ta proces je subjektiven in lahko na rezultat oziroma pravilo vpliva v zadostni meri, da bodo posledično odločitve na podlagi tega pravila nadaljnje primere karakterizirale na podoben način. To je pomembno, saj kadar odločitve, ki so posledica predsodkov služijo kot primer

[28] Barocas, S., Selbst, A., D.: Big Data's Disparate Impact, v: California Law Review, 104 (2016) 617, str. 678-680
[29] Gillis, T. B., Spiess, J.: Big Data and Discrimination, v: University of Chicago Law Review, 86 (2019) 459, str. 471
[30] Barocas, S., Selbst, A., D.: Big Data's Disparate Impact, v: California Law Review, 104 (2016) 617, str. 680-681.

pravilnih odločitev, sistem podatkovnega rudarjenja ustvarja pravila, ki odsevajo te predsodke in so diskriminatorna. [31]

Pri podatkovnem rudarjenju ne gre zgolj za nevarnost podedovanja predhodne diskriminatorne pristranskosti, temveč lahko odseva trenutno obstoječe predsodke in diskriminatorno stanje v družbi. Ker se postopek podatkovnega rudarjenja zanaša na učne primere kot resnično podlago, bo v primeru, da so ti primeri zastrupljeni s predsodki ali odsevajo diskriminatorno stanje, rezultat nezanesljiv ali celo diskriminatoren.[32] Pri tem se lahko pojavi konstantno dopolnjevanje zaradi česar je rezultat nezanesljiv ali celo diskriminatoren.

5.5.3 Zbiranje podatkov

Veliko pozornosti je potrebno posvetiti samemu zbiranju podatkov, ki služijo kot učni primeri. Učenje na podlagi napačnih, delnih ali nereprezentativnih podatkov lahko vodi do odločitev, ki imajo diskriminatoren učinek zoper zaščitene skupine. Določena baza podatkov lahko zajema neproporcionalno manjše število podatkov o posameznikih iz določene zaščitene skupine ali pa so podatki, ki jih zajema o članih te skupine nižje kvalitete. Nekateri so v teh bazah podatkov nenamerno pozabljeni, saj zaradi revščine, lokacije ali načina življenja o njih obstaja manjša količina podatkov, zaradi česar so nekatere skupnosti in državljani masovno spregledani.[33] Tukaj vidimo problem, namreč tovrstne odločitve ne zadevajo vedno zgolj posameznikov, katerih podatki so se zbirali oziroma, ki so prispevali podatke, temveč tudi tistih, katerih podatki se niso zbrali.

Podatkovno rudarjenje je še posebej občutljivo iz vidika statistične pristranskosti, saj vzorce oziroma pravila, ki jih tovrsten sistem odkriva uporabniki tretirajo kot generalna odkritja kljub temu, da analizirani podatki vključujejo zgolj delni vzorec relevantne populacije, zajet v določenem omejenem časovnem obdobju. Reprezentativnost teh podatkov se pogosto preprosto domneva, vendar je ta domneva pogosto napačna. Efektivnost podatkovnega rudarjenja je pogojena z kvaliteto podatkov, ki služijo kot učni primeri. Če baza podatkov ne zajema kvalitetnega in korektnega vzorca podatkov, ki zadevajo določeno skupino, je rezultat lahko diskriminatoren zoper to skupino. Prav tako je lahko škodljiva

[31] Ibidem, str. 681-682.
[32] Ibidem, str. 682-683.
[33] Ibidem, str. 684-685.

prekomerna reprezentacija določene skupine v bazi učnih primerov, saj lahko vodi do neproporcionalno visoke količine negativnih odločitev za člane te skupine.[34] Povedano drugače, kadar določeno skupino ljudi opazujemo bolj pogosto oziroma dalj časa, pri njej zabeležimo večje število opazovanih lastnosti.

Kadar gre za pomanjkanje podatkov o določeni skupini ljudi lahko podatkovni rudarji proaktivno pomanjkanje podatkov nadomestijo z pretiranim vzorčenjem te skupine in s tem nekoliko zmanjšajo pristranskost rezultata. Podobno je mogoče sicer storiti tudi retroaktivno, kadar zaznamo, da je rezultat diskriminatoren zaradi nereprezentativnosti. Ker sta proaktivno pretirano vzorčenje in retroaktivno popravljanje baze podatkov mogoči, nudi kljub mnogim pomanjkljivostim tovrsten pristopom pozitivne manipulacije učnih primerov najbolj perspektivni in efektivni način odpravljanja negativnih rezultatov, ki nastanejo v vseh mehanizmih podatkovnega rudarjenja, ki sem jih predstavil. [35] V primerih pretirane ali borne reprezentativnosti podatkov o določeni skupini je izključitev (zaščitene) lastnosti, ki definira to skupino, za namen odločanja, lahko škodljiva, saj v tem primeru druge lastnosti ocenjujemo skupno za predstavnike zaščitene skupine in druge, kljub temu, da so modeli ustvarjeni na gmoti podatkov, ki so za zaščiteno skupino nereprezentativni. S tem ko algoritem upošteva lastnost, ki določa zaščiteno skupino, lahko prilagodi težo lastnosti, ocena katerih temelji na analizi nereprezentativih podatkov.[36]

5.5.4 Določitev analiziranih lastnosti

Za proces podatkovnega rudarjenja je potrebno izbrati, katere lastnosti mora sistem opazovati, saj na njih temelji odločitev. Ta del postopka je zelo pomemben, saj je subjektivne narave in izbor lastnosti, ki ugaja določenim skupinam ali zgolj večini, lahko vodi do diskriminacije zaščitenih skupin. Problem je zasidran v dejstvu, da so obravnavani podatki reducirana predstavitev resničnega življenja in zato pogosto pomanjkljivi za ugotovitev kritičnih lastnosti. Nemogoče je zajeti in v modele vključiti vse lastnosti posameznika in vse okoljske vidike. Odločitve, ki temeljijo na statističnih vendar neuniverzalnih generalizacijah so racionalne, vendar hkrati pogosto nepoštene. [37] Možna je formalna izločitev prepovedanih lastnosti, na primer

[34] Ibidem, str. 686-887
[35] Ibidem, str. 718-719
[36] Gillis, T. B.: False Dreams of Algorithmic Fairness: The Case of Credit Pricing, str. 50
[37] Barocas, S., Selbst, A., D.: Big Data's Disparate Impact, v: California Law Review, 104 (2016) 617, str. 688

rase ali spola, s čimer bi izključili vplive teh lastnosti, ki niso povezani z drugimi lastnostmi.[38] Tovrstna prepoved uporabe določenih lastnosti pri odločanju je še posebej privlačna, saj jih je pri avtomatiziranih sistemih mogoče formalno izključiti, med tem ko to ni mogoče pri človeškem odločanju, pri katerem je določena lastnost, kljub prepovedi, dejasnko lahko upoštevana. Gre za stalno problematiko protidiskriminacijske zakonodaje. Pri človeškem odločanju je namreč težavno dokazati, da se določena lastnost ni upoštevala.

Problem je tudi to, da sistem umetne inteligence lahko razvije nove diskriminatorne skupine z določenimi lastnostmi , ki sicer ne spadajo pod neposredno zaščitene skupine, vendar vseeno nepravično razlikujejo ljudi in povzročajo socialno neenakost.[39] Opozoriti moremo, da ima izključitev za odločanje občutljivih lastnosti (na podlagi katerih temeljijo zaščitene skupine) omejen učinek v smislu preprečevanja diskriminacije, in zadostuje zgolj omejenemu vidiku protidiskriminacijskega prava, saj so drugi podatki lahko v močni korelaciji s tovrstnimi občutljivimi lastnostmi[40](več v nadaljevanju o posrednih podatkih). Izključitev občutljivih lastnosti morda ni popolnoma zaželjena, saj vključitev tovrstnih lastnosti lahko omogoči algoritmu, da popravi diskriminatoren vpliv drugih podatkov, ki na zaščiteno skupino vplivajo pristransko.[41] Omejitev analiziranih lastnosti je prav tako problematična, saj znižuje natančnost napovedi.[42]

Poseben pojav oziroma vrsto diskriminacije, ki jo moramo tukaj izpostaviti je tako imenovan »redlining«. Redlining označuje zavrnitev storitev osebi, ki živi na določenem območju (ali na podlagi druge
navidezno nediskriminatorne lastnosti), kljub temu, da posameznik izpolnjuje pogoje za tovrstno storitev (neodobritev kredita sicer kreditno sposobni osebi, ker živi v ekonomsko šibkejši soseski). Izraz se navezuje na domnevno prakso hipotekarnih posojilodajalcev, po kateri naj bi na zemljevidih z rdečimi črtami označevali soseske, katerih prebivalcem ne želijo odobriti kreditov. [43]Posebni primeri redlininga so primeri racionalnega rasizma. Gre za primere, kjer se za podatkovno rudarjenje rasa kot analizirana lastnost eksplicitno upošteva, vendar ne

[38] Gillis, T. B., Spiess, J.: Big Data and Discrimination, v: University of Chicago Law Review, 86 (2019) 459, str. 468
[39] Borgesius, F. Z.:Discrimination, artificial intelligence, and algorithmic decision-making, Directorate General of Democracy, Council of Europe, Strasbourg, 2018, str., 5
[40] Gillis, T. B., Spiess, J.: Big Data and Discrimination, v: University of Chicago Law Review, 86 (2019) 459, str. 464
[41] Ibidem, str. 471-472
[42] Gillis, T. B.: False Dreams of Algorithmic Fairness: The Case of Credit Pricing, str. 43
[43] Federal Fair Lending Regulations and Statutes Fair Housing Act, str 1

zlonamerno. V teh primer je razlog za vključitev rase kot analizirane lastnosti v tem, da se v tej lastnosti nahaja določena statistično generalizirana lastnost, do katere uporabniki sistema na ravni posameznika nimajo dostopa ali je ta težaven (zdravstvena kartoteka, statistično je določena skupina bolj izpostavljena določenim zdravstvenim stanjem). Gre za uporabo hitro dosegljivih generaliziranih podatkov, saj je dostop do specifičnih podatkov otežen ali onemogočen. [44] Ekonomisti tovrstno uporabo imenujejo tudi statistična diskriminacija. Pri takšni uporabi zaščitena lastnosti sama po sebi ni stvar interesa, temveč algoritem presoja na podlagi lastnosti, ki so v visoki statistični korelaciji s to lastnostjo.[45]

5.5.5 Posredni podatki ali »proxy«

Pri posrednih podatkih govorimo o tistih podatkih, ki so sami po sebi nevtralni, vendar lahko delijo ljudi v razrede. Določena lastnost, ki se opazuje je lahko manj ali bolj pogosta v določenih zaščitenih skupinah. Gre za problem, ki mu raziskovalci rečejo odvečni zapis. Govorimo o primerih, ko je posameznikova pripadnost določeni skupini prepoznavna iz nekega drugega podatka. Do tega pride kadar je določen podatek oziroma lastnost v močni korelaciji z določeno skupno. [46] Informacija glede posameznikove zaščitene lastnosti je vtisnjena v njegovih drugih podatkih, zaradi česar je algoritmu lahko znana (oziroma jo ta predvideva), tudi kadar je formalno izključena.[47]

Efektivni način preprečevanja diskriminacije zaradi posrednih podatkov je zmanjšanje natančnost njihovih determinacij.[48] Podatki, ki so povezani z zaščitenimi lastnostmi, lahko služijo kot relevantne informacije za odločanje in hkrati kot posredni podatki, za zaščiteno in formalno izključeno lastnost. Sposobnost algoritma, da odkrije zaščiteno lastnost na podlagi drugih podatkov je manj problematična, kadar upoštevanje zaščitene lastnosti služi zgolj za obravnavo drugih lastnosti (prej omenjena statistična diskriminacija). Kadar zaščitena lastnost ni stvar presoje sama po sebi oziroma ni stvar interesa, bo algoritem neposredno iskal posredne podatke za določitev podatkov, za določitev katerih se sicer uporablja korelacija z zaščiteno lastnostjo, ter s tem ignoriral odkrito zaščiteno lastnost. Zaradi

[44] Barocas, S., Selbst, A., D.: Big Data's Disparate Impact, v: California Law Review, 104 (2016) 617, str. 690
[45] Gillis, T. B.: False Dreams of Algorithmic Fairness: The Case of Credit Pricing, str. 46
[46] Barocas, S., Selbst, A., D.: Big Data's Disparate Impact, v: California Law Review, 104 (2016) 617, str. 691-692
[47] Gillis, T. B.: False Dreams of Algorithmic Fairness: The Case of Credit Pricing, str. 42.
[48] Borgesius, F. Z.:Discrimination, artificial intelligence, and algorithmic decision-making, Directorate General of Democracy, Council of Europe, Strasbourg, 2018, str. 13.

tega bo z razvojem tovrstnega sistema postala uporaba zaščitenih lastnosti nepotrebna.[49]

Še ena perspektivna metoda preprečevanja algoritemske diskriminacije zaradi posrednih podatkov je ortogonalizacija vhodnih podatkov. Gre za statistično metodo, ki v tem kontekstu pomeni, da vstopni podatki, ki so v močni korelaciji z zaščitenimi lastnostmi, ne služijo kot posredni podatki za te zaščitene lastnosti. Takšna metoda je še posebej efektivna, kadar je nek podatek v korelaciji tako s zaščiteno lastnostjo, kakor tudi s neko drugo lastnostjo, ki je objektivno pomembna za natančno napoved. Pri takšnem statističnem pristopu ločimo fazo učenja in fazo odločanja. Pri fazi učenja zaščiteno lastnost (npr. raso) upoštevamo kot opazovano lastnost. Na podlagi rezultata te faze ocenimo težo, ki jo ta lastnost ima pri odločanju. Pri postopku odločanja pa te zaščitene lastnosti ne upoštevamo, oziroma se algoritem te lastnosti ne zaveda. Na ta način, kljub temu, da se je algoritem učil s upoštevanjem zaščitene lastnosti, pri odločanju te lastnosti ne upošteva. S tem je zmanjšan negativen učinek uporabe posrednih podatkov, saj ta metoda izloči neposreden vpliv zaščitene lastnosti na odločitev. Na žalost je uporaba te metode v kontekstu strojnega učenja težavna, saj temelji na tem, da algoritmu lažemo oziroma ga zavajamo. Pri tej metodi namreč od algoritma zahtevamo, da optimizira napoved ob upoštevanju določene lastnosti, kasneje pri fazi odločanja pa ga prikrajšamo podatkov glede te lastnosti. To ni problem v fazi, ko zgolj ugotavljamo učinek te lastnosti na odločitev, vendar je problematično kasneje v fazi odločanja, saj je napoved algoritma optimizirana za uporabo te lastnosti.[50]

5.5.6 Zakrivanje namerne diskriminacije

Velik problem podatkovnega rudarjenja je, da se z uporabo katerega koli od prej naštetih mehanizmov lahko zakrije namerna diskriminacija. Vsaka od prej omenjenih oblik diskriminacije je namreč lahko namerno izvedena. Možna je na primer uporaba redlininga brez kakršnih koli ekonomskih razlogov, namreč iz popolnoma diskriminatornih razlogov. Ob uporabi s strani nekoga, ki želi odločati dikriminatorno, je podatkovno rudarjenje nevarno orodje, saj lahko odkrije, da je posameznik član določene skupine, kljub temu, da ta lastnost nikjer ni navedena. To je mogoče z analizo podatkov, ki imajo močno korelacijo z določeno skupino,

[49] Gillis, T. B.: False Dreams of Algorithmic Fairness: The Case of Credit Pricing, str. 46.
[50] Ibidem, str. 63-68.

oziroma posrednimi podatki. Analiza teh podatkov omogoča namerno diskriminacijo, tudi kadar upravljalci sistema nimajo dostopa do občutljivih informacij. Prav tako prikrije dejstvo, da so odločevalci odločali na podlagi občutljivih lastnosti. [51]

5.6 Obstoječi in možni zaščitni ukrepi za boj zoper algoritemsko diskriminacijo

Sistemi umetne inteligence vsekakor lahko delujejo diskriminatorno, vendar to ne pomeni, da iz tega vidika odločajo slabše kot ljudje. V algoritemskem odločanju pogosto vidimo možnost odločanja, ki formalno ne bazira na zaščitenih lastnostih, vendar ima tovrstno odločanje pomembne omejitve.[52] Sistem umetne inteligence pogosto diskriminira zato, ker je bil učen na podlagi podatkov, ki odsevajo človeško diskriminacijo. Potrebno je postaviti vprašanje, ali je naš cilj, da tovrsten sistem odloča kot človek ali popolnoma nediskriminatorno. [53]Menim, da je načeloma boljše strmeti k popolnoma nediskriminatornemu sistemu, še posebej kadar je sam cilj uporabe tovrstnega sistem najti odgovor, ki je na podlagi izmerljivih kvalitet, iz vidika opazovanih lastnosti objektiven in natančen. Vendar zaradi človeške vloge pri ustvarjanju teh sistemov, oziroma kot sem pojasnil prej, neizbežnega dejstva, da so primeri iz katerih se sistem uči pogosto zastrupljeni s človeško subjektivnostjo, ki pogosto temelji na diskriminatornih predsodkih in pristranskosti, je obstoj popolnoma nedisrkiminatornega sistema vprašljiv. Kljub temu, da stremimo k sistemom, ki ne diskriminirajo, moremo predvideti tovrstno diskriminacijo, podobno kot pri ljudeh, ter v ta namen implementirati določene preventivne regulacije, sisteme varnostnih mrež in možnosti restitucije.

Najbolj pogosti in efektivni orodji za preprečevanje diskriminacije s strani umetne inteligence sta protidiskriminacijska zakonodaja in zakonodaja za zaščito podatkov. Protidsikriminacijske določbe so pomanjkljive v smislu, da določajo omejeno količino zaščitenih skupin, med tem ko umetna inteligenca ustvarja nove diskriminatorne skupine. Zakonodaja o zaščiti podatkov zmanjšuje tveganje tovrstne diskriminacije, na primer tako, da zahteva transparentnost glede obdelave

[51] Barocas, S., Selbst, A., D.: Big Data's Disparate Impact, v: California Law Review, 104 (2016) 617, str. 692-693.
[52] Gillis, T. B., Spiess, J.: Big Data and Discrimination, v: University of Chicago Law Review, 86 (2019) 459, str. 468.
[53] Borgesius, F. Z.:Discrimination, artificial intelligence, and algorithmic decision-making, Directorate General of Democracy, Council of Europe, Strasbourg, 2018, str. 18.

osebnih podatkov. Smernice so prav tako dobro orodje saj se hitro spreminjajo in so lahko specifične. [54]

Problem preprečevanja diskriminacije v digitalni dobi je, da protidiskrimnacijska zakonodaja temelji na zastareli paradigmi kavzalnosti, pri čemer kot relevantno opazujemo (in dokazujemo) ali je imela posameznikova zaščitena lastnost (oziroma upoštevanje te lastnosti) vpliv na odločitev. To je problematično saj strojno učenje temelji na korelaciji in ne kavzalnosti. Pri uporabi algoritmov za napoved, je cilj čim večja natančnost napovedi in le ta določa kvaliteto sistema. Zaradi tega protidisrkiminacijka regulacija ne more temeljiti na tradicionalni analizi vzročnosti.[55] Ta ni efektivna zaradi možnosti formalne izključitve lastnosti, ki določajo skupino, ki je domnevno diskriminirana, med tem ko s tovrstno izključitvijo neugodna obravnava ni izključena, zaradi korelacije te skupine z drugimi upoštevanimi lastnostmi. Dokazovati smiselno oziroma za diskriminacijo relevantno korelacijo je zelo težko, saj je vpogled v samo odločanje avtomatiziranih sistemov pogosto tehnično nemogoč. Domnevni žrtvi disriminacije s tem preostane zgolj dokazovanje na podlagi statistike odločitev, vendar ta ne more služiti kot dokaz, saj je lahko plod obravnavane populacije in ne diskriminatornega postopka odločanja.

Velik del protiskriminacijske pravne doktrine se osredotoča na regulacijo vhodnih podatkov, kar sledi logiki tradicionalne protidiskriminacijske zakonodaje, s tem da omejuje to, kar gre v algoritem. Tovrstni ukrepi so neprimerni zaradi treh razlogov. Pogosto ne izpolnjujejo lastnih ohlapnih ciljev pravičnosti, ni jih mogoče praktično implementirati oziroma niso primerni za sisteme strojnega učenja in so lahko za zaščitene skupine celo škodljivi in prispevajo k diskriminatorni obravnavi.[56] Kljub temu, da strmino k avtomatiziranim sistemom z željo transparentnega in objektivnega odločanja, se moremo zavedati, da ima zgolj regulacija upoštevanih lastnosti omejen učinek. Res je, da pri tovrstnih sistemih lahko dosežemo dejansko izključitev določenih lastnosti za namen odločanja, vendar če nas resnično skrbi rezultat teh sistemov, moremo iz vidika protidiskriminacijske zakonodaje strmeti onkraj preprostih omejitev upoštevanih lastnosti, saj imajo te omejitve omejen ali celo negativen učinek.[57] Meja med empirično relevantnim in pravno dopustnim nikoli ne izgine, med tem ko postopoma izginja razlika med sistemom, ki se zaveda

[54] Ibidem, str. 5-33.
[55] Gillis, T. B.: False Dreams of Algorithmic Fairness: The Case of Credit Pricing, str. 43.
[56] Ibidem, str. 42.
[57] Gillis, T. B., Spiess, J.: Big Data and Discrimination, v: University of Chicago Law Review, 86 (2019) 459, str. 473.

zaščitene lastnosti in tistim , ki se ne, zaradi česar je prepoved vhodnih informacij nesmiselna. [58]

Možen način regulacije vhodnih podatkov je določitev dopustnih lastnosti za odločanja. Za razliko s prej omenjeno regulacijo lastnosti, ki se jih za namen odločanje ne bi smelo upoštevati, tovrstna regulacija določa lastnosti, ki se lahko uporabljajo za odločanje in prepoveduje uporabo drugih lastnosti. Namesto določitve nedopustnih lastnosti, določa dopustne. Pri tem konceptu se ponovno pojavi problem določitve dopustnih lastnosti. Če je namreč namen regulacije uporaba zgolj relevantnih informacij, je takšna omejitev nesmiselna, saj sistem, katerega cilj je ustvarjati čim bolj natančne napovedi, za razliko od človeka, sam najboljše presodi, katere značilnosti so najbolj relevantne za natančno napoved. Omejitev analiziranih lastnosti iz tega vidika zgolj zmanjšuje kvaliteto napovedi.[59] Zaradi specifične narave odločitev za različne namene bi za takšno regulacijo bili primerni zgolj sektorski regulatorji.

5.7 Pravica, da za posameznika ne velja odločitev, ki temelji na avtomatki obdelavi podatkov

Zelo pomembna pravica za boj zoper algoritemsko diskriminacijo je določena v prvem odstavku 22. člena Uredbe o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES[60] (v nadaljevanju GDPR), namreč pravica, da za posameznika, na katerega se nanašajo posebni podatki ne velja odločitev, ki temelji zgolj na avtomatizirani obdelavi podatkov, vključno z oblikovanjem profilov, ki ima pravne učinke v zvezi z njim ali na podoben način nanj znatno vpliva.[61] Oblikovanje profila generalno pomeni določitev določenih lastnosti posameznika ali skupine in obravnava tega posameznika ali skupine obziroma na te lastnosti. Pravica, ki jo določa 22. člen GDPR, primarno vpliva na drugi del, oblikovanje profila in s tem služi kot varovalo pred kategorizacijo, oceno in diskriminacijo posameznikov.[62]

---

[58] Gillis, T. B.: False Dreams of Algorithmic Fairness: The Case of Credit Pricing, str. 49.
[59] Ibidem, str. 58-60.
[60] Uredba (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES (Splošna uredba o varstvu podatkov) (Besedilo velja za EGP), Uradni list Evropske unije, L 119, 4.5.2016, str. 1–88.
[61] 22. člen GDPR.
[62] Mendoza, I., Bygrave, L. A., The Right Not To Be Subject to Automated Decisions Based on Profiling, v: Universitz of Oslo Faculty of Law Legal Studies Research Paper Series, (2017) 2017-20, str. 1

Preprosta kategorizacija te določbe kot pravice ni popolnoma natančna, saj sooznačuje pravico, katero lahko uveljavlja nosilec pravice, oziroma oseba na katero se nanašajo osebni podatki. Iz stroge besedne razlage prvega odstavka 22. člena vidimo, da prej opredeljen posameznik nima pravice nečesa storiti, temveč pravico, da se ga na določen način ne obravnava, kar vodi do razumevanja tega člena kot določene prepovedi in ne pravice, ki jo zaščiten posameznik mora uveljavljati. Če bi to določilo razlagali kot posameznikovo pravico do pritožbe na tovrstno odločanje, bi njen učinek bil odvisen od uveljavljanja pravice s strani posameznika, če pa določilo razlagamo kot kvalificirano prepoved, jo tisti, ki izvaja tovrstno odločitev more spoštovati neodvisno od nosilca pravice.[63] V primeru, da bi bilo zahtevano uveljavljanje te pravice s strani posameznika, na katerega se osebni podatki v obdelavi nanašajo, bi tovrsten zaščitni ukrep imel manjšo moč, saj bi bil odvisen ne le od posameznikovega poznanja te pravice, temveč tudi njegovega zavedanja, da odločitev na podlagi njegovih osebnih podatkov sprejema avtonomen sistem. Tovrstno interpretacijo je potrdila tudi delovna skupina WP29[64] in zagotovila, da ta prepoved, ki se navezuje na avtomatizirano določanje, posameznika ščiti ne glede na njegovo uveljavljanje te pravice.

Kot lahko izberemo iz prvega odstavka 22. člena, je ta pravica določena pod tremi pogoji.:

1. Sprejeta mora biti odločitev
2. Pri določanju so bili uporabljeni osebni podatki
3. Odločitev temelji zgolj na avtomatizirani obdelavi, vključno z oblikovanjem profilov

Prvi odstavek 22. člena zadeva odločitve, ki so sprejete zgolj na podlagi avtomatizirane obdelave, kar pomeni, da je do odločitve prišlo brez človeške udeležbe. Tej določbi se ne da izogniti zgolj s fiktivno človeško udeležbo, na primer tako, da človek odločitev zgolj posreduje, saj v tem primeru še vedno gre za odločitev, ki temelji na avtomatizirani obdelavi. Kriterij človeške udeležbe je zadoščen, kadar upravljalec zagotovi, da je človeški nadzor na postopek odločanja smiseln in izveden s strani nekoga, ki je kompetenten in ima avtoriteto odločitev

[63] Ibidem.
[64] Delovna skupina ustanovljena na podlagi 29. člena Direktive 95/46/ES, Article 29 Data Protection Working Party.

spremeniti. Primerno bi bilo, da upravljalec kot del ocene učinka v zvezi z varstvom podatkov (v nadaljevanju DPIA[65]) določi in zabeleži tovrstno človeško udeležbo. [66]

Pri razlagi drugega dela tega pogoja pride do vprašanja obsega tega določila, saj je pomembno določiti kaj iz vidika te direktive pomenita avtomatizirana obdelava in oblikovanje profilov, ter kakšna je njivna korelacija iz vidika tega določila. Problematičen je del določila »vključno z«, saj poraja vprašanje, ali dodatek oblikovanja profilov obseg določila oži s tem da konkretizira, da se določilo nanaša zgolj na avtomatizirano obdelavo, ki vključuje tudi oblikovanje profilov, ali obseg določala širi oziroma konkretizira, s tem da dodaja nov proces za sprejemanje odločitev oziroma z namenom jasnosti konkretizira oblikovanje profilov, kot za to določilo relevantno obliko avtonomne obdelave podatkov. Razlika je v tem, ali se določilo nanaša samo na odločitve sprejete na podlagi avtomatizirane obdelave, pri kateri je bilo prisotno oblikovanje profilov, ali se nanaša na odločitve sprejete na podlagi vsake avtomatizirane obdelave (osebnih) podatkov. Med tem, ko v slovenskem prevodu GDPR besedna interpretacija vodi do druge možnosti, je v primeru nekaterih drugih jezikov manj jasna (ang. Includes, v tem primeru je možna dvojna interpretacija).

Pojma obdelava in oblikovanje profilov sta opredeljena v 4. členu.

- „obdelava“ pomeni vsako dejanje ali niz dejanj, ki se izvaja v zvezi z osebnimi podatki ali nizi osebnih podatkov z avtomatiziranimi sredstvi ali brez njih, kot je zbiranje, beleženje, urejanje, strukturiranje, shranjevanje, prilagajanje ali spreminjanje, priklic, vpogled, uporaba, razkritje s posredovanjem, razširjanje ali drugačno omogočanje dostopa, prilagajanje ali kombiniranje, omejevanje, izbris ali uničenje[67]
- „oblikovanje profilov“ pomeni vsako obliko avtomatizirane obdelave osebnih podatkov, ki vključuje uporabo osebnih podatkov za ocenjevanje nekaterih osebnih vidikov v zvezi s posameznikom, zlasti za analizo ali predvidevanje uspešnosti pri delu, ekonomskega položaja, zdravja,

[65] Kratica izvira iz angleškega pojma *Data Protection Impact Assessment.*
[66] Article 29 Data Protection Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016 679, str. 20-21.
[67] 4(2). člen GDPR.

> osebnega okusa, interesov, zanesljivosti, vedenja, lokacije ali gibanja tega posameznika[68]

Kot vidimo v opredelitvi oblikovanja profilov (»pomeni vsako obliko avtomatizirane obdelave osebnih podatkov«) je oblikovanje profilov vrsta avtomatske obdelave, kar odraža prej pojasnjeno konkretizacijo obsega določila. Vendar kot pojasnjujeta Mendoza in Bygrave, recital 71 vodi do interpretacije, da je oblikovanje profilov element avtomatizirane obdelava, v kontekstu tega določila. V omenjenem recitalu namreč piše: » Taka obdelava vključuje „oblikovanje profilov" v kakršni koli obliki avtomatizirane obdelave osebnih podatkov, na podlagi katerih se ocenjujejo osebni vidiki v zvezi s posameznikom,…«[69]. Vlogo vključenosti pojma »oblikovanje profilov« pojasnjujeta kot kriterij za to določbo relevantne avtomatizirane obdelave podatkov. Na podlagi tega se zavzemata za ožji obseg te določbe, namreč v odnosu zgolj do avtomatizirane obdelave, katere del je obvezno tudi oblikovanje profilov. To pojasnjujeta tudi s tem, da se pripravna dela GDPR fokusirajo pretežno na nevarnosti oblikovanja profilov in da je tovrstna interpretacija bolj smiselna iz vidika ozadja 22. člena. S tem bi domet tega člena prav tako bil širši kakor domet njegovega prednika(DPD člen 15).[70]

Vendar, kot je pojasnjeno v smernicah delovne skupine WP29, se četrti odstavek 4. člena GDPR, ki določa oblikovanje profilov nanaša na vsako obliko avtomatizirane obdelave in ne na obdelavo, ki je zgolj oziroma popolnoma avtomatizirana. To pomeni, da kljub temu, da je uporaba avtomatizirane obdelave podatkov pogoj za oblikovanje profilov v smislu GDPR, človeška vključenost v ta postopek ne pomeni, da ne gre za oblikovanje profilov. [71]Oblikovanje profilov pogosto vključuje prediktivne elemente, zaradi česar ustvarjeni profili pogosto niso natančni, k čemur prav tako prispeva nepravilen zajem obdelovanih podatkov, obdelava irelevantnih podatkov ali pa so podatki obdelani izven konteksta. Upoštevati moremo tudi možne napake v samem algoritmu glede prepoznavanja korelacij. [72]

---

[68] 4(4). člen GDPR.
[69] Recital 71 GDPR.
[70] Mendoza, I., Bygrave, L. A., The Right Not To Be Subject to Automated Decisions Based on Profiling, v: Universitz of Oslo Faculty of Law Legal Studies Research Paper Series, (2017) 2017-20, str. 13-14.
[71] Article. 29 Data Protection Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016 679, str. 6.
[72] Ibidem, str. 24.

Kot je v smernicah v nadaljevanju pojasnjeno se odločitve na podlagi avtomatizirane obdelave podatkov sprejemajo na podlagi podatkov, ki so jih neposredno zagotovili obravnavani posamezniki, podatkov zajetih z opazovanjem posameznikov in izvedenih podatkov (me te sodijo tudi profili, ki so bili že ustvarjeni). [73]Ta opredelitev je ključnega pomena iz vidika določila 22(1) člena, saj pozornost iz oblikovanj profila kot postopka, osredotoči na rezultat tega postopka. Kot je v smernicah nadalje pojasnjeno, odločanje na podlagi avtomatizirane obdelave podatkov lahko poteka z ali brez oblikovanja profilov in da lahko gre za ločena postopka ali ne. Prav tako opozarja, da se postopek oblikovanja profilov, oziroma njegov rezultat uporablja tudi za odločanje, ki ni avtomatizirano, temveč ga vrši človek.[74]

Za razumevanje obsega tega določila je prvotno treba poudariti, da avtomatizirani sistemi obdelave podatkov ne sprejemajo odločitve. Odločitev sprejema lahko zgolj človek. Avtomatiziran sistem obdelave podatkov lahko človeku nudi zgolj odgovor (predlog ali navodilo), kako naj odloči. To smiselno izhaja tudi iz same formulacije določila 22(1) člena, ki govori o odločitvah, ki temeljijo zgolj na avtomatizirani obdelavi podatkov in ne na odločitvah, ki jih ti sistemi sprejmejo, saj le ti tega iz pravnega vidika niso sposobni. Smiselno s predhodnim pojasnilom pogoja, da odločitev temelji zgolj na avtomatizirani obdelavi podatkov, lahko »odgovor«, v smislu 22. člena določimo kot informacijo, ki popolnoma določa človekovo odločitev, brez njegove smiselne interakcije. To pomeni, da je človekova odločitev identična odgovoru in temelji zgolj na njem (v tem primeru gre za navodilo, kako odločiti). Takšen odgovor lahko delimo na neposreden in posreden odgovor. Za tovrstno delitev moremo postopek odločanje obravnavati kot iskanje odgovora na določeno vprašanje. Preprost primer bi bilo v postopku odločanja o odobritvi kredita. V tem primeru bi za odločanje bilo zastavljeno vprašanje, ali kreditojemalcu odobriti kredit. Možna odgovora, ki prav tako označujeta odločitev sta DA ali NE. Program, ki ga odločevalec za namen odločitve uporabi, lahko ustvari posreden ali neposreden odgovor na zastavljeno vprašanje. Neposredni odgovorov bi bil DA ali NE med tem ko bi posreden odgovor bil drugačen na primer, da je kreditojemalec kreditno spodoben. Med tem ko takšen odgovor ni identičen kateremu od možnih odgovorov za odločitev ima močnejšo korelacijo z enim iz med njiju (odgovor kreditno sposoben usmerja odločevalca proti odgovoru DA). Tukaj je potrebno

[73] Ibidem, str. 7-8.
[74] Ibidem.

opozoriti, da ne glede na to, ali gre za posredni ali neposredni odgovor, ni nujno, da sodi v domet 22. člena. Odločevalec lahko tovrstni avtomatiziran postopek uporabi zgolj kot nasvet (odloča sam vendar odločitev zgolj preveri s tovrstnim sistemom). Takšna uporaba je praktično problematična, saj bi v tovrstnem primeru resnično vlogo takšnega sistema lahko določali zgolj na podlagi primerjave večje količine odločitev odločevalca z odgovori sistema in njegove svobode arbitrarnega odločanja. Posredni odgovor prav tako lahko služi zgolj kot izpolnitev enega izmed več kriterijev na podlagi katerih odločevalec odloča, lahko pa neposredno določa odločitev, če izpolnjuje edini kriterij odločanja ali nosi takšno težo, da drugi kriteriji odločitve ne morejo spremeniti in če odločevalec ne more odločiti kontradiktorno temu odgovoru. (Primer: odgovor sistema je , da je kreditojemalec kreditno sposoben, odločevalec pa glede na podana navodila kredite odobrava zgolj pod pogojem kreditne sposobnosti).

Oblikovanje profilov moramo za lažje razumevanje tega določila obravnavati ločeno kot postopek obdelave podatkov in kot izveden podatek oziroma profil, ki ga ta postopek ustvari. Pomen tovrstne ločitve je v tem, da vloga oblikovanja profilov ni samo odločanje, temveč ustvarjanje izvedenih podatkov (kot izhaja iz 4(4) člena oceno nekaterih osebnih vidikov), na podlagi katerih (vključno z ali brez drugih podatkov) z avtomatizirano obdelavo sprejemajo odločitve. Postopek oblikovanja profila je lahko združen z avtomatizirano obdelavo podatkov, na kateri temelji odločitev ali pa ločen postopek. Kot ločen postopek je lahko namenjen neposrednemu odločanju ali zgolj za namen oblikovanja profila.

Oblikovan profili glede na uporabo lahko služi zgolj kot izveden podatek (oseba A je dober voznik, vendar to ni edina kvalifikacija na podlagi katere se presoja premija zavarovanja) ali pa kot predhodno opisan posredni odgovor (oseba A je dober voznik, ta lastnost je odločilna). V tej delitvi najdemo smisel eksplicitne omembe oblikovanja profilov v prvem odstavku 22. člena GDPR, saj je oblikovanje profilov, ki je samostojno določen pojem v GDPR lahko vrsta avtomatizirane obdelave podatkov, zgolj na kateri temelji odločitev.

Kot sem omenil prej, lahko v procesu oblikovanja profila sodeluje človek. Na podlagi tega bi bila možna preprosta razlaga, da omejitev, določena v prvem odstavku 22. člena GDPR velja za postopke oblikovanja profila, če oblikovan profil služi kot predhodno opisan posredni odgovor in če v postopku oblikovanja ni sodeloval človek. Vendar menim, da je tovrstna interpretacija neustrezna, saj sama

po sebi ne zahteva efektivne človeške udeležbe, kot sem jo pojasnil predhodno pri razlagi, kdaj odgovor temelji zgolj na podlagi avtomatizirane obdelave podatkov. Da tovrsten profil ne sodi pod prepoved, ki jo določa prvi odstavek 22. člena GDPR, more človek v procesu oblikovanja profila sodelovati na način , ki je smiseln in izveden s strani nekoga, ki je kompetenten in ima avtoriteto vplivati na dejanski profil.

Na podlagi pojasnjenega je razumna interpretacija tega določila v okviru širšega obsega, namreč, da prepoved iz 22(1) člena zajema vse odločitve, ki temeljijo zgolj na podlagi avtomatizirane obdelave, tako tiste, ki vključujejo oblikovanje profilov kot del oziroma vrsto obdelave podatkov, kot tudi tiste, ki tega ne vključujejo.

Širša razlaga, ki ščiti posameznika tudi v odsotnosti oblikovanja profila, je prav tako smiselna zato, ker ima nenazadnje tudi zgolj avtomatizirana obdelava podatkov lahko sporne, celo diskriminativne učinke zaradi omejenega obsega presojanih lastnosti ter potencialno sporne postavitve kriterijev in meril odločanja. Nenazadnje, kot bom pojasnil v nadaljevanju, to določilo zadeva odločitve, ki imajo pravne ali podobne učinke. V tem smislu gre za odločitve, ki so enako pomembne iz vidika zaščite posameznika. Določitev enake mere pozornosti pri preprostemu avtomatiziranemu odločanju, tudi če temelji samo na objektivnih parametrih, je pomembna zaradi možnosti napak pri različnih fazah, pomembnih za tovrstno obdelavo (napake pri zajemu podatkov, sortiranju teh podatkov, itd) Preprost primer je določitev kazni za prehitro vožnjo na podlagi podatkov o izmerjeni hitrosti in identifikaciji vozila z registersko tablico, ki jih je zabeležila kamera ob cestišču in obdelal avtomatiziran sistem. Pri obeh podatkih lahko pride do napak (napačen avtomatiziran prepis tablice, ki temelji na računalniškem vidu in izmerjeni hitrosti, ki je zaradi tehničnih problemov lahko absurdno nepravilna, kar bi človek ob pregledu opazil, sistem avtomatizirane obdelave pa morda ne bi (npr. če sistem določa kazen ob prekoračitvi hitrosti 50km/h in nima *priučene* razumne zgornje meje hitrosti, ki jo avti lahko dosežejo, bo izdal kazen v primeru, kjer bo izmerjena hitrost 6000000 km/h, kljub temu, da avto takšne hitrosti ne more doseči in lahko opravičljivo sklepamo, da je zabeležena hitrost posledica tehnične napake merilne naprave ali drugih okoljskih vplivov, ki napravo motijo). Človek, ki bi takšno meritev pregledal, bi takoj videl ,da je z meritvijo nekaj narobe. Seveda lahko v sistem opisan v našem primeru vključimo razumno zgornjo mejo izmerjene hitrosti, vendar je vprašljivo ali tovrsten sistem lahko optimiziramo, da je odporen na, oziroma da zazna, prisotnost vseh vplivov, ki lahko vodijo do napačne meritve. To je še veliko

težje v primeru kompleksnih sistemov avtomatizirane obdelave podatkov, ki presojajo na podlagi več lastnosti in podatke črpajo iz več virov.

5.7.1 Odločitev ima pravne učinke v zvezi z njim ali na podoben način nanj znatno vpliva

Prepoved določena v 22. členu posameznika ščiti, če ima odločitev pravne učinke v zvezi z njim ali na podoben način nanj znatno vpliva. Ta pogoj je izpolnjen, če odločitev delno ali popolnoma določi ali spremeni posameznikove pravice ali dolžnosti oziroma ima posledice, ki so več kot malenkostne za dobrobit posameznika. [75]

Kot pojasnjuje delovna skupina WP29, gre v smislu 22. člena za pravni učinek, če odločitev vpliva na posameznikove pravice (pravica do združevanja), kot tudi če odločitev vpliva na posameznikov pravni status (npr. pridobitev državljanstva) ali na njegovee pravice v pogodbenem razmerju (prenehanje pogodbe). Tudi če učinki odločitve ne vplivajo na posameznikove pravice ali obligacije, sodijo pod to določilo, če ga prizadenejo primerljivo s tistimi, ki imajo pravni učinek. [76]

Delovna skupina WP29 posebej izpostavlja učinke, ki znatno vplivajo na posameznikove okoliščine, vedenje in odločitve, ki imajo na njega dolgotrajen učinek in ki v skrajnih primerih vodijo do diskriminacije. Kot primere znatnih učinkov navajajo tiste, ki vplivajo na posameznikovo finančno stanje (dostop do kredita), njegov dostop do zdravstvenih storitev, zaposlitve in izobraževanja. Opozarja, da ima tovrstni učinek lahko tudi targetirano oglaševanje, ki temelji na podlagi oblikovanja profilov, glede na njeno intruzivnost (če vključuje sledenje uporabnikom širom različnih strani, naprav in storitev), glede na pričakovanja in želje posameznika na katerega se navezuje, glede na način oglaševanja in kadar uporablja šibkosti targetiranega posameznika. Poudarjajo primere targetiranega oglaševanja visoko obrestnih kreditov posameznikom s šibkim finančnim stanjem in cenovnega spreminjanja ponudb za storitve in izdelke, če tovrstno prilagajanje onemogoči dostop zaščitenih skupin do teh storitev in izdelkov. Opozarjajo, da dejanja in stanja drugih prav tako lahko močno vplivajo na učinke zoper obravnavanega posameznika

[75] Mendoza, I., Bygrave, L. A., The Right Not To Be Subject to Automated Decisions Based on Profiling, v: Universitz of Oslo Faculty of Law Legal Studies Research Paper Series, (2017) 2017-20, str. 12, 20.
[76] Article 29 Data Protection Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016 679, str. 21.

(pogoji posojila se presojajo glede na kreditno sposobnost drugih prebivalcev območja, kjer posameznik živi.[77]

Kot opozarjata Bygraves in Mendoza ne smemo spregledati recital 38 GDPR, ki odraža, da kadar avtomatizirano sprejemanje odločitev zadeva otroka, je tovrstna odločitev znatna v smislu 22. člena.[78]Recital pojasnjuje potrebo posebnega varstva otrok, saj se ti morda ne zavedajo zadevnih tveganj, posledic in zaščitnih ukrepov, ter pojasnjuje, da privolitev »nosilca starševske odgovornosti ne bi smela biti potrebna v okviru storitev preventive ali svetovanja, ki se nudijo neposredno otroku.«[79]

5.7.2 Izjeme prepovedi določila 22. člena GDPR

Drugi odstavek 22. člena določa tri izjeme prepovedi iz prvega odstavka, namreč če je odločitev:

1. Nujna za sklenitev ali izvajanje pogodbe med posameznikom, na katerega se nanašajo osebni podatki, in upravljavcem podatkov[80]

Uporaba postopkov za avtomatizirano odločanje za namen sklepanja pogodb je pogosto zaželjena saj je pogosto bolj praktična in včasih edina izvedljiva možnost (sklepanje velikih količin pogodb). Za uporabo teh procesov iz vidika te izjeme, mora upravljalec podatkov biti sposoben utemeljiti, da so tovrstni procesi za ta namen nujni, kar pa niso, če obstajajo drugi efektivni in manj intruzivni načini za doseg tega namena. Upoštevati je potrebno tudi pomen in uporabo avtomatiziranih sistemov za odločanje v predhodni fazi sklenitve pogodbe (na primer filtriranje kandidatov za delovno mesto, ki ne ustrezajo objektivnim pogojem, v primeru velike količine kandidatov).[81]

[77] Ibidem, str. 21-22.
[78] Mendoza, I., Bygrave, L. A., The Right Not To Be Subject to Automated Decisions Based on Profiling, v: Universitz of Oslo Faculty of Law Legal Studies Research Paper Series, (2017) 2017-20, str. 12.
[79] Recital 38 GDPR.
[80] 22(2a). člen GDPR.
[81] Article 29 Data Protection Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016 679, str. 23.

2. Dovoljena v pravu Unije ali pravu države članice, ki velja za upravljavca in določa tudi ustrezne ukrepe za zaščito pravic in svoboščin ter zakonitih interesov posameznika, na katerega se nanašajo osebni podatki,[82]

V recitalu 71 GDPR poudarjeno, da bi sprejemanje odločitev, na podlagi avtomatizirane obdelave podatkov moralo biti dovoljeno »kadar ga izrecno dovoljuje pravo Unije ali pravo države članice, ki velja za upravljavca, tudi za namene spremljanja in preprečevanja zlorab in davčnih utaj v skladu s predpisi, standardi in priporočili institucij Unije ali nacionalnih nadzornih teles ter zagotavljanje varnosti in zanesljivosti storitve, ki jo zagotavlja upravljavec…«[83] Na podlagi tega lahko sklepamo, da je ta izjema bila sprejeta pretežno za namen uporabe tovrstnih procesov za namen izvajanja funkcij državnih organov in institucij.

3. Utemeljena z izrecno privolitvijo posameznika, na katerega se nanašajo osebni podatki[84]

Ker avtomatizirana obdelava podatkov za namen odločanja predstavlja veliko tveganje za posameznika, na katerega se ti podatki nanašajo, je primerna višja raven nadzora tega posameznika nad uporabo njegovih osebnih podatkov.[85] Privolitev posameznika, na katerega se nanašajo osebni podatki pomeni »vsako prostovoljno, izrecno, informirano in nedvoumno izjavo volje posameznika, na katerega se nanašajo osebni podatki, s katero z izjavo ali jasnim pritrdilnim dejanjem izrazi soglasje z obdelavo osebnih podatkov, ki se nanašajo nanj«[86]. Kot izhaja iz definicije je privolitev ustrezna če ustreza štirim pogojem:

4. Je dana prostovoljno

Ta pogoj je izpolnjen kadar je posameznik resnično imel svobodo in nadzor izraziti svojo voljo. Kadar posameznik ni imel dejanske izbire, je bil k soglasju privolitvi primoran ali bi bil v primeru ne privolitve deležen negativnih posledic, privolitev za izpolnitev pogojev GDPR ni ustrezna. Privolitev prav tako ni ustrezna, če je del privolitev pogojev uporabe, o katerih se posameznik ne more pogajati. Načelno

[82] 22(2b). člen GDPR.
[83] recital 71 GDPR.
[84] 22(2c). člen GDPR.
[85] Article 29 Data Protection Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016 679, str. 24.
[86] 4(11). člen GDPR.

velja, da privolitev ni prostovoljna, če je posameznik ne more umakniti ali zavrniti brez škode.[87]

5. Je izrecna

Privolitev posameznika mora biti izrecna za eno ali več določenih namenov. Namen te zahteve je zagotoviti posamezniku ustrezno mero nadzora nad obdelavo njegovih podatkov.[88] Ta zahteva je poudarjena tudi v prvem odstavku 6. člena GDPR, kjer je kot pogoj, da je obdelava zakonita določeno, da »posameznik, na katerega se nanašajo osebni podatki, je privolil v obdelavo njegovih osebnih podatkov v enega ali več določenih namenov«[89].

6. Je dana informirano

GDPR zahteva, da je privolitev informirana. Informiranost posameznikov je za njihovo privolitev pomembna, saj zgolj tako lahko sprejmejo informirano odločitev, razumejo, k čemu soglašajo in zgolj tako lahko efektivno uveljavljajo svojo pravico do zadržanja soglasja. Da je izpolnjen ta pogoj mora posameznik biti seznanjen vsaj z identiteto upravljalca podatkov, namena vsakega postopka obdelave, za katerega upravljalec skuša pridobiti privolitev, kakšne vrste podatkov bodo zbrane in uporabljene, z informacijami o uporabi podatkov za avtomatizirano odločanje v skladu s 22(2)(c) členom GDPR (ki določa izjemo v primeru privolitve, ki jo trenutno obravnavamo) in v primeru prenosov podatkov, za katere se uporabljajo ustrezni zaščitni ukrepi, s temi, kot so določeni v 46. členu GDPR.[90] V zadevi *Planet49*[91] je Sodišče potrdilo, da »mora jasna in izčrpna obvestitev uporabniku omogočiti, da z lahkoto ugotovi posledice morebitne dane privolitve, in zagotoviti, da je ta privolitev dana ob popolni seznanjenosti z dejstvi. Ta obvestitev mora biti jasno razumljiva in dovolj podrobna, da uporabnik lahko razume delovanje uporabljenih piškotkov«. V tej zadevi je sodišče prav tako pojasnilo, da je namestitev piškotkov vrsta obdelave osebnih podatkov, skladno s določbami GDPR, zato takšna pojasnilna dolžnost smiselno velja splošno za obdelavo osebnih podatkov.

[87] European Data Protection Board, Guidelines 05/2020 on consent under Regulation 2016/679, version 1.1, 2020, str. 7.
[88] Ibidem, str. 13-14.
[89] 95/46/ES, 6(1a). člen GDPR.
[90] European Data Protection Board, Guidelines 05/2020 on consent under Regulation 2016/679, version 1.1, 2020, str. 15-16.
[91] Zadeva C-673/17, *Planet 49,* ECLI:EU:C:2019:801.

Prav tako je odločilo, da morajo informacije o namestitvi piškotkov zajemati trajanje delovanja piškotkov in z možnost oziroma nezmožnost tretjih oseb, da dostopajo do teh piškotkov.

7. Dana z nedvoumna izjavo volje

Za privolitev je potrebna izjava ali jasno pritrdilno dejanje, ki mora biti s strani posameznika dano na aktiven način. Privolitev k določeni obdelavi more biti očitna. Jasno pritrdilno dejanje torej pomeni aktivno dejanje, s katerim posameznik izraža privolitev za določeno obdelavo. [92] V recitalu 32 GDPR je nadalje določeno, »da je posameznik, na katerega se nanašajo osebni podatki, prostovoljno, specifično, ozaveščeno in nedvoumno izrazil soglasje k obdelavi osebnih podatkov v zvezi z njim, kot je s pisno, tudi z elektronskimi sredstvi, ali ustno izjavo. To lahko vključuje označitev okenca ob obisku spletne strani, izbiro tehničnih nastavitev za storitve informacijske družbe ali katero koli drugo izjavo ali ravnanje, ki v tem okviru jasno kaže na to, da posameznik, na katerega se nanašajo osebni podatki, sprejema predlagano obdelavo svojih osebnih podatkov. Molk, vnaprej označena okenca ali nedejavnost zato ne pomenijo privolitve.«[93] Glede vnaprej označenih okenc je Sodišče odločilo v predhodno omenjeni zadevi *Planet49*[94], namreč, da ne gre za veljavno privolitev, kadar je potrditveno polje predhodno označil ponudnik storitve in ki bi ga moral uporabnik, da zavrne svojo privolitev odznačiti. Dejstvo, da je posameznik želel dostopati do določene storitve (v primeru te zadeve sodelovanje v nagradni igri) ne more zadostovati kot veljavna privolitev, v tem primeru za namestitev piškotkov.

Pri spletnem dostopanju do storitev vseh vrst praktično stalno dajemo privolitev v obliki sklepanja pogodb s enim klikom (označitev okenca, pritisk gumba s napisano: Se strinjam). Problem sklepanja spletnih pogodb z enim klikom je, da ljudi primora k avtomatskemu ravnanju, brez razmisleka. Ljudje se pri sklepanju spletnih pogodb le redko vprašajo glede vsebine pogodb in strank, s katerimi te pogodbe sklepajo. Problem je v tem da svoboda do sklenitve pogodbe zahteva tudi obratno, svobodo ne skleniti pogodbo in ko sklepanje postane avtomatično izgineta obe, saj več ne govorimo o svobodi in avtonomiji.[95]

---

[92] European Data Protection Board, Guidelines 05/2020 on consent under Regulation 2016/679, version 1.1, 2020, str. 18.
[93] Recital 32 GDPR.
[94] C-673/17, *Planet 49,* ECLI:EU:C:2019:801.
[95] Povzeto po: <http://cyberlaw.stanford.edu/blog/2019/02/electronic-contracts-and-illusion-consent> (13.4.2020).

5.7.2 Omejitev izjem

V tretjem odstavku 22. člena je določeno, da v primerih odločitev, ki so nujne za sklenitev ali izpolnitev pogodbe in odločitev, ki so utemeljene z izrecno privolitvijo, nosi upravljalec podatkov dolžnost da »izvede ustrezne ukrepe za zaščito pravic in svoboščin ter zakonitih interesov posameznika, na katerega se nanašajo osebni podatki, vsaj pravice do osebnega posredovanja upravljavca, do izražanja lastnega stališča in izpodbijanja odločitve.«[96] Pravice navedene v tem odstavku ne predstavljajo vseh možnih zaščitnih ukrepov temveč zgolj minimalne zahteve.[97] Posebej pomembna je pravica do osebnega posredovanja upravljalca, saj kot je pojasnila delovna skupina WP29, mora pregled odločitve speljati oseba, ki ima avtoriteto in sposobnost odločitev spremeniti. Pri pregledu mora upoštevati vse relevantne podatke, vključno z vsemi podatki, ki mu jih dodatno zagotovi posameznik, na katerega se osebni podatki nanašajo. Upravljalec podatkov je dolžan obravnavanim posameznikom zagotoviti uveljavljanje iz 3. odstavka 22. člena GDPR.[98]

Omenjene izjeme iz 2. odstavka 22. člena so na podlagi 4. odstavka tega člena prav tako omejene, kadar odločitve temeljijo na podlagi posebnih vrst osebnih podatkov, kot so določeni v prvem odstavku 9. člena GDPR. Osebni podatki posebnih vrst so podatki, »ki razkrivajo rasno ali etnično poreklo, politično mnenje, versko ali filozofsko prepričanje ali članstvo v sindikatu, in obdelava genetskih podatkov, biometričnih podatkov za namene edinstvene identifikacije posameznika, podatkov v zvezi z zdravjem ali podatkov v zvezi s posameznikovim spolnim življenjem ali spolno usmerjenostjo.«[99] Odločitev, ki temelji zgolj na avtomatizirani obdelavi podatkov, vključno z osebnimi podatki posebnih vrst po tem takem velja, kadar gre za primer, ki ga določa ena iz med prej opisanih izjem iz 2. odstavka 22. člena GDPR in če so izpolnjeni pogoji, ki jih določata točki a in g, drugega odstavka 9. člena.[100] Ti določata, da je uporaba posebnih vrst osebnih podatkov dovoljena, kadar:

---

[96] 22(3). Člen GDPR.
[97] Mendoza, I., Bygrave, L. A., The Right Not To Be Subject to Automated Decisions Based on Profiling, v: Universitz of Oslo Faculty of Law Legal Studies Research Paper Series, (2017) 2017-20, str. 15.
[98] Article 29 Data Protection Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016 679, str. 27.
[99] 9(1). Člen GDDPR.
[100] Article 29 Data Protection Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016 679, str. 24.

- posameznik, na katerega se nanašajo osebni podatki, je dal izrecno privolitev za obdelavo navedenih osebnih podatkov za enega ali več določenih namenov, razen kadar pravo Unije ali pravo države članice določa, da posameznik, na katerega se nanašajo osebni podatki, ne sme odstopiti od prepovedi iz odstavka 1 (člena 9 GDPR)[101]
- obdelava je potrebna iz razlogov bistvenega javnega interesa na podlagi prava Unije ali prava države članice, ki je sorazmerno z zastavljenim ciljem, spoštuje bistvo pravice do varstva podatkov ter zagotavlja ustrezne in posebne ukrepe za zaščito temeljnih pravic in interesov posameznika, na katerega se nanašajo osebni podatki.[102]

Poleg teh pogojev, za veljavnost odločitev, ki temeljijo na osebnih podatkih posebnih vrst, se zahteva, da se izvajajo ustrezni ukrepi za zaščito pravic in svoboščin ter zakonitih interesov posameznika, na katerega se nanašajo osebni podatki, kakor je določeno sicer že v 3. odstavku 22. člena GDPR. Razlika je seveda v tem, da se 4. odstavek nanaša na vse tri izjeme iz 2. odstavka, se pravi tudi kadar je uporaba avtomatizirane obdelave osebnih podatkov za odločanje dovoljena s strani EU ali države članice. Pomembno je tudi poudariti, da za razliko od 3. odstavka, 4. odstavek ne določa, da more upravljalec podatkov zagotoviti omenjene zaščitne ukrepe, temveč zgolj, da se tovrstni ukrepi izvajajo. Tovrstna formulacija določbe smiselno nakazuje na dolžnost EU ali držav članic, da zagotovi izvajanje tovrstnih zaščitnih ukrepov, kadar je uporaba avtomatiziranega odločanja dovoljena s strani EU ali državne članice (izjema) in kadar se osebni podatki posebnih vrst obdelujejo iz razlogov bistvenega javnega interesa na podlagi prava Unije ali prava države članice (kakor je določeno v 9 (2g)).

5.8 Ocena učinka v zvezi z varstvom podatkov

DPIA je postopek namenjen opisu obdelave, oceni njene nujnosti in proporcionalnosti in kot pomoč pri odpravi tveganj, ki zadevajo pravice in svoboščine posameznikov, ki izvirajo iz obdelave osebnih podatkov, s tem da tovrstna tveganja oceni in določi ukrepe za njihovo odpravo. Povedano drugače, DPIA je orodje za doseganje in dokazovanje skladnosti z določili GDPR.[103]

---

[101] 9(2a). člen GDPR.
[102] 9(2g). člen GDPR.
[103] Article 29 Data Protection Working Party, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, 2017, str. 4.

V 35. členu GDPR je določena DPIA, ki jo upravljalec mora opraviti kadar je možno, »da bi lahko vrsta obdelave, zlasti z uporabo novih tehnologij, ob upoštevanju narave, obsega, okoliščin in namenov obdelave povzročila veliko tveganje za pravice in svoboščine posameznikov.«[104]V točki a 3. odstavka 35. člena je nadalje določeno, da se DPIA zahteva v primeru »sistematičnega in obsežnega vrednotenja osebnih vidikov v zvezi s posamezniki, ki temelji na avtomatizirani obdelavi, vključno z oblikovanjem profilov, in je osnova za odločitve, ki imajo pravne učinke v zvezi s posameznikom ali nanj na podoben način znatno vplivajo«.[105] Pozorni moramo biti na formulacijo določila saj se navezuje na vrednotenje osebnih vidikov, ki temelji na avtomatizirani obdelavi podatkov in ne *zgolj* na avtomatizirani obdelavi podatkov. Zaradi tega se to določilo nanaša na odločanje, vključno s oblikovanjem profilom, s pravnim ali podobnim učinkom, ki je delno ali popolnoma avtomatizirano.[106]

5.9 Prepoznavanje diskriminacije in predhodni preizkus sistemov umetne inteligence

Algoritemsko odločanje predstavlja možnost transparentnost, saj teoretično nudi možnost rekonstrukcije postopka odločanja, ki pri ljudeh ni mogoča. Ta transparentnost je vendarle še vedno omejena s sposobnostjo razumevanja delovanja teh sistemov. Možen način interpretacije algoritmičnih odločitev je na primer analiza upoštevanih podatkov.[107]

Velik problem boja zoper algoritemsko diskriminacijo je zaznavanje tovrstne diskriminacije. Zaradi zapletenosti sistemov, ki temeljijo na strojnem učenju, je pogosto težko razumeti, kako ta deluje in sprejema odločitve. Upravljalec podatkov mora posamezniku, na katerega se osebni podatki navezujejo postopek sprejemanja odločitev pojasniti na preprost način, ki ne rabi vsebovati temeljite razlage ali razkritja uporabljenega algoritma. Tovrstno pojasnilo mora biti za posameznika, katerega osebni podatki se obdelujejo smiselno.[108] Kadar sistem vključuje tako

[104] 35(1). Člen GDPR.
[105] 35(3a). člen GDPR.
[106] Article 29 Data Protection Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016 679, str. 29.
[107] Gillis, T. B., Spiess, J.: Big Data and Discrimination, v: University of Chicago Law Review, 86 (2019) 459, str. 474-475.
[108] Article. 29 Data Protection Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016 679, str. 14.

oblikovanje profilov, kakor tudi avtomatizirano odločanje na podlagi teh profilov, pojasnilna dolžnost velja glede obeh procesov.[109]

Na podlagi načela transparentnosti, kot ga določa GDPR, morajo upravljalci posameznikom, na katere se osebni podatki nanašajo, na razumljiv in preprost način razložiti, kako poteka postopek oblikovanja profilov in avtomatiziranega odločanja. Kadar se oblikovanje profila uporablja za odločanje (tako v obsegu 22. člena ali ne) mora biti posameznik, na katerega se osebni podatki v obdelavi nanašajo obveščen tako o postopku oblikovanja profila, kot tudi o namenu uporabe tega profila za odločanje. [110] V recitalu 60 GDPR je eksplicitno določeno: »Načeli poštene in pregledne obdelave zahtevata, da je treba posameznika, na katerega se nanašajo osebni podatki, obvestiti o obstoju dejanja obdelave in njegovih namenih. Upravljavec bi moral posamezniku, na katerega se nanašajo osebni podatki, zagotoviti vse dodatne informacije, potrebne za zagotavljanje poštene in pregledne obdelave ob upoštevanju specifičnih okoliščin in okvira obdelave osebnih podatkov. Poleg tega bi moral biti ta posameznik obveščen o oblikovanju profilov in njegovih posledicah.«[111]

Nedavna odkritja na področju računalništva in statistike ponujajo različne vidike glede tega, kdaj algoritem odloča pravično. Vendar se na žalost večina teh odkritji temelji na statistični analizi rezultatov algoritma in ne samih delov procesa algoritemskega odločanja.[112]

Prednost avtomatiziranega odločanja je, da tovrsten sistem lahko preizkusimo pred uporabo. S predhodnim preizkusom lahko ugotovimo, ali je postopek pravičen in s tem nediskriminatoren. V tovrstnem preizkusu bi se sistem uporabil za odločanje o hipotetični (testni) populaciji, s čimer bi se odkrilo razlikovanje odločanja glede na zaščitene skupine. Problem je, da je tovrsten preizkus praktično težaven, saj je preprosta analiza razlikovanja rezultatov glede na pripadnost posameznikov določenim skupinam *prima facie* primer različnega oziroma pristranskega odločanja. Oceniti, kdaj je rezultat resnično diskriminatoren je težavno, saj ne poznamo

[109] Ibidem, str. 23.
[110] Ibidem, str. 16.
[111] Recital 60 GDPR.
[112] Gillis, T. B., Spiess, J.: Big Data and Discrimination, v: University of Chicago Law Review, 86 (2019) 459, str. 465

kriterijev za primerjavo dveh posameznikov, pri določanju, ali sta bila obravnavana različno. S tem se tovrstna analiza rezultatov osredotoča na preprosto primerjavo.[113]

Smiselno bi bilo, da bi se za uporabo v javnem sektorju smeli uporabljati zgolj sistemi, ki bi bili predhodno preizkušeni za tveganje in bi bili sposobni pregleda in revizije njihovih odločitev oziroma rezultatov. Takšen pogoj bi morda bil koristen tudi za uporabo tovrstnih sistemov v zasebnem sektorju, kadar ima uporaba tovrstnih sistemov znatne učinke.[114]Menim, da bi za presojo, kdaj bi tovrsten pogoj bil ustrezen za zasebni sektor najbolj efektivno služil kriterij relevantnega učinka, kot je določen v prvem odstavku 22. člena, namreč kadar ima pravne učinke v zvezi posameznikom, čigar podatki se obdelujejo ali na podoben način nanj znatno vpliva. Seveda se moramo zavedati, da je tovrsten pogoj uporabe tehnično izredno zahteven in pogosto celo neizvedljiv. Pri obravnavi regulacije avtomatiziranega odločanja seveda strmimo k čim večji varnosti posameznikov, ki jih te odločitve prizadenejo in preglednosti postopka odločanja, vendar vselej moramo pri določanju tovrstnih zahtev postopati razumno. Pri presoji, kdaj določiti takšne ukrepe, moramo vselej upoštevati tehnično izvedljivost samih ukrepov in ali določen sistem, v kontekstu uporabe oziroma glede na to, kdo ga uporablja, predstavlja tako veliko tveganje, daje tovrstna zahteva utemeljena. Pri tem menim, da je tovrstna zahteva vsekakor bolj potrebna in s tem primerna za sisteme, ki so v uporabi v javnem sektorju. Tako drastične zahteve bi bilo razumljivo zahtevati zgolj pri postopkih avtomatiziranega odločanja, ki imajo znatni učinek na ljudi, katere odločitve teh sistemov zadevajo.

Kot sem pojasnil prej, imajo po prepovedi iz prvega odstavka 22. člena GDPR tovrstne odločitve veljavo zgolj v primeru opisanih izjem, med katerimi bo praktično najbolj pogosta uporaba na podlagi izrecnega soglasja. To sicer v primeru sistemov, ki se uporabljajo v zasebnem sektorju teoretično ni sporno. Problematična je uporaba, ki temelji na privolitvi v javnem sektorju, saj je, kot opozarja tudi delovna skupinaWP29[115]vprašljivo, če je v odnosu do obdelave podatkov v javnem sektorju sploh možno podati prostovoljno privolitev, saj zaradi pomembnosti storitev, ki jih nudi javni sektor in pomanjkanja alternativ, posameznik, na katerega se podatki navezujejo tovrstne obdelave dejansko ne more zavrniti. Recital 43 GDPR namreč

[113] Ibidem, str. 479-481.
[114] Borgesius, F. Z.:Discrimination, artificial intelligence, and algorithmic decision-making, Directorate General of Democracy, Council of Europe, Strasbourg, 2018, str. 35.
[115] European Data Protection Board, Guidelines 05/2020 on consent under Regulation 2016/679, version 1.1, 2020, str. 8

določa, da za »zagotovitev, da je privolitev dana prostovoljno, privolitev ne bi smela biti veljavna pravna podlaga za obdelavo osebnih podatkov v posebnem primeru, ko obstaja očitno neravnotežje med posameznikom, na katerega se nanašajo osebni podatki, in upravljavcem, zlasti kadar je upravljavec javni organ in je zato malo verjetno, da je bila privolitev dana prostovoljno v vseh okoliščinah te specifične situacije.«[116] Za avtomatizirano odločanje v kontekstu javnega servisa, ki ima učinke, ki so potrebni za veljavo prepovedi prvega odstavka 22. člena GDPR je zatorej smiselno, da je uporaba avtomatiziranega odločanja dopustna zgolj v primeru, da je dovoljena v pravu države članice EU. V tem primeru morejo biti določeni tudi ustrezni ukrepi za zaščito pravic in svoboščin ter zakonitih interesov posameznikov, na katere se nanašajo osebni podatki. Menim, da je v takšnem primeru potrebna še večja zaščita posameznikov, čigar osebni podatki se obdelujejo in da so v takšnem primeru prej opisani pogoji uporabe ne le utemeljeni temveč potrebni.

5.10 Zaključek

Med tem ko umetna inteligenca omogoča precej natančne napovedi in formalno izključitev obravnave določenih lastnosti posameznikov, se moramo zavedati možnosti, da ima lahko uporaba tovrstne tehnologije za namen odločanja diskriminatoren učinek in k uporabi takšnih sistemov pristopati z vsaj takšno mero previdnosti, kakor pri človeškem odločanju. Odločanje, ki temelji na avtomatiziranih sistemih je lahko na prvi pogled vsekakor zastrašujoče, še posebej kadar gre za sisteme namenjene množičnemu odločanju, ki temeljijo na strojnem učenju in njihov postopek odločanja pogosto ni popolnoma razumljiv niti upravljalcem teh sistemov. Avtomatizirane odločitve lahko in pogosto imajo pomemben učinek na posameznika, katerega zadevajo, zaradi česar je popolnoma upravičen strah tega posameznika, da ta odločitev ne bo pravična in da bo zgolj del nepojasnljive statistike. Kljub temu, da je najbolj privlačna lastnost avtomatiziranega odločanja domnevna popolna nevtralnost tovrstnih sistemov, strah in nezaupanje do teh sistemov verjetno temelji na pomanjkanju človeškega stika, saj v tem primeru sklepamo, da je odločevalcu vsaj nekoliko mar in da nismo zgolj ime na seznamu. Seveda realno stanje po navadi ne ustreza takšni predstavi.

Glavni vir regulacije avtomatiziranih sistemov predstavlja GDPR. Ta sicer dopušča razvoj umetne inteligence, v uravnoteženem razmerju zaščite osebnih podatkov in

[116] Recital 43 GDPR.

ekonomskih interesov, vendar nudi zgolj omejena navodila, kako to razmerje doseči. Vsebuje namreč obilje načel in odprtih standardov, zadostitev katerih pogosto zahteva tehtanje nasprotujočih si interesov. V primeru umetne inteligence je ta nejasnost še toliko bolj izrazita, zaradi novosti in kompleksnosti te tehnologije in širokega spektra njenih učinkov.[117]

Pogosta kritika prava je, da stalno zaostaja s tehnološkim razvojem, vendar je pomembno, da z regulacijo tehnologije ne prehitevamo. Postavljanje nerealnih pogojev za uporaba avtomatiziranih sistemov zgolj ovira razvoj in uporabo teh sistemov. Dodatna regulacija morda sploh ni rešitev problema. Glede na to, da je pretežni del uporabe tovrstnih sistemov pogojen z izrecnim soglasjem posameznikov, katerih podatki se obdelujejo, je morda čas, da tudi ti posamezniki prevzamejo smiselno odgovornost za zaščito lastnih interesov. Dodatna regulacija, ki temelji na odprtih standardih in načelih (bolj natančna regulacija je zaradi specifične narave obravnavane tehnologije izjemno težavna) zaradi nejasnosti zgolj zmanjšuje konkurenčnost trga EU za razvoj tovrstne tehnologije. Informacijska ozaveščenost in zaščita osebnih podatkov sta temi, ki sta večini ljudi tuji in dolgočasni, saj se ne zavedajo mogočih implikacij njihovih »odločitev« pri uporabi digitalnih storitev in deljenju osebnih podatkov. Vprašanje je, kdaj bosta ti temi za mnoge postali zanimivi. Za marsikoga morda prepozno ali celo nikoli.

Seznam literature in virov

Članki in poglavja iz knjig

Barocas, S., Selbst, A., D.: Big Data's Disparate Impact, v: California Law Review, 104 (2016) 617, str. 672-678

Borgesius, F. Z.:Discrimination, artificial intelligence, and algorithmic decision-making, Directorate General of Democracy, Council of Europe, Strasbourg, 2018.

Gillis, T. B., Spiess, J.: Big Data and Discrimination, v: University of Chicago Law Review, 86 (2019) 459.

Gillis, T. B.: False Dreams of Algorithmic Fairness: The Case of Credit Pricing, <https://projects.iq.harvard.edu/fintechlaw/publications/false-dreams-algorithmic-fairness-case-credit-pricing>

Han, J. Pei, J. Kamber, M.: Data Mining: Concepts and Techniques, 2. izdaja, Morgan Kaufman Publishers, San Francisco, 2006, str. 6

Mendoza, I., Bygrave, L. A., The Right Not To Be Subject to Automated Decisions Based on Profiling, v: Universitz of Oslo Faculty of Law Legal Studies Research Paper Series, (2017) 2017-20.

Sartor, G.: The impact of the General Data Protection Regulation (GDPR) on artificial intelligence, European Parlimentary Research Service, Bruselj, 2020.

Pravni viri

[117] Sartor, G.: The impact of the General Data Protection Regulation (GDPR) on artificial intelligence, European Parlimentary Research Service, Bruselj, 2020, str. 7.

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

Zakon o varstvu pred diskriminacijo (Uradni list RS, št. 33/16 in 21/18 – ZNOrg).

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 – Mednarodne pogodbe, št. 7/94).

Pogodba o Evropski uniji, Uradni list Evropske unije, C 326, 26.10.2012, str. 13–390.

Listina Evropske Unije o človekovih pravicah, Uradni list Evropske unije, C 83/389, str 391–407.

Direktiva Sveta 2000/43/ES z dne 29. junija 2000 o izvajanju načela enakega obravnavanja oseb ne glede na raso ali narodnost, Uradni list Evropske unije, L 180, 19.7.2000, str. 22–26.

Direktiva Sveta 2000/78/ES z dne 27. novembra 2000 o splošnih okvirih enakega obravnavanja pri zaposlovanju in delu, Uradni list Evropske unije, L 303, 2.12.2000, str. 16–22.

Direktiva Sveta 2004/113/ES z dne 13. decembra 2004 o izvajanju načela enakega obravnavanja moških in žensk pri dostopu do blaga in storitev ter oskrbi z njimi, Uradni list Evropske unije, L 373, 21.12.2004, str. 37–43.

Direktiva 2006/54/ES Evropskega parlamenta in Sveta z dne 5. julija 2006 o uresničevanju načela enakih možnosti ter enakega obravnavanja moških in žensk pri zaposlovanju in poklicnem delu (preoblikovano), Uradni list Evropske unije, L 204, 26.7.2006, str. 23–36

Uredba (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES (Splošna uredba o varstvu podatkov) (Besedilo velja za EGP), Uradni list Evropske unije, L 119, 4.5.2016, str. 1–88.

Article 29 Data Protection Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016 679.

Article 29 Data Protection Working Party, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, 2017

European Data Protection Board, Guidelines 05/2020 on consent under Regulation 2016/679, version 1.1, 2020

Sodna praksa

C-673/17, *Planet 49,* ECLI:EU:C:2019:801.

C-236/09, *Test-Achats,* ECLI:EU:C:2011:100

C-157/15, *Achbita,* ECLI:EU:C:2017:203

Moustaquim v Belgium, št. 12313/86, ECLI:CE:ECHR:1991:0218JUD001231386.

Thlimmenos v Greece, št. 34369/97, ECLI:CE:ECHR:2000:0406JUD003436997.

Spletni viri

<http://cyberlaw.stanford.edu/blog/2019/02/electronic-contracts-and-illusion-consent> (13.4.2020).

DOI
https://doi.org/10.18690/um.pf.4.2023.6

ISBN
978-961-286-774-4

6 ENAKOST ŽENSK IN MOŠKIH, PRAVICE OTROK IN PRAVICE STAREJŠIH V POVEZAVI Z UMETNO INTELIGENCO

TIJA POJE LUČEV
Univerza v Mariboru, Pravna fakulteta, Maribor, Slovenija
tija.poje@student.um.si

Umetna inteligenca je eno izmed na novo razvitih in obravnavanih področij današnje družbe, za katero je značilno, da živi v informacijski dobi. Ker uporaba umetne inteligence povzroči številne etične dileme, predvsem glede poseganja v človekove pravice, je to področje tudi izredno pravno zanimivo, še posebej glede regulacije umetne inteligence tako, da bi bila ta zaupanja vredna in zakonita. Prispevek temelji na raziskovanju in nato predstavitvi, kako razvoj in uporaba umetne inteligence vplivata na človekove pravice. Raziskovanje je osredotočeno na poseg v tri temeljne človekove pravice, to so pravica do enakosti žensk in moških, pravice otrok in pravice starejših. Tako je v raziskovalni nalogi predstavljeno, kateri akti na mednarodni, evropski in nacionalni ravni določajo varstvo in spoštovanje teh pravic. Nadalje je pojasnjeno, kako umetna inteligenca vpliva na te pravice v praksi in kakšne iniciative se izvajajo z namenom, da se uresniči varstvo teh pravic pred vplivi umetne inteligence ter kakšni ukrepi naj bi se izvedli v prihodnje.

Ključne besede:
umetna inteligenca,
pravica do enakosti žensk in moških,
pravice otrok,
pravice starejših,
regulacija

Univerzitetna založba Univerze v Mariboru

DOI
https://doi.org/
10.18690/um.pf.4.2023.6

ISBN
978-961-286-774-4

6 Equality Between Men and Women, the Rights of Children and the Rights of Elderly in Connection With Artificial Intelligence

Tija Poje Lučev
University of Maribor, Faculty of Law, Maribor, Slovenia
tija.poje@student.um.si

Keywords:
artificial intelligence,
equality of men and women,
children's rights,
rights of the elderly,
regulation

Artificial intelligence is one of the newly developed and addressed areas of today's society, which is characterized by living in the information age. As the use of artificial intelligence raises a number of ethical dilemmas, especially regarding the encroachment on human rights, this area is also extremely interesting from a legal perspective- specially with regard to regulating artificial intelligence so that it is trustworthy and legitimate. The following article is based on research and presents how the development and use of artificial intelligence affect human rights. The research focuses on the interference with the three fundamental human rights, namely the right to equality between women and men, the rights of children and the rights of the elderly. Thus, the research paper shows which acts at the international, European and national level determine the protection and respect of these rights. It further explains how artificial intelligence affects these rights in practice and what initiatives are being taken to protect these rights from the effects of artificial intelligence and what measures should be taken in the future.

University of Maribor Press

6.1 Uvod

Razvoj in uporaba umetne inteligence je novost, ki prinaša posebne izzive, zato je potrebno pripraviti določene etične smernice glede na obstoječi regulativni okvir temeljnih vrednot, na katerih temelji Evropska unija (v nadaljevanju EU), ali pa celo postaviti neka nova regulativna pravila. Toda vnaprejšnja *ex ante* regulacija področja je težavna zaradi določenih značilnosti raziskovanja umetne inteligence in umetne inteligence same. Kljub temu bosta samo na tak način, s spoštovanjem etičnih vrednot, lahko razvoj in uporaba umetne inteligence veljala za zaupanja vredna.[1] Pri doseganju zaupanja vredne umetne inteligence je tako pomembno, da se z njeno uporabo spoštujejo temeljne človekove pravice. Te so bistven element vsake posamezne države, ki želi biti pravna in socialna država. Zato je pomembno, da je umetna inteligenca zakonita in da spoštuje vse pravne predpise, vključno s tistimi, ki predpisujejo spoštovanje človekovih pravic. V okviru tega se mora spoštovati tudi etična načela in vrednote. Ker ima umetna inteligenca že trenutno in bo še posebej v bližnji prihodnosti imela velik vpliv na posameznega človeka in njegove pravice, se je ob zavedanju tega začelo tako na mednarodni ravni in ravni EU, kot tudi na nacionalni ravni sprejemati različne ukrepe za ureditev zaupanja vredne umetne inteligence. Podlaga za to so temeljne človekove pravice in zato je potrebno sprejeti tudi ukrepe, ki bodo uresničili ustrezno spoštovanje potencialno ranljivih oseb in skupin, med katere med drugim sodijo tudi ženske, otroci in starejši. Pravice teh treh skupin oseb, in vpliv umetne inteligence nanje, bodo predstavljene v nadaljevanju.

6.2 Enakost žensk in moških

6.2.1 Pravni okvir: prepoved diskriminacije glede na spol

Ena temeljnih človekovih pravic je prepoved diskriminacije. Pravica do enakosti in zaščita pred diskriminacijo je univerzalna pravica, ki je urejena na nacionalni, evropski in mednarodni ravni. Urejajo jo Splošna deklaracija o človekovih pravicah[2], Konvencija ZN o odpravi vseh oblik diskriminacije žensk[3] in tudi Konvencija

[1] Gre za koncept, ki ga na ravni Evropske Unije pripravlja Evropska Komisija. V okviru tega je ustanovila strokovno skupino na visoki ravni, ki je aprila 2019 objavila smernice za zaupanja vredno umetno inteligenco. V februarju 2020 je EK izdala Belo knjigo o umetni inteligenci, kjer je smisel tega koncepta okvirno predstavljen.
[2] Sklep o objavi besedila Splošne deklaracije človekovih pravic (Uradni list RS – Mednarodne pogodbe, št. 3/18).
[3] Zakon o ratifikaciji Konvencije ZN o odpravi vseh oblik diskriminacije žensk (Uradni list SFRJ – Mednarodne pogodbe št. 11/81) in Akt o notifikaciji nasledstva glede konvencij Organizacije združenih narodov in konvencij,

Mednarodne organizacije dela, ki še posebej prepoveduje diskriminacijo na področju dela in zaposlovanja.[4]

Evropska konvencija o varstvu človekovih pravic (v nadaljevanju EKČP)[5] v 14. členu določa, da je uživanje pravic in svoboščin zagotovljeno vsem ljudem brez razlikovanja glede na spol, raso, barvo kože, jezik, vero, politično ali drugo prepričanje, narodnostni ali socialni izvor, pripadnost narodni manjšini, lastnino, rojstvo ali kakšne druge okoliščine. Torej prepovedano je kakršnokoli razlikovanje glede na spol, kar pomeni, da mora biti tudi pri uporabi umetne inteligence zagotovljena enakost žensk in moških. Pri umetni inteligenci enakost pomeni, da delovanje sistema ne sme dati nepošteno pristranskih rezultatov. V preprečevanju nepoštene pristranskosti se poleg pravice do enakosti, odraža tudi načelo pravičnosti. Zato je potrebno z ukrepi ureditve umetne inteligence spodbujati enake možnosti v smislu dostopa do zaposlovanja, blaga in storitev. Pravica do enakosti je tudi ena izmed vrednot na katerih temelji EU (2. člen Pogodbe o Evropski uniji[6] - v nadaljevanju PEU) in se zato bori proti diskriminaciji ter spodbuja enakost žensk in moških (3. člen PEU). V skladu z 8. členom Pogodbe o delovanju EU[7] (v nadaljevanju PDEU) si mora EU v vseh svojih dejavnostih prizadevati odpravljati neenakosti in spodbujati enakost med moškimi in ženskami ter 19. člen PDEU določa, da je Svet tisti, ki lahko po posebnem zakonodajnem postopku in po odobritvi Evropskega parlamenta soglasno sprejme ustrezne ukrepe za boj proti diskriminaciji na podlagi spola, rase ali narodnosti, vere ali prepričanja, invalidnosti, starosti ali spolne usmerjenost Podobno kot EKČP, tudi Listina EU o temeljnih pravicah (v nadaljevanju Listina EU)[8] v 21. členu določa, da je prepovedana vsakršna diskriminacija na podlagi spola, rase, barve kože, etničnega ali socialnega porekla, genetskih značilnosti, jezika, vere ali prepričanja, političnega ali drugega mnenja, pripadnosti narodnostni manjšini, premoženja, rojstva, invalidnosti, starosti ali

sprejetih v Mednarodni agenciji za atomsko energijo (Uradni list RS – Mednarodne pogodbe, št. 9/92, 9/93, 5/99, 9/08, 13/11, 9/13 in 5/17).

[4] Konvencija št. 111 o diskriminaciji pri zaposlovanju in poklicih - Akt o notifikaciji nasledstva glede konvencij UNESCO, mednarodnih večstranskih pogodb o zračnem prometu, konvencij mednarodne organizacije dela, konvencij mednarodne pomorske organizacije, carinskih konvencij in nekaterih drugih mednarodnih večstranskih pogodb (Uradni list RS – Mednarodne pogodbe, št. 15/92, 1/97 in 17/15).

[5] 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 – Mednarodne pogodbe, št. 7/94).

[6] Pogodba o Evropski uniji, Uradni list Evropske unije, C 326, 26.10.2012, str. 13–390.

[7] Pogodba o delovanju Evropske Unije, Uradni list Evropske unije, C 326/47, str. 47-390.

[8] Listina Evropske Unije o človekovih pravicah, Uradni list Evropske unije, C 83/389, str. 391–407.

spolne usmerjenosti. Listina EU posebej ureja tudi prej omenjeno področje enakosti pri dostopanju do zaposlovanja, blaga in storitve ter v 23. členu določa, da se mora enakost žensk in moških zagotoviti na vseh področjih, vključno z zaposlovanjem, delom in plačilom za delo. Nadalje je v drugem odstavku istega člena določeno, da načelo enakosti ne preprečuje ohranitve ali sprejetja ukrepov o specifičnih ugodnostih v korist nezadostno zastopanega spola. Torej vsi ukrepi sprejeti zgolj v korist žensk, z namenom, da se doseže enakost, so v skladu s tem drugim odstavkom. Glede na navedene določbe vidimo, da primarno pravo EU, to so obe Pogodbi in Listina, določa spoštovanje načela enakega obravnavanja in je to eno temeljnih načel na katerih EU temelji. V skladu z ustaljeno sodno prakso Sodišča to načelo terja, da se primerljivi položaji ne obravnavajo različno in da se različni položaji ne obravnavajo enako, razen če je tako obravnavanje objektivno upravičeno in primerljivost položajev je treba presojati glede na cilj in namen akta Unije, s katerim je uvedeno zadevno razlikovanje.[9] Takšno obravnavo izpostavlja tudi Sodišče EU v zadevi Association Belge des Consommateurs Test-Achats in drugi[10] ter je zato v tej zadevi odločilo, da so določbe, ki bi zadevnim državam članicam omogočale odstopanja od pravila enakih premij in dajatev za oba spola v nasprotju z uresničevanjem cilja enakega obravnavanja žensk in moških. Kajti za namene uporabe načela enakega obravnavanja žensk in moških, sta položaj žensk in položaj moških glede premij in dajatev zavarovanj, ki jih ti sklenejo, primerljiva.

Sekundarno pravo, ki na ravni EU uresničuje načelo enakega obravnavanja, določeno v primarnem pravu EU, vključuje Direktivo Sveta 2000/78/ES o splošnih okvirih enakega obravnavanja pri zaposlovanju in delu[11] (v nadaljevanju: Direktiva 2000/78/ES), Direktivo Sveta 2004/113/ES o izvajanju načela enakega obravnavanja moških in žensk pri dostopu do blaga in storitev ter oskrbi z njimi[12] (v nadaljevanju: Direktiva 2004/113/ES) in Direktivo 2006/54/ES Evropskega parlamenta in Sveta o uresničevanju načela enakih možnosti ter enakega

[9] Glej zadevo C-127/07, *Arcelor Atlantique et Lorraine in drugi*, ECLI:EU:C:2008:728, točka 23.
[10] Zadeva C-236/09 , *Association Belge des Consommateurs Test-Achats in drugi*, ECLI:EU:C:2011:100.
[11] Direktiva Sveta 2000/78/ES z dne 27. novembra 2000 o splošnih okvirih enakega obravnavanja pri zaposlovanju in delu, Uradni list Evropske unije, L 303, 2.12.2000.
[12] Direktiva Sveta 2004/113/ES z dne 13. decembra 2004 o izvajanju načela enakega obravnavanja moških in žensk pri dostopu do blaga in storitev ter oskrbi z njimi, Uradni list Evropske unije, L 373, 21. 12. 2004.

obravnavanja moških in žensk pri zaposlovanju in poklicnem delu[13] (v nadaljevanju: Direktiva 2006/54/ES).

Tudi na nacionalni ravni je urejena pravica do prepovedi diskriminacije. Ker gre za temeljno pravico, je urejena že na ustavni ravni. Tako 14. člen Ustave Republike Slovenije[14] (v nadaljevanju: Ustava RS) določa, da so v Sloveniji vsakomur zagotovljene enake človekove pravice in temeljne svoboščine, ne glede na narodnost, raso, spol, jezik, vero, politično ali drugo prepričanje, gmotno stanje, rojstvo, izobrazbo, družbeni položaj, invalidnost ali katerokoli drugo osebno okoliščino. Varstvo oseb pred diskriminacijo, tudi glede na spol, konkretneje ureja Zakon o varstvu pred diskriminacijo (ZVarD),[15] s katerim se je v slovenski pravni red implementiralo prej omenjene Direktivo 2000/78/ES, Direktivo 2004/113/ES in Direktivo 2006/54/ES.V prvem odstavku 2. člena ta zakon določa, da je treba zagotoviti enako obravnavanje, zlasti med drugim tudi v zvezi s pogoji za dostop do zaposlitve in z dostopom do dobrin in storitev. V primeru, da oseba meni, da je ali je bila diskriminirana, lahko s tožbo zahteva prenehanje diskriminacije in izplačilo nadomestila zaradi diskriminacije oziroma objavo sodbe (1. odst. 39.člena ZVarD). Podrobneje je enakost med spoloma urejena v Zakonu o enakih možnostih žensk in moških[16].

6.2.2 Diskriminacija glede na spol v praksi

Spoštovanje pravice do enakosti žensk in moških sicer predvideva naveden pravni okvir, vendar pa je vprašanje, koliko se to resnično spoštuje tudi v praksi. Kot kažejo študije se predvideva, da bo od delavcev več kot 57% žensk, na katere bo vplivala uporaba digitalizacije na delovnem področju.[17] Kritična je izguba delovnih mest v vseh kategorijah, ki so tradicionalno zagotavljala ženskam dostop do trga dela. Še predvsem predstavlja veliko tveganje za gospodinjstva z eno zaposleno osebo, ki jih

[13] Direktiva 2006/54/ES Evropskega parlamenta in Sveta z dne 5. julija 2006 o uresničevanju načela enakih možnosti ter enakega obravnavanja moških in žensk pri zaposlovanju in poklicnem delu (preoblikovano), Uradni list Evropske unije, L 204 , 26. 7. 2006.
[14] Ustava Republike Slovenije (Uradni list RS, št. 33/91-I, 42/97 – UZS68, 66/00 – UZ80, 24/03 – UZ3a, 47, 68, 69/04 – UZ14, 69/04 – UZ43, 69/04 – UZ50, 68/06 – UZ121,140,143, 47/13 – UZ148, 47/13 – UZ90,97,99 in 75/16 – UZ70a).
[15] Zakon o varstvu pred diskriminacijo (Uradni list RS, št. 33/16 in 21/18 – ZNOrg).
[16] Zakon o enakih možnostih žensk in moških (Uradni list RS, št. 59/02, 61/07 – ZUNEO-A, 33/16 – ZVarD in 59/19).
[17] EU report on the future of work, str. 48, <https://ec.europa.eu/digital-single-market/en/news/future-work-work-future> (8.4.2020).

vodijo nizko izobražene ženske.[18] Prav tako naj bi zaradi uporabe umetne inteligence izgubilo svojo službo dvakrat več žensk kot moških. V čem se skrivajo razlogi za to? Značilno je, da se še danes ženske bolj zaposluje na delovnih mestih, za katere je večja verjetnost, da bo prišlo do avtomatizacije.[19] Za primer lahko vzamemo delovno mesto prodajalca v trgovini, kjer je kar 73% zaposlenih ženskega spola.[20] Nadalje se neenakost kaže tudi pri izobrazbi. Na področju EU ima samo 24 od 1000 žensk z informacijsko in komunikacijsko tehnologijo (v nadaljevanju IKT) povezano izobrazbo.[21] Že zdaj je manj žensk zaposlenih v delovnih mestih povezanih z IKT, vendar pa se ta razlika manjša.[22] Uporaba umetne inteligence pri izbiranju med kandidati za delo, katerega se bo zaposlilo, lahko prav tako vodi do pristranskosti in neenakosti. Družbe, kot so Pepsi, Amazon in Ikea so le nekatere od mnogih (število le teh se veča), ki so preizkusile ali uporabile algoritme, da odločijo o tem, koga naj zaposlijo.[23] Tako je na primer, družba Amazon svoje delavce izbirala in zaposlovala s pomočjo uporabe umetne inteligence, katere algoritmi so se kasneje izkazali, da so favorizirali kanditate moškega spola.[24] Algoritmi so bili namreč zasnovani na podlagi vzorcev v življenjepisih, poslanih Amazonu v zadnjih desetih letih, katere so večinoma poslali moški, kar je odraz moške prevlade v tehnološkem sektorju.[25] Ko pride do neenakega obravnavanja kot posledica uporabe umetne inteligence, se srečamo s pomembnim problemom: koga naj neenako obravnavana oseba toži? Na primer, ženska, ki je bila neenako obravnavana zaradi uporabe avtomatiziranega zaposlovanja, bo težko verjetno tožila delodajalca, saj ni on diskriminiral. To pomeni, da značilnosti umetne inteligence ogrožajo nekatre vidike okvirov za odgovornost na ravni Unije, kot tudi na nacionalni ravni in bi lahko zmanjšale njihovo učinkovitost. Ker bi bilo škodo težko povezati s človeškim ravnanjem, v tem primeru z ravnanjem delodajalcem, bi bilo utemeljevanje odškodninskih

[18] Klaus S.: Četrta industrijska revolucija, prevedel Igor Pauletič, World Economic Forum, Ženeva, 2016, str.55, <http://assets.cdnma.com/8475/assets/Cetrta-industrijska-revolucija.pdf> (13.4.2020).
[19] EU report on the future of work, str. 48, < https://ec.europa.eu/digital-single-market/en/news/future-work-work-future> (8.4.2020).
[20] Taylor, K.: Women are twice as likely than men to lose their jobs to robots, 26.6.2017 <https://www.businessinsider.com/women-twice-as-likely-as-men-to-lose-their-jobs-to-automation-2017-6> (8.4.2020).
[21] <https://ec.europa.eu/digital-single-market/en/women-ict> (15.4.2020).
[22] Women in digital age - final report (2018),
<https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=50224> (21.4.2020).
[23] Holmes A.: AI could be the key to ending discrimination in hiring, but experts warn it can be just as biased as humans, https://www.businessinsider.nl/ai-hiring-tools-biased-as-humans-experts-warn-2019-10/ (27.6.2020).
[24] Manyika J., Silberg J., Presten B.: What do we do about the biases in AI., <https://hbr.org/2019/10/what-do-we-do-about-the-biases-in-ai> (19.5.2020).
[25] <https://www.euronews.com/2018/10/10/amazon-scraps-secret-ai-recruiting-tool-that-showed-bias-against-women> (25.5.2020).

zahtevkov težavno in predrago, oškodovanci pa bi morda ostali brez primerne odškodnine.[26] Zaradi kompleksnosti umetne inteligence in vključitve več akterjev pri razvoju in uporabi umetne inteligence, bi lahko oškodovancem bilo težko identificirati odgovorno osebo in dokazati vsa dejstva za uveljavanje odškodninskega zahtevka. Poleg tega ne bi bilo jasno, kako dokazati krivdo, kadar umetna inteligenca deluje avtonomno, ali kaj se šteje za napako osebe, ki se zanaša na uporabo umetne inteligence.[27] Dokazovanje, da je algoritem diskriminiral, je zahtevno.[28] Situacijo še dodatno zaplete odsotnost sodne prakse na tem področju. Zato se strinjam s Komisijo, ko v Poročilu o vprašanjih varnosti in odgovornosti, ki jih sprožajo umetna inteligenca, internet stvari in robotika,[29] navaja, da bi v skladu s poročilom[30] podskupine za nove tehnologije v okviru strokovne skupine za odgovornost in nove tehnologije veljalo razmisliti o prilagoditvi nacionalnih zakonov za olajšanje dokaznega bremena žrtev škode, povezane z umetno inteligenco. Veljalo bi lahko obrnjeno dokazno breme, da dokazuje povzročitelj škode. Glede na prej omenjeni primer, ko pride do pristranskosti pri izbiri kandidata z uporabo umetne inteligence, menim, da bi tu lahko prišla v poštev odgovornost delodajalca. Ne krivdna, ampak koncept objektivne odškodninske odgovornosti. Kajti on je tisti, ki je dovolil uporabo pristranske umetne inteligence, zato bi moral za to dejanje odgovarjati objektivno. Ali pa vsaj solidarno odgovarjati s tistim, ki je razvil pristransko umetno inteligenco. Še večji problem je, ko kandidatke za razpisano delo sploh ne vedo, da je postopek izbire potekal na način uporabe umetne inteligence in tako niti ne vedo, da je bila mogoče kršena njihova pravica do enake obravnave zaradi pristranske umetne inteligence. Menim, da jih je zato v okviru njihovih pravic potrebno opozoriti, da so v stiku z umetno inteligenco. Pravico do tega, to je seznanitve posameznika o tem, da se njegovi podatki obdelujejo na podlagi avtomatiziranega sprejemanja odločitev, jim zagotavlja že Uredba (EU) 2016/679 Evropskega parlamenta in Sveta o varstvu posameznikov pri obdelavi osebnih podatkov in o

[26] Komisija, Poročilo vprašanjih varnosti in odgovornosti, ki jih sprožajo umetna inteligenca, internet stvari in robotika, COM(2020) 64 final, str.13.
[27] Ibidem, str 15.
[28] Agencija Evropske unije za temeljne pravice (FRA), #BigData: Discrimination in data-supported decisionmaking, 2018, str. 7, <https://fra.europa.eu/en/publication/2018/bigdata-discrimination-data-supported-decision-making> (27.6.2020).
[29] Ibidem, str. 14.
[30] Expert Group on Liability and New Technologies – New Technologies Formatio, Liability for Artificial Intelligence and other emerging technologies, 2019, dostopno na <https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=63199> (27.6.2020).

prostem pretoku takih podatkov (v nadaljevanju Splošna uredba o varstvu podatkov).[31]

Do neenakosti prihaja tudi pri pošiljanju personaliziranih oglasov preko digitalnih medijev, saj imajo ženske manjše možnosti, da bodo prišle v stik z oglasi za delovna mesta z višjo plačo in določenih karier, saj umetna inteligenca poveže določene kariere zgolj z moškimi, saj je že sedaj tam večina zaposlenih moških. Za primer lahko vzamemo dogodek, ko je Facebook oglase za bolje plačana dela objavljal oziroma prikazoval moškim uporabnikom te aplikacije, medtem, ko je ženskam prikazoval oglase za manj plačana dela.[32] Navedeno prikazuje dejstvo, da se neenakost med spoloma kaže tudi že v samem razvoju umetne inteligence, kjer prihaja do pomanjkanja žensk.[33] Glede na navedeno, me ne preseneča dejstvo, da se bo neenkost kazala tudi pri uporabi umetne inteligence. Saj če je že v samem procesu razvijanja, ki ga opravlja človek in je ta v večini primerov moškega spola, prisotna pristranskost glede spola, potem bo tudi rezultat, ki se bo kazal v umetni inteligenci, pristranski.[34] Torej algoritme, kot tudi orodja umetne inteligence, razvija človek in ti so pristranski tolikor kolikor so pristranske osebe, ki jih razvijajo. Ker je za umetno inteligenco značilno, da se uči od že prej obstoječih podatkov, ki jih je ustvaril človek, je torej ta pristranska, če so že ti prej obstoječi podatki pristranski. Odraz tega je na primer mogoče opaziti, ko se uporabi umetno inteligenco pri izbiri kandidata za delo. Če se gradi model na podlagi skupnih značilnosti podatkov glede trenutno zaposlenih in trenutne delovne sile, ki ni raznolika, tudi umetna inteligenca ne bo izbirala raznolikih kandidatov. Ali pa bo odražala dejstvo, da so delodajalci tradicionalno preferirali moške kandidate nad ženskimi kandidatkami.[35] Še večji problem nastane, če ti algoritmi niso zasnovani za samo enkratno odločanje, ampak so primerni za daljše obdobje. Ker odločitve, ki temeljijo na algoritimih, oblikujejo podatke za naslednji oziroma prihodnji algoritem, ki se bo na podlagi teh podatkov učil, to pomeni da se bo neenakost vedno znova ponavljala. Nadaljna presoja bo

[31] Uredba (EU) 2016/679 Evropskega Parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES, UL L 119, 4.5.2016; Glej drugi odstavek, točka f 13. člena in prvi odstavek, točka h 15. člena Splošne uredbe o varstvu podatkov.

[32] Rodriguez Martinez M., Gaubert J.: International Women day: how can algorithms be sexist, 2020, <https://www.euronews.com/2020/03/08/international-women-s-day-our-algorithms-are-sexist> (25.5.2020).

[33] Women in digital age - final report (2018), <https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=50224> (21.4.2020), str. 132.

[34] Ibidem.

[35] Holmes, A.: AI could be the key to ending discrimination in hiring, but experts warn it can be just as biased as humans.

temeljila zgolj na algoritmih, kar v primeru zaposlovanja pomeni, da bodo algoritmi odločali zgolj na podlagi povratnih informacij o osebah z določenimi lastnostmi, ki so bile že predhodno izbrane. Zato je pomembno, da se bo algoritme analizirano, povratne informacije podrobno ocenjevalo, in se posledično ugotovi ali je potrebno algoritme popraviti, da se prepreči diskriminacijo in na koncu doseže natančnejše rezultate.[36] Nasprotno pa se lahko umetno inteligenco uporabi za izničeneje pristranskosti pri zaposlovanju. Če že ni mogoče odpraviti človeške pristranskosti, je pa mogoče odpraviti pristranskost v umetni inteligenci. Ker jo lahko oblikujejmo, to pomeni, da lahko odstranimo pomankljivosti, in jo naredimo pravično. Da bi to dosegli, bi morali slediti ideji testiranja izdelkov preden se jih da v promet. Za primer vzemimo novi avto. Preden ga bo nekdo vozil, ga je potrebno varnostno testirati. Če ne dosega standardov varnosti, je potrebno to odpraviti in avto popraviti. Tako bi se tudi orodja umetne inteligence moralo prej testirati. Če se ne doseže standarda pravičnosti, je to potrebno odpraviti preden se orodja umetne inteligence da v promet ter se jih začne uporabljati.[37]

Neenakost se ne kaže samo na področju zaposlovanja, dela in izobrazbe v zvezi z digitalizacijo. Mogoče je zaslediti neenakost tudi v zvezi z nasiljem na internetu, saj je tega deležno veliko več žensk in deklet, kot pa moških.[38] Prav tako se neenakost pojavlja pri digitalni vključenosti. Glede na raziskave je več žensk, ki še nikoli ni uporabljalo interneta, kot pa moških.[39] Gre predvsem za ženske z nižjo izobrazbo. Posledično to pomeni, da podatki, ustvarjeni na internetu, ne predstavljajo določene skupine oseb, kar pa predstavlja prikrajšanost žensk in lahko vodi do prepovedane diskriminacije.

[36] Agencija Evropske unije za temeljne pravice (FRA), #BigData: Discrimination in data-supported decisionmaking, 2018, str. 7, <https://fra.europa.eu/en/publication/2018/bigdata-discrimination-data-supported-decision-making> (27.6.2020), str.10.
[37] Polli F.: Using AI to Eliminate Bias from Hiring, 2019, <https://hbr.org/2019/10/using-ai-to-eliminate-bias-from-hiring> (27.6.2020).
[38] Sample I.: Internet 'is not working for women and girls', says Berners-Lee, 2020, <https://www.theguardian.com/global/2020/mar/12/internet-not-working-women-girls-tim-berners-lee> (24.4.2020).
[39] FRA, Data quality and artificial intelligence – mitigating bias and error to protect fundamental rights, 2019, <https://fra.europa.eu/en/publication/2019/data-quality-and-artificial-intelligence-mitigating-bias-and-error-protect> (30.5.2020).

Neenakosti glede na spol je mogoče zaznati tudi pri uporabi tehnologije za prepoznavanje obraza. Glede na rezultate študij je veliko tehnologij za prepoznavanje obrazov pristranskih.[40] Nadalje raziskava kaže na to, da bo tehnologija za prepoznavanje obrazov imela veliko več težav pri identifikaciji žensk kot pa moških, še posebej pri ženskah temnejše polti. Te težave se izkazujejo v tem, da tehnologija napačno identificira.

Vse navedeno ogroža uspeh pri enakosti med spoloma, ki je bil dosežen do danes. Izhajajoč iz navedenega lahko opazimo, da je še vedno dandanes, in tudi bo v prihodnje prisotna neenakost pri zaposlovanju. Te razlike, ki nastopijo kot posledica uporabe tehnologije, kažejo na to, da je neenakost med spoloma v digitalni dobi posledica vztrajanja močnih in nezavednih pristranskosti glede tega, katero delovno mesto je primerno za določen spol in kdo je česa zmožen pri posameznem delu. Toda, ali gre res za nezavedno dejanje? V vsakem primeru je neizogibno, da bo uporaba tehnologije povzročila družbene in kulturne spremembe na tem področju.

6.2.3 Iniciative v zvezi z razlikami glede spola

Razlik glede spola in posledic le tega se zaveda tudi Evropska komisija, zato si je za cilj zadala, da naj bi se na področju Evropske unije sprejeli akti, s katerimi naj bi se v področje dela povezanih z digitalizacijo, vključevalo več žensk.[41] Eden izmed korakov proti temu je Digital Education Action plan, ki spodbuja ženske k temu, da se izobražujejo za delovna mesta povezana z IKT.[42] Prav tako je do 9.4.2019 27 držav (med njimi tudi Slovenija) podpisalo Deklaracijo žensk v digitalnem svetu.[43] Cilj te je povečati politično prednost premajhne zastopanosti žensk v digitalni ekonomiji. Prav tako se k podpisu poziva posamezna podjetja, ki naj tako pomagajo zapreti luknjo pri zaposlovanju žensk in moških v digitalizaciji.[44]

---

[40] Singer N., Metz C.: Many Facial-Recognition Systems Are Biased, Says U.S. Study, 2019, <https://www.google.com/url?sa=t&source=web&rct=j&url=https://www.nytimes.com/2019/12/19/technology/facial-recognition-bias.amp.html&ved=2ahUKEwjqwsK3pvjpAhVh7aYKHd3KB4kQFjAAegQIAhAB&usg=AOvVaw3w9XvA0vHBmnnhh_4HQ833&ampcf=1> (10.6.2020).

[41] <https://ec.europa.eu/digital-single-market/en/women-ict> (20.4.2020).

[42] <https://ec.europa.eu/digital-single-market/en/women-ict> (20.4.2020).

[43] Deklaracija je dostopna na <https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=58562> (20.4.2020).

[44] <https://ec.europa.eu/digital-single-market/en/women-ict> (20.4.2020).

Na evropski ravni se bo pri oblikovanju zakonite umetne inteligence moralo upoštevati Direktivo 2006/54/ES. To direktivo navaja Bela knjiga o umetni inteligenci,[45] ko opredeljuje regulativni okvir za umetno inteligenco in možne prilagoditve pravnega okvira v zvezi z umetno inteligenco. Bela knjiga nadalje navaja, da si je še posebej treba prizadevati za povečanje števila žensk, ki se usposabljajo in so zaposlene na tem področju. Prav tako navaja, da naj se sistemi umetne inteligence učijo iz nabora podatkov, ki je dovolj reprezentativni in v katerem so ustrezno zastopani vidiki spola. Glede ureditve umetne inteligence na področju enakosti dostopa do blaga in storitev, pa bo potrebno upoštevati Direktivo 2004/113/ES. V poštev pride še Resolucija Evropskega parlamenta o enakosti spolov in krepitvi vloge žensk v digitalni dobi,[46] v kateri Parlament poziva Evropsko komisijo in države članice k sprejemu ukrepov, katerih cilj je krepitev dostopa žensk do informacijske družbe, izboljšanje in povečanje uporabe informacijske in komunikacijske tehnologije, povečanje vloge žensk v sektorju IKT, spodbujanje znanja na področju IKT med ženskami, in sicer prek izobraževanja in usposabljanja, spodbujanje zaposlovanja in podjetniškega duha med ženskami z redno uporabo interneta in digitalnih storitev, razvoj spletnih vsebin, ki spodbujajo enakost spolov, omogočanje stalne izmenjave in širjenja informacij ter posredovanja vrednot o enakosti spolov, spodbujanje dostopa do informacijske in komunikacijske tehnologije in njihove uporabe kot orodja za boj proti diskriminaciji in nasilju na podlagi spola, spodbujanje mednarodnega sodelovanja, usklajevanje poklicnega in zasebnega življenja ter oblikovanje, izvajanje, razširjanje in vrednotenje politik in načrtov na področju enakosti spolov. K temu poziva iz naslednjih razlogov, ki jih v resoluciji izpostavi. Navaja, da lahko obenem digitalizacija trga dela ustvari novo razsežnost izključenosti, med njimi tudi tveganje spolne segregacije. Nadalje navaja, da je velika razlika med spoloma pri dostopu do poklicnih in izobraževalnih možnosti na področju informacijske in komunikacijske tehnologije ter računalniškega znanja in da je digitalna doba povečala kakršnekoli oblike zlorab in nasilja nad ženskami. Nadalje v pošev pride tudi Resolucija Evropskega parlamenta z dne 17. aprila 2018 o krepitvi vloge in položaja žensk in deklet prek digitalnega sektorja[47], v kateri Parlament poziva Komisijo in države članice k izvajanju podobnih ukrepov zaradi

[45] Evropska komisija, BELA KNJIGA o umetni inteligenci - evropski pristop k odličnosti in zaupanju, COM(2020) 65 final.
[46] Resolucija Evropskega parlamenta z dne 28. aprila 2016 o enakosti spolov in krepitvi vloge žensk v digitalni dobi (2015/2007(INI)), Uradni list Evropske unije, C 66, 21.2.2018.
[47] Resolucija Evropskega parlamenta z dne 17. aprila 2018 o krepitvi vloge in položaja žensk in deklet prek digitalnega sektorja (2017/3016(RSP)), Uradni list Evropske unije, C 390, 18.11.2019.

podobnih razlogov, kot v prej omenjeni Resoluciji. Nazadnje bo v poštev prišla tudi Resolucija Evropskega parlamenta o celoviti evropski industrijski politiki na področju umetne inteligence in robotike,[48] v kateri Parlament podarja, da z umetno inteligenco prihajajo tudi izzivi v zvezi z zagotavljanjem nediskriminacije. Poudarja tudi pomen kakovosti podatkov, saj lahko uporaba zastarelih, nepopolnih ali nepravilnih podatkov slabe kakovosti privede do slabih napovedi in posledično do diskriminacije in pristranskosti. Poleg tega poudarja še, da je treba pri razširjanju umetne inteligence in robotike v celoti upoštevati človekove pravice, v strojih in robotih pa se nikakor ne bi smeli odražati stereotipi glede žensk ali druge oblike diskriminacije. Parlament opozarja tudi, da sistemi umetne inteligence ne bi smeli ustvarjati ali krepiti pristranskosti in tako poudarja, da je treba pri razvoju in uporabi algoritmov v vse faze, od zasnove do izvajanja, vključiti premisleke o pristranskosti in pravičnosti ter da je treba zato podatkovne nize in algoritme redno preverjati, da bi zagotovili natančno sprejemanje odločitev. Zato Parlament poziva Komisijo, države članice in organe za varstvo podatkov, naj odkrivajo diskriminacijo in pristranskost v algoritmih in si ju po najboljših močeh prizadevajo zmanjšati ter naj zasnujejo trden skupni etični okvir za pregledno obdelavo osebnih podatkov in avtomatizirano odločanje, ki bo usmerjal uporabo podatkov in izvrševanje zakonodaje Unije. Komisijo in države članice, poziva še, naj preučijo oblikovanje evropske regulativne agencije za umetno inteligenco in algoritemsko odločanje, med drugim tudi z nalogo preiskave domnevnih primerov kršitev pravic s strani algoritemskih sistemov odločanja, tako za posamezne odločitve (na primer posamezna odstopanja), kot tudi za statistične vzorce odločanja (na primer diskriminatorna pristranskost). Na ravni Evropske Unije je ustanovljena institucija za enakost med spoloma -European Institute for Gender Equality, ki skrbi, da se to pravico do enakosti spoštuje.

Na nacionalni ravni je bila v skladu s 15. členom Zakona o enakih možnostih žensk in moških sprejeta Resolucija o nacionalnem programu za enake možnosti žensk in moških 2015-2020.[49] Gre za strateški dokument vlade Slovenije, ki določa cilje in ukrepe ter ključne nosilce politik za uresničevanje enakosti spolov na posameznih področjih življenja žensk in moških v Republiki Sloveniji za obdobje od 2015 do 2020. Ta med ključnimi cilji navaja med drugim tudi odpravo neravnovesij med

[48] Resolucija Evropskega parlamenta z dne 12. februarja 2019 o celoviti evropski industrijski politiki na področju umetne inteligence in robotike (2018/2088(INI)).
[49] Resolucija o nacionalnem programu za enake možnosti žensk in moških 2015–2020 (Uradni list RS, št. 84/15).

spoloma ter spolne segregacije na področju zaposlovanja in odpravo neenakosti v izobraževanju in znanosti. Za uresničevanje teh ciljev navaja tudi določene ukrepe v tej smeri. Tako naj bi se oblikovalo programe in projekte za spodbujanje žensk k izbiri poklicev v perspektivnih sektorjih, kot je tudi IKT. Nadalje naj bi se mlade spodbujalo k izobraževanju v sektorju visokih tehnologij, pri čemer so ženske velik potencial. Kot pomembno vlogo pri oblikovanju teh programov izpostavlja raziskave o enakosti spolov, katerih je na področju Slovenije malo. Zato je eden od sprejetih ukrepov tudi spodbujanje in podpora raziskavam.

Veliko vlogo pri preprečevanju diskriminacije pa nimajo samo države s svojo politko in pravnim redom, ampak tudi družbe, ki ustvarjajo oziroma razvijajo tehnologijo. Tako je na primer v zadnjem času velik korak v smeri zmanjševanja negativnih učinkov na področju pristranske umetne inteligence storila družba IMB s svojo odločitvijo, da preneha z ustvarjanjem in prodajo tehnologije za prepoznavanje obrazov.[50] Gre za prvi korak proti odgovornosti družb za promoviranje umetne inteligence, ki je pravična in odgovorna. Takšnim ukrepom je sledil tudi Amazon, ko je sprejel odločitev, da za eno leto prepove uporabo svoje tehnologije za prepoznavanje obrazov Rekognition.[51] Amazon upa, da bo vlada ta čas izkoristila za sprejetje močnejših ukrepov in pravil za bolj etično in pravičnejšo uporabo tehnologije za prepoznavanje obrazov. To pomanjkanje močne pravne ureditve kaže na dejstvo, da ne glede na to, kaj velike družbe na tem področju počnejo, je tehnologija za prepoznavanje obrazov zaradi pomanjkljive pravne ureditve dostopna za zlorabo in nepravilno uporabo.

[50] Hern A.: IBM quits facial-recognition market over police racial-profiling concerns, 2020, <https://www.google.com/amp/s/amp.theguardian.com/technology/2020/jun/09/ibm-quits-facial-recognition-market-over-law-enforcement-concerns> (10.6.2020).
[51] Levy A., Hirsch L.: Amazon bans police use of facial recognition technology for one year, 2020, <https://www.google.com/amp/s/www.cnbc.com/amp/2020/06/10/amazon-bans-police-use-of-facial-recognition-technology-for-one-year.html> (10.6.2020).

6.3 Pravice otrok

6.3.1 Pravni okvir

Na mednarodni ravni otrokom[52] njihove temeljne pravice zagotavlja Konvencija ZN o otrokovih pravicah[53] (v nadaljevanju: Konvencija). V povezavi njihovih pravic z digitalizacijo, predvsem pravice do zasebnosti, dostojanstva in zaščite pred kakršnokoli obliko napada, je pomemben 16. člen Konvencije, ki določa, da noben otrok ne sme biti izpostavljen samovoljnemu ali nezakonitemu vmešavanju v njegovo zasebno življenje, družino, dom ali dopisovanje, niti nezakonitim napadom za njegovo čast in ugled (1. odst.). Proti takšnemu vmešavanju ali napadom ima otrok pravico do zakonitega varstva (2.odst.). Nadalje jim na mednarodni ravni temeljne pravice zagotavlja tudi EKČP, po kateri imajo v skladu z 8. členom zagotovljeno pravico do spoštovanja njihovega zasebnega in družinskega življenja, doma in dopisovanja. Na ravni EU jim pravice zagotavlja Listina EU. Tako 24. člen Listine EU določa, da imajo otroci pravico do potrebnega varstva in skrbi za zagotovitev njihove dobrobiti. Ti svoje mnenje svobodno izražajo. V skladu z 8. členom Listine EU in 16. členom PDEU imajo tudi otroci pravico do varstva osebnih podatkov, ki se nanašajo nanje. Še posebej jim varstvo pravice do tega zagotavlja Splošna uredba o varstvu podatkov. Pomembne so predvsem določbe, ki se nanašajo na otroke. Ti potrebujejo posebno varstvo glede svojih osebnih podatkov, saj se morda manj zavedajo tveganj, posledic in zaščitnih ukrepov in svojih pravic v zvezi z obdelavo osebnih podatkov. Poleg 7. člena, ki določa splošne pogoje v zvezi s privolitvijo obdelave osebnih podatkov, je v zvezi z otroki pomemben 8. člen, ki določa pogoje, ki se uporabljajo za privolitev otroka v zvezi s storitvami informacijske družbe. Glede na 8. člen morata biti izpolnjena dva pogoja. In sicer, da je obdelava povezana s storitvami informacijske družbe, ki se ponujajo neposredno otroku (usmeritev na 25. točko 4. člena Uredbe), in da obdelava temelji na privolitvi. Tako posebno varstvo bi moralo zadevati zlasti uporabo osebnih podatkov otrok v namene trženja ali ustvarjanja osebnostnih ali uporabniških profilov in zbiranje osebnih podatkov v

[52] Za otroka se šteje praviloma šteje oseba, mlajša od osemnajst let- glej 1. člen Konvencije.
[53] Zakon o ratifikaciji Konvencije ZN o otrokovih pravicah (Uradni list SFRJ – Mednarodne pogodbe št. 15/90) in Akt o notifikaciji nasledstva glede konvencij Organizacije združenih narodov in konvencij, sprejetih v Mednarodni agenciji za atomsko energijo (Uradni list RS – Mednarodne pogodbe, št. 9/92, 9/93, 5/99, 9/08, 13/11, 9/13 in 5/17).

zvezi z otroki pri uporabi storitev, ki se nudijo neposredno otroku.[54] Prvi odstavek 8. člena določa, da v kolikor gre za vprašanje zakonitosti privolitve za obdelavo osebnih podatkov, ki se nanašajo na posameznika, in je ta v zvezi s storitvami informacijske družbe, ki se ponujajo neposredno otroku, je obdelava osebnih podatkov otroka zakonita, kadar ima otrok vsaj 16 let. Če je otrok mlajši od 16 let, je takšna obdelava zakonita le, če in kolikor takšno privolitev da ali odobri nosilec starševske odgovornosti za otroka. Lahko pa države članice za te namene z zakonom določijo nižjo starost, ki nikoli ne sme biti nižja od 13 let. Če bo potrjen predlog Zakona o varstvu osebnih podatkov (ZVOP-2),[55] bo privolitev veljavna, če jo bo podala mladoletna oseba, stara 15 let ali več. Dosedanji in trenutno veljavni Zakon o varstvu podatkov (ZVOP-1)[56] te starostne meje ne ureja. Nadalje drugi odstavek določa, da si mora upravljalec ob upoštevanju razpoložljive tehnologije v takih primerih razumno prizadevati za preveritev, ali je nosilec starševske odgovornosti za otroka dal ali odobril privolitev. Seveda je potrebno pred podajo privolitve vsakega posameznika, tudi otroke, ustrezno informirati. Jasno jim mora biti predstavljeno, kateri osebni podatki bodo obdelovani, za katere namene, kakšne so njihove pravice itd.[57] Poleg tega je pomembno, da mora upravljavec sprejeti ustrezne ukrepe, da otroku, na katerega se nanašajo osebni podatki, posreduje vse informacije in sporočila, povezana z obdelavo, v jedrnati, pregledni, lahko dostopni, in njemu razumljivi obliki.[58] Nadalje jim je na ravni EU varstvo pred spolnimi napadi oziroma zlorabami zagotavlja sprejeta Direktiva 2011/92/EU Evropskega parlamenta in Sveta o boju proti spolni zlorabi in spolnemu izkoriščanju ter otroški pornografiji.[59]

Pomen varstva otrok in njegovih pravic se kaže tudi na nacionalni ravni. V tretjem odstavku 53. člena Ustave RS je določeno, da je država dolžna varovati družino, materinstvo, očetovstvo, otroke in mladino ter ustvarjati za to varstvo potrebne razmere. Nadalje Ustava še posebej ureja pravice otrok in je tako v 56. členu

[54] Informacijski pooblaščenec, Privolitev, <https://www.ip-rs.si/zakonodaja/reforma-evropskega-zakonodajnega-okvira-za-varstvo-osebnih-podatkov/kljucna-podrocja-uredbe/privolitev/#c1932> (17.6.2020).
[55] Besedilo Predloga Zakona o varstvu podatkov (ZVOP-2), EPA: 2733 – VII, < https://www.dz-rs.si/wps/portal/Home/deloDZ/zakonodaja/izbranZakonAkt?uid=C1257A70003EE6A1C12582670045DF4F&db=kon_zak&mandat=VII&tip=doc> (2.6.2020).
[56] Zakon o varstvu osebnih podatkov (Uradni list RS, št. 94/07 – uradno prečiščeno besedilo).
[57] Glej 13. člen Direktive Evropskega parlamenta in Sveta 95/46/ES z dne 24. oktobra 1995 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov, Uradni list Evropske unije, L 281, 23.11.1995, str. 31–50.
[58] Ibidem, prvi odstavek 12. člena.
[59] Direktiva 2011/93/EU Evropskega parlamenta in Sveta z dne 13. decembra 2011 o boju proti spolni zlorabi in spolnemu izkoriščanju otrok ter otroški pornografiji in nadomestitvi Okvirnega sklepa Sveta 2004/68/PNZ, Uradni list Evropske unije, L 335, 17.12.2011.

določeno, da otroci uživajo posebno varstvo in skrb ter da človekove pravice in temeljne svoboščine otroci uživajo v skladu s svojo starostjo in zrelostjo. Otrokom se zagotavlja posebno varstvo pred gospodarskim, socialnim, telesnim, duševnim ali drugim izkoriščanjem in zlorabljanjem. Nacionalna zakonodaja omogoča tudi zaščito otrok v vlogi potrošnikov. Zakon o varstvu potrošnikov pred nepošteno poslovno prakso,[60] ki implementira Direktivo Evropskega parlamenta in Sveta 2005/29/ES o nepoštenih poslovnih praksah podjetij v razmerju do potrošnikov na notranjem trgu,[61] vsebuje določbe za preprečevanje izkoriščanja potrošnikov, ki so še posebej ranljivi zaradi starosti (3. odst. 4.člena). Nepoštene prakse so prepovedane. Pod agresivne poslovne prakse, ki so prepovedane, sodi tudi neposredno spodbujanje otrok z oglaševanjem izdelkov k nakupu (5. točka 1.odst. 10. člena).

Vsem navedenim aktom je skupno, da se v vseh zadevah, povezanih z otroki, zasleduje njihova največja korist[62], tudi pri uporabi digitalizacije.

6.3.2 Pravice otrok v praksi

Otroci so ena najbolj ranljivih skupin, katere pravice je potrebno varovati in spoštovati. Gre za osebe, ki praviloma ne razumejo tveganj in posledic svojih dejanj ali dejanj drugih, katerim so lahko izpostavljeni, ter se ne morejo sami braniti. Dejstvo, da otrokom pogosto manjka zavedanja in zmožnosti predvidevanja posledic, jih naredi še bolj ranljive. Medtem pa dejstvo, da predstavljajo kar eno tretjino vseh uporabnikov interneta predstavlja, kako zelo so izpostavljeni nevarnostim.[63] Zato je potrebno, da se jih s pravom zaščiti in pri vseh ukrepih, sprejetih glede otrok, je potrebno upoštevati dobrobit otroka in otrokovo največjo korist.[64] Velik vpliv na njihove pravice ima tudi uporaba digitalizacije. Sicer jim ta lahko prinese številne priložnosti, vendar pa so zaradi nje lahko izpostavljeni

[60] Zakon o varstvu potrošnikov pred nepoštenimi poslovnimi praksami (Uradni list RS, št. 53/07)
[61] Direktiva Evropskega parlamenta in Sveta 2005/29/ES z dne 11. maja 2005 o nepoštenih poslovnih praksah podjetij v razmerju do potrošnikov na notranjem trgu ter o spremembi Direktive Sveta 84/450/EGS, direktiv Evropskega parlamenta in Sveta 97/7/ES, 98/27/ES in 2002/65/ES ter Uredbe (ES) št. 2006/2004 Evropskega parlamenta in Sveta (Direktiva o nepoštenih poslovnih praksah) (Besedilo velja za EGP), Uradni list Evropske unije, L 149, 11.6.2005.
[62] Glej 3. člen, 1. odst. Konvencije o otrokovih pravicah.
[63] Viola de Azevedo Cunha, M.: Child Privacy in the Age of Web 2.0 and 3.0: Challenges and Opportunities for Policy - Innocenti Discussion Paper, UNICEF Office of Research – Innocenti, 2017, str. 6, <https://www.unicef-irc.org/publications/pdf/Child_privacy_challenges_opportunities.pdf> (25.6.2020).
[64] 3. člen Konvencije o otrokovih pravicah: "*otrokova korist je glavno vodilo*".

različnim tveganjem, ki lahko škodljivo vplivajo na njihove pravice, kar pa ni v skladu z načelom preprečevanja škode. Tako so otroci lahko žrtve spletnega nadlegovanja in nasilja, posega v pravico do zasebnosti, zlorabe osebnih podatkov, kibernetske kriminalitete, izpostavljenosti neprimernim vsebinam in celo spolne zlorabe.[65] Internet in družbeni mediji se pogosto uporabljajo za širjenje sovraštva, nasilja in nadlegovanja med otroki. To lahko pripelje do tragičnih posledic, kar ponazarjajo tudi nedavni primeri, ko so si številni najstniki vzeli življenje potem, ko so domnevno doživeli nasilje in bili spodbujeni k storitvi samomora na družbenih mediji.[66] Zaradi navedenih razlogov in zaradi njihove ranljivosti pred uresničitvijo teh razlogov, je otrokom potrebno nuditi posebno varstvo.

Uporaba digitalizacije vključuje tudi obdelavo ogromnih količin osebnih podatkov z uporabo tehnik rudarjenja podatkov.[67] Tako kljub nekaterim pozitivnim učinkom, ki jih ima uporaba digitalizacije za otroke, saj lahko ti z njo odkrivajo in pridobivajo nove informacije ter izražajo svoja mnenja, ima na drugi strani tudi negativne učinke, saj določenim akterjem odpira možnosti sledenja, zbiranja in obdelave dejanj otrok. [68] Ravno iz teh razlogov vplivanja na otrokovo pravico do zasebnosti, je to področje postalo izredno pravno zanimivo. Eden izmed pravno zanimivih vidikov varstva pravice otroka do zasebnosti predstavlja tudi pravica do izbrisa[69] (»pravica do pozabe) osebnih podatkov, ki se na nanašajo na določeno osebo. Ta pravica omogoča otroku, da lahko tudi kasneje v življenju zahteva izbris podatkov in tako ne rabi trpeti dolgoročnih resnih posledic zaradi podatkov, katere je objavil ali objavo katerih je dovolil v času, ko še ni bil popolnoma zrel za razumevanje tveganj, ki jih njegovo dejanje lahko povzroči. Ali pa v primerih, ko so soglasje namesto njega podali starši, on pa se s tem ne strinja. Za tak primer bi lahko šlo, ko starši objavijo sliko otroka na svojih družbenih omrežjih, ta pa se kasneje, ko lahko oblikuje svojo voljo, s takšno objavo ne strinja. Ko torej govorimo o pravici do pozabe v zvezi z otroki, se le te ne uporablja samo kot pravico, ampak tudi kot nekakšno sredstvo

[65] About Better Internet for Kids, <https://ec.europa.eu/digital-single-market/en/content/creating-better-internet-kids-0> (24.4.2020).
[66] Komisar za človekove pravice, Protecting children's rights in the digital world: an ever-growing challenge – komentar, <https://www.coe.int/en/web/commissioner/-/protecting-children-s-rights-in-the-digital-world-an-ever-growing-challen-1> (29.6.2020).
[67] FRA, Handbook on European law relating to the rights of the child, 2015, str. 190, <https://fra.europa.eu/sites/default/files/fra_uploads/fra-ecthr-2015-handbook-european-law-rights-of-the-child_en.pdf> (15.4.2020).
[68] Viola de Azevedo Cunha, M.: Child Privacy in the Age of Web 2.0 and 3.0: Challenges and Opportunities for Policy, str. 8.
[69] Glej 17. člen Splošne uredbe o varstvu podatkov.

zaščite otroka pred kršitvami njegove pravice do zasebnosti, dostojanstva ali kakšne druge pravice, pa ne obstaja nobena boljša rešitev za zaustavitev kršenja.[70] Nezakoniti poseg v pravico do zasebnosti in zasebnega življenja je preko uporabe digitalizacije mogoče izvesti na več načinov. Na primer kraja identitete predstavlja samo eno izmed nevarnosti posega v zasebnost. Tak primer posega je obravnavalo Evropsko sodišče za človekove pravice v zadevi K.U. proti Finski.[71] Do posega v zasebno življenje naj bi prišlo zaradi spletne objave oglasa spolne narave brez vednosti otroka. Sodišče je odločilo, da je država kršila pravico do spoštovanja zasebnega življenja s tem, ko ni zahtevala oziroma omogočila identifikacijo osebe, ki je na spletu objavila oglas, s katerim je žalila drugo osebo in posegla v njeno zasebno življenje.

Vrsto tveganj za otroke, ki jih lahko povzroči umetna inteligenca, predstavlja tudi vsakodnevna uporaba algoritmov za povečanje števila avtomatiziranih odločitev na spletu. Če zasebnost in drugi etični standardi niso vgrajeni v algoritme, potem uporaba le teh lahko privede do diskriminacije otrok na podlagi njihove države izvora, narodnosti in/ali veroizpovedi.[72] Takšna diskriminacija lahko omeji prihodnje priložnosti otrok v zvezi z njihovo izobrazbo in kariero ter celo izpostavi otroke okrepljenemu državnemu nadzoru, če se zdi, da ustrezajo skupini oseb, za katero obstaja večja verjetnost, da se bo v prihodnosti vedla na kazniv način. Do diskriminacije lahko pride, ker algoritmi delujejo na podlagi podatkov iz katerih so se učili in če ti podatki vsebujejo kakršnokoli pristranskost, bo obdelava, ki jo izvaja algoritem, sledila temu vzorcu.

IKT in digitalni mediji so dodali novo dimenzijo otrokovi pravici do izobraževanja.[73] Tako je mogoča uporaba tehnologije tudi za izobraževanje otrok, vključno s potekom pouka na daljavo. To je možično prišlo v poštev sedaj, v času pandemije koronavirusa. Zato se je tu smiselno vprašati, ali je sploh vsem otrokom omogočen dostop do interneta in ali sploh imajo tehnologijo, s katero lahko dostopajo do interneta. Kajti že 2. člen EKČP določa pravico do izobraževanja in da ta nikomur ne sme biti odvzeta. Otrokom, ki se sedaj ne morejo udeleževati pouka na daljavo,

[70] Viola de Azevedo Cunha, M.: Child Privacy in the Age of Web 2.0 and 3.0: Challenges and Opportunities for Policy, str. 16.
[71] *K.U. v. Finland, št. 2872/02, 2 December 2008*.
[72] Viola de Azevedo Cunha, M.: Child Privacy in the Age of Web 2.0 and 3.0: Challenges and Opportunities for Policy, str. 10.
[73] <https://home.crin.org/briefing-childrens-rights-in-the-digital-age> (14.4.2020).

zato ker nimajo tehnologij, s katerimi bi dostopali do interneta ali nimajo že samega interneta, je torej v tem primeru odvzeta pravica do izobraževanja in vprašanje je, koliko so posamezne države ukrepale v tej smeri, da otrokom to pravico zagotovijo in zavarujejo. Dva glavna tipa ukrepov, ki so jih države članice EU izvajale, sta:

- več kot polovica držav članic je prikrajšanim učencem zagotovila računalnike in internetno povezavo ter
- drugje se je pouk predvajal preko nacionalnega televizijskega programa.[74]

Slovenija spada med prvo skupino držav članic in je tako začela projekt "DIGI šola", s katerim je zbrala več kot 1.300 računalnikov in 950 modemov za otroke, ki so potrebovali te naprave. Te donacije je opravil Zavod za šolstvo, skupaj z ministrstvom za izobraževanje, znanost in šport in drugimi organizacijami (npr. Zveza prijateljev mladine).[75] Vendar se je potrebno zavedati, da ta številka donirane IKT opreme ne pokriva vseh otrok, ki nima le teh. Tako je ostalo še kar nekaj otrok, ki ni imelo in se jim ni zagotovilo naprav, s katerimi bi dostopali do izobraževanja na daljavo ali pa ni imelo dostopa do internetne povezave.[76] To vodi do dejstva, da v času izobraževanja niso bili vsem otrokom zagotovljeni enaki pogoji. Sedaj, ko so se otroci lahko vrnili nazaj v šole, se ta neenakost tudi kaže v dejanskem stanju. Mogoče je opaziti, kdo od otrok se pouka na daljavo ni mogel udeleževati.[77] Prišlo je do diskriminacije, ki je prepovedana na podlagi več aktov, sprejetih na nacionalni ravni ali na mednarodni ravni, pa učinkujejo in zavezujejo tudi znotraj slovenskega pravnega reda. V Sloveniji trenutno poteka obširna raziskava v zvezi z izobraževanjem na daljavo, v katero so zajeti ravnatelji, učenci, dijaki in učitelji.[78] To raziskavo je organiziral Zavod za šolstvo in izsledke le te bodo na Zavodu za šolstvo predvidoma predstavili v juliju. Prav tako bo v povezavi z rezultati raziskave in zbranimi podatki v času izobraževanja na daljavo Zavod za šolstvo skupaj z ministrstvom za izobraževanje, znanost in šport pripravilo izhodišča glede izvedbe

[74] FRA, Coronavirus pandemic in the EU - Fundamental rights implication: With a focus on contact tracing apps, Publications Office of the European Union, Luxembourg, 2020, str. 23, <https://fra.europa.eu/sites/default/files/fra_uploads/fra-2020-coronavirus-pandemic-eu-bulletin-may_en.pdf> (29.5.2020).
[75] Zavod Republike Slovenije za šolstvo, Tablični računalniki za otroke iz socialno šibkejših družin <https://www.zrss.si/objava/tablicni-racunalniki-za-otroke-iz-socialno-sibkejsih-druzin> (18.6.2020).
[76] Husejnović K.: 'Vidi se, da vsi otroci doma niso imeli enakih pogojev', 2020, <https://www.24ur.com/novice/korona/pouk-na-daljavo.html> (16.6.2020).
[77] Ibidem.
[78] Zavod Republike Slovenije za šolstvo, Analiza izobraževanja na daljavo v času epidemije <https://www.zrss.si/objava/analiza-izobrazevanja-na-daljavo-v-casu-epidemije-2> (16.6.2020).

šolanja na daljavo za primere, ko bi bilo to potrebno zopet izvesti. Ta izhodišča bodo prejele šole v Sloveniji. Zavod za šolstvo pripravlja tudi različne oblike usposabljanj za učitelje in ravnatelje, da bodo v primeru ponovne potrebe po zapiranju oddelkov ali šol, vsi bolje pripravljeni na to. Vendar na splošno je ocena Zavoda za šolstvo, da so se v času izobraževanja na daljavo vse šole v Sloveniji zelo angažirale, zato menijo, da je bilo izobraževanje na daljavo v posebnih razmerah uspešno izvedeno.[79] Glede na to, da je prišlo do nastopa izrednega dogodka, kot je pandemija, in se kaj takega ni moglo pričakovati, se lahko strinjam z oceno Zavoda v smeri, da so se na koncu šole dobro spoprijele s spletnim poučevanjem. Glede nekih obveznosti bi se na šoli vendarle lahko malo popustilo. Menim, da je današnji obseg snovi, predvsem v nižjih razredih osnovne šole, preobsežen, in če se že na splošno le tega ne more zmanjšati, bi se ga lahko vsaj v času izrednih razmer in šolanja na daljavo. Že same razmere (nov način poteka pouka, neveščost z opravljanjem IKT opreme, zaprtost in izoliranost zaradi pandemije itd.) so povzročile velik stres za otroka, stopnja le tega se je po mojem mnenju samo še povečala z velikim obsegom snovi, ki so jo morali predelati, nekateri celo sami. Zato bi bilo mogoče v bodoče razmisliti o zmanjšanju obsega snovi na splošno, predvsem faktografskih podatkov, in namesto tega kot obvezni predmet, katerega se niti ne bi rabilo ocenjevati, uvedli predmet o računalništvu. Pri tem predmetu se ne bi pridobivalo samo znanj o izbraževanju na daljavo, ampak bi lahko otroci pridobivali tudi druga znanja povezana z uporabo informacijskih tehnologij. Bistvo bi torej bilo v tem, da se otroke nauči kako upravljati z IKT in pri tem zaščititi svoje pravice ter kako ukrepati v primeru, ko mislijo, da je prišlo do kršitev le teh. Npr. pridobivali bi veščine v zvezi z zaščito pred kibernetskimi napadi, pred škodljivo vsebino ali pa kako zaščititi svojo zasebnost pri uporabi umetne inteligence ipd. Tako so se tudi šole zaradi izkušenj z izobraževanjem na daljavo odločile spodbujati k obisku obveznih ali neobveznim izbirnih predmetov s področja računalništva.[80] Menim, da je to korak v pravo smer. Vendar mora tudi vlada povečati svojo vlogo pri tem. Tudi šole sedaj pričakujejo od ministrstva, da bodo na podlagi dosedanjih izkušenj pripravili poenotene strokovne usmeritve glede pouka na daljavo.[81] Tako lahko vsi upamo, da bo sedanja izkušnja spodbudila zakonodajne organe države k boljšemu urejanju in sprejemanju ukrepov ne samo v povezavi z izobraževanjem na daljavo, ampak v povezavi s celotnim

[79] Husejnović K.: 'Vidi se, da vsi otroci doma niso imeli enakih pogojev', 2020, <https://www.24ur.com/novice/korona/pouk-na-daljavo.html> (16.6.2020).
[80] Ibidem.
[81] Ibidem.

razvojem in uporabo umetne inteligence v šolstvu. Tudi na ravni EU so začeli ukrepati v tej smeri. Evropska komisija je začela javno posvetovanje na ravni EU z namenom zagotoviti, da bo njen novi akcijski načrt za digitalno izobraževanje odražal izkušnje EU na področju izobraževanja in usposabljanja v času koronavirusne krize. Tako bo Evropska komisija septembra 2020 predstavila nov akcijski načrt za digitalno izobraževanje, ki bo predstavljal ključni instrument v procesu okrevanja po COVID-19, pri čemer se bodo upoštevale izkušnje iz krize, načrt pa bo odražal dolgoročno vizijo za evropsko digitalno izobraževanje.[82] Cilji tega načrta so povečati digitalno pismenost, pomagati državam EU sodelovati pri prilagajanju sistemov izobraževanja in usposabljanja digitalni dobi ter izkoristiti potencial interneta, da se zagotovi dostop do spletnega učenja vsem.

Čas pandemije zaradi nalezljive bolezni COVID-19 in izvajanje različnih ukrepov za obvladovanje le te, je povzročilo tudi težave z izvrševanjem stikov staršev z otroki. Pri stikih gre primarno za pravico otrok,[83] vendar gre tudi za pravico staršev.[84] Glede na sodno prakso pa zajema tudi pravico starih staršev.[85] Tako nekateri starši zaradi bojazni pred okužbe otroka z boleznijo COVID-19 preprečujejo določene stike otroka s staršem, od katerega ja ta ločen, in zahtevajo pred sodišči s predlogi za izdajo začasnih odredb prepoved izvajanja stikov.[86] Ali pa zahtevajo izdajo začasne odredbe o stikih, ker mu drugi starš ne dovoli stika iz tega istega razloga. V skladu s sodno prakso bo sodiščem pri odločanju moralo biti osnovno vodilo sledenje otrokovi koristi, vsebino tega pravnega standarda je potrebno ugotoviti in opredeliti glede na vsak konkretni primer in pri tem upoštevati vse okoliščine, vključno s trenutnim stanjem pandemije.[87] Tudi Ministrstvo za pravosodje je podalo izjavo[88] glede teh okoliščin in v njej apelira na starše, da so v svojih postopanjih razumni in odgovorni, da ne ogrožajo koristi svojih otrok iz takšnih in drugačnih razlogov. V kolikor pa ni mogoče zagotavljati oziroma izvajati stikov zaradi nevarnosti širjenja

[82] Evropska komisija začenja javno posvetovanje o novem akcijskem načrtu za digitalno izobraževanje, Sporočilo za medije, 18.6.2020 <https://ec.europa.eu/commission/presscorner/detail/sl/ip_20_1066> (27.6.2020).
[83] 9. člen, 3. odst. Konvencije o otrokvih pravicah: »*Države pogodbenice spoštujejo pravico otroka, ki je ločen od enega ali od obeh staršev, da redno vzdržuje osebne stike in neposredno zvezo z obema, razen če je to v nasprotju z njegovimi koristmi «.*
[84] Glej 141. člen Družinskega zakonika.
[85] Glej zadevo C-335/17, *Valcheva,* ECLI:EU:C:2018:359.
[86] Emeršič Polić K.: Izvrševanje stikov z otrokom med pandemijo koronavirusa COVID-19, <https://pirc-musar.si/sl/izvrsevanje-stikov-z-otrokom-med-pandemijo-koronavirusa/> (27.6.2020).
[87] Glej Višje sodišče v Ljubljani, sklep IV Cp 661/2010, 17. marec 2010.
[88] Izvrševanje pravnomočnih sodnih odločb, ki urejajo stike otroka s tistim od staršev, ki mu otrok ni dodeljen v varstvo in vzgojo, 19.3.2020 <https://www.gov.si/novice/2020-03-19-izvrsevanje-pravnomocnih-sodnih-odlocb-ki-urejajo-stike-otroka-s-tistim-od-starsev-ki-mu-otrok-ni-dodeljen-v-varstvo-in-vzgojo/> (27.6.2020).

koronavirusa Ministrstvo predlaga, da se za zagotovitev stika, ki je namenjen ohranjanju odnosa z drugim staršem, poslužujejo tehnologije, telefonov, morebitnih videokonferenc ipd.. Toda Višje sodišče v Mariboru je odločilo, da popolna preprečitev neposrednih stikov in omejitev na video klice in skupne sprehode v prisotnosti obeh staršev z upoštevanjem distance, ne zagotavlja največje otrokove koristi.[89]

Razmere pandemije so imele velik negativni vpliv še prav posebej na eno skupino otrok. Gre za otroke s posebnimi potrebami.[90] Ti potrebujejo številne in različne terapije, ki so za njihovo zdravstveno stanje zelo pomembne. Kajti pomoč in oskrba, ki jo potrebujejo, ne more potekati na daljavo. Tako je tudi Društvo psihologov Slovenije opozorilo, da so bili otroci s posebnimi potrebami med najbolj prizadetimi, njihovi starši pa posledično nadpovprečno obremenjeni.[91] Mogoče bi se v tem primeru lahko izkazala uporaba umetne inteligence kot pozitivna stvar, saj bi se lahko uporabilo robote, ki bi namesto zdravstvenega osebja izvajali potrebno oskrbo.

Družbe vidijo otroke tudi kot pomemben trg, saj vplivajo na potrošniške odločitve družine. Informacije o spletnih navadah in vedenju otrok so torej komercialno privlačne, saj družbam pomagajo razviti učinkovite poslovne strategije glede doseganja pomebnega deleža spletnega trga. Ker je danes preživljanje časa na spletu ena glavnih aktivnosti otrok, predstavljajo ti zelo pomemben del potrošništva.[92] Iz teh razlogov se jim tudi zagotavlja posebno varstvo v takih okoliščinah v skladu s prej navedenima (v poglavju 3.1.) Direktivo 2005/29/ES in Zakonom o varstvu potrošnikov pred nepošteno poslovno prakso.

6.3.2 Iniciative v zvezi z varstvom pravic otrok

Zaradi vseh prej navedenih vplivov, ki jih ima digitalizacija na pravice otrok, so se na mednarodni ravni oblikovale različne institucije za varstvo otrokovih pravic, kot tudi bili sprejeli različni ukrepi za zaščito temeljnih pravic v povezavi z digitalizacijo.

---

[89] Višje sodišče v Mariboru, Sklep III Cp 295/2020, 21. maj 2020.
[90] Peljhan M., Koronavirus in otroci s posebnimi potrebami, 2020, <https://www.rtvslo.si/kolumne/koronavirus-in-otroci-s-posebnimi-potrebami/518153> (16.6.2020).
[91] Društvo psihologov Slovenije, O kriznih dogodkih in odzivih nanje <http://www.dps.si/za-javnost/koronavirus/> (16.6.2020).
[92] Viola de Azevedo Cunha, M.: Child Privacy in the Age of Web 2.0 and 3.0: Challenges and Opportunities for Policy, str.9

Na mednarodni ravni je Odbor ZN za otrokove pravice izdal priporočila,[93] v skladu s katerimi bi morali imeti vsi otroci možnost varnega dostopa do IKT in imeti zagotovljeno polno sodelovanje, izražanje, iskanje informacij ter uživanje vseh pravic brez kakršnekoli diskriminacije. V okviru Združenih narodov je ustanovljena tudi organizacija UNICEF, ki je posvečena izključno otrokom in skrbi za njihovo preživetje, zaščito in razvoj. [94]

Svet Evrope je sprejel Strategijo za otrokove pravice (2016-2021).[95] V okviru te se Svet Evrope zavzema, da bo spodbujal in varoval otrokove pravice do nediskriminacije, dostopa do informacij, svobode izražanja in sodelovanja v digitalnem okolju v sodelovanju z drugimi zainteresiranimi stranmi, dejavnimi na tem področju. Prav tako bo zagotovil vodenje in podporo državam članicam pri zagotavljanju pravic udeležbe in zaščite otrok v digitalnem okolju. Leta 2018 je bila ta strategija okrepljena še s sprejetjem Smernic za spoštovanje, varstvo in izpolnitev pravic otrok v digitalnem okolju (*Guidelines to respect, protect and fulfil rights of the child in the digital environment*).[96] Te smernice oziroma priporočila so naslovljena na vse države članice Sveta Evrope in jim predstavljajo vodilo pri spoštovanju, varstvu in izpolnitvi pravic otrok v digitalnem okolju. Njihov namen je pomagati državam in drugim zainteresiranim v njihovih prizadevanjih za sprejetje celovitega strateškega pristopanja k digitalizaciji. Svet Evrope je zaradi širjenja sovraštva, nasilja in nadlegovanja med otroki preko uporabe interneta in družbenih medijev, oblikoval tudi kampanjo "Brez sovražnega govora" in vlaga v vrsto ukrepov na področju izobraževanja o internetu.[97]

Na ravni EU je bila leta 2012 sprejeta Strategija boljši internet za otroke[98], katere glavni cilji so:

- spodbujanje ustvarjanja ustvarjalnih in poučnih spletnih vsebin za otroke ter spodbujati pozitivne spletne izkušnje za majhne otroke;

[93] Priporočila so dostopna na <https://www.ohchr.org/_layouts/15/WopiFrame.aspx?sourcedoc=/Documents/HRBodies/CRC/Discussions/2014/DGD_report.pdf&action=default&DefaultItemOpen=1> (4.5.2020).
[94] <https://www.unicef.si/> (4.5.2020).
[95] Svet Evrope, Strategija za otrokove pravice, CM(2015)175-final, 3. marec 2016.
[96] Odbor ministrov Sveta Evrope, Guidelines to respect, protect and fulfil the rights of the child in the digital environment - Recommendation CM/Rec(2018)7 of the Committee of Ministers, 2018.
[97] < https://www.coe.int/en/web/no-hate-campaign> (30.5.2020).
[98] Evropska komisija, Evropska strategija za boljši internet za otroke, COM/2012/0196 final, 2.maj 2012.

- povečanje ozaveščenosti, vključno z učenjem digitalne pismenosti in spletne varnosti v vseh šolah EU;
- ustvariti varno okolje za otroke z ustreznimi starostnimi nastavitvami zasebnosti, širšo uporabo starševskega nadzora ter razvrstitvijo vsebin glede na določene starostne meje;
- boj proti prisotnosti spolne zlorabe otrok na spletu.

Nekateri cilji iz te Strategije glede zasebnosti so se na ravni EU dosegli s sprejetjem prej omenjene in prestavljene Splošne uredbe o varstvu podatkov. Kot rezultat te strategije je nastal program Boljši internet za otroke.[99] Del tega programa je evropska mreža centrov za varnejši internet INSAFE, v kateri delujejo nacionalne točke osveščanja o varnih in učinkovitih načinih rabe interneta ter IKT. Tekom let so se tako razvili različni viri za obravnavo pomislekov, povezanih z digitalnim življenjem otrok. Znotraj mreže deluje tudi slovenski Center za varnejši internet (SIC), za spodbujanje varnejše uporabe interneta in mobilnih tehnologij med otroki.[100]

EU želi narediti korak naprej predvsem pri zaščiti otrok pred spolno zlorabo na spletu. Vsakršna dejanja spolne zlorabe in spolnega izkoriščanja otrok ter otroška pornografija predstavljajo hude kršitve temeljnih človekovih pravic, zlasti pravic otrok do zaščite in dobrobiti, kot je določeno v prej omenjenima Konvenciji in Listini EU. Na žalost so vse oblike spolnih zlorab otrok vse pogostejše in se z uporabo novih tehnologij in spleta širijo.[101] Vzrok širjenja je tudi v tem, da so z uporabo tehnologij spolne zlorabe otrok lažje izvedljive in lažje se dostopa do vsebin le teh. Da spolno izkoriščanje otrok in otroška pornografija predstavljata hudo kršitev človekovih pravic in temeljnih pravic otroka do skladne skladne vzgoje in razvoja, izpostavlja tudi Višje sodišče v Ljubljani v zadevi z opravilno številko II Kp 9220/2011,[102] pri kateri je odločalo o zakonitosti pridobitve dokazov, ki so bili pridobljeni s posegom v obtoženčevo pravico do (komunikacijske) zasebnosti. Ker spolna zloraba otrok predstavlja tako hud poseg v pravice otrok, je sodišče v tej zadevi odločilo, da se lahko zaradi namena pridobitve podatkov v elektronsko komunikacijskem omrežju, ki razkrivajo in dokazujejo kazniva dejanja obtoženca,

[99] Evropska komisija, Creating a better Internet for kids <https://ec.europa.eu/digital-single-market/en/policies/better-internet-kids> (30.5.2020).
[100] BIK, Team, Happy world children' day!, 2019, dostopno na <https://www.betterinternetforkids.eu/web/portal/practice/awareness/detail?articleId=5252966> (30.5.2020).
[101] <https://home.crin.org/briefing-childrens-rights-in-the-digital-age> (13.4.2020).
[102] Višje sodišče v Ljubljani, sklep II Kp 9220/2011, 7. December 2012.

poseže v pravico do zasebnosti. Ta ustavna pravica je manjšega pomena od ustavne pravice varovanja pravic otrok in ne more biti absolutna, ampak je omejena z varstvom pravic in koristi otrok. Evropsko komisijo so h koraku naprej v varovanju otrok pred spletnimi spolnimi zlorabami spodbudile zadnje ugotovitve, da se je med časom obvezne karantene po državah članic zaradi preprečitve širjenja nalezljive bolezni Covid-19, kar občutno povečala spletna spolna zloraba otrok.[103] Zaenkrat je na ravni EU sprejeta Direktiva 2011/92/EU. Gre za direktivo, ki boj proti temu ureja na splošno. Nimamo pa na ravni EU sprejete direktive, ki bi urejala boj proti temu v digitalnem okolju. Evropska komisarska Johanssona meni, da je vprašanje, kako narediti internet varno mesto za otroke, eno najpomembnejših vprašanj in navaja, da če imamo že obvezujočo zakonodajo za odkrivanje goljufij v zvezi z avtorskimi pravicami na digitalnem trgu[104] in tako ščitimo avtorske pravice, lahko zaščitimo tudi otroke. Po njenem mnenju se varstvo otrokovih pravic ne izvaja dovolj dobro. Tako je Evropska komisija predlagala vrsto ukrepov, kako okrepiti izvrševanje prava, da se otroke pred tako zlorabo zaščiti in tudi storilce lažje izsledi in kazensko ovadi. Ugotovitev storilca kaznivega dejanja pa predstavlja problem pri sprejetju ukrepov in regulativni ureditvi zaščite otrok pred spolnimi zlorabami na spletu. Splet uporabnikom omogoča anonimnost, prikrivanje identitete, to pa otežuje preiskovanje in pregon kaznivih dejanja, katerih žrtve so otroci. Eden od pomembnejših ukrepov je, da se zagotovi sodelovanje vseh potrebnih vključenih organizacij in organov na svetovni ravni. Prav tako se iz ukrepov ne izključuje možnosti nadaljnje zakonodaje za tehnološke družbe. Tudi sodelovanje z velikani družbenih medijev bo pomembno za boj proti širjenju nezakonitih vsebin na spletu.[105]

[103] McCaffrey, D. & Gill J.: EU wants to step up fight to protect children from sexual abuse online, 2020. Dostopno na <https://www.euronews.com/2020/06/09/eu-wants-to-step-up-fight-to-protect-children-from-sexual-abuse-online> (17.6.2020).
[104] Direktiva (EU) 2019/790 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/ES (Besedilo velja za EGP), PE/51/2019/REV/1, Uradni list Evropske unije, L 130, 17.5.2019, str. 92–125.
[105] McCaffrey D. & Gill J., EU wants to step up fight to protect children from sexual abuse online, 2020, <https://www.euronews.com/2020/06/09/eu-wants-to-step-up-fight-to-protect-children-from-sexual-abuse-online> (17.6.2020).

Na nacionalni ravni je v okviru strategije Evropa 2020 bil oblikovan dokument Digitalna Slovenija 2020 – Strategija razvoja informacijske družbe do leta 2020[106], kjer je zajeto tudi področje kibernetske varnosti. V okviru tega bo Slovenija do leta 2020 vzpostavila učinkovit sistem zagotavljanja kibernetske varnosti, ki bo preprečeval in tudi odpravljal posledice varnostnih incidentov. To bo dosegla z različnimi ukrepi, med drugim tudi z ukrepom osveščanja o varni rabi interneta za otroke, najstnike, starše in učitelje.

Poleg tega Slovenija izvaja še določene dejavnosti na področju varstva otrokovih pravic v digitalnem okolju. Kot izhaja iz priporočila Slovenije,[107] ki ga je ta dala Odboru ZN za otrokove pravice kot v pomoč Odboru pri oblikovanju splošnega mnenja o pravicah otrok v zvezi z digitalnim okoljem, je Slovenija vključena v program za otroke 2019-2024, kjer se osredotoča na spletno varnost otrok za reševanje najbolj pomembnih vprašanj, saj večina otrok ima neomejen dostop do spleta, medtem ko se ne zaveda tveganj. Nadalje izhaja iz priporočila, da izvaja več projektov glede spletne varnosti in pomoči. Gre za projekt KLIK-OFF, ki obravnava kibernetsko nasilje in nadlegovanje ter se osredotoča na dejavnosti osveščanja in preprečevanja (izvajanje le teh po šolah). Vzpostavljen je tudi center ODJAVA, kjer se nudi psihološko svetovanje otrokom glede prekomerne uporabe interneta, spletne zlorabe, ipd.

Ugotovimo lahko, da je kot najpogostejši ukrep za zaščito otrok pri uporabi umetne inteligence ta, da se jih glede tega izobražuje in osvešča. Nadalje bi bilo potrebno na tem področju sprejeti še več zakonodaje, kot tudi izvajati strožjo izvršitev že obstoječih aktov. Tako se otroci lahko s pravilno izobrazbo in usklajenimi prizadevanji s strani držav članic, ponudnikov internetnih storitev in vzgojiteljev naučijo, kako se uspešno izogniti tveganjem, ki ji prinaša uporaba digitalizacije in kako izkoristiti številne priložnosti le te.

---

[106] Digitalna Slovenija 2020 – Strategija razvoja informacijske družbe do leta 2020 <https://www.gov.si/assets/ministrstva/MJU/DID/Strategija-razvoja-informacijske-druzbe-2020.pdf> (6.4.2020).

[107] Concept note for the general Comment on children's rights in relation to the digital environment – Slovenia's comment, maj 2019 <https://www.ohchr.org/Documents/HRBodies/CRC/GCChildrensDigitalEnvironment/States/Slovenia.docx > (25.5.2020).

6.4 Pravice starejših

6.4.1 Pravni okvir

Na splošno pravo za človekove pravice ne obravnava v zadostni meri posebne in edinstvene potrebe starejših, saj je v aktih, ki urejajo človekove pravice težko zaslediti določbe, ki bi posebej urejale pravice starejših.[108] Zaenkrat še ni celovitega mednarodnega instrumenta, ki bi ustrezno obravnaval posebno varstvo, ki ga potrebujejo starejši. Vendar pa obstaja veliko mednarodnih instrumentov, ki prepoznavajo posebne pravice vseh oseb in se seveda lahko uporabijo tudi za starejše osebe. Tako je na mednarodni ravni za starejšo osebo pomembna določba 25. člena, 1. odst. Splošne deklaracije človekovih pravic, ki ji zagotavlja pravico do življenjske ravni, ki njej in njeni družini omogoča zdravje in blaginjo, vključno s hrano, obleko, bivališčem, zdravstveno oskrbo in potrebnimi socialnimi storitvami ter pravico do varnosti v primeru brezposelnosti, bolezni, invalidnosti, vdovstva, starosti ali druge nezmožnosti pridobivanja sredstev za preživljanje zaradi okoliščin, neodvisnih od njene volje. Nadalje je za pravice starejših oseb pomemben tudi Mednarodni pakt o ekonomskih, socialnih in kulturnih pravicah,[109] predvsem določbe, ki določajo pravico do socialne varnosti (9. člen), pravico do ustreznega življenjskega standarda (11.člen), pravico do najvišjega dosegljivega standarda fizičnega in mentalnega zdravja (12.člen), pravico do izobraževanja (13.člen) ter pravice povezane z delom (6. in 7.člen). Vredno je omeniti tudi načela za starejše osebe, [110] ki jih je sprejela Genaralna skupščina ZN in v katerih ta izpostavlja, da je voljnim in sposobnim starejšim osebam potrebno zagotoviti priložnosti, da sodelujejo in prispevajo k socialnemu življenju družbe. Načelo 7 določa, da starejše osebe morajo ostati vključene v družbo in aktivno sodelovati pri oblikovanju ter izvajanju politik, ki neposredno vplivajo na njihovo počutje. Nadalje načelo 16 določa, da bi starejše osebe morale med drugim imeti dostop tudi do izobraževalnih in kulturnih virov družbe.

---

[108] Tonolo S.: International human rights law and the protection of elderly in Europe, v: Medicine, Law&Society, 11 (2018) 2, str. 107-120, <https://journals.um.si/index.php/medicine/article/view/118> (25.6.2020).
[109] Zakon o ratifikaciji Fakultativnega protokola k Mednarodnemu paktu o državljanskih in političnih pravicah (Uradni list RS – Mednarodne pogodbe, št. 9/93).
[110] United Nations Principles for Older Persons , Adopted by General Assembly resolution 46/91 of 16 December 1991, ostopna na <https://www.ohchr.org/EN/ProfessionalInterest/Pages/OlderPersons.aspx> (24.6.2020).

Na ravni EU podlago za sprejem ukrepov za vključitev starejših v razvoj in uvajanje v sisteme umetne inteligence predstavlja 25. člen Listine EU, ki določa, da je treba priznavati in spoštovati pravico starejših do sodelovanja v družbenem in kulturnem življenju. Digitalizacija, ki doživlja razmah, pa trenutno predstavlja velik del našega družbenega in kulturnega življenja. To pomeni, da predstavlja vključitev starejših v razvoj in uporabo digitalizacije del njihove pravice. Ker lahko uporaba umetne inteligence pipelje tudi do prepovedane diskriminacije na podlagi starosti, je vredno omeniti akte, ki določajo varstvo pred tem. Primarni zakon na ravni EU, ki ureja varstvo pred prepovedano diskriminacijo, je PEU, kjer je v 2. členu prepoved diskriminacije določena kot vrednota, na kateri temelji EU in se tako bori proti diskriminaciji ter spodbuja socialno pravičnost in varstvo, enakost žensk in moških, solidarnost med generacijami in varstvo pravic otrok. Da gre za eno temeljnih načel evropskega prava je poudarilo tudi sodišče EU v zadevi Mangold.[111] Sodišče je tako izpostavilo, da je načelo prepovedi diskriminacije zaradi starosti treba obravnavati kot splošno načelo prava Skupnosti in je zato v tej zadevi odločilo, da nacionalno sodišče v skladu s splošnim načelom enakega obravnavanja ne glede na starost ne sme uporabiti določb nacionalnega prava, ki so v nasprotju z njim. Tudi 10. člen PDEU določa, da si EU pri opredeljevanju in izvajanju svojih politik in dejavnosti prizadeva za boj proti diskriminaciji, med drugim tudi na podlagi starosti. Prepoved diskriminacije na podlagi starosti določa tudi 21. člen Listine EU. Na nacionalni ravni pa je za področje regulativnega okvira za razvoj in uporabo umetne inteligence potrebno upoštevati Ustavo RS, ki prepoveduje diskriminacijo na podlagi kakršnekoli osebne okoliščine[112] in Zakon o varstvu pred diskriminacijo.

6.4.2 Pravice starejših v praksi

Tako kot imamo na eni strani kot ranljivo skupino oseb otroke, ki so zaradi dejstva, da so se rodili ali/in odraščali v digitalni dobi, posledično vešči pri uporabi tehnologij ter digitalnih medijev, imamo na drugi strani popolno nasprotje pri ranljivi skupini starejših oseb, katerim svet digitalizacije predstavlja popolnoma novi svet, katerega niso navajeni. Za današnjo dobo je značilno starajoče se prebivalstvo, kar pomeni, da se vse države soočajo z večjim številom in deležom starejših oseb v svoji populaciji. V letu 2019 je 703 milijonov oseb, starejših od 65 let, sestavljalo del

[111] C-144/04, *Mangold*, ECLI:EU:C:2005:709.
[112] Glej 14. člen Ustave RS.

svetovnega prebivalstva.[113] Pričakovano je, da se bo število le teh do leta 2050 ponovno podvojilo in doseglo 1,5 milijarde. Tako naj bi do leta 2050 ena od šestih oseb bila starejša od 65 let. Tudi Slovenija ni izjema pri soočanju s starajočim se prebivalstvom. Po podatkih statističnega urada je v Sloveniji danes več kot 420 tisoč prebivalcev starejših od 65 let. Čez pet let jih bo več kot 470 tisoč, leta 2030 več kot pol milijona. Čez 30 let bo starejši od 65 let že vsak tretji prebivalec Slovenije.[114] Inovacije in tehnologija bi lahko predstavljale preobrazbo ekonomskega in socialnega sodelovanja in zdravja starejših oseb, ki ostajajo najbolj izpostavljeni digitalni izključenosti. Ker starejše osebe sodijo med ranljivejše skupine oseb, jim je potrebno zagotoviti ustrezno spoštovanje njihovih pravic v povezavi z digitalizacijo. Zato je v skladu z načelom preprečevanja škode potrebno, da so sistemi umetne inteligence in okolja, v katerih delujejo, varna in zaščitena ter da se zato posledično starejšim kot ranljivim osebam nameni večjo pozornost in se jih vključi v razvoj ter uvajanje sistemov umetne inteligence.[115] Kajti dejstvo je, da živimo v svetu, v katerem je naše delo, kvaliteta življenja, zdravje in okolje spremenjeno zaradi vpliva umetne inteligence. Del tega sveta so tudi starejši in kljub napredku, ki ga svet doživlja, veliko starejših oseb zaostaja in se sooča z ovirami, ki jih ločujejo od polnega sodelovanja v socialnem, kulturnem, gospodarskem in političnem življenju.[116] Zato je potrebno ukrepati v smeri digitalne vključenosti za starejše in vsakemu posamezniku v vsaki družbi zagotoviti možnost pridobitve digitalnih veščin.

V povezavi z digitalizacijo se pogosto uporablja tudi pojem digitalna pismenost, katero se pogosto opredeljuje kot "življenjska spretnost", oblika individualne tehnološke kompetence, ki predstavlja predpogoj za polno sodelovanje v družbenem življenju. Ta pismenost pa je ravno to, kar starejšim primanjkuje in tako starejši ljudje ob digitalizaciji postajajo nepismeni, nebogljeni in nesposobni. Zaradi pomanjkanj teh znanj so torej posledično prikrajšani in izključeni, kar je v nasprotju z njihovimi

[113] United Nations, Department of Economic and Social Affairs, Population Division. World Population Ageing 2019: Highlights (ST/ESA/SER.A/430), 2019, <https://www.un.org/en/development/desa/population/publications/pdf/ageing/WorldPopulationAgeing2019-Highlights.pdf> (15.6.2020).
[114] Biti v Sloveniji star, 20.6.2020 <https://www.24ur.com/novice/inspektor/biti-v-sloveniji-star.html> (20.6.2020).
[115] Strokovna skupina na visoki ravni za umetno inteligenco, Etične smernice za zaupanja vredno umetno inteligenco, 2019, str. 15, <https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=60438> (28.3.2020).
[116] United Nations Social development network (UNDSN), Why are Digital Skills Critical for Older Persons?, 2018, <https://unsdn.org/2018/02/12/digital-skills-for-older-persons/> (16.6.2020).

pravicami. Poleg že socialne izključenosti,[117] katero trpijo starejši na sploh, se v tej nalogi izpostavlja predvsem digitalno izključenost[118] starejših in kot je že bilo omenjeno predstavljajo starejše osebe skupino oseb, ki je ravno najbolj izpostavljena tej digitalni izključenosti. Kjer se pojavlja tveganje izključenosti oseb, se ta z uporabo IKT in na sploh z razvojem digitalizacije še poveča,[119] kar je mogoče opaziti ravno pri starejših.

Digitalna izključenost starejših se je ponovno lahko pokazala sedaj, v času širjenja nalezljive bolezni COVID-19. Trenutno je Vlada RS v predlogu novele tretjega protikoronskega zakona[120] pripravila pravno podlago za uvedbo mobilne aplikacije za spremljanje stikov z okuženimi osebami s koronavirusom in nadzor karanten. Tako je torej v obravnavi predlog zakona, s katerim naj bi se zaradi preprečevanja širjenja nalezljive bolezni COVID-19 določala vzpostavitev in zagotavljanje delovanja mobilne aplikacije za obveščanje oseb o stikih z okuženimi z virusom SARS-CoV-2. Namestitev in uporaba te aplikacije bi bila sicer prostovoljna, z izjemo okuženih oseb z virusom, ki bi si potem to aplikacijo morale obvezno namestiti. Tu pa se sedaj pojavi problem, saj si nekateri posamezniki, ki bi se izkazali za okužene, aplikacije niti ne bi moglo naložiti, ker nimajo novejšega pametnega telefona. Le na teh namreč aplikacije zanesljiveje delujejo, kot kažejo izkušnje, kar pomeni, da bi bil velik del populacije, tudi najranljivejši del, iz tega ukrepa izključen.[121] Med to populacijo sodi tudi veliko starejših. Na izključenost le teh opozarja informacijski pooblaščenec v svojem mnenju o predlogu zakona glede aplikacije za sledenje kontaktov.[122] Nadalje navaja, da je zaradi dejstva, da si veliko posameznikov aplikacije ne bo moralo naložiti aplikacije, posledično izredno težko utemeljiti sorazmernost in nujnost obvezne aplikacije. Saj glede na to, da je aplikacija lahko

[117] Socialna izključenost pomeni nesprejemanje posameznika ali skupine ljudi s strani družbenega okolja. Temelji lahko na rasi, etničnosti, jeziku, kulturi, religiji, spolu, starosti, socialnem razredu, ekonomskem ali zdravstvenem stanju. Socialna izključenost odvzema človeku njegove temeljne pravice in veže nase revščino, prikrajšanost in nestrpnost (definicija dostopna na: <http://www.inst-antonatrstenjaka.si/gerontologija/slovar/1026.html> (11.6.2020)).

[118] Kljub tesni povezanosti digitalne izključenosti in socialne izključenosti, ta dva pojma ne smemo enačiti.

[119] Mcloughlin, S.: Connecting the dots: young people, social inclusion and digitalisation - Rapporteur Report, 2018, <https://www.researchgate.net/publication/332212146_Connecting_the_dots_young_people_social_inclusion_and_digitalisation_-_Rapporteur_Report> (19.5.2020).

[120] Besedilo Predloga zakona o interventnih ukrepih za pripravo na drugi val COVID-19, EPA 1249-VIII, <https://www.dz-rs.si/wps/portal/Home/deloDZ/zakonodaja/izbranZakonAkt?uid=660D433BFF5F87E6C125859700317B0C&db=pre_zak&mandat=VIII&tip=doc> (30.06.2020).

[121] Informacijski pooblaščenec: Predlog zakona glede aplikacija za sledenje kontaktov, <https://www.ip-rs.si/novice/predlog-zakona-glede-aplikacija-za-sledenje-kontaktov-1191/> (26.6.2020).

[122] Ibidem.

učinkovita le, če jo naloži več kot polovica populacije, že dejstvo, da velik del populacije niti nima primernih telefonov za to, postavi presojo nujnosti in sorazmernosti pod velik vprašaj. Nujnost in sorazmernost morata biti izpolnjeni, saj predstavljata med drugim tudi pogoja za dopustitev novih pravnih podlag, ki bi nalagale obvezno rabo aplikacije. V okviru Evropskega pravnega reda je lahko sprejemljiva le prostovoljna namestitev aplikacije, ki bi zbirala kakršnekoli osebne podatke. Zato morajo nove pravne podlage, ki bi nalagale obvezno rabo aplikacije (npr. za potrjeno okužene), spoštovati temeljne standarde varstva pravic posameznikov. Te morajo biti zakonite in ustavne, časovno omejene, morajo biti nujne in sorazmerne glede na zasledovani cilj, ki je v tem primeru omejevanje epidemije COVID-19, in tega cilja ni mogoče doseči z milejšimi sredstvi. Te aplikacije za sledenje posegajo in tako odpirajo veliko vprašanj glede zasebnosti posameznikov ter varstva njihovih osebnih podatkov. Še posebej, ker se zdravstveni podatki v skladu s Splošno uredbo o varstvu podatkov[123] štejejo za občutljive podatke, ki jih je dovoljeno obdelovati le pod strogimi zahtevami. EU podpira uporabo mobilnih aplikacij kot pomoč pri zajezitvi širjenja COVID-19. Evropska komisija je zato sprejela priporočilo[124] za podporo postopni odpravi zajezitvenih ukrepov zaradi koronavirusa z mobilnimi podatki in aplikacijami. V njem so določena ključna načela za uporabo mobilnih aplikacij pri ukrepih omejevanja socialnih stikov ter opozarjanju, preprečevanju in sledenju stikov. Pri kakršnikoli uporabi aplikacij in podatkov bi bilo treba upoštevati varnost podatkov ter temeljne pravice EU, kot sta zasebnost in varstvo podatkov. Nato pa je objavila še usmeritve[125] za zgotovitev standardov polnega varstva podatkov pri aplikacijah za boj proti pandemiji.

Dejstvo glede starejših osebah, da jih večina ne uporablja nikakršnega digitalnega medija in omrežja, pa se kaže tudi v posledicah osamljenosti starejših. Do nekakšne mere poskušajo ta primanjkljaj nadomestiti različne ustanove socialne države ter razne humanitarne in prostovoljske mreže. V primeru, da se poskrbi za starejše, da so tudi ti digitalno vključeni, bi lahko s pomočjo orodij umetne inteligence oblažili njihovo osamljenost in jim pomagali, da so bolj socialno angažirani. To jim lahko

[123] Glej 9. člen Splošne uredbe o varstvu podatkov.
[124] Priporočilo Komisije (EU) 2020/518 z dne 8. aprila 2020 o skupnem naboru orodij za uporabo tehnologije in podatkov za boj proti krizi zaradi COVID-19 in izhod iz nje, zlasti v zvezi z mobilnimi aplikacijami in uporabo anonimiziranih podatkov o mobilnosti, UL L 114, 14.4.2020.
[125] Sporočilo Komisije Usmeritve v zvezi z varstvom podatkov za aplikacije, ki podpirajo boj proti pandemiji COVID-19 2020/C 124 I/01, Uradni list Evropske unije, C 124I , 17.4.2020.

pomaga zmanjšati tveganja za nastanek kakršnihkoli kognitivnih motenj ali demence.[126] Tako na primer sedaj raziskovalci iz družbe IBM skupaj z Univerzo v Kaliforniji izvajajo raziskavo, katere namen je preizkusiti in odkriti, kako lahko umetno inteligenco uporabimo za odkrivanje blagih kognitivnih motenj.[127] Poleg tega in možnosti do lažje interakcije z drugimi, se robote in druga orodja lahko uporabi tudi kot sredstvo komuniciranja s starejšimi in tako posledično se zmanjša njihovo osamljenost. Vendar je tudi tu zopet potrebno vzeti v obzir etične pomisleke, na katere opozarjajo razne mednarodne in nacionalne institucije za varstvo človekovih pravic. Tako bi bilo treba te umetne sprejemljevalce razumeti kot nekakšen dodatek k redni interaciji s človekom in družbo, ne pa kot nadomestitev tega.

Ker starejše osebe po večini niso navajene digitalnega okolja, niti nimajo digitalnih veščin, ne preseneča dejstvo, da je med populacijo visoka stopnja posameznikov, ki niso še nikoli uporabljali interneta, ravno med starejšimi. Posledično podatki, ustvarjeni na internetu, ne predstavljajo določene skupino oseb - v tem primeru starejših oseb.[128] To pa vodi do diskriminacije, ki je sicer prepovedana. Prepoved diskriminacije v vseh okoliščinah glede na starost je pravica, ki je tudi zajeta v pravice starejših. Načelo nediskriminacije na podlagi starosti je ena temeljih načel evropskega prava in tako posledično predstavlja eno temeljnih pravic, ki jih je potrebno zavarovati pred vplivi, ki jih prinaša umetna inteligenca.

Digitalizacija vpliva tudi na starejše osebe, ki so še v delovnem razmerju. Ker prinaša digitalizacija številne novosti, katerim se starejši delavci težje prilagajajo, je potrebno to vzeti v obzir in poskrbeti za vključevanje, prilagoditve in učenje novih znanj starejših v delovnem razmerju.[129] Potrebno bo obravnavati preobrazbe, ki se bodo zgodile v delovnih okoljih zaradi digitalizacije in pri obravnavanju naj se poudarek daje na to, kakšne vplive bodo inovacije imele na veščine, naloge in vloge, ki jih dejansko trenutno opravljajo starejši. Pri samem usposabljanju pa je potrebno, da so

---

[126] 5 Ways that Artificial Intelligence Will Impact the Senior Living Industry, 6.6.2018 <https://www.welbi.co/single-post/5-ways-that-artificial-intelligence-will-impact-the-senior-living-industry> (27.6.2020).
[127] Ibidem.
[128] FRA: Data Quality and AI-mitigating bias and error to protect fundamental rights, Focus paper, 11.6.2019, <https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-data-quality-and-ai_en.pdf> (27.6.2020).
[129] Checcucci P.: The silver innovation. Older workers characteristics and digitalisation of the economy, Intervento a "ASTRIL Conference", Università Roma Tre, Roma, 2018, str. 19, <http://oa.inapp.org/xmlui/handle/123456789/329> (21.5.2020).

programi in strategije, s katerimi se to izvaja, opisane na razumljiv način za starejše osebe. Pozorni moramo biti na vključenost starejših delavcev in če oziroma kako so njihove kognitivne sposobnosti vzete v obzir.

Eden od primerov priložnosti, ki jih prinaša umetna inteligenca s poseganjem v osebnost starejših je, da je umetno inteligenco mogoče uporabiti za zdravljenje in oskrbo starejših oseb.[130] Ker je za Evropo značilno starajoče se prebivalstvo, predstavljata umetna inteligenca in robotika dobri orodji za pomoč negovalcem, podporo oskrbi starejših in spremljanje stanj pacientov v realnem času, s čimer se lahko privede do reševanja življenj. Na primer na Japonskem že uporablajo raznolika orodja umetne inteligence, vključajoč robote, senzorje in programsko opremo, namesto zdravstvenih delavcev, da se odpravi primanjkljaj ustrezno usposobljenih zdravstvenih delavcev.[131] Ta orodja oziroma pripomočki bodo zdravstvenim delavcem omogočili boljši pregled nad zdravjem starejših. Večja zbirka podatkov o zdravstvenem stanju pa jim bo omogočila postavljanje natančnejših diagnoz. Prav tako se z napravami umetne inteligence lahko izvede bolj natančno odkrivanje in preprečevanje tveganj fizičnega ali duševnega zdravja.[132] Zgodnejša odkrivanja tako lahko preprečijo nastanek resnejših težav z zdravjem in posledično podaljšajo življenje.

6.4.3 Iniciative v zvezi z varstvom pravic starejših

Dejstva, da se v svetu povečuje število in delež starejših, se zavedajo tudi organi na mednarodni ravni, ravni EU in nacionalni ravni. Tako je na ravni EU Evropska komisija glede na priložnosti in izzive, povezane s pravicami, potrebami in zahtevami naraščajočega prebivalstva, začela strategijo Srebrne ekonomije.[133] Kot del te se omenja prednosti, ki jih tehnologija lahko doprinese zdravstveni oskrbi starejših, vključno z roboti in drugimi napravami, ki bi lahko pomagale. V strategiji je omenjena tudi potreba po širjenju in povezovanju tehnologij, ki so uporabnikom

[130] Strokovna skupina na visoki ravni za umetno inteligenco, Etične smernice za zaupanja vredno umetno inteligenco, str. 40.
[131] 5 Ways that Artificial Intelligence Will Impact the Senior Living Industry, 6.6.2018 <https://www.welbi.co/single-post/5-ways-that-artificial-intelligence-will-impact-the-senior-living-industry> (27.6.2020).
[132] Strokovna skupina na visoki ravni za umetno inteligenco, Etične smernice za zaupanja vredno umetno inteligenco, str. 40.
[133] The Silver economy – final report, 2018, <https://op.europa.eu/en/publication-detail/-/publication/a9efa929-3ec7-11e8-b5fe-01aa75ed71a1> (28.6.2020).

prijazne in pomagajo starejšim premagati socialno izolacijo. Zato se med drugim kot ključno priporočilo, kako spodbuditi rast srebrne ekonomije navaja tudi podpora tehnološki in digitalni revoluciji na področju zdravstvene oskrbe.[134]

Nadalje se na ravni EU zavedajo tudi izključenosti starejših in zato se kot ene ključnih smernic za oblikovanje zaupanja vredne inteligence predvideva spodbujanje usposabljanja in izobraževanja, da bodo vse skupine oseb, vključno s starejšimi, seznanjene in usposobljene že za uporabo umetne inteligence.[135] Tako so tudi na nacionalni ravni v okviru dokumenta Digitalna Slovenija 2020 kot strateški cilji med drugim določeni:

- Izboljšanje digitalne pismenosti prebivalstva;
- Izboljšanje e-kompetenc in e-veščin prebivalstva;
- Večja e-vključenost in omogočanje dostopa do e-storitev vsem skupinam prebivalstva, še posebej manj izobraženim, starejšim, invalidom in neaktivnim;
- Izboljšanje spletne dostopnosti v skladu z mednarodnimi smernicami;
- Izboljšanje kakovosti sistema vzgoje in izobraževanja z odprtimi učnimi okolji, smiselno uporabo IKT v učnih procesih in z učinkovitimi digitalnimi učnimi vsebinami;
- Optimizacija vodenja in upravljanja vzgojno izobraževalnih zavodov z digitalizacijo poslovanja;
- Zagotoviti ustrezno omrežno in storitveno digitalno infrastrukturo za potrebe izobraževanja, raziskovanja in kulture.

Usmeritve glede prilagajanja delovnih mest in procesov starejši delovni sili ter tehnološkemu napredku in digitalizaciji na nacionalni ravni vključuje Strategija dolgožive družbe.[136] To je leta 2017 sprejela Vlada Republike Slovenije kot ukrep spoprijemanja z demografskimi spremembami, ki jih prinaša starajoče se prebivalstvo in zaradi zavedanja, da je treba temu prilagoditi obstoječe sisteme in

[134] Ibidem, str. 43.
[135] Strokovna skupina na visoki ravni za umetno inteligenco, Etične smernice za zaupanja vredno umetno inteligenco.
[136] Urad RS za makroekonomske analize in razvoj (UMAR), Strategija dolgožive družbe, 2017, dostopno na: <https://www.umar.gov.si/fileadmin/user_upload/publikacije/kratke_analize/Strategija_dolgozive_druzbe/Strategija_dolgozive_druzbe.pdf> (26.5.2020).

ureditve ter tako izkoristiti zmogljivosti spremenjene starostne strukture. Ustvariti moramo možnosti in priložnosti za kakovostno življenje vseh generacij in dostojno staranje. Tako je ta strategija oblikovana na konceptu aktivnega staranja, ki poudarja aktivnost in ustvarjalnost v vseh življenjskih obdobjih, skrb za zdravje in medgeneracijsko sodelovanje ter solidarnost.[137] Usmeritve v okviru strategije izhajajo tudi iz zavedanja, da so človekove pravice enake za vse ljudi ne glede na starost. Strategija dolgožive družbe temelji na štirih temeljih in sicer na:

- trg dela in izobraževanje
- samostojno, zdravo in varno življenje vseh generacij
- vključenost v družbo
- oblikovanje okolja za aktivnost v celotnem življenjskem obdobju[138]

V okviru vključenosti v družbo podaja strategija usmeritve za medgeneracijsko sodelovanje, prostovoljstvo, uporaba IKT za komunikacijo, preprečevanje diskriminacije in nasilja v družbi in politično udejstvovanje. V okviru oblikovanja okolja za aktivnost v celotnem življenskem obdobju pa podaja usmeritve za prilagoditev v gospodarstvu, bivalnih razmer in prometne ureditve s podporo IKT in tehnoloških rešitev. Lahko vidimo, da vključuje tudi rešitve in usmeritve glede tehnološkega razvoja in digitalizacije dolgožive družbe in njihovih pravic v zvezi s tem. Te usmeritve v okviru Strategije dolgožive družbe predstavljajo tudi pomoč pri pripravi akcijskih načrtov.[139] Leta 2018 pa je bil ustanovljen Svet za aktivno staranje in medgeneracijsko sodelovanje.

Glede uporabe orodij umetne inteligence in robotov kot v pomoč pri zdravstveni oskrbi ali pri odpravljanju osmljenosti starejših, Odbor za državljanske svoboščine, pravosodje in notranje zadeve v Poročilu s priporočili Komisiji o pravilih civilnega prava o robotiki[140] podaja mnenje, da je potrebno obravnavati in preučiti psihološke in družbene učinke interakcije ljudi in robotov. Tudi Odbor za pravne zadeve v istem

[137] Ibidem, str. 5.
[138] Ibidem, str. 6.
[139] Kenda, A.: Usmeritve na področju aktivnega staranja, v: Kovšca, A., in drugi: Starejši kot sedajnost in prihodnost družbe, Zbornik referatov in razprav, št. 3, 2018, str. 21-30, <http://www.ds-rs.si/sites/default/files/dokumenti/ds_zbornik_starejsi_notranjost_e.pdf> (30.5.2020).
[140] Poročilo s priporočili Komisiji o pravilih civilnega prava o robotiki, 2015/2103(INL) z dne 27. januarja 2017, <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A8-2017-0005+0+DOC+XML+V0//SL> (28.6.2020).

Poročilu navaja, da se razvoj robotike in umetne inteligence lahko načrtuje in mora načrtovati tako, da bo ohranil dostojanstvo, samostojnost in samoodločanje posameznikov, zlasti na področju nege ljudi in druženja ter pri zdravstvenih napravah, ki ozdravljajo ali izboljšujejo zdravstvena stanja ljudi. Zato tudi EU financira projekt CARESSES, ki se ukvarja z roboti za oskrbo starejših, pri čemer je poudarek na njihovi kulturni občutljivosti.[141]

Obravnavanje tega je pomembno, saj kljub koristim, ki bi jih uporaba umetne inteligence doprinesla pri oskrbi starejših, se tu pojavijo tudi etični pomisleki, povezani s/z:

- možnim zmanjšanjem števila človeških stikov;
- povečanjem občutka objektivizacije in izguba nadzora;
- izgubo zasebnosti;
- izgubo osebne prostosti;
- prevaro in infantilizacijo;
- okoliščinami, v katerih je treba starejšim ljudem omogočiti nadzor nad roboti.[142]

Kajti, če bi prišlo do nastopa katerih izmed teh pomislekov, bi prišlo do kršenja pravice starejših, ki jo določa 25. člen Listine EU. Kršena bi bila njihova pravica do dostojnega in samostojnega življenja ter sodelovanja v družbenem in kulturnem življenju. Poleg etičnih pomislekov, s katerimi se tu srečujemo, je pomembno omeniti še vprašanje, kako je glede odgovornosti za škodo, ki bi jo povzročil robot pri oskrbi starejših. Kdo odgovarja za nastalo škodo? Zaenkrat to vprašanje še ni urejeno.[143] Je pa pomembno, da se to pravno uredi. Tako tudi Odbor za pravne zadeve v Poročilu s priporočili Komisiji o pravilih civilnega prava o robotiki navaja, da je človeštvo zdaj na pragu obdobja, ko vedno bolj napredni roboti, androidi in druge oblike na pragu umetne inteligence povzročajo novo industrijsko revolucijo, ki bo vplivala na celotno družbo, in da je zelo pomembno, da zakonodajalci obravnavajo vse njene pravne in etične posledice. Poudarijo tudi, da bolj kot so roboti avtonomni, tem manj jih je mogoče obravnavati kot preprosta orodja v rokah

[141] <http://caressesrobot.org/en/project/> (4.4.2020).
[142] European Parliamentary Research Service (EPRS), The ethics of artificial intelligence: Issues and initiatives – study, 2020, <https://www.europarl.europa.eu/stoa/en/document/EPRS_STU(2020)634452> (22.6.2020).
[143] Jakšić, J.: Ali je pravo pripravljeno na izzive umetne inteligence?, v: Pravna praksa, št. 43, 2017, str. 17-19.

drugih akterjev. Problem, ki se pojavi v zvezi z roboti, je predvsem v tem, da je naravo delovanja tovrstnih entitet težko uvrstiti v zdajšnje pravne kategorije, saj gre za neke vrste "bitja" sui generis. Glede na veljavne pravne ureditve v evropskih državah izhaja dejstvo, da se robote ne more šteti odgovorne za svoja ravnanja.[144] Kajti zaenkrat se jih v pravu še vedno obravnava kot stvar in tako nimajo pravne subjektivitete. Zato veljavna pravila o odgovornosti zajemajo zgolj primere, ko se vzrok za robotovo dejanje lahko poveže z določenim človeškim agentom, kot je na primer proizvajalec, upravljavec, lastnik ali uporabnik, pri čemer pa bi ta agent lahko predvidel in preprečil robotovo škodljivo vedenje. Tudi glede na dosedanjo sodno prakso je nastopila odgovornost in sankcioniranje za škodljiva ravnanja zaradi uporabe informacijske tehnologije in programske opreme sankcioniralo samo takrat, ko je krivdno (praviloma malomarno) ravnal razvijalec, ustvarjalec ali programer.[145] Ta bi se potem lahko razbremenil svoje odgovornosti, če je škoda nastala brez njegove krivde, kar pomeni, da ne odgovarja, če je ravnal po pravilih stroke in s potrebno skrbnostjo. Tako stališče je izoblikovalo newyorško vrhovno sodišče v zadevi Jones proti W+M Automation, Inc.,[146] kjer je odločilo, da lastnik robota za njegovo ravnanje ne odgovarja, če ravna v skladu s pravili stroke. Kar vključuje tudi to, da proizvajalec ni odgovoren za škodo, če dokaže, da raven znanosti in tehničnega napredka v času, ko je dal proizvod v promet, ni bila takšna, da bi bilo mogoče napako na proizvodu odkriti.[147] In kako ukrepati v primeru, ko ni človeške krivde, saj velikokrat ni mogoče predvideti nastanka škode. V takšnem primeru bi se lahko uporabil institut odškodninskega prava, to je koncept objektivne odgovornosti, odgovarjanje ne glede na krivdo. V skladu z Direktivo 85/374 proizvajalec proizvoda odgovarja ne glede na krivdo, če oškodovanec uspe dokazati škodo, napako na proizvodu in vzročno zvezo med napako in škodo.[148] Vendar je v večini primerih težko dokazati napako in vzročno zvezo. Zato bi mogoče bilo smiselno, da se na ravni EU vzpostavijo pravila, ki nacionalnim pravnim redom nalagajo uporabo pravil za obrnjeno dokazno breme pri dokazovanju. Naj dokazuje tisti, ki ima koristi od tega, da je določen proizvod dal v promet.

144 Ibidem.
145 Ibidem.
146 Sodba pritožbenega oddelka Vrhovnega sodišča v New Yorku v zadevi Jones v. W+M Automation, Inc. 31 A.D.3d 1099 (2006) z dne 7. julija 2006.
147 Glej 7(e). člen Direktive Sveta z dne 25. julija 1985 o približevanju zakonov in drugih predpisov držav članic v zvezi z odgovornostjo za proizvode z napako, Uradni list Evropske unije, L 210, 7.8.1985, str. 29–33.
148 Glej 4. člen Direktive 85/374.

Ugotovimo lahko, da so starejše osebe že dolgo v ozadju politik držav. Dejstva, da se položaju pravic starejših po vsem svetu ne posveča dovolj pozornosti in da različne človekove pravice niso ustrezno zaščitene s starostjo ljudi, se zaveda tudi OZN.[149] Zato eno pomembnejših iniciativ v zvezi z varstvom pravic starejših predstavlja pobuda za sprejete Konvencije o pravicah starejših. Tako delovna skupina OZN za staranje razpravlja o sprejetju posebne konvencije o pravicah starejših, kot je bilo to že prej storjeno za pravice otrok, žensk in invalidov. Zagovorniki za sprejem konvencije navajajo, da je Konvencija ZN o pravicah starejših ljudi s posebnim poročevalcem nujna, da bi zagotovili spoštovanje pravic starejših žensk in moških, saj bi vladam držav članic nudila pravni okvir, vodstvo in pomoč do boljše zagotovitve realizacije pravic starih ljudi v starajočih se družbah.[150] Konvencijo o pravicah starejših ljudi potrebujemo, ker:

- je starostna diskriminacija nesprejemljiva in jo moramo ustrezno nasloviti,
- človekove pravice spreminjajo življenja in omogočajo varno, dostojno in enakopravno življenje v družbi,
- obstoječe mednarodno in regionalno pravo o človekovih pravicah pravic starejših ne zaščiti v zadostni meri,
- so človekove pravice povezane z razvojem in blagostanjem,
- so človekove pravice standard za različne storitve.[151]

Menim, da če bi prišlo do sprejetja te konvencije, bi bilo smiselno vanjo vključiti tudi določbe, ki bi urejale pravice starejših v povezavi z razvojem in uporabe umetne inteligence, saj je nesporno, da ta povezava že je in bo v prihodnosti stalnica vsakdanjega življenja starejših oseb ter bo v veliki meri vplivala nanje.

6.5 Zaključek

Vsak poseg v človekove pravice ali kakršnokoli vplivanje nanje mora biti zaradi pomembnosti spoštovanja le teh zakonito in pravno utemeljeno. Spoštovanje človekovih pravic predstavlja tudi eno izmed vrednot, na katerih temeljijo

[149] Zveza društev upokojencev Slovenije <http://www.zdus-zveza.si/belgijska-resolucija-podpira-mednarodno-konvencijo-o-clovekovih-pravicah-starejsih> (29.6.2020).
[150] Starc M.: Pravice starejših ljudi, v: Kakovostna starost, letnik 13, št. 4, 2010, <http://www.inst-antonatrstenjaka.si/tisk/kakovostna-starost/clanek.html?ID=899> (30.6.2020).
[151] Ibidem.

mednarodne organizacije, EU in posledično tudi države članice ter se zato morajo vse s svojim pravom boriti proti vsakršnem nespoštovanju človekovih pravic in nezakonitem posegu vanje. Kot lahko opazimo iz prispevka, je eno izmed aktualnih področij, ki lahko privede do posega v človekove pravice, umetna inteligenca. Razvoj in uporaba le te med drugim predstavlja tudi velik poseg v pravico do enakosti moških in žensk, pravice otrok in pravice starejših. Glede na ugotovitve iz prispevka naj bi uporaba umetna inteligenca in novih tehnologij povzročila številne nevarnosti pri spoštovanju teh treh človekovih pravic. Tako naj bi se zaradi uporabe umetne inteligence pojavile neenakosti med ženskami in moškimi pri dostopu do zaposlovanja, storitev in blaga. In sicer je mogoče ugotoviti, da bi v večini primerov zaradi uporabe in razvoja umetne inteligence bile ženske v slabšem položaju v primerjavi z moškimi. V večini primerov uporaba umetne inteligence pusti negativni vpliv tudi na otrocih in njihovih pravicah, saj so ti zaradi te izpostavljeni spletnemu nadlegovanju in nasilju, posegu v pravico do zasebnosti, zlorabi osebnih podatkov, kibernetski kriminaliteti, neprimernim vsebinam in celo spolnim zlorab. Vendar pa lahko uporaba umetne inteligence otrokom doprinese tudi dobre priložnosti, npr. možnost udejanjanja pravice do informiranja in podajanja mnenj ali pravice do izobraževanja. Pozitivno, vendar v večji meri negativno vpliva umetna inteligenca prav tako na pravice starejših, saj ta negativno vodi med drugim tudi do tega, da so starejši digitalno izključeni, digitalno nepismeni in diskriminirani. Pozitivno pa se jo lahko uporabi za zdravljenje in oskrbo starejših. Glede na ugotovitve raziskovalne naloge je mogoče opaziti, da pravo najmanj varuje in zapostavlja ravno starejše in njihove pravice. Tako je bilo že preteklosti in kot je videti, se bo ta vzorec ponavljal še dalje, tudi glede regulacije pravic starejših v povezavi z umetno inteligenco.

Torej uporaba umetna inteligenca prinaša s seboj številne etične dileme in nevarnosti glede spoštovanja ter varstva človekovih pravic, zato je tudi pomembno, da se to področje ustrezno regulirala. Kot je mogoče ugotoviti iz raziskovalne naloge so mednarodne organizacije, EU in države članice sicer začele z izvajanjem ukrepov za varstvo človekovih pravic v povezavi z umetno inteligenco, vendar pa so še oddaljene od tega, da bi to tudi ustrezno regulirale.

Tako lahko zaključim, da je v praksi čedalje več primerov, ko se pravo sooča z zapletenimi vprašanji uporabe umetne inteligence, povezanimi z varstvom pravice do enakosti, pravic otrok in pravic starejših, a je normativno urejanje teh vprašanj skopo in šele v povojih. Prav tako so glede na pomembnost tematike precej skopi

tudi izsledki pravne teorije. Toda mogoče je opaziti korake proti odpravi teh primanjkljajev.

Seznam literature in virov

Monografje

Klaus S.: Četrta industrijska revolucija, prevedel Igor Pauletič, World Economic Forum, Ženeva, 2016, dostopno na <http://assets.cdnma.com/8475/assets/Cetrta-industrijska-revolucija.pdf> (13.4.2020).

Članki in poglavja iz knjig

Starc M.: Pravice starejših ljudi, v: Kakovostna starost, letnik 13, št. 4, 2010.
Jakšić, J.: Ali je pravo pripravljeno na izzive umetne inteligence?, v: Pravna praksa, št. 43, 2017.

Pravni viri

Ustava Republike Slovenije (Uradni list RS, št. 33/91-I, 42/97 – UZS68, 66/00 – UZ80, 24/03 – UZ3a, 47, 68, 69/04 – UZ14, 69/04 – UZ43, 69/04 – UZ50, 68/06 – UZ121,140,143, 47/13 – UZ148, 47/13 – UZ90,97,99 in 75/16 – UZ70a).
Zakon o varstvu pred diskriminacijo (Uradni list RS, št. 33/16 in 21/18 – ZNOrg).
Zakon o enakih možnostih žensk in moških (Uradni list RS, št. 59/02, 61/07 – ZUNEO-A, 33/16 – ZVarD in 59/19).
Zakon o varstvu potrošnikov pred nepoštenimi poslovnimi praksami (Uradni list RS, št. 53/07)
Zakon o varstvu osebnih podatkov (Uradni list RS, št. 94/07 – uradno prečiščeno besedilo).
Besedilo Predloga Zakona o varstvu podatkov (ZVOP-2), EPA: 2733 – VII, < https://www.dz-rs.si/wps/portal/Home/deloDZ/zakonodaja/izbranZakonAkt?uid=C1257A70003EE6A1C12582670045DF4F&db=kon_zak&mandat=VII&tip=doc> (2.6.2020).
Besedilo Predloga zakona o interventnih ukrepih za pripravo na drugi val COVID-19, EPA 1249-VIII, <https://www.dz-rs.si/wps/portal/Home/deloDZ/zakonodaja/izbranZakonAkt?uid=660D433BFF5F87E6C125859700317B0C&db=pre_zak&mandat=VIII&tip=doc> (30.06.2020).
Zakon o ratifikaciji Konvencije ZN o odpravi vseh oblik diskriminacije žensk (Uradni list SFRJ – Mednarodne pogodbe št. 11/81) in Akt o notifikaciji nasledstva glede konvencij Organizacije združenih narodov in konvencij, sprejetih v Mednarodni agenciji za atomsko energijo (Uradni list RS – Mednarodne pogodbe, št. 9/92, 9/93, 5/99, 9/08, 13/11, 9/13 in 5/17).
Zakon o ratifikaciji Fakultativnega protokola k Mednarodnemu paktu o državljanskih in političnih pravicah (Uradni list RS – Mednarodne pogodbe, št. 9/93).
Konvencija št. 111 o diskriminaciji pri zaposlovanju in poklicih - Akt o notifikaciji nasledstva glede konvencij UNESCO, mednarodnih večstranskih pogodb o zračnem prometu, konvencij mednarodne organizacije dela, konvencij mednarodne pomorske organizacije, carinskih konvencij in nekaterih drugih mednarodnih večstranskih pogodb (Uradni list RS – Mednarodne pogodbe, št. 15/92, 1/97 in 17/15).
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 – Mednarodne pogodbe, št. 7/94).
Zakon o ratifikaciji Konvencije ZN o otrokovih pravicah (Uradni list SFRJ – Mednarodne pogodbe št. 15/90) in Akt o notifikaciji nasledstva glede konvencij Organizacije združenih narodov in konvencij, sprejetih v Mednarodni agenciji za atomsko energijo (Uradni list RS – Mednarodne pogodbe, št. 9/92, 9/93, 5/99, 9/08, 13/11, 9/13 in 5/17).
Svet Evrope, Strategija za otrokove pravice, CM(2015)175-final, 3. marec 2016.
Odbor ministrov Sveta Evrope, Guidelines to respect, protect and fulfil the rights of the child in the digital environment - Recommendation CM/Rec(2018)7 of the Committee of Ministers, 2018.
Pogodba o Evropski uniji, Uradni list Evropske unije, C 326, 26.10.2012, str. 13–390.
Pogodba o delovanju Evropske Unije, Uradni list Evropske unije, C 326/47, str. 47-390.
Listina Evropske Unije o človekovih pravicah, Uradni list Evropske unije, C 83/389, str. 391–407.

Uredba (EU) 2016/679 Evropskega Parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES, UL L 119, 4.5.2016; Glej drugi odstavek, točka f 13. člena in prvi odstavek, točka h 15. člena Splošne uredbe o varstvu podatkov.
Direktiva Sveta z dne 25. julija 1985 o približevanju zakonov in drugih predpisov držav članic v zvezi z odgovornostjo za proizvode z napako, Uradni list Evropske unije, L 210, 7.8.1985, str. 29–33.
Direktiva Evropskega parlamenta in Sveta 95/46/ES z dne 24. oktobra 1995 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov, Uradni list Evropske unije, L 281, 23.11.1995, str. 31–50.
Direktiva Sveta 2000/78/ES z dne 27. novembra 2000 o splošnih okvirih enakega obravnavanja pri zaposlovanju in delu, Uradni list Evropske unije, L 303, 2.12.2000.
Direktiva Sveta 2004/113/ES z dne 13. decembra 2004 o izvajanju načela enakega obravnavanja moških in žensk pri dostopu do blaga in storitev ter oskrbi z njimi, Uradni list Evropske unije, L 373, 21. 12. 2004.
Direktiva Evropskega parlamenta in Sveta 2005/29/ES z dne 11. maja 2005 o nepoštenih poslovnih praksah podjetij v razmerju do potrošnikov na notranjem trgu ter o spremembi Direktive Sveta 84/450/EGS, direktiv Evropskega parlamenta in Sveta 97/7/ES, 98/27/ES in 2002/65/ES ter Uredbe (ES) št. 2006/2004 Evropskega parlamenta in Sveta (Direktiva o nepoštenih poslovnih praksah) (Besedilo velja za EGP), Uradni list Evropske unije, L 149, 11.6.2005.
Direktiva 2006/54/ES Evropskega parlamenta in Sveta z dne 5. julija 2006 o uresničevanju načela enakih možnosti ter enakega obravnavanja moških in žensk pri zaposlovanju in poklicnem delu (preoblikovano), Uradni list Evropske unije, L 204 , 26. 7. 2006.
Direktiva 2011/93/EU Evropskega parlamenta in Sveta z dne 13. decembra 2011 o boju proti spolni zlorabi in spolnemu izkoriščanju otrok ter otroški pornografiji in nadomestitvi Okvirnega sklepa Sveta 2004/68/PNZ, Uradni list Evropske unije, L 335, 17.12.2011.
Direktiva (EU) 2019/790 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/ES (Besedilo velja za EGP), PE/51/2019/REV/1, Uradni list Evropske unije, L 130, 17.5.2019, str. 92–125.
Evropska komisija, BELA KNJIGA o umetni inteligenci - evropski pristop k odličnosti in zaupanju, COM(2020) 65 final.
Evropska komisija, Evropska strategija za boljši internet za otroke, COM/2012/0196 final, 2.maj 2012.
Priporočilo Komisije (EU) 2020/518 z dne 8. aprila 2020 o skupnem naboru orodij za uporabo tehnologije in podatkov za boj proti krizi zaradi COVID-19 in izhod iz nje, zlasti v zvezi z mobilnimi aplikacijami in uporabo anonimiziranih podatkov o mobilnosti, UL L 114, 14.4.2020.
Resolucija Evropskega parlamenta z dne 12. februarja 2019 o celoviti evropski industrijski politiki na področju umetne inteligence in robotike (2018/2088(INI)).
Resolucija Evropskega parlamenta z dne 17. aprila 2018 o krepitvi vloge in položaja žensk in deklet prek digitalnega sektorja (2017/3016(RSP)), Uradni list Evropske unije, C 390, 18.11.2019.
Resolucija Evropskega parlamenta z dne 28. aprila 2016 o enakosti spolov in krepitvi vloge žensk v digitalni dobi (2015/2007(INI)), Uradni list Evropske unije, C 66, 21.2.2018.
Resolucija o nacionalnem programu za enake možnosti žensk in moških 2015–2020 (Uradni list RS, št. 84/15).
Sporočilo Komisije Usmeritve v zvezi z varstvom podatkov za aplikacije, ki podpirajo boj proti pandemiji COVID-19 2020/C 124 I/01, Uradni list Evropske unije, C 124I , 17.4.2020.

Sodna praksa

Višje sodišče v Ljubljani, sklep IV Cp 661/2010, 17. marec 2010.
Višje sodišče v Mariboru, Sklep III Cp 295/2020, 21. maj 2020.
Višje sodišče v Ljubljani, sklep II Kp 9220/2011, 7. December 2012.
Sodba pritožbenega oddelka Vrhovnega sodišča v New Yorku v zadevi Jones v. W+M Automation, Inc. 31 A.D.3d 1099 (2006) z dne 7. julija 2006.
K.U. v. Finland, št. 2872/02, 2 December 2008.
C-144/04, *Mangold*, ECLI:EU:C:2005:709.
C-127/07, *Arcelor Atlantique et Lorraine in drugi*, ECLI:EU:C:2008:728.
C-236/09 , *Association Belge des Consommateurs Test-Achats in drugi*, ECLI:EU:C:2011:100.
C-335/17, *Valcheva,* ECLI:EU:C:2018:359.

Spletni viri

< https://www.coe.int/en/web/no-hate-campaign> (30.5.2020).
<http://caressesrobot.org/en/project/> (4.4.2020).
<https://ec.europa.eu/digital-single-market/en/women-ict> (15.4.2020).
<https://ec.europa.eu/digital-single-market/en/women-ict> (20.4.2020).
<https://home.crin.org/briefing-childrens-rights-in-the-digital-age> (14.4.2020).
<https://home.crin.org/briefing-childrens-rights-in-the-digital-age> (13.4.2020).
<https://www.euronews.com/2018/10/10/amazon-scraps-secret-ai-recruiting-tool-that-showed-bias-against-women> (25.5.2020).
<https://www.ohchr.org/_layouts/15/WopiFrame.aspx?sourcedoc=/Documents/HRBodies/CRC/Discussions/2014/DGD_report.pdf&action=default&DefaultItemOpen=1> (4.5.2020).
<https://www.unicef.si/> (4.5.2020).
5 Ways that Artificial Intelligence Will Impact the Senior Living Industry, 6.6.2018 <https://www.welbi.co/single-post/5-ways-that-artificial-intelligence-will-impact-the-senior-living-industry> (27.6.2020).
About Better Internet for Kids, <https://ec.europa.eu/digital-single-market/en/content/creating-better-internet-kids-0> (24.4.2020).
Agencija Evropske unije za temeljne pravice (FRA), #BigData: Discrimination in data-supported decisionmaking, 2018, str. 7, <https://fra.europa.eu/en/publication/2018/bigdata-discrimination-data-supported-decision-making> (27.6.2020).
Agencija Evropske unije za temeljne pravice (FRA), #BigData: Discrimination in data-supported decisionmaking, 2018, str. 7, <https://fra.europa.eu/en/publication/2018/bigdata-discrimination-data-supported-decision-making> (27.6.2020), str.10.
BIK, Team, Happy world children' day!, 2019, dostopno na <https://www.betterinternetforkids.eu/web/portal/practice/awareness/detail?articleId=5252966> (30.5.2020).
Biti v Sloveniji star, 20.6.2020 <https://www.24ur.com/novice/inspektor/biti-v-sloveniji-star.html> (20.6.2020).
Checcucci P.: The silver innovation. Older workers characteristics and digitalisation of the economy, Intervento a "ASTRIL Conference", Università Roma Tre, Roma, 2018, str. 19, <http://oa.inapp.org/xmlui/handle/123456789/329> (21.5.2020).
Concept note for the general Comment on children's rights in relation to the digital environment – Slovenia's comment, maj 2019 <https://www.ohchr.org/Documents/HRBodies/CRC/GCChildrensDigitalEnvironment/States/Slovenia.docx> (25.5.2020).
Digitalna Slovenija 2020 – Strategija razvoja informacijske družbe do leta 2020 <https://www.gov.si/assets/ministrstva/MJU/DID/Strategija-razvoja-informacijske-druzbe-2020.pdf> (6.4.2020).
Društvo psihologov Slovenije, O kriznih dogodkih in odzivih nanje <http://www.dps.si/za-javnost/koronavirus/> (16.6.2020).
Emeršič Polić K.: Izvrševanje stikov z otrokom med pandemijo koronavirusa COVID-19, <https://pirc-musar.si/sl/izvrsevanje-stikov-z-otrokom-med-pandemijo-koronavirusa/> (27.6.2020).
EU report on the future of work, str. 48, < https://ec.europa.eu/digital-single-market/en/news/future-work-work-future> (8.4.2020).
EU report on the future of work, str. 48, <https://ec.europa.eu/digital-single-market/en/news/future-work-work-future> (8.4.2020).
European Parliamentary Research Service (EPRS), The ethics of artificial intelligence: Issues and initiatives – study, 2020, <https://www.europarl.europa.eu/stoa/en/document/EPRS_STU(2020)634452> (22.6.2020).
Evropska komisija začenja javno posvetovanje o novem akcijskem načrtu za digitalno izobraževanje, Sporočilo za medije, 18.6.2020 <https://ec.europa.eu/commission/presscorner/detail/sl/ip_20_1066> (27.6.2020).
Evropska komisija, Creating a better Internet for kids <https://ec.europa.eu/digital-single-market/en/policies/better-internet-kids> (30.5.2020).
Evropska komisija, Poročilo vprašanjih varnosti in odgovornosti, ki jih sprožajo umetna inteligenca, internet stvari in robotika, COM(2020) 64 final
Expert Group on Liability and New Technologies – New Technologies Formatio, Liability for Artificial Intelligence and other emerging technologies, 2019, dostopno na <https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=63199> (27.6.2020).

FRA, Coronavirus pandemic in the EU - Fundamental rights implication: With a focus on contact tracing apps, Publications Office of the European Union, Luxembourg, 2020, str. 23, <https://fra.europa.eu/sites/default/files/fra_uploads/fra-2020-coronavirus-pandemic-eu-bulletin-may_en.pdf> (29.5.2020).

FRA, Data quality and artificial intelligence – mitigating bias and error to protect fundamental rights, 2019, <https://fra.europa.eu/en/publication/2019/data-quality-and-artificial-intelligence-mitigating-bias-and-error-protect> (30.5.2020).

FRA, Handbook on European law relating to the rights of the child, 2015, str. 190, <https://fra.europa.eu/sites/default/files/fra_uploads/fra-ecthr-2015-handbook-european-law-rights-of-the-child_en.pdf> (15.4.2020).

FRA: Data Quality and AI-mitigating bias and error to protect fundamental rights, Focus paper, 11.6.2019, <https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-data-quality-and-ai_en.pdf> (27.6.2020).

Hern A.: IBM quits facial-recognition market over police racial-profiling concerns, 2020, <https://www.google.com/amp/s/amp.theguardian.com/technology/2020/jun/09/ibm-quits-facial-recognition-market-over-law-enforcement-concerns> (10.6.2020).

Holmes A.: AI could be the key to ending discrimination in hiring, but experts warn it can be just as biased as humans, https://www.businessinsider.nl/ai-hiring-tools-biased-as-humans-experts-warn-2019-10/ (27.6.2020).

Husejnović K.: 'Vidi se, da vsi otroci doma niso imeli enakih pogojev', 2020, <https://www.24ur.com/novice/korona/pouk-na-daljavo.html> (16.6.2020).

Informacijski pooblaščenec, Privolitev, <https://www.ip-rs.si/zakonodaja/reforma-evropskega-zakonodajnega-okvira-za-varstvo-osebnih-podatkov/kljucna-podrocja-uredbe/privolitev/#c1932> (17.6.2020).

Informacijski pooblaščenec: Predlog zakona glede aplikacija za sledenje kontaktov, <https://www.ip-rs.si/novice/predlog-zakona-glede-aplikacija-za-sledenje-kontaktov-1191/> (26.6.2020).

Izvrševanje pravnomočnih sodnih odločb, ki urejajo stike otroka s tistim od staršev, ki mu otrok ni dodeljen v varstvo in vzgojo, 19.3.2020 <https://www.gov.si/novice/2020-03-19-izvrsevanje-pravnomocnih-sodnih-odlocb-ki-urejajo-stike-otroka-s-tistim-od-starsev-ki-mu-otrok-ni-dodeljen-v-varstvo-in-vzgojo/> (27.6.2020).

Kenda, A.: Usmeritve na področju aktivnega staranja, v: Kovšca, A., in drugi: Starejši kot sedajnost in prihodnost družbe, Zbornik referatov in razprav, št. 3, 2018, str. 21-30, <http://www.ds-rs.si/sites/default/files/dokumenti/ds_zbornik_starejsi_notranjost_e.pdf> (30.5.2020).

Klaus S.: Četrta industrijska revolucija, prevedel Igor Pauletič, World Economic Forum, Ženeva, 2016, str.55, <http://assets.cdnma.com/8475/assets/Cetrta-industrijska-revolucija.pdf> (13.4.2020).

Komisar za človekove pravice, Protecting children's rights in the digital world: an ever-growing challenge – komentar, <https://www.coe.int/en/web/commissioner/-/protecting-children-s-rights-in-the-digital-world-an-ever-growing-challen-1> (29.6.2020).

Levy A., Hirsch L.: Amazon bans police use of facial recognition technology for one year, 2020, <https://www.google.com/amp/s/www.cnbc.com/amp/2020/06/10/amazon-bans-police-use-of-facial-recognition-technology-for-one-year.html> (10.6.2020).

Manyika J., Silberg J., Presten B.: What do we do about the biases in AI., <https://hbr.org/2019/10/what-do-we-do-about-the-biases-in-ai> (19.5.2020).

McCaffrey, D. & Gill J.: EU wants to step up fight to protect children from sexual abuse online, 2020. Dostopno na <https://www.euronews.com/2020/06/09/eu-wants-to-step-up-fight-to-protect-children-from-sexual-abuse-online> (17.6.2020).

Mcloughlin, S.: Connecting the dots: young people, social inclusion and digitalisation - Rapporteur Report, 2018, <https://www.researchgate.net/publication/332212146_Connecting_the_dots_young_people_social_inclusion_and_digitalisation_-_Rapporteur_Report> (19.5.2020).

Peljhan M., Koronavirus in otroci s posebnimi potrebami, 2020, <https://www.rtvslo.si/kolumne/koronavirus-in-otroci-s-posebnimi-potrebami/518153> (16.6.2020).

Polli F.: Using AI to Eliminate Bias from Hiring, 2019, <https://hbr.org/2019/10/using-ai-to-eliminate-bias-from-hiring> (27.6.2020).

Poročilo s priporočili Komisiji o pravilih civilnega prava o robotiki, 2015/2103(INL) z dne 27. januarja 2017, <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A8-2017-0005+0+DOC+XML+V0//SL> (28.6.2020).

Rodriguez Martinez M., Gaubert J.: International Women day: how can algorithms be sexist, 2020, <https://www.euronews.com/2020/03/08/international-women-s-day-our-algorithms-are-sexist> (25.5.2020).

Sample I.: Internet 'is not working for women and girls', says Berners-Lee, 2020, <https://www.theguardian.com/global/2020/mar/12/internet-not-working-women-girls-tim-berners-lee> (24.4.2020).
Singer N., Metz C.: Many Facial-Recognition Systems Are Biased, Says U.S. Study, 2019, <https://www.google.com/url?sa=t&source=web&rct=j&url=https://www.nytimes.com/2019/12/19/technology/facial-recognition-bias.amp.html&ved=2ahUKEwjqwsK3pvjpAhVh7aYKHd3KB4kQFjAAegQIAhAB&usg=AOvVaw3w9XvA0vHBmnnhh_4HQ833&ampcf=1> (10.6.2020).
Strokovna skupina na visoki ravni za umetno inteligenco, Etične smernice za zaupanja vredno umetno inteligenco, 2019, str. 15, <https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=60438> (28.3.2020).
Taylor, K.: Women are twice as likely than men to lose their jobs to robots, 26.6.2017 <https://www.businessinsider.com/women-twice-as-likely-as-men-to-lose-their-jobs-to-automation-2017-6> (8.4.2020).
The Silver economy – final report, 2018, <https://op.europa.eu/en/publication-detail/-/publication/a9efa929-3ec7-11e8-b5fe-01aa75ed71a1> (28.6.2020).
Tonolo S.: International human rights law and the protection of elderly in Europe, v: Medicine, Law&Society, 11 (2018) 2, str. 107-120, <https://journals.um.si/index.php/medicine/article/view/118> (25.6.2020).
United Nations Principles for Older Persons , Adopted by General Assembly resolution 46/91 of 16 December 1991, <https://www.ohchr.org/EN/ProfessionalInterest/Pages/OlderPersons.aspx> (24.6.2020).
United Nations Social development network (UNDSN), Why are Digital Skills Critical for Older Persons?, 2018, <https://unsdn.org/2018/02/12/digital-skills-for-older-persons/> (16.6.2020).
United Nations, Department of Economic and Social Affairs, Population Division. World Population Ageing 2019: Highlights (ST/ESA/SER.A/430), 2019, <https://www.un.org/en/development/desa/population/publications/pdf/ageing/WorldPopulationAgeing2019-Highlights.pdf> (15.6.2020).
Urad RS za makroekonomske analize in razvoj (UMAR), Strategija dolgožive družbe, 2017, dostopno na: <https://www.umar.gov.si/fileadmin/user_upload/publikacije/kratke_analize/Strategija_dolgozive_druzbe/Strategija_dolgozive_druzbe.pdf> (26.5.2020).
Viola de Azevedo Cunha, M.: Child Privacy in the Age of Web 2.0 and 3.0: Challenges and Opportunities for Policy - Innocenti Discussion Paper, UNICEF Office of Research – Innocenti, 2017, str. 6, <https://www.unicef-irc.org/publications/pdf/Child_privacy_challenges_opportunities.pdf> (25.6.2020).
Viola de Azevedo Cunha, M.: Child Privacy in the Age of Web 2.0 and 3.0: Challenges and Opportunities for Policy.
Women in digital age - final report (2018), <https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=50224> (21.4.2020).
Women in digital age - final report (2018), <https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=50224> (21.4.2020), str. 132.
Zavod Republike Slovenije za šolstvo, Analiza izobraževanja na daljavo v času epidemije <https://www.zrss.si/objava/analiza-izobrazevanja-na-daljavo-v-casu-epidemije-2> (16.6.2020).
Zavod Republike Slovenije za šolstvo, Tablični računalniki za otroke iz socialno šibkejših družin <https://www.zrss.si/objava/tablicni-racunalniki-za-otroke-iz-socialno-sibkejsih-druzin> (18.6.2020).
Zveza društev upokojencev Slovenije <http://www.zdus-zveza.si/belgijska-resolucija-podpira-mednarodno-konvencijo-o-clovekovih-pravicah-starejsih> (29.6.2020).

DOI
https://doi.org/10.18690/um.pf.4.2023.7

ISBN
978-961-286-774-4

7 TEMELJNE PRAVICE IN IZZIVI DIGITALIZACIJE: IZOBRAŽEVANJE, DELO IN SODSTVO

ŽIVA ŠUTA
Univerza v Mariboru, Pravna fakulteta, Maribor, Slovenija
ziva.suta@student.um.si

Ključne besede:
umetna inteligenca, digitalizacija, (digitalni) notranji trg, človekove pravice, e- izobraževanje, delovno pravo, pravica do poštenega sojenja

V 21. stoletju se z umetno inteligenco (UI) srečujemo na vsakem koraku, od šolanja do opravljanja dela in v prostem času. Za študente prava je tema zelo aktualna, saj se predvideva, da bo pravni postopek v prihodnosti potekal s pomočjo UI. Posledično bo temu potrebno prilagoditi tudi sistem izobraževanja in opravljanje pravniškega poklica. Poleg tega je vse več izdelkov in storitev na voljo v digitalni obliki. A države članice EU opozarjajo, da trenutno ni skupnega evropskega okvira, ki bi poenotil ali približal njihove zakonodaje na tem področju družbenega življenja. Dobro poznavanje sistemov UI, kar danes še predstavlja relativno nepoznano področje ali t.i. črno škatlo (ang. black box), je predpogoj za razumevanje njihovega vpliva na temeljne človekove pravice. Le na podlagi teh ugotovitev lahko zakonodajalci v demokratičnih družbah uredijo pravna razmerja in pri tem upoštevajo vzpostavljena načela, doktrino in sodno prakso, na katerih temelji in lahko v celoti razcveti notranji trg 21. stoletja.

Univerzitetna založba Univerze v Mariboru

DOI
https://doi.org/
10.18690/um.pf.4.2023.7

ISBN
978-961-286-774-4

Keywords:
artificial intelligence,
digitalisation,
(digital) internal market,
human rights,
e-education,
labour law, fair trial

7 TEMELJNE PRAVICE IN IZZIVI DIGITALIZACIJE: IZOBRAŽEVANJE, DELO IN SODSTVO

ŽIVA ŠUTA
University of Maribor, Faculty of Law, Maribor, Slovenia
ziva.sutae@student.um.si

In the 21st century AI can be encountered at every turn, from education to work and in our spare time. For law students it presents a very topical issue as it is anticipated that legal proceedings in the future will be conducted with the interference of AI. As a result, the education system and the legal profession will also need to be adapted. In addition, there are more and more products and services available in digital form. With this in mind, EU Member States are pointing at the current absence of a common European framework, that would unify and harmonise their legislation in this area of social life. Good knowledge of AI systems, which today still represents an unknown area or a so called *black box*, is a prerequisite for understanding their impact on fundamental human rights. Only on this basis can legislators in open societies regulate legal relations, taking into account established principles, doctrine and case law on which the internal market of the 21st century is based and can flourish in the future.

University of Maribor Press

7.1 Uvod

7.1.1 Digitalščina

Evropa je dom vodilni raziskovalni skupnosti za umetno inteligenco (v nadaljevanju UI) in gosti manjša podjetja s strokovnimi znanji na področju UI, vendar njen digitalni trg zaostaja v primerjavi z ameriškim, kjer zmogljivosti, zlasti z vidika podatkov, zagotavljajo pogoje za inovacije večjega obsega. Tako kot parni stroj ali elektrika v preteklosti UI spreminja naš svet, našo družbo in našo industrijo. Kljub temu da je razvoj UI in robotike močno pridobil na pomenu in prisotnosti v našem vsakdanjem življenju šele v zadnjih desetletjih, pa je ideja o avtonomnih bitjih, različnih od človeka, začela zelo zgodaj buriti človeško domišljijo in željo po stvaritvi tovrstnega bitja. Zametke o avtonomnih bitjih, drugačnih od človeka, je možno zaslediti že v najstarejših mitologijah (npr. grška mitologija), kakor tudi pri entuziastičnih znanstvenikih, ki so svoje ideje o avtonomnih bitjih pretvorili na različne načine v „realnost“.[1]

Od uporabe virtualnih osebnih pomočnikov, ki nam organizirajo delovni dan, do potovanja s samovozečimi vozili in uporabe telefonov, ki nam predlagajo pesmi ali restavracije, ki bi nam lahko bile všeč, je UI postala resničnost. Poleg tega, da nam olajšuje življenje, nam UI pomaga tudi pri reševanju nekaterih največjih svetovnih izzivov, od zdravljenja kroničnih bolezni ali manjšanja števila smrtnih žrtev v prometnih nesrečah do boja proti podnebnim spremembam ali predvidevanja kibernetskih groženj. V naslednjem desetletju se bo pojavilo še nešteto drugih primerov, ki si jih danes ne znamo niti predstavljati.[2]

Zgoraj navedeni primeri so prikaz koristne uporabe UI v praksi. Težave v zvezi z UI pa se pojavijo že pri poskusu njene opredelitve. V Slovarju slovenskega knjižnega jezika je UI *"sposobnost stroja, računalnika, da rešuje umske probleme"*. Angleški slovar Collins jo definira kot *"vrsto računalniške tehnologije, ki se ukvarja z izdelavo strojev, ki izvajajo delo na inteligenten način, podoben človeškemu"*. Problem pri opredeljevanju UI

[1] Kraljić, S. in Ivanc, T.: Pravni izzivi uporabe robotov v medicini, v: 28. posvetovanje Medicina, pravo & družba: Globalizacija medicine v 21. stoletju. 28.-30. marec 2019, Univerzitetna založba Univerze v Mariboru, 2019, str. 33.
[2] Sporočilo Komisije Evropskemu parlamentu, Evropskemu svetu, Svetu, Evropskemu ekonomsko-socialnemu odboru in Odboru regij, Umetna inteligenca za Evropo, COM (2018) 237 final, str. 1.

predstavlja predvsem definiranje postopkov, ki jih je mogoče označevati za inteligentne.[3]

EU jo opredeljuje kot sisteme, ki z analiziranjem svojega okolja in ukrepanjem (delno samostojnim) za doseganje posebnih ciljev kažejo inteligentno ravnanje. Ti lahko v celoti temeljijo na programski opremi in delujejo v virtualnem svetu (npr. glasovni pomočniki, programska oprema za analizo slik, iskalniki, sistemi za prepoznavanje govora in obraza) ali pa so vdelani v strojno opremo (npr. napredni roboti, samostojni avtomobili, brezpilotni zrakoplovi ali aplikacije za internet stvari).[4]

Kot znanstvena disciplina UI vključuje več pristopov in tehnik, kot so strojno učenje (katerega posebna primera sta globoko učenje in spodbujevano učenje), strojno sklepanje (ki vključuje načrtovanje, časovno razporejanje, predstavitev znanja in sklepanje, iskanje in optimizacijo) in robotiko (ki vključuje nadzor, zaznavanje, senzorje in aktuatorje, pa tudi vgraditev vseh drugih tehnik v kibernetsko-fizične sisteme).[5]

Odbor regij EU uporablja tudi izraz „digitalna kohezija“, ki daje pomembno dodatno razsežnost tradicionalnemu pojmu ekonomske, socialne in teritorialne kohezije, opredeljene v členu 3 Pogodbe EU. Predlaga splošno razpravo o prihodnji vlogi digitalizacije pri spodbujanju kohezije v Evropski uniji ob pojavu demografskih izzivov, podnebnih sprememb in spreminjajočega se delovnega okolja.[6]

Danes se mediji veliko sprašujejo o tem, ali bodo roboti nadomestili zdravnike, sodnike in druge poklice ter katerim novim poklicem bomo priča zaradi razvoja tehnologije. Robot (izvira iz češke besede *»robota«* in pomeni prisilno delo) lahko opredelimo kot avtonomen stroj, ki je sposoben izvajati človeška dejanja. Posledično ima robot fizično naravo, sposobnost avtonomnega izvajanja oziroma ukrepanja brez človekovega posredovanja in je vizualno podoben ljudem. Pisec znanstvene fantastike Isaac Asimov je leta 1942 predstavil kratko zgodbo Runaround, v kateri je predstavil tri zakone robotike (ang. *three laws of robotics*): a)

[3] Marguč, K.: Trajnostna evolucijska etika kot odgovor na problem vrzeli racionalnosti med umetno inteligenco in potrošnikom, v: Res novae, celovita revija za znanost, 2 (2017) 2, str. 78.
[4] Sporočilo Komisije Evropskemu parlamentu, Evropskemu svetu, Svetu, Evropskemu ekonomsko-socialnemu odboru in Odboru regij, Umetna inteligenca za Evropo, COM (2018) 237 final, str. 1.
[5] Strokovna skupina na visoki ravni za umetno inteligenco: Etične smernice za zaupanja vredno umetno inteligenco. Bruselj, 2019, str. 45.
[6] Mnenje Evropskega odbora regij- Digitalna Evropa za vse: uvajanje pametnih in vključujočih rešitev na terenu, 2020/C 39/18, str. 2.

robot ne sme nikoli škodovati človeškemu bitju; b) robot mora upoštevati ukaze, ki jih dajejo ljudje, razen če nasprotuje prvemu zakonu; c)in robot mora varovati svoj lasten obstoj, če to ni v nasprotju s prvima dvema zakonoma. Tem je potrebno slediti tudi danes.[7]

Prednosti in koristi UI so se do danes pokazale na več področjih človekovega življenja.

- *Izboljšanje dostopa do zdravstvene oskrbe in napovedovanje izbruhov bolezni*: UI je vplivala na napredovanje diagnostike in preprečevanje okužb. Tudi žrtve izbruhov nalezljivih bolezni imajo koristi od uporabe UI, saj lahko zdravstveni delavci predčasno posredujejo informacije in tako preprečijo izbruh,
- *olajšanje življenja slabovidnim*: orodja za prepoznavanje informacij slabovidnim ljudem prispevajo k boljšemu krmarjenju po internetu in v 'resničnem' svetu,
- *optimizacija kmetijstva in pomoč kmetom pri prilagajanju spremembam*: UI združuje informacije iz globalnih satelitskih posnetkov z vremenskimi in agronomskimi podatki, da kmetom pomaga izboljšati pridelke, prepoznati in zdraviti bolezni pridelkov ter se prilagoditi spremenljivim okoljem,
- *zmanjševanje podnebnih sprememb, napovedovanje naravnih nesreč in ohranjanje prostoživečih živali*: UI se že uporablja za razvrščanje podnebnih modelov in napovedovanje ekstremnih vremenskih dogodkov, pa tudi za boljše napovedovanje in odzivanje na naravne katastrofe.[8]

Škodljiva UI lahko poseže zlasti na naslednja področja:

- *pristranskost v kazenskem pravosodju*: uporaba UI v tem kontekstu se pogosto pojavlja za ocenjevanje tveganja, ali bo obdolženec ponovil kaznivo dejanje, za katero je obsojen. UI pripomore tudi k temu, da z uporabo različnih podatkov iz sodnih in drugih uradnih evidenc z verjetnostjo napovejo, kje

[7] Kraljić, S. in Ivanc, T.: Pravni izzivi uporabe robotov v medicini, v: 28. posvetovanje Medicina, pravo & družba: Globalizacija medicine v 21. stoletju. 28.-30. marec 2019, Univerzitetna založba Univerze v Mariboru, 2019, str. 34, 35.

[8] Andersen, L. in drugi: HUMAN RIGHTS IN THE AGE OF ARTIFICIAL INTELLIGENCE, Access Now, November 2018, str. 13-16.

in kdaj se bo zgodil zločin, in ustrezno usmerjajo ukrepe kazenskega pregona.

- *nevarnost množičnega nadzora*: glede na to, da UI zagotavlja zmogljivost za obdelavo in analizo več tokov podatkov v določenem času, ni presenetljivo, da se že uporablja za omogočanje množičnega nadzora po vsem svetu. Najbolj razširjen in nevaren primer tega je uporaba UI v programski opremi za prepoznavanje obraza. Čeprav je tehnologija še vedno nepopolna, vlade iščejo tehnologijo prepoznavanja obraza kot orodje za spremljanje svojih državljanov, olajšanje profiliranja določenih skupin ter celo prepoznavanje in lociranje posameznikov,[9]
- *spodbujanje finančne diskriminacije*: algoritmi se že dolgo časa uporabljajo za ustvarjanje bonitetnih ocen in obveščanje o posojilih. Z naraščanjem podatkov znotraj UI, sistemi zdaj uporabljajo strojno učenje za vključevanje in analizo nefinančnih podatkovnih točk za določitev kreditne sposobnosti; od tega, kje ljudje živijo, do njihovih navad brskanja po internetu in do odločitev o nakupu. Rezultati teh sistemov so znani kot e-ocene, za razliko od formalnih kreditnih točk pa večinoma niso urejeni,
- *diskriminacija na sploh*: digitalni razkorak ločuje tiste, ki imajo dostop do IKT in spretnosti za njegovo uporabo, od tistih, ki tega niso in so zato izključeni iz družbe in družbenega življenja,
- *pomoč širjenju dezinformacij*: UI je mogoče uporabiti za ustvarjanje in širjenje ciljno usmerjene propagande. Težavo predstavljajo algoritmi socialnih medijev, ki spodbujajo vsebino, ki jo posamezniki kasneje zelo pogosto tudi obiščejo. Roboti, prikriti kot resnični uporabniki, nadalje širijo vsebino zunaj ozko usmerjenih krogov družbenih medijev tako, da delijo povezave do lažnih virov in aktivno komunicirajo z uporabniki. Mnogi verjamejo, da bo tehnologija v prihodnosti uporabljena za ustvarjanje ponarejenih videoposnetkov svetovnih voditeljev za zle namene. Čeprav se zdi, da so ponaredki še vedno uporabljeni kot del resničnih propagandnih ali dezinformacijskih kampanj, ponarejeni avdio in video posnetki še vedno niso dovolj dobri, da bi bili videti povsem človeški.

[9] Primer takšnega ravnanja je ukrep izraelske vlade, ki je v času pandemije Covid-19 sledila svojim državljanom preko mobilnih telefonov. (Israel to track mobile phones of suspected corona virus cases 17.3.2020 < https://www.theguardian.com/world/2020/mar/17/israel-to-track-mobile-phones-of-suspected-coronavirus-cases> (20.5.2020)).

Seveda lahko ima tudi „koristna“ UI potencialno negativne posledice. Npr. številne aplikacije UI v zdravstvu predstavljajo resne grožnje zasebnosti in tvegajo diskriminacijo prebivalcev ter omogočajo lastništvo podatkov v velikih podjetjih. Podobno so nekateri primeri uporabe, kategorizirani kot "škodljivi", nastali kot posledica dobrih namenov, čeprav lahko povzročijo znatno škodo.[10]

7.1.2 Enotni digitalni trg

Dve tretjini Evropejk in Evropejcev menita, da najnovejše digitalne tehnologije pozitivno vplivajo na družbo, gospodarstvo in njihovo življenje. Večina vprašanih meni, da morajo EU, organi držav članic in podjetja sprejeti ukrepe, ki bi obravnavali vprašanja, ki jih odpira digitalizacija.[11] *Digital Economy and Society Index* (DESI) iz leta 2018 je pokazal, da Evropa postaja vse bolj digitalna, vendar pa ostaja prepad v digitalnem znanju med Evropejci. Približno 43% Evropejcev še vedno nima osnovnih digitalnih spretnosti, 13% pa jih še nikoli ni obiskalo spleta. Pomembne razlike ostajajo med državami članicami EU.[12]

Danes je vse več izdelkov in storitev na voljo v digitalni obliki. Če gledamo filme ali se potegujemo za javna naročila, če nakupujemo ali študiramo, pri tem zelo verjetno uporabljamo (ali bi lahko uporabljali) spletna orodja. Približno 40 % svetovnega prebivalstva je zdaj povezanega z internetom; leta 1995 so bili le 4%. Med letoma 2008 in 2012 se je svetovna čezmejna trgovina s podatki povečala za 49%, trgovina z blagom ali storitvami pa je zrasla le za 2,4%.

EU temelji na popolnoma integriranem notranjem trgu in odprtem svetovnem gospodarskem sistemu. To v digitalnem svetu vključuje prost pretok informacij in globalne vrednostne verige, ki jih olajšuje brezplačen, odprt in varen internet. Prehod na enotni digitalni trg EU, ki temelji na podpori za pošteno konkurenco ter korenini

[10] Andersen, L. in drugi: HUMAN RIGHTS IN THE AGE OF ARTIFICIAL INTELLIGENCE, Access Now, November 2018, str. 13-16.
[11] Sporočilo Komisije Evropskemu parlamentu, Evropskemu svetu, Svetu, Evropskemu ekonomsko-socialnemu odboru in Odboru regij o vmesnem pregledu izvajanja strategije za enotni digitalni trg Povezani enotni digitalni trg za vse, COM(2017) 228 final, str. 3.
[12] European Commission: Inspirational practises for tomorrow's inclusive digital world: Technical Dossier No. 10, May 2019, str.9.

v naših temeljnih vrednotah in temeljnih pravicah in svoboščinah, lahko Evropi pomaga pri obravnavanju številnih svetovnih gospodarskih izzivov, ki so pred njo.[13]

EU je že leta 2006 izpostavila pomen ozaveščanja o digitalnem razvoju in napredkih in poudarila: *"Ob svojem razvoju se enotni trg srečuje z novimi in širšimi izzivi. Priložnosti, ki jih ustvarjajo svoboda in mobilnost ter odprava čezmernih upravnih in regulativnih kontrol, morajo biti usmerjene v ustvarjanje novih delovnih mest in zmanjšanje razlik med bogatimi in revnimi ter med starimi in novimi članicami Unije. To pomeni usklajevanje izobraževalne politike, vključno z dostopom do vseživljenskega učenja. Prav tako to pomeni preprečevanje digitalnega prepada, ki nastaja med državljani in regijami s popolnim dostopom do interneta in hitrih širokopasovnih tehnologij, in tistimi, ki tega dostopa nimajo".*[14]

Namen enotnega digitalnega trga je, da se z odpravo regulativnih ovir enako stori na digitalnem področju. Enotni digitalni trg, ki pomeni odmik od sedanjih 27 nacionalnih trgov EU, je usklajeno in integrirano evropsko območje brez ovir za uporabo digitalnih in spletnih tehnologij ter storitev.[15]

A države članice opozarjajo, da trenutno ni takšnega skupnega evropskega okvira. Nemška komisija za etiko podatkov je pozvala k petstopenjskemu sistemu, ki temelji na tveganju in zajema vse od popolne neregulacije za najbolj neškodljive sisteme UI do popolne prepovedi najnevarnejših sistemov. Danska je uvedla prototip pečata etičnih podatkov, Malta pa je uvedla prostovoljni sistem certificiranja UI. Če EU ne zagotovi pristopa na ravni EU, obstaja resnično tveganje razdrobljenosti notranjega trga, ki bi ogrozila cilje zaupanja, pravne varnosti in uvajanja na trg.[16]

Zakonodajni okvir bi bilo mogoče po mnenju Komisije izboljšati tako, da se 1) *učinkovito uporablja in izvršuje obstoječa zakonodaje EU in nacionalna zakonodaja*- nepreglednost UI povzroča težko odkrivanje in dokazovanje morebitnih kršitev zakonov, vključno s kršitvami pravnih določb, ki ščitijo temeljne pravice; 2) *omeji področje uporabe obstoječe zakonodaje EU*- odprto ostaja vprašanje, ali zakonodaja EU o varnosti proizvodov pokriva samostojno programsko opremo, poleg tega pa

[13] Sporočilo Komisije Evropskemu parlamentu, Evropskemu svetu, Svetu, Evropskemu ekonomsko-socialnemu odboru in Odboru regij o vmesnem pregledu izvajanja strategije za enotni digitalni trg Povezani enotni digitalni trg za vse, COM(2017) 228 final, str. 24.
[14] Evropska Unija: Živeti bolje v EU: Kaj pomeni enotni trg za vas. Luxembourg: Urad za uradne publikacije Evropskih skupnosti, 2006, str. 21.
[15] Evropska komisija, Evropska unija in enotni digitalni trg, 2017, str. 2.
[16] Evropska komisija, BELA KNJIGA o umetni inteligenci - evropski pristop k odličnosti in zaupanju, COM(2020) 65 final, str. 11.

trenutno veljavna zakonodaja EU o varnosti se uporablja za proizvode in ne za storitve in tako načeloma tudi ne za storitve, ki temeljijo na tehnologiji UI (npr. zdravstvene storitve, finančne storitve, transportne storitve); 3) obravnava *spreminjajoča se funkcionalnost sistemov UI*- integracija programske opreme v proizvode, vključno z UI, lahko spremeni funkcionalnost takšnih proizvodov in sistemov tekom njihovega življenjskega cikla, kar lahko povzroči nova tveganja, ki niso bila prisotna, ko je bil sistem dan na trg; 4) odpravi *negotovost glede delitve odgovornosti med različnimi gospodarskimi subjekti v dobavni verigi*- zakonodaja EU o odgovornosti za proizvode določa odgovornost proizvajalcev, a dopušča, da odgovornost drugih v dobavni verigi urejajo nacionalna pravila o odgovornosti; 5) *spremeni koncept varnosti*- tveganja so lahko povezana s kibernetskimi grožnjami, tveganji za osebno varnost (na primer v povezavi z novimi uporabami UI, kot so gospodinjske naprave), tveganji, ki izhajajo iz izgube povezljivosti itd.[17]

Komisija tudi poudarja, da je v najbolj oddaljenih regijah zaradi njihovih omejitev in oddaljenosti od evropske celine težko vzpostaviti digitalno infrastrukturo. Zato je potrebno poskrbeti, da bodo imele tudi te regije polno pravico do povezljivosti.[18] Predsednica Komisije von der Leyen je v svojih političnih usmeritvah izpostavila *"potrebo po tem, da mora imeti vsak državljan oz. državljanka, vsaka zaposlena oseba in podjetnik oz. podjetnica pošteno možnost, da uživa koristi naše vedno bolj digitalizirane družbe ne glede na to, kje živi. Digitalne rešitve, kot so komunikacijski sistemi, umetna inteligenca ali kvantne tehnologije, lahko obogatijo naše življenje na veliko načinov. Vendar pa koristi, ki jih prinašajo digitalne tehnologije, niso brez tveganj in stroškov. Državljani in državljanke nimajo več občutka, da imajo nadzor nad svojimi osebnimi podatki in so vedno bolj preobremenjeni z umetnimi zvabljanji njihove pozornosti. Zlonamerne kibernetske dejavnosti lahko ogrozijo našo osebno blaginjo ali kritično infrastrukturo in širše varnostne interese. Cilj evropskega pristopa k umetni inteligenci je spodbujati inovacijske zmogljivosti Evrope na področju umetne inteligence, hkrati pa podpirati razvoj in uvajanje etične in zaupanja vredne umetne inteligence v vse sektorje gospodarstva EU. Umetna inteligenca mora delati za ljudi in biti sila za dobro v družbi."*[19]

[17] Ibidem, str. 15, 16.
[18] Mnenje Evropskega odbora regij- Digitalna Evropa za vse: uvajanje pametnih in vključujočih rešitev na terenu, 2020/C 39/18, str. 1.
[19] Sporočilo Komisije Evropskemu parlamentu, Svetu, Evropskemu ekonomsko-socialnemu odboru in Odboru regij, Oblikovanje digitalne prihodnosti Evrope, COM(2020) 67 final, str. 1.

7.2 Vpliv umetne inteligence na človekove pravice[20]

Doslej je standardno strojno učenje ponujalo izboljšano sposobnost spremljanja in dokumentiranja vojnih zločinih in drugih kršitev človekovih pravic. Digitalna tehnologija v 21. stoletju je začela tisto, kar nekateri imenujejo "zlata doba nadzora" - ne le od držav in korporacij, temveč tudi nekaterih nedržavnih akterjev. Če se kaj zgodi kjerkoli na svetu, obstaja velika možnost, da bo dogodek posnela kamera. Mednarodno kazensko sodišče v Haagu je izdalo obtožnico za aretacijo libijskega vodje na podlagi ugotovitev iz satelitskih posnetkov in videoposnetkov usmrtitev iz socialnih omrežij, ki jih je naročil oz. izvedel sam. Stavbe, ceste, drevesa, hribi in druge geografske značilnosti v videoposnetkih so zaradi visoke ločljivosti izdale izvršene zločine glede na čas in kraj.[21]

Varstvo človekovih pravic je na univerzalnem nivoju zagotovljeno s tremi pravnimi kodifikacijami OZN, to so Splošna deklaracija o človekovih pravicah (SDČP),[22] Mednarodni pakt o državljanskih in političnih pravicah (MPDPP)[23] in Mednarodni pakt o ekonomskih, socialnih in kulturnih pravicah (MPESK)[24]. Na ravni EU so človekove pravice zagotovljene z Listino EU o temeljnih človekovih pravicah (LEUČP),[25] Svet Evrope pa jih je leta 1950 uzakonil z Evropsko konvencijo o človekovih pravicah (EKČP).[26]

LEUČP opisuje človekove pravice s sklicevanjem na dostojanstvo, svoboščine, enakost in solidarnost, pravice državljanov in pravičnost. Skupni temelj, ki združuje te pravice je zakoreninjen v spoštovanju človekovega dostojanstva, s čimer odraža, kar opisujemo kot „na človeka osredotočen pristop“, pri katerem ima človek edinstven in neodtujljiv moralni status primarnosti na civilnem, političnem, gospodarskem in družbenem področju. Nadrejenost človeštva nad drugimi oblikami življenja, ki jim pravo daje manjšo zaščito, se postavlja pod vprašaj v 21. stoletju s

[20] Glej razpredelnico v Prilogi.
[21] Livingston, S., in Risse, M.: The Future Impact of Artificial Intelligence on Humans and Human Rights, v: Ethics & International Affairs, 33 (2019) 2, str. 143, 144.
[22] Splošna deklaracija o človekovih pravicah, Resolucija št. 217 A (III), 10 December 1948.
[23] Mednarodni pakt o državljanskih in političnih pravicah, Treaty Series, vol. 999, 16 December 1966, str. 171.
[24] Mednarodni prakt o ekonomskih, socialnih in kulturnih pravicah, UN General Assembly, Treaty Series, vol. 993, 16 December 1966, str. 3.
[25] Listina Evropske Unije o človekovih pravicah, Uradni list Evropske unije, C 83/389, str. 391–407.
[26] 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 – Mednarodne pogodbe, št. 7/94).

predvidenim prihodom subjektov, ki niso primerljivi obstoječim živim bitjem, a so kljub temu podobno odzivni, intelektualni in morda celo bolj moralni od ljudi.

Čeprav so pravice iz Listine EU pravno zavezujoče, je pomembno priznati, da temeljne pravice v vsakem primeru ne zagotavljajo celovitega pravnega varstva. Glede Listine EU je npr. treba poudariti, da je njeno področje uporabe omejeno na področja prava EU. Mednarodno pravo o človekovih pravicah, zlasti EKČP predstavlja pravno zavezujočo kodifikacijo za države članice, in to tudi na področjih, ki ne spadajo v področje uporabe zakonodaje EU. SDČP prav tako ne predstavlja zavezujoče kodifikacije, saj jo uvrščamo v mehko pravo (ang. *soft law).* Hkrati je treba poudariti, da temeljne pravice uživajo posamezniki in (deloma) skupine na podlagi moralnega statusa, ki ga imajo kot ljudje, neodvisno od njihove pravne moči.[27]

Da se zagotovi skladnost zakonodaje posamezne države z mednarodnimi kodifikacijami za varstvo človekovih pravic, je potrebno zagotoviti, da njihova zakonodaja ustvarja pogoje, ki prispevajo k spoštovanju človekovih pravic s strani ustvarjalcev UI in ne ustvarjajo ovir za učinkovito odgovornost in odpravo kršitev človekovih pravic, povezanih z UI. Potrebno bi bilo preučiti, ali so trenutno razpoložljivi pravni okviri ustrezni ali pa jih je treba prilagoditi tako, da bo uporaba sistemov UI skladna s pravom človekovih pravic. Zdi se, da bo potrebno vzpostaviti nov pravni okvir za kodificiranje nekaterih načel in zahtev v povezavi z etičnimi kodeksi, ki zavezujejo razvijalce UI, da ravnajo odgovorno. Ker pa je tehnologija (vključno z UI) nadnacionalna, je potrebno vzpostaviti pravni okvir na mednarodnem nivoju in ga nato prenesti in upoštevati v nacionalnemu redu.[28]

7.3 Izobraževanje in umetna inteligenca

Samoumevno se zdi, da si pri računanju pomagamo s kalkulatorjem, pri predstavitvah seminarskih nalog z diaprojekcijo, predvajamo filme, zlahka prevajamo iz enega jezika v drugega, beremo šolsko literaturo na računalnikih ali tablicah ipd. Pomožne tehnologije, npr. pretvorba besedila v govor ali obratno, možnosti povečanja ali zmanjšanja besedila (zoom), avtomatično predvidevanje besedila, preverjanje črkovanja in sprotni iskalniki so le nekateri primeri tehnologije,

[27] Strokovna skupina na visoki ravni za umetno inteligenco: Etične smernice za zaupanja vredno umetno inteligenco, 2019, str. 11, 12.
[28] Council of Bars & Law Societies of Europe: CCBE CONSIDERATIONS ON THE LEGAL ASPECTS OF ARTIFICIAL INTELLIGENCE, Bruselj, 2020, str. 14.

ki so bili prvotno zasnovani za pomoč invalidnim osebam. Pri izobraževanju otrok s posebnimi potrebami so pristopi, ki temeljijo na UI, pripomogli k zgodnjemu odkrivanju disleksije. Švedsko podjetje "Lexplore", je razvilo sistem, ki hitro pregleda študente v nevarnosti in odkriva disleksijo s sledenjem bralnim očesom. Uspešno so razvili tudi sisteme, ki temeljijo na UI za diagnozo motnje spektra avtizma in hiperaktivnosti s pomanjkanjem pozornosti (ADHD). Zlasti interakcija otrok-robot omogoča nove oblike diagnostike in izobraževalne aplikacije za posebne potrebe.

Uporaba teh tehnoloških rešitev se je pozneje razširila in jih danes najdemo v vseh računalnikih kot del njihovega osnovnega programskega paketa. Te tehnologije danes povečujejo interakcijo med učenci po vsem svetu, odpirajo nove priložnosti in oblikujejo izobraževalni sistem. Ta vrsta interakcije med ljudmi in stroji oz. med ljudmi preko strojev predstavlja možnost za korenite spremembe v učnem okolju, vpliva na to, kako si zapomnimo informacije, dostopamo do njih in jih ustvarjamo, hkrati pa prinaša velik kulturni napredek za nekatere in digitalno stagnacijo za druge. S pogledom nazaj zadnjih trideset let, je moč ugotoviti, da ima vpliv tehnologije na naša življenja poseben pomen v šolskih sistemih po svetu.[29]

7.3.1 Prednosti in slabosti

Akademski svet postaja bolj priročen in personaliziran zaradi številnih aplikacij in spletnih platform za izobraževanje. To je spremenilo način, kako se ljudje učijo, saj so poučna gradiva dostopna vsem prek pametnih naprav in računalnikov. Danes študentom ni treba fizično obiskovati fakultete, da bi študirali, potrebujejo zgolj računalnike in internetno povezavo.

Izobraževanje ima lahko koristi od večje odprtosti razredov, življenjskih izkušenj in projektov ter novih učnih orodij, gradiv in prosto dostopnih učnih virov. Učenci se lahko usposabljajo s spletnim sodelovanjem. Dostop do digitalnih tehnologij in njihova uporaba lahko pomagata zmanjšati učne razlike med učenci iz socialno-ekonomsko privilegiranih in prikrajšanih okolij. S prilagojenimi metodami poučevanja in osredotočanjem na posamezne učence je mogoče povečati njihovo motivacijo.

[29] Timms, M.: Letting Artificial Intelligence in Education Out of the Box: Educational Cobots and Smart Classrooms, International Journal of Artificial Intelligence in Education, 26 (2016), sr. 701–712.

Trenutni sistemi UI so uspešni pri združevanju podatkov iz raznolikih baz in prepoznavanju vzorcev njihove uporabe, npr. za hitro preverjanje domačih nalog, odzivov učencev, primerjave s predhodno pridobljenimi ocenami in rezultati ipd. Sistemi UI se uporabljajo tudi za preverjanje prisotnosti učencev, njihove pozornosti in dinamike pogovorov. To ustvarja etične in pravne pomisleke za nevsiljivo spremljanje študentov. Etično manj problematični so sistemi, ki uporabljajo manj natančne podatke.[30]

UI omogoča tudi avtomatizacijo administrativnih nalog, kar izobraževalnim ustanovam omogoča, da skrajšajo čas, potreben za dokončanje določenih nalog, tako da lahko učitelji preživijo več časa s študenti. Učitelj namreč porabijo veliko časa za ocenjevanje izpitov, ocenjevanje domačih nalog in zagotavljanje dragocenih odgovorov svojim učencem. Danes lahko tehnologijo uporabijo za avtomatizirano razvrščanje in pregledovanje testov, esejev ali študentskih vprašanj.

Raziskave kažejo, da je takojšnja povratna informacija eden od ključev uspešnega poučevanja. Skozi aplikacije, ki jih poganja UI, učenci dobijo ciljno usmerjene in prilagojene odgovore svojih učiteljev. Študente lahko naučijo tudi glede na izzive, s katerimi se srečujejo pri preučevanju gradiva v razredu. Zahvaljujoč UI lahko pametni učiteljski sistemi, kot je Carnegie Learning[31] ali slovenski Razlagamo si[32] ponudijo hitre povratne informacije in neposredno sodelujejo s študenti. Čeprav so te metode še vedno v začetni fazi, lahko kmalu digitalni učitelji postanejo realnost.

Vsakodnevna izpostavljenost digitalnim podatkom, ki jih večinoma upravljajo nerazumljivi algoritmi, ustvarja očitna tveganja in bolj kot kdaj koli zahteva kritično mišljenje ter sposobnost pozitivnega in kompetentnega vključevanja v digitalno okolje. Soočamo se z vse večjo potrebo po medijski pismenosti ter vrsti digitalnih spretnosti in kompetenc, vključno z varnostjo, zanesljivostjo in zasebnostjo, vendar je prenos teh znanj, spretnosti in kompetenc na širše prebivalstvo ter v naprednejše poklice in sektorje še vedno izziv.[33]

---

30 Timms, M.: Letting Artificial Intelligence in Education Out of the Box: Educational Cobots and Smart Classrooms, International Journal of Artificial Intelligence in Education, 26 (2016), str. 701–712.

31 Carnegie Learning. Več na: https://www.carnegielearning.com/.

32 Razlagamo si. Več na: https://razlagamo.si/.

33 Sporočilo Komisije Evropskemu parlamentu, Svetu, Evropskemu ekonomsko-socialnemu odboru in Odboru regij o akcijskem načrtu za digitalno izobraževanje {SWD(2018) 12 final}, str. 2.

7.3.2 Ukrepi

Izobraževalni sistemi trenutno niso dovolj opremljeni, da bi odražali potrebe prihodnosti in študente pripravili na življenje z UI in na trg dela. Zagotovitev učnih načrtov, pripravljenih za prihodnost, vključuje pregledovanje jezikovnih, matematičnih in tehnoloških doktrin in raziskav in zagotavljanje zadostne pozornosti digitalni pismenosti. Študenti morajo biti ustrezno pripravljeni na delo z UI, kar zahteva predhodno ustrezno in temeljito izobraževanje iz predmetov, povezanih z UI ter podpora države, izobraževalnih ustanov in učiteljev. Za vse študente je osnovno znanje in razumevanje, ki sta potrebna za krmarjenje po UI svetu bistvenega pomena.[34]

Oblikovalci učnih načrtov morajo upoštevati neenakosti med učenci, npr. glede na demografske dejavnike kot so starost, spol in socialno-ekonomsko ozadje. Sposobnost generiranja takšnih analiz omogoča izobraževalnim sistemom, da spoznajo izobraževalne pomanjkljivosti, ki jih občutijo ranljive skupine prebivalstva.[35] Pri ugotavljanju tega pa ostaja velik problem, da so podatki o prikrajšanih skupine trenutno še vedno nepopolni. Raziskava UNICEF-a[36] iz leta 2016 je pokazala, da od 19 anketiranih držav 19 sploh ni imelo podatkov o otrocih s posebnimi potrebami, za številne države, ki so te podatke imele, pa niso navedle invalidnosti. Begunci, ki se šolajo v nacionalnih šolah prav tako pogosto niso identificirani kot begunci v nacionalnem izobrazbene statistike, kar otežuje spremljanje in ocenjevanje njihovih učnih rezultatov. Vendar pa izobraževalni sistem sam po sebi ni edini vir podatkov. Podatki o gospodinjstvih, kot jih posebej omenja UIS, so prav tako kazalci dejavnikov, ki lahko predstavljajo težave pri učenju v šoli. Enako lahko rečemo za podatke, ki jih zbirajo drugi, npr. Ministrstvo za zdravje.

Evropska komisija je v svojem **Akcijskem načrtu za digitalno izobraževanje iz leta 2018**[37] predstavila prednostne naloge na področju izobraževanja (kot nezavezujoč pravni akt, priporočila), ki naj v državah članicah služijo razvoju

[34] UNESCO: Artificial Intelligence in Education: Challenges and Opportunities for Sustainable Development, France: Paris, 2019, str. 26.
[35] Servoz, M.: AI, The future of work? Work of the future! On how artificial intelligence, robotics and automation are transforming jobs and the economy in Europe, Evropska komisija, 2019, str. 60.
[36] UNICEF: Technical Guidance: Guide for Including Disability in Education Management Information Systems, 2016, str. 5-9.
[37] Povzeto po: Sporočilo Komisije Evropskemu parlamentu, Svetu, Evropskemu ekonomsko-socialnemu odboru in Odboru regij o akcijskem načrtu za digitalno izobraževanje, COM(2018) 22 final, str. 4-12.

spretnosti in znanj, potrebnih za delo na področju UI ter strokovno izpopolnjevanje delovne sile, da bo pripravljena na preobrazbo, ki jo ta prinaša. V nadaljevanju na kratko predstavljam te ukrepe ter obete v zvezi z njimi.

- **Prednostna naloga 1:** boljše izkoriščanje digitalne tehnologije pri učenju in poučevanju

Široka razsežnost digitalnega razkoraka lahko povzroči mnoge pravne in etične dileme, zato naj države članice v prvi vrsti poskrbijo za zagotovitev pravičnosti in kakovosti dostopa in infrastrukture vsem svojim državljanom. Šole in institucije za usposabljanje so raznolike, prav tako se zelo razlikujejo njihova opremljenost, spretnosti učiteljev in pristopi k uporabi tehnologije. Po vsej Evropi obstajajo mesta, kjer so inovacije na področju digitalnega izobraževanja posebno razvite. Visoka kakovost in enak dostop prinašata tudi bolj inovativno in izpolnjujočo učno izkušnjo. Prva prednostna naloga Komisije je torej boj za zmanjševanje neenakosti in izključenosti v digitalnem izobraževanju.

- **Prednostna naloga 2:** razvijanje ustreznih digitalnih kompetenc in spretnosti za digitalno preobrazbo

Med osnovna znanja, potrebna na vseh področjih življenja, spadajo digitalne spretnosti skupaj z bralno in računsko pismenostjo. Kljub temu ima po mnenju Komisije preveč državljanov omejeno ali zastarelo digitalno kompetenco. Pomeni samozavestno in kritično uporabo digitalne tehnologije in obsega znanje, spretnosti in odnose, ki jih v hitro razvijajoči se digitalni družbi potrebujejo vsi državljani. Evropski okvir digitalne kompetence za državljane[38] digitalno kompetenco opisuje na petih področjih: informacijska in podatkovna pismenost, komuniciranje in sodelovanje, ustvarjanje digitalnih vsebin, varnost in dobro počutje ter reševanje problemov.

Čeprav se fantje in dekleta v podobni meri zanimajo za digitalne tehnologije in imajo na tem področju podobne kompetence, se za razvijanje tega zanimanja v okviru študija ali svoje poklicne poti odloča manj deklet. Dekleta in mlade ženske potrebujejo pozitivne zglede, vzornike in podporo, da premagajo stereotipe in se

[38] European Digital Competence Framework for Citizens. Več na: https://ec.europa.eu/social/main.jsp?catId=1315&langId=en.

zavejo, da lahko tudi one zgradijo izpolnjujočo in uspešno kariero na področju informacijskih in komunikacijskih tehnologij ter naravoslovja, tehnike, inženirstva in matematike. Povečanje deleža žensk v tovrstnih poklicih bo pripomoglo k sprostitvi evropskega digitalnega potenciala in zagotovilo, da imajo ženske enakopravno vlogo pri oblikovanju digitalnega sveta. V EU je med strokovnjaki na področju IKT manj kot petina žensk.

V ta namen Komisija spodbuja tečaje programiranja v vseh evropskih šolah, vključno z okrepljenim sodelovanjem šol v evropskem tednu programiranja in odprto znanost ter znanost za državljane v Evropi s tečaji stalnega strokovnega razvoja o odprti znanosti v visokošolskih institucijah. Z evropsko kampanjo ozaveščanja, namenjeno izobraževalcem, staršem, učencem, dijakom in študentom, želi krepiti varnost na spletu, kibernetsko higieno in medijsko pismenost ter spodbuditi k učenju ljudi za samozavestno in odgovorno uporabo tehnologije.

- **Prednostna naloga 3**: izboljševanje izobraževalnih sistemov z boljšo analizo podatkov in predvidevanjem

Inovacije uporabnikov so ključnega pomena za zgodnje sprejetje inovacijskih rešitev za reševanje izzivov s področja izobraževanja. Podatki in trendi s področja izobraževanja se navadno zbirajo od zgoraj navzdol, tj. zbiranje vodijo mednarodne organizacije in vlade. Vidik uporabnika pogosto ni dovolj upoštevan, kar bi lahko omejilo mogoče rešitve za določeno potrebo. To še posebno drži v času inovacij uporabnikov, ko lahko posamezniki sami razvijajo rešitve za težave, s katerimi se soočajo.

Komisija želi od leta 2018 izvajati poskusne projekte na področju UI in učne analitike, da bi bolje izkoriščali ogromno količino podatkov, ki so zdaj na voljo, in tako pripomogli k reševanju specifičnih problemov ter izboljšanju izvajanja in spremljanja izobraževalnih politik. Spodbuja uvajanje strateškega predvidevanja v zvezi s trendi, povezanimi z digitalno preobrazbo, ki so ključni za prihodnost izobraževalnih sistemov, in sicer v tesnem sodelovanju s strokovnjaki iz držav članic, ter izkoriščati obstoječe in prihodnje oblike evropskega sodelovanja na področju izobraževanja in usposabljanja.

7.3.3 Primeri dobrih praks[39]

V Italiji je Evropski socialni sklad financiral večino ukrepov v nacionalnem načrtu za digitalno izobraževanje (Piano Nazionale Scuola Digitale, PNSD). Eden izmed podprtih projektov je *„Formazione all'innovazione didattica e organzativa"* (Usposabljanje za izobraževalne in organizacijske inovacije), strateška akcija, ki ponuja prilagojeno usposabljanje učencev in učiteljev vseh italijanskih šol. Projekt odgovarja na potrebo po dolgoročni viziji izobraževanja v digitalni dobi, ki je povezana z izzivi, s katerimi se italijanska družba spopada pri spodbujanju celovitega in vseživljenjskega učenja zunaj učilnic. Ti izzivi so povezani predvsem s: 1) povečanjem kakovosti in ustreznosti učenja, z namenom, da postane bolj interaktivno in povezano z digitalnimi vsebinami; 2) povečati vpliv učiteljev s pomočjo digitalizacije; in 3) odpravljanje neenakosti z boljšim digitalnim dostopom in nižjimi stroški.

Udeleženci so morali izpolniti anketo o zadovoljstvu uporabnikov, ki je tudi ocenila, kako koristno je bilo usposabljanje za njihovo delo. Odgovori približno 100 000 udeležencev so potrdili, da večina meni, da so premostili digitalni razkorak, ki je obstajal pred usposabljanjem, in se sedaj počutijo bolj kompetentne za uporabo informacijske in komunikacijske tehnologije (IKT). Večina učiteljev je verjela, da so izboljšali svojo pripravo, zlasti v zvezi s tem, da se bolj izkoristijo aplikacije, metodologije in IKT ter aktivne ali skupne učne metode. Pomembno je poudariti splošno prepričanje vseh udeležencev, da bodo informacije, pridobljene med usposabljanjem, zelo koristne v njihovem delovnem kontekstu.

Tudi **Hrvaška** priznava pomen IKT za njen izobraževalni sistem in gospodarski razvoj. S sistemom za razvoj digitalno zrelih šol, e-šol, želi do leta 2022 uvesti IKT v šolske sisteme. "Digitalna zrelost" šol je koncept, ki postaja z razvojem tehnologije vse pomembnejši. Digitalno zrele šole imajo sistematičen pristop k uporabi IKT pri načrtovanju in vodenju šol ter v svojih izobraževalnih in poslovnih procesih, sistematično se lotevajo razvoja digitalnih kompetenc osebja in učencev. Program je razdeljen na dve fazi: pilotni projekt 2015–2018 v 10% šol v državi, ki mu sledi celotno izvajanje v obdobju 2019–2022, ob upoštevanju rezultatov pilotskega programa.

[39] Povzeti po: European Commission: Inspirational practises for tomorrow's inclusive digital world, Technical Dossier no. 10, 2019, str. 22-29.

Pilotna faza je bila izvedena v 151 osnovnih in srednjih šolah na Hrvaškem, v katere je bilo vključenih več kot 7000 učiteljev in več kot 23 000 učencev. Sredstva ESS so sodelujoče šole opremila z najnovejšo opremo IKT, kot so interaktivne učilnice in predstavitvene učilnice, več kot 1 1200 računalnikov za učitelje, več kot 10 000 tabličnih računalnikov za učence, kot tudi potrebno WLAN infrastrukturo v šolskih stavbah. Financiranje ESS je pilotnim e-šolam omogočilo razvoj digitalnih izobraževalnih vsebin, vključno z: e-vsebine za 16 različnih naravoslovnih predmetov z več kot 100 različnimi moduli; in 240 učnih scenarijev in 72 digitalnih knjižnih poročil. Pomagalo je tudi pri izvedbi 1 900 delavnic, e-predavanj in spletnih seminarjev za izgradnjo zmogljivosti ravnateljev, učiteljev, podpornega osebja in šolskih administratorjev za izvajanje IKT v šolah. S tem so e-šole okrepile zmogljivosti na osnovno- in srednješolskem izobraževanju na Hrvaškem za pripravo učencev na nadaljnje izobraževanje, trg dela in vseživljenjsko učenje.

Pilotni projekt se je na **Portugalskem** začel leta 2015 na povabilo generalnega direktorata za izobraževanje, ki sta ga izvedla CDD (*Centro de cidadania Digital,* Center za digitalno vključevanje) in *Apps for Good (*mednarodni program s sedežem v Londonu, ustanovljen leta 2010). Cilj je zdaj razširiti program na 162 šol v severni, osrednji in Alentejo regiji Portugalske.

Projekt naj bi prispeval k državljanski ozaveščenosti, socialni vključenosti in prihodnji zaposljivosti, ter družbo naredil bolj dejavno in participativno. Projekt podpira preoblikovanje idej mladih v aplikacije, ki imajo neposredne koristi za skupnost. To spreminja ustaljeno pedagoško paradigmo. *App for Good* s pomočjo strokovne skupnosti spodbujajo ujemanje med šolami (študenti) in realnim kontekstom industrije. Program vsebuje: 1) vsebinsko platformo; 2) metodološko usposabljanje za vzgojitelje; 3) redno spremljanje učencev (na spletu in v živo); 4) organizira tekmovanja med šolami v znanju IKT in ponuja štipendije. Njegov cilj je ustvariti novo generacijo reševalcev problemov in digitalnih izdelovalcev: študentje z znanjem in samozavestjo za gradnjo, trženje in zagon digitalnih orodij za reševanje težav skupnosti.

Okvirnemu programu je v obdobju 2018–19 sledilo 180 partnerskih šol po vsej Portugalski, ki izobražujejo 450 vzgojiteljev in 3 000 10-18-letnikov. Poročilo o vplivu programa 2017–18 kaže, da je 80% udeležencev menilo, da je bolje znanje in na sploh ozaveščanje glede tehnologije način za reševanje socialnih problemov in izboljšanje spretnosti. Glede osebnega razvoja so poročali o izboljšanih spretnostih

za reševanje problemov (80%), timskem delu (85%), komunikaciji (76%) in tehničnim znanjem (75%). App for Good je spodbudil tudi razvoj veščin IKT za učitelje in predavatelje, za katere je UNESCO ugotovil, da so bolj sodelovalni (73%), bolj samozavestni pri poučevanju (72%), bolj zadovoljni (84%), bližje študentom (84%) in z več znanja o sposobnosti njihovih študentov (89%).Na Portugalskem je 45% udeležencev v letih 2018-19 bilo žensk.

V zadnjih 20 letih je **Grčija** razvila in izvajala državni sistem za vključevanje digitalnih tehnologij v izobraževanje, zlasti v pedagoško prakso. Potreba učiteljev osnovnih in srednjih šol po razvijanju osnovnih znanj in veščin na področju IKT je bila prvič obravnavana v Grčiji s pobudo, imenovano *A-Level Training*, ki se je izvajalo med leti 2000–2004, leta 2005 pa mu je sledilo usposabljanje na delovnem mestu, ki je učiteljem omogočilo uporabo in uporabo digitalnih tehnologij v učiteljski praksi - tako imenovano usposabljanje na ravni B. Program usposabljanja na delovnem mestu je bil leta 2016 nadgrajen in razširjen na vse učne discipline z obogateno in osveženo vsebino.

Udeleženci so se vsak teden, zunaj šolskih ur, udeležili 3-urnega 'treninga' digitalnih veščin, ki so ga vodili kvalificirani učitelji IKT. Financiranje ESS je projektu omogočilo usposabljanje 300 novih trenerjev na ravni B, da bi zagotovili pokritost po vsej državi. Inovativni vidik novega programa je uporaba mešanega sistema učenja, kombinacija učnih tečajev na daljavo, posnetih dejavnosti učenja na daljavo in, kjer je to mogoče, nekaj osebnih sestankov. Eden od razlogov za uporabo te metode je povezan s širjenjem programa po vsej državi in s specifičnim zemljepisom Grčije z veliko odročnih območij in na tisočih otokov, zaradi česar je lokalno usposabljanje težko in drago.

Približno 27 500 učiteljev osnovnih in srednjih šol se je od leta 2016 izobraževalo na IKT stopnji (približno 20% vseh učiteljev iz grših šol). Cilj projekta je bil, da se do sredine leta 2019 usposobi 35 000 učiteljev. Izobraževalna skupnost je ta program usposabljanja dobro sprejela. Projekt je prav tako posodobil, razširil in prilagodil obstoječo knjižnico učnih in podpornih gradiv.

Tudi **Litva** v zadnjih letih prednostno obravnava celovito uporabo digitaliziranih vsebin in orodij v predšolski vzgoji, pri otrokih v osnovnošolskem izobraževanju ter uporabo računalnikov in elektronskih storitev med starostjo 16–74 +. Litvanska nacionalna digitalna koalicija aktivno prispeva k in usklajuje izvajanje Programa

razvoja informacijske družbe za obdobje 2014–2020 „Digitalna agenda za Litvo“. Cilj digitalne agende je izkoristiti priložnosti, ki jih ponuja IKT, za izboljšanje kakovosti življenja, povečati produktivnost podjetij in zagotoviti, da lahko 85% prebivalstva Litve dostopa do interneta, 95% podjetij pa ima hiter internet. Programi ESS za obdobje 2014–2020 so prispevali k razvoju in preizkušanju izobraževalnih vsebin in organizacijskih modelov v predšolskem, osnovnošolskem in srednješolskem izobraževanju.

Več kot 3 500 učiteljev iz vseh litovskih srednjih šol je bilo poučenih za uporabo digitalnih orodij v učilnici, 119 učiteljev (predavateljev) je bilo usposobljenih za pomoč drugim učiteljem za učinkovito uporabo digitalnih učnih orodij, pridobljeno in prilagojeno je bilo 20 digitalnih učnih gradiv, izdelana je bila zbirka kriterijev za vrednotenje digitalnih učnih pripomočkov in digitalnih učbenikov ter oblikovana metodologija za prilagajanje in razvoj digitalnih učnih gradiv.

Projekt je na koncu ustvaril in podprl enotno eLearning okolje, ki vsebuje bazo učbenikov in podatkov o učnih sredstvih ter se povezuje z obstoječim izobraževalnim portalom *www.e-mo¬kykla.lt*. Portal vsebuje tudi forum za izobraževalno skupnost, koledar, sistem za opomnike in vprašanja učencem in učiteljem (javnim in zasebnim).

7.4 Delo in umetna inteligenca

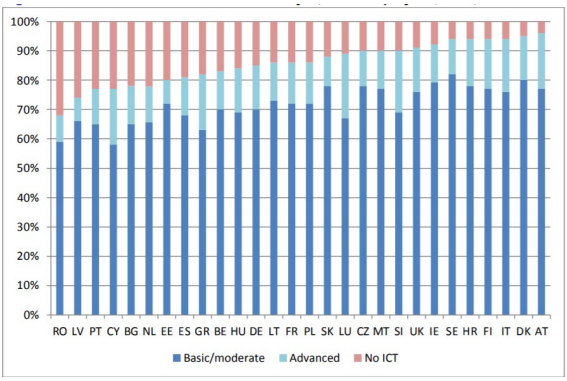
Pogoj za ustrezen prehod delavcev v z digitalizacijo prepredeno delovno sfero, je sistem obveščanja o trgu dela, ki predvideva dolgoročne trende in spretnosti, ki so v koraku z razvojem. Z namenom podpore državam članicam EU, socialnim partnerjem in drugim zainteresiranim osebam CEDEFOP, Evropski center za razvoj poklicnega usposabljanja, redno spremlja spremembe na trgu in analizira možne rešitve in tveganja. Temelj njegovega delovanja je ideja, da predvidevanje v ves čas spreminjajočem digitalnem svetu predstavlja ključni faktor za prilagoditev delovnega procesa na te spremembe.

7.4.1 Raziskava European Skills and Jobs (CEDEFOP)[40]

Cedefop je analiziral več kot 70 milijonov spletnih oglasov za zaposlitev v državah članicah EU. Podatki kažejo, katera delovna mesta ponujajo delodajalci in katere veščine pri tem zahtevajo. Hitrost sprememb zahteva prilagajanje in mešanje tradicionalne inteligence z umetno, zato je jasno, da je sposobnost prilagoditve spremembam na vrhu seznama. Velikokrat delodajalci kot pogoje postavijo sposobnosti skupinskega dela, uporaba računalnika, znanje angleščine in sposobnosti komunikacije s strankami. Te predstavljajo tretjino spretnosti, ki jih delodajalci iščejo preko spletnih oglasov za delo.

V okviru vprašanja, kako bodo delavci v prihodnje usklajevali delovni proces z inovacijami UI, je CEDEFOP-ova raziskava razlikovala med tremi IT nivoji, in sicer nizko (uporaba osebnega računalnika, tabličnega računalnika ali mobilne naprave za elektronsko pošto ali brskanje po internetu), osnovno (obdelava besedil ali ustvarjanjem dokumentov in preglednic) in visoko **ravnjo oz. naprednim znanjem IKT** (razvoj programske opreme, aplikacij ali programiranja, uporaba računalniške sintakse in statistične analize). Raziskovalci so dopustili tudi možnost, da delavci na nekaterih delovnih mestih sploh ne potrebujejo veščin IKT. Večina (52%) delavcev v EU je izjavila, da je za opravljanje delovnih nalog potrebna osnovna raven IKT, 19% pa, da zadošča nizka raven. Približno 14% potrebuje visoko raven IKT, v nasprotju s 14%, ki je navedlo, da na svojem delovnem mestu sploh ne potrebujejo veščin IKT. Švedska, Danska in Irska so države, v katerih več kot 80% delovne sile potrebuje vsaj osnovno raven znanj IKT, v nasprotju s Ciprom, Romunijo in Grčijo, kjer enako velja za približno 60% delavcev. Portugalska, Bolgarija, Latvija in Nizozemska imajo najvišji delež zaposlenih (več kot petino), ki pri svojem delu ne potrebujejo znanja IKT. Slovenija na grafu ne izstopa, saj spada med države, v katerih se povprečno zahteva vsaj osnovno znanje IKT, ima pa enega izmed najvišjih deležev poklicev z naprednim znanjem IKT.

[40] Cedefop: The great divide: Digitalisation and digital skill gaps in the EU workforce, #ESJsurvey Insights. Thessaloniki: Greece. No 9, 2016.



Slika 1: Stopnja znanja s področja IKT na delovnih mestih v državah članicah EU (ang. *ICT-related work skills in EU Member States*)

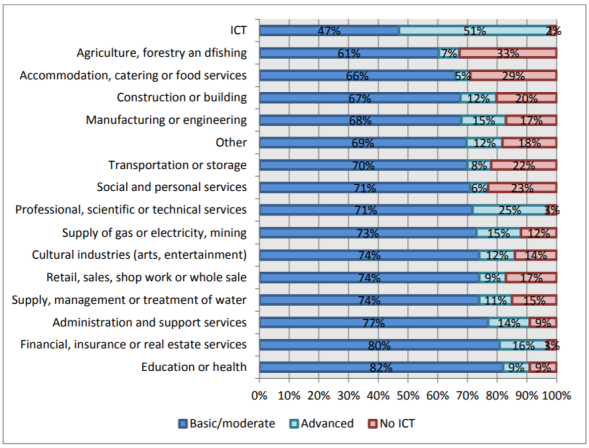
Vir: Cedefop, 'The great divide: Digitalisation and digital skill gaps in the EU workforce', 2016

Analiza nadalje razkriva, da je izključitev nekaterih skupin prebivalstva iz napredka digitalne dobe zelo pomembna značilnost evropskega trga dela in poglablja razkorak med delavci. Posamezniki največji del svojega življenja preživijo na delovnem mestu. V primeru zaposlitve na delovnih mestih, ki digitalnih tehnologij ne potrebujejo ali ne uporabljajo, so morda manj naklonjeni uporabi digitalnih tehnologij tudi zunaj delovnih mest in ne bodo razvili digitalne usposobljenosti, ki bo v prihodnosti pogoj za aktivno udeležbo v družbi. Iz spodnje slike je razvidno, da se za izjemno velik delež določenih podskupin delovne sile v EU ne zahteva znanj in spretnosti IKT. Kar 33% zaposlenih v kmetijskem sektorju in 29% v sektorju nastanitve, gostinstva in prehrambenih storitev je izjavilo, da ne potrebujejo veščin IKT za opravljanje svojih nalog. Pri teh poklicih imajo ročne ali druge spretnosti pomembnejšo vlogo. Da bi ublažile izključenost določenih skupin iz uporabe IKT, so številne države sprejele ukrepe, ki povečujejo dostop do IKT usposabljanja in aktivnega učenja. Vzpostavile so digitalne programe, ki upoštevajo potrebe ogroženih skupin in spodbujajo digitalno vključenost za vse.

Verjetno je, da bodo napredne digitalne spretnosti, zlasti programiranje in kodiranje, postale ključni predpogoj za vstop na številna delovna mesta in vplivala na delovni čas in plačilo za delo. Raziskava razkriva, da se po upoštevanju različnih dejavnikov, od katerih je odvisno plačilo za delo, npr. spol, starost, stopnja izobrazbe, delovna doba, sposobnost za učenje, urna postavka zviša za približno 3,7%, kadar se na delovnem mestu zahteva osnovno znanje IKT. Posamezniki, zaposleni na delovnih mestih, ki sploh ne potrebujejo veščin IKT, prejemajo približno 8% nižjo povprečno

plačo na uro v primerjavi z drugimi enakovrednimi zaposlenimi, ki delo opravljajo s pomočjo IKT. Plačna osnova se v primeru naprednih IKT znanj v Veliki Britaniji in Nemčiji dvigne na kar 7-8%, medtem ko na Češkem delavci, ki ne potrebujejo nobenih veščin IKT, prejemajo približno 20% nižje plače.

Spodnja slika prikazuje **vpliv tehnologije na veščine,** ki se zahtevajo od delavcev v posameznih panogah dela. Ob upoštevanju spreminjanja plač, delovnega časa in drugih delovnopravnih vidikov v odvisnosti od veščin IKT, ti niso le goli podatki, ampak odražajo vpliv na temeljne pravice delavcev v EU.



Slika 2: Prikaz panog glede na stopnjo znanja s področja IKT (ang. *Industries by level of ICT skills*)

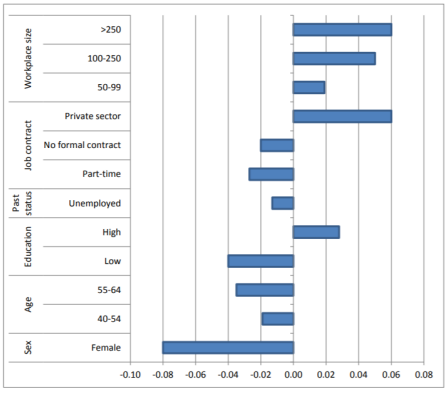
Vir: Cedefop, 'The great divide: Digitalisation and digital skill gaps in the EU workforce', 2016

Kljub pričakovanemu naraščajočemu pomenu naprednih digitalnih veščin na evropskem trgu dela, podatki raziskave razkrivajo, da so nekatere **skupine zaposlenih v EU** trenutno v slabšem položaju. Delavke, starejši delavci, nizko izobraženi, delavci s krajšim delovnim časom in brezposelni imajo manj možnosti, da bodo v okviru svojega (nadaljnjega) dela potrebovali napredne veščine IKT.

Raziskava je poleg problema izključitve določenih skupin delovne sile iz digitalne ekonomije zbirala tudi podatke **o vrzeli med spretnostmi delavcev v EU (nizka, osnovna in visoka raven veščin oz. znanja), o neusklajenosti med zahtevanimi spretnostmi na delu in njihovim trenutnim znanjem in sposobnostim dela z IKT.** Anketiranci so morali oceniti, v kolikšni meri njihova lastna znanja presegajo

ali zaostajajo za tistimi, ki so potrebne za opravljanje delovnih nalog. V nekaterih državah (npr. Romunija, Ciper, Grčija in Nizozemska) se lahko majhne razlike v digitalni spretnosti pripišejo nižji povprečni stopnji intenzivnosti spretnosti znotraj delovnih mest, ki zahtevajo osnovne veščine IKT. Nasprotno pa imajo lahko države na višjem koncu spektra, kot so Bolgarija, Portugalska in Estonija, večji delež vrzeli v digitalni spretnosti, saj so nekateri delavci digitalno bolj usposobljeni, drugi pa manj. Pravzaprav pregled podatkov iz raziskovanja CEDEFOP razkriva, da so v vzorcu posameznikov, ki so navedli, da njihova delovna mesta zahtevajo osnovne digitalne spretnosti, opazne razlike glede pomena digitalnih spretnosti ter drugih kognitivnih in 'mehkih' veščin. Nekatere države (npr. Avstrija, Belgija, Finska) imajo višjo povprečno stopnjo pomembnosti digitalnih veščin (na lestvici 0-10, kjer 10 pomeni, da so veščine IKT bistvene za opravljanje dela); ta presega oceno osem, v nasprotju z drugimi (Češka, Bolgarija, Španija, Hrvaška), ki imajo povprečno oceno približno sedem.

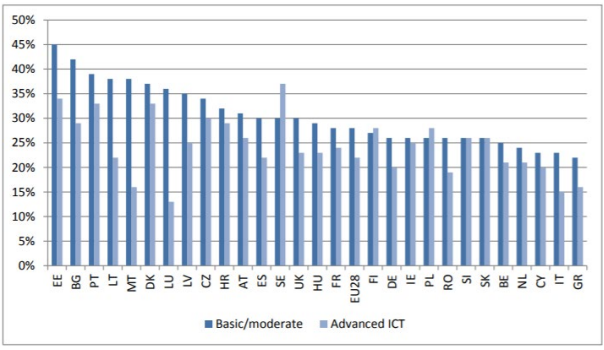
Figure 4 **Probability of requiring advanced ICT skills for job, adult employees, 2014, EU-28**



Slika 3: Stopnja potrebe po znanju s področja IKT
(ang. *Probability of requiring advanced ICT skills for job*)
Vir: Cedefop, 'The great divide: Digitalisation and digital skill gaps in the EU workforce', 2016

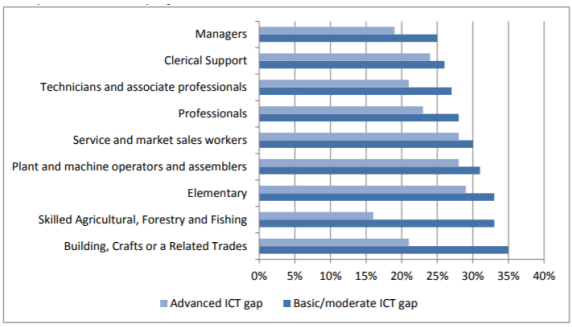
Slika prikazuje, da je delež zaposlenih, ki občutijo negativne posledice zaradi vrzeli v digitalni spretnosti, približno 17%. V Estoniji znaša ta podatek 31%, na Malti 29%, 26% na Danskem, 12% v Grčiji in na Nizozemskem. V povprečju je približno 28% evropske delovne sile svojo raven osnovnih digitalnih veščin uvrstilo precej nizko v primerjavi s tem, kar se na delovnem mestu zahteva. Približno 22% tistih, ki so zaposleni na delovnih mestih, ki zahtevajo napredno digitalno znanje, je v nevarnosti

spremembe pod vplivom digitalizacije. Približno 40% delovnih mest v Estoniji, Bolgariji in na Portugalskem je prizadetih zaradi vrzeli v digitalni spretnosti. Spodbuden je podatek, da je v Sloveniji ta vrzel skoraj ničelna.



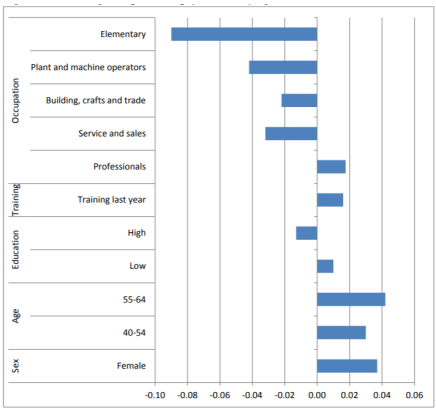
Slika 4: Vpliv IKT na delovna razmerja v državah članicah EU
(ang. *The impact of ICT on labour relations in EU Member States*)
Vir: Cedefop, 'The great divide: Digitalisation and digital skill gaps in the EU workforce', 2016

Pri tem je v EU več kot tretjina zaposlenih v kmetijskem sektorju, nastanitvenih, gostinskih in prehrambenih storitvah ter socialnih storitvah, prizadetih zaradi vrzeli v digitalnih spretnostih. Nasprotno pa manj kot četrtina delavcev na področju IKT ter finančnih, zavarovalniških in nepremičninskih storitev čuti manjše razlike v digitalni usposobljenosti. Slika poudarja, da je več kot tretjina delavcev v gradbeništvu in obrtnih **poklicih nagnjena k razlikam v digitalni spretnosti.**



Slika 5: Razmerje med stopnjo in vrsto izobrazbe ter vplivom IKT
(ang: *Relationship between the level and type of education and the ICT gap*)
Vir: Cedefop, 'The great divide: Digitalisation and digital skill gaps in the EU workforce', 2016

Raziskava ESJ poleg razlik v pojavnosti razlik v digitalni spretnosti med različnimi sektorji gospodarske dejavnosti in poklicev omogoča tudi nadaljnjo razčlenitev in preučevanje povezave med digitalnimi razlikami v usposobljenosti in različnimi demografskimi in družbenoekonomskimi značilnostmi delavcev v EU. Iz grafa je razvidno, da so značilnosti, ki vzdržujejo digitalni razkorak (npr. velikost podjetja, spol, stopnja izobrazbe itd.), povezane tudi z višjim **tveganjem za delavce, ki trdijo, da trpijo zaradi digitalnih vrzeli v usposobljenosti.** Zlasti ženske, starejši in nižje izobraženi delavci, imajo večjo verjetnost digitalnih razlik v spretnostih.



Slika 6: Ogrožene skupine delavcev
(ang: *vulnerable groups of workers*)
Vir: Cedefop, 'The great divide: Digitalisation and digital skill gaps in the EU workforce', 2016

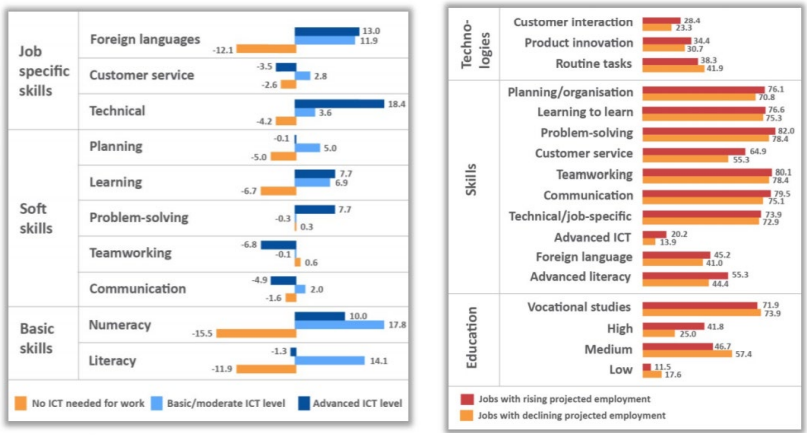
Preobrazba, ki jo prinaša uvedba digitalnih tehnologij na delovnih mestih, ne vpliva samo na povpraševanje po digitalnih spretnostih, ampak prinaša določene prednosti. Uporaba IKT pri delu vpliva na posameznikovo splošno sposobnost opravljanja delovnih nalog. Običajno višja pogostost in razpoložljivost informacij, povezanih z digitalnimi delovnimi mesti, zahtevata osnovne veščine in višjo stopnjo načrtovanja, osebno prilagodljivost ter sposobnost pregledovanja in filtriranja bistvenih dokazov. To vpliva tudi na sposobnost medosebne interakcije in komunikacije s strankami - na primer naraščajoči pomen e-trgovine je manj odvisen od interakcije med seboj, kar je značilno za ne-digitalne komercialne transakcije. Raziskava je poleg poizvedovanja o ravni IKT, ki je potrebna na določenih delovnih mestih, anketirance tudi pozvala, naj navedejo pomembnost nabora desetih drugih kognitivnih, nekognitivnih in specifičnih spretnosti. Na podlagi teh informacij je na sliki prikazana (ocenjena) verjetnost, da bo delo uporabnika IKT odvisno tudi od veščin,

ki niso neposredno povezane z IKT. Verjetnosti so bile ocenjene s primerjavo vzorcev zaposlenih, ki so navedli, da je za njihovo delo potrebna osnovna ali visoka raven IKT s tistimi, ki ne potrebujejo veščin IKT za opravljanje svojih nalog. Upoštevane so bile tudi druge ključne demografske in socialno-ekonomske razlike med obema skupinama (npr. spol, starost, stopnja izobrazbe).

Iz spodnjih grafov je razvidno, da je za delavca pomembno, da ima poleg tehničnih znanj, tudi **druge spretnosti in zanimanja.** Uspešnost dela na z IKT povezanih delovnih mestih je močno odvisna od sposobnosti kritičnega mišljenja delavcev ter spretnosti reševanja problemov, pa tudi pri učenju, prilagajanju in uporabi novih metod in tehnologij pri delu (učne spretnosti). Poleg tega obstaja pomembna povezava med uporabo IKT in potrebo po znanju tujega jezika, da lahko opravlja svoje delovne naloge. Glede na dopolnjevanje digitalnih in nedigitalnih veščin na delovnem mestu je mogoče iz podatkov raziskave razbrati tudi naravo digitalne vrzeli med različnimi delovnimi mesti. Analiza razkriva, da imajo zaposleni, ki jih prizadenejo spretnosti v IKT, večjo nagnjenost k sočasnim vrzeli v svojih drugih spretnostih (pismenost, računanje), pa tudi njihovih tehničnih sposobnosti. Podobno je podana tudi povezava med pojavnostjo razlik v znanju IKT in nezmožnostjo delavcev, da se še naprej urijo in učijo novih znanj na svojih delovnih mestih.

Raziskovanje, analiziranje in razmišljanje o spremembah, ki jih zaznavamo vsak dan, so lahko pomembna podlaga za iskanje rešitev na delovnih mestih. Široko soglasje o informacijskih standardih je lahko temelj za brezhibno podporo pri učenju o UI in nadgradnji veščin z znanjem IKT. Nacionalni kvalifikacijski in validacijski sistemi, ki omogočajo evidentiranje potrdil o izobraževanju, pridobljenih zunaj formalnega izobraževalnega sistema, igrajo ključno vlogo. Digitalni portfelji postajajo vse bolj pomembni pri usklajevanju politike in zagotavljanju učenja odraslih. Dobro uporabljeni portfelji omogočajo kakovostne napotitve med storitvami, ki ocenjujejo potrebe po spretnostih in nudijo karierne nasvete. To omogoča prilagajanje učenja uporabnikom in njihovem razpoložljivem času. Rešitve se lahko nanašajo na posebnosti učenja na delovnem mestu, situacij v učilnici ali uporabe doma.[41]

[41] Povzeto po: Cedefop: The great divide: Digitalisation and digital skill gaps in the EU workforce, #ESJsurvey Insights. Thessaloniki: Greece, No 9, 2016.



Slika 7: Prikaz delovnih veščin, povezanih z IKT
(ang: *ICT-related work skills*)
Vir: Cedefop: People, machines, robots and skills, julij 2017

7.4.2 Pravice delovnega prava

Postavlja se vprašanje, kaj natančno prinaša pojav UI z vidika delovnega prava. Ali bi moralo pravo priznati pravico do štirideset urnega delavnika tudi robotom? Ali bodo roboti upravičeni do plačanega dopusta? Kaj pa bolniški stalež zaradi pregretja ali virusa v sistemu? Čeprav je njihova utemeljitev veliko bolj filozofsko kot delovnopravno vprašanje, delovno in socialno pravo teh vprašanj ne ureja, zato je odgovor nikalen.[42] Kljub temu pa bi bilo smiselno urediti določene položaje sodelovanja človeka in robota pri delu ter druge spremembe na delovnih mestih. Z drugimi besedami, delovno pravo lahko ustvari nov pravni okvir in okolje za predvidevanje in vključevanje preobrazbe, ki jo povzroča uvedba UI na način, ki ublaži prehod delavca na digitalno delovno mesto.

7.4.2.1 Delovno razmerje

Zaradi sprememb, ki jih prinaša digitalizacija, postaja ločnica med delavci in neodvisnimi izvajalci čedalje bolj zabrisana. To prinaša v delovno okolje določeno stopnjo pravne negotovosti, predvsem za delavce, ki so doslej opravljali delo po delodajalčevih navodilih in njegovim nadzorom.

[42] Ducorps-Prouvost, E.: Labor Law And The Challenges Of Artificial Intelligence : 1st Part Of A Trilogy, Soulier Avocats, 2018.

Delovno razmerje kot ga razumemo v tradicionalnem smislu je razmerje med delavcem in delodajalcem, v katerem se delavec na podlagi **pogodbe o zaposlitvi** prostovoljno vključi v organiziran delovni proces delodajalca in v njem za plačilo, osebno in nepretrgano opravlja delo po navodilih in pod nadzorom delodajalca (4. člen Zakona o delovnih razmerjih, ZDR-1[43]). Poleg pogodb o zaposlitvi se kot pravne podlage za opravljanje različnih oblik dela uporabljajo **avtorske in podjemne pogodbe, pogodba o poslovodenju, osebno dopolnilno delo, začasno in občasno delo upokojencev, pripravništvo, s.p. in ostale oblike opravljanja gospodarske dejavnosti**. Za razliko od delavca neodvisni izvajalec samostojno opravlja delo, a v okviru dogovorjenih obveznosti in vnaprej določenih opravil. Kot rezultat UI se na delovnem mestu pojavljajo še ne poznane oblike opravljanja dela, ki jih s težavnostjo umestimo v katero izmed navedenih.

Primer takšnega trenda je t.i. *latte machiatto* delovno okolje, pri katerem zaposleni ne sedijo v pisarnah na sedežu delodajalca, ampak v kavarni za vogalom in delo opravljajo na svojih prenosnih računalnikov. Delo je tako mogoče opravljati po vsem svetu in pri tem vključiti v delovni proces osebe, ki se ne nahajajo v istem kraju. Klasično delovno mesto tako služi samo vzdrževanju socialne mreže s sodelavci. S tem postaja meja med poklicnim in zasebnim življenjem zabrisana, kar ima za posledico določene obremenitve za zaposlene ter nove organizacijske možnosti za delodajalce. Spremenila tudi vloga nadrejenih, ki se odslej soočajo z glavnim izzivom nadzora nad delavci in vzpostavitvijo osebnega stik prek tehničnih poti.

Trendu fleksibilnega delovnega časa se je torej pod vplivom UI pridružil še fleksibilnejši kraj dela. Čeprav se na prvi pogled zdi takšna rešitev dobra, prinaša z vidika **razlikovanja med delavci in samostojnimi izvajalci** določene slabosti. Če kraj dela poleg delovnega časa postane bolj prožen in je zaposlenim dana večja svoboda, postane težje razlikovati med neodvisnimi pogodbeni izvajalci in delavci, predvsem tistimi, ki sklenejo pogodbo o zaposlitvi s krajšim delovnim časom. Razlikovanje je pomembno zlasti z vidika socialnih pravic, saj imajo delavci s krajšim delovnim časom polne pravice iz delovnega prava (npr. zaščita pred nepoštenim odpuščanjem, plačani dopust, porodniški dopust, nadomestilo za brezposelnost), neodvisni izvajalci pa na splošno nimajo teh socialnovarstvenih koristi, četudi morda

[43] Zakon o delovnih razmerjih (Uradni list RS, št. 21/13, 78/13 – popr., 47/15 – ZZSDT, 33/16 – PZ-F, 52/16, 15/17 – odl. US, 22/19 – ZPosS in 81/19).

njihov delovni čas v tednu presega največji obseg ur delavcev s krajšim delovnim časom.

Ne glede na označitev strank v pogodbi, je razvrstitev posameznika v eno izmed teh kategorij odvisna od vsebine dejanske izvedbe dela. Opredelitev oseb je odvisna torej od konkretne naloge oz. opravila. Nekateri samostojni pogodbeniki so ekonomsko odvisni od določenega podjetja, tudi če imajo sicer druge posle in stranke. Bolj kot je razmerje med zunanjim izvajalcem in podjetjem izrazito, večja je verjetnost, da bodo sodišča predpostavila obstoj delovnega razmerja med njima, četudi ne obstaja pisna pogodba o zaposlitvi. Možna posledica navedenega je upravičenost neodvisnega izvajalca do pravic socialne varnosti in sodelovanja v podjetju, na volitvah predstavnikov delavcev ali v primeru odpovedi, nadaljevanja zaposlitve med postopkom odpuščanja - čeprav se je bil namen temu izogniti. Potrebno bi bilo torej dopustiti prerazvrstitev osebe v drugo kategorijo in jo od primera do primera obravnavati kot delavca oz. samostojnega izvajalca.

Ne samo, da je problematično ločevanje med delavci in neodvisnimi izvajalci, enako velja tudi za **diferenciacijo med delodajalci in tretjimi osebami**, npr. strankami. Postaja vse pogosteje, da ni samo delavčev delodajalec, ki je naveden v pisni pogodbi o zaposlitvi, tisti, ki daje navodila in izvaja nadzor nad delom.

Tipičen primer so matrične organizacijske strukture, pri katerih gre za dvojno vodenje oz. obliko povezovanja v oddelke po proizvodih in funkcijah, a hkrati odgovornost obema vodjema. V nekaterih primerih imajo stranke in dajalci franšiz moč določiti delovne pogoje posameznih zaposlenih. Druga situacija, v kateri je lahko meja med njima nejasno določena, je skupni podjem, pa tudi organizacija dela, pri kateri zaposleni prehajajo iz enega podjetja v drugega po dogovoru, da je zaposleni „izposojen" drugemu, če prvotni delodajalec trenutno nima opravil zanj. Čeprav se zdi takšna ureditev popolnoma legitimna, poleg tega pomeni določeno prednost za majhna in srednja podjetja, ki združijo svoje znanje in se hitreje odzovejo na naročila ter spremembe v poslovanju, je dejstvo, da lahko delodajalec v resnici postane kdo drug, predmet mnogih kritik in se celo označuje kot **suženjstvo 21. stoletja.** Zato tudi ne preseneča dejstvo, da je takšno poslovanje v evropskih državah dopustno zgolj v posebnih okoliščinah in pod izjemnimi pogoji.[44]

[44] Wisskirschen, G. in drugi: Artificial Intelligence and Robotics and Their Impact on the Workplace, IBA Global Employment Institute, 2017, str. 92-94.

7.4.2.2 Pošteni in pravični delovni pogoji

Novejše oblike opravljanja dela zahtevajo natančno pravno ureditev. Vrzeli pravne ureditve se kažejo v temeljnih elementih socialne zaščite - to je z vidika brezposelnosti, bolezni, nesreč na delovnem mestu ipd. Če se bo trenutni trend nadaljeval in bodo fleksibilne in nestandardne oblike zaposlitve še naprej naraščale (kot se predvideva), bi morala politika pregledati status teh vrst zaposlitve in po potrebi nanje razširiti zakonodajo.

Prvi korak na tem področju je storila EU s Priporočilom Sveta o dostopu do socialne zaščite za delavce in samozaposlene.[45] Priporočilo zagotavlja, da delavci in samozaposleni v primerljivih pogojih uživajo pravice iz sistema socialne varnosti, olajšuje prenos pravic socialne varnosti z enega na drugo delovno mesto, ter o pravicah in obveznosti iz sistema socialne varnosti delavcem in samozaposlenim zagotavlja pregledne informacije. Zatem je Komisija predstavila svoje predloge v Direktivi o preglednih in predvidljivih delovnih pogojih,[46] katere namen je zagotoviti, da nekatere pravice (pravica do informacij iz člena 3, minimalna predvidljivost dela iz člena 10, varstvo pred odpovedjo in dokazno breme iz člena 18, pravica do pravnega sredstva iz člena 16), zajemajo vse delavce v vseh oblikah dela, vključno s tistimi v najbolj fleksibilnih nestandardnih in novih oblikah dela, kot so priložnostna dela, dela na spletnih platformah ipd. Načela in pravice, določene v obeh pobudah, bi morale biti podlaga vseh prihodnjih prilagoditev zakonodaje o pogojih dela v UI in robotiki, o katerih se opredeljujemo v naslednjih točkah.

7.4.2.3 Koncept delovnega časa in počitkov

Dolžina delovnega časa se je od industrijskih revolucij do danes spreminjala. V obdobju po prvi industrijski revoluciji je bil delovni čas skoraj polno delovno leto in 69-urni delovni teden, v drugi industrijski revoluciji je posledično sledil niz predpisov, ki so omejili ure dela na 12 na dan v VB in do 8 ur na dan v ZDA. Keynes je napovedoval štiriurni delovni dan (kar ustreza 20-urnemu delovnemu tednu), v Sovjetski zvezi pa so napovedovali 5-urni delavnik. Te napovedi se niso uresničile,

[45] Priporočilo Sveta z dne 8. novembra 2019 o dostopu delavcev in samozaposlenih oseb do socialne zaščite, 2019/C 387/01, 15. november 2019.
[46] Direktiva (EU) 2019/1152 Evropskega parlamenta in Sveta z dne 20. junija 2019 o preglednih in predvidljivih delovnih pogojih v Evropski uniji, PE/43/2019/REV/1, Uradni list Evropske unije, L 186, 11.7.2019, str. 105–121.

trend upadanja delovnega časa pa se je ustavil okoli 80. let prejšnjega stoletja, z razpadom Sovjetske zveze, pojavom interneta, drugačnim življenjskim slogom ter prostega gibanja delavcev v okviru notranjega trga EU, ko je moč znova opaziti povečanje delovnega časa.[47]

Doslej je bilo po vsem svetu značilno, da so bili delavci prisotni v pisarni na sedežu delodajalca, kjer so opravljali svoje delo in po osmih do desetih urah zapustili delovno mesto. Čeprav obstaja nekaj zaposlenih, ki ima raje jasno določen in enakomeren delovni čas ter popoldneve brez službenih opravil, večina delavcev upa na večjo prilagodljivost. Starši lahko svoj začetek dela prilagodijo urniku vrtca ali šole, sodelujejo v jutranji športni aktivnosti ali se izobražujejo. Ta oblika fleksibilnega dela je posebej privlačna za ženske, nedvomno pa bi imeli prav vsi koristi od bolje uravnoteženega poklicnega in zasebnega življenja. Zaradi naraščanja števila univerzitetnih diplomantov, se je povprečna starost delavcev ob prvi zaposlitvi povečala, veliko izmed njih pa ustvari družine v relativno kratkem času po prvi zaposlitvi. Evropska komisija je v svojem delovnem programu napovedala sveženj ukrepov za reševanje izzivov, s katerimi se soočamo pri usklajevanju poklicnega in zasebnega življenja. Z izboljšanjem udeležbe žensk na trgu dela, bi ta pobuda prispevala k prednostnim nalogam Komisije v zvezi z delovnimi mesti in rastjo v okviru demografskih izzivov. Ti modeli to omogočajo se delavci lažje osredotočijo na svoje zasebno življenje skladno z njihovimi individualnimi potrebami.[48]

Največje povpraševanje po stalni dosegljivosti obstaja v storitvenem sektorju, v katerem se zahteva visoka stopnja zaupanja med strankami (npr. odvetništvo, svetovanje, zdravstvena nega). Stranke ponavadi naročajo storitve v popoldanskih urah, med vikendi in pred prazniki. Zaradi digitalizacije pričakujejo, da bodo prodajalci in ponudniki storitev na voljo tudi izven običajnih delovnih ur. Inteligentni stroji in učinkovita logistika bi morali omogočati ponudbo izdelkov in storitev, ki so prilagojeni željam vsakega kupca. To lahko uspe le, če so ponudniki na voljo kadar koli. A delo, ki je enostransko prilagojeno samo željam strank in zahteva neprestano pripravljenost, lahko privede do izolacije posameznika, preobremenjenosti in zdravstvenih težav.

---

[47] Samothrakis, S.: Viewpoint: Artificial Intelligence and Labour, Proceedings of the Twenty-Seventh International Joint Conference on Artificial Intelligence, v: Proceedings of the Twenty-Seventh International Joint Conference on Artificial Intelligence, IJCAI-18, str. 5653.

[48] Wisskirschen, G. in drugi: Artificial Intelligence and Robotics and Their Impact on the Workplace, IBA Global Employment Institute, 2017, str. 69.

Francoska vlada je temu trendu nasprotovala in leta 2017 sprejela zakon, ki predpisuje pravico do 'prekinitve povezave' po končanem delu („*le droit ŕ la déconnexion*“)[49]. [50]

Povečano robotizacija lahko privede tudi do povečanja delovnega časa. Sedanja okvirna zakonodaja, ki obravnava delovni čas v EU, je Direktiva EU o delovnem času.[51] Ali in kako bo treba nacionalno zakonodajo prilagoditi tako, da odraža povečano uporabo UI v gospodarstvu je odvisno od več dejavnikov. Ker za robote ne veljajo predpisi o delovnem času, se lahko strojni nadzorniki soočajo z daljšim delovnim časom. Države članice morajo vsem delavcem omejiti tedenskega delovnega časa, ki v povprečju ne sme presegati 48 ur, vključno s kakršnim koli plačani letni dopust in dodatno varstvo pravic delavcev, ki opravljajo nočno in nevarno delo. Poleg pomislekov o zmanjšanju delovnega časa zaradi avtomatizacije, je treba upoštevati tudi druge posledice. Zmanjšanje časa dela pomeni tudi povečanje stroškov dela, kar lahko ima negativne posledice za konkurenčnost izvozno usmerjenih podjetij, če se produktivnost ne bo ustrezno povečala.

Direktiva EU o delovnem času od držav članic EU zahteva, da delavcem zagotovijo naslednje pravice:

- omejitev tedenskega delovnega časa na povprečno 48 ur, vključno z nadurami, (člen 6)
- najmanjši dnevni čas počitka 11 zaporednih ur v 24-urnem obdobju, (člen 3)
- odmor za počitek med delovnim časom, če delovni dan presega šest ur, (člen 4)
- dnevni počitek za vsako sedemdnevno obdobje, (člen 5)
- plačan letni dopust v najmanj štirih tednih na leto, (člen 7)
- posebna pravila za nočno delo; ure ne smejo presegati povprečno osem ur v 24-urnem obdobju, (člen 8)

[49] Več na: https://www.senat.fr/dossier-legislatif/pjl15-610.html.
[50] Wisskirschen, G. in drugi: Artificial Intelligence and Robotics and Their Impact on the Workplace, IBA Global Employment Institute, 2017, str. 71.
[51] DIREKTIVA 2003/88/ES EVROPSKEGA PARLAMENTA IN SVETA z dne 4. novembra 2003 o določenih vidikih organizacije delovnega časa, Uradni list Evropske unije, L 299, 18.11.2003, str. 9–19.

- nočni delavci, pri katerih delo vključuje posebne nevarnosti ali težje fizično delo ali duševni napor ne sme delovati več kot osem ur v kateremkoli obdobju 24 ur,
- nočni delavci imajo pravico do brezplačne zdravstvene ocene in pod določene okoliščine, ki jih je treba prenesti na vsakodnevno delo (poglavje 3).

7.4.2.4 Pravica do varnih in zdravih delovnih pogojev

Za zdravje je najprej odgovoren vsak posameznik, država pa je v sodelovanju z različnimi strokami in znanostmi pristojna in odgovorna za ustvarjanje pogojev, v katerih lahko ljudje skrbimo za zdrav življenjski slog.[52] Kot eno izmed temeljnih človekovih vrednot je zdravje pogoj za aktivno vključevanje posameznika v družbeno okolje, brez njega tudi delo ni opravljeno. Številni predstavniki delavcev se strinjajo, da bo zaradi digitalizacije veliko tveganj in nevarnih nalog, ki so jih prej opravljali zaposleni, prenesenih na robote. Zaradi tega pozdravljajo digitalizacijo, a vztrajno stojijo za stališčem, da mora osrednja vloga v delovnem procesu ostati človeku. Robote je treba prilagoditi človekovim potrebam in ne obratno.[53] Direktiva o strojih[54] je določila minimalne standarde, ki jih morajo izpolnjevati vsi strojni izdelki v EU, pri čemer je ključnega pomena pravilo, da se stroji ne smejo uporabljati, dokler varnostni napotki v zvezi z posamezno delovno mesto zaposlenega, ki dela s stroji, niso zagotovljeni.

Uporaba avtonomnih sistemov v podjetjih lahko predstavlja veliko nevarnost, če delavci, ki z njimi opravljajo delo, niso poučeni o njihovi uporabi. Čeprav je v primeru okvare ali napake po navadi takoj sprožen samodejni postopek za ustavitev obratovanja, temu ni mogoče slepo zaupati. Tudi če je postopek prekinjen, ga je včasih težko izklopiti, tako da bi bila vsa tveganja za nesrečo s tem preprečena. Prva zabeležena smrt, ki jo je "povzročil" robot, se je zgodila leta 1981 v Kawasakijevi tovarni na Japonskem, v kateri je delavec vstopil v območje omejenega gibanja, da bi opravil določena vzdrževalna dela na robotu, a ga je ta zaznal kot potencialno nevarnost in ga s svojo hidravlično roko potisnil v bližnji stroj, kar je povzročilo

[52] Lahe, M.: Ohranjanje in krepite v zdravja predšolskih otrok, v: Metodicki obzori 12, 6 (2011) 2, str. 157.
[53] Wisskirschen, G. in drugi: Artificial Intelligence and Robotics and Their Impact on the Workplace, IBA Global Employment Institute, 2017, str. 62.
[54] DIREKTIVA 2006/42/ES EVROPSKEGA PARLAMENTA IN SVETA z dne 17. maja 2006 o strojih in spremembah Direktive 95/16/ES, Uradni list Evropske unije, L 157, 9.6.2006, str. 24–86.

nenadno smrt.[55] V ZDA so zabeležili primere, ko so zaposleni utrpeli hude poškodbe zaradi izklopa sistema, npr. delavec je utrpel hude telesne poškodbe zaradi ponovnega zagona strojev, kljub siceršnji prekinitvi pogona, ali ker je sodelavec v sili zasukal stikalo. Število smrti, ki so jih v zadnjih 30 letih povzročili roboti v ZDA, znaša 33%.[56]

Kljub temu je potreben ločen pregled posameznih sektorjev, saj je stopnja avtomatizacije v proizvodnji, v avtomobilski in kemični industriji ali kmetijstvu dobro napredovala, enako tudi v poklicih v zvezi z informacijsko tehnologijo, mediji, financami in zavarovalništvom, medtem ko proizvodnja tekstila, gostinstvo, gradbeništvo in nega zaostajajo. Razlike se kažejo tudi med državami. V ZDA se ustvarjalci UI osredotočajo predvsem na vesoljsko robotiko, na Japonskem izdelujejo 'ljudi robote', v Nemčiji pa je poudarek na robotih v tovarnah.

Za zagotovitev učinkovite zaščite in varne uporabe tehnologije na delovnem mestu je posledično potrebno izvajati redne preglede in ocene tveganja, v primeru nevarnih pripomočkov, ki jih v določenem podjetju ni mogoče nadzirati, pa izogibanje tem. V primeru nespoštovanja varnostnih predpisov naj bremeni delodajalca visoka kazen. Vse pogosteje pa se ugotavlja, da tveganje za nesrečo na delovnem mestu ne izvira zgolj iz inteligentnih strojev, delovnega okolja, drugih ljudi ali nevarnih snovi, ki se uporabljajo, ampak je glavni vzrok za vse nesreče pri delu človekova malomarnost. Posledično je toliko bolj pomembno izobraževanje o uporabi teh strojev in delovanje v smeri preprečitve posameznih nesreč, kot pa poznejše ugotavljanje 'storilca'.[57]

7.4.2.4 Pravica do ustreznega plačila za delo

Ali in kako naj se nacionalna zakonodaja o minimalnih plačah prilagodi spremembam, ki jih prinaša UI na plačilo za delo, še ni jasno. Trenutno pozna 22 od 27 držav članic institut minimalne plače, to so vse razen Avstrije, Danska, Finske, Cipra, Italije in Švedske. Dejstvo, da je UI zabrisala meje med delovnim časom in zasebnim življenjem, pomeni, da ni zastarel samo tradicionalni model delovnega

[55] Jakšić, J.: Ali je pravo pripravljeno na izzive umetne inteligence?, v: Pravna praksa, 43 (2017), str. 17-19.
[56] Wisskirschen, G. in drugi: Artificial Intelligence and Robotics and Their Impact on the Workplace, IBA Global Employment Institute, 2017, str. 63.
[57] Ibidem, str. 119.

časa, na podlagi katerega je zaposleni prejel določeno plačilo za določeno število ur, ampak v zvezi z njim tudi plačilo za opravljeno delo.

Postavlja se vprašanje, ali bi morala biti v digitalnem delovnem okolju struktura plačil utemeljena na produktivnosti delavca in ne določenemu številu ur, ki jih preživi na delovnem mestu.

Če je odgovor pritrdilen, takšen sistem delavcu omogoča, da izpolni delovnopravne obveznosti kadarkoli in kjerkoli. To sicer od zaposlenega zahteva visoko stopnjo discipline, a ga hkrati ideja o večjem zaslužku motivira, kar ima pozitivne posledice tudi za delodajalca. Obenem takšna ureditev predstavlja določena tveganje, kot je *workacholism,* stres, samomorilnost delavcev, z vidika delodajalca pa tudi pomanjkanja nadzora. Npr. v Nemčiji (podobno kot v Sloveniji, skladno s 6. in 133. členom ZDR-1) velja zakon iz leta 2017, ki delodajalcem nalaga, da zaposlenemu izplačajo enak znesek plače za enako delo na delovnih mestih, ki zahtevajo enako znanje, trud in odgovornost in ki se izvajajo v podobnih delovnih pogojih. Vendar je izraz "enako delo" razmeroma nejasen. Poleg tega veljavno nemško pravo delodajalcem otežuje vzpostavitev poštenih in pravno skladnih delovnih razmer glede uspešnosti zaposlenih. Tudi če je delodajalec sposoben dokazati, da drugačno plačo povzročajo dejavniki, ki niso diskriminatorni, npr izobrazba, izkušnje, poslovne potrebe, dolžina zaposlitve ipd., je neenako plačilo včasih obravnavano kot diskriminatorno. Drug primer zadeva zaposlenega v Franciji, ki ima 35-urni delovni teden, od 9. do 17. ure z enournim odmorom za kosilo, a ne dobi plačila za telefonski klic, ki ga je opravil ob 21. uri zvečer z ameriškim vodjo za trgovino, da bi ga obvestil o trenutnem stanju projekta, čeprav opravlja obveznosti iz delovnega razmerja. Če bi obveljal sistem s prilagodljivim delovnim časom in plačilom, povezanim s uspešnostjo, bi delavcu pripadalo primerno plačilo za telefonski klic, kar daje zaposlenim občutek, da prejemajo plačilo za svojo stalno razpoložljivost in pripravljenost za delo, kar bi jih navadno tudi motiviralo.[58]

Plačila na podlagi delovne uspešnosti se po navadi izplačujejo za opravljeno delo (nagrada za količino) ali kakovost izdelka (nagrada za kakovost), izpolnjevanje rokov (nagrada za izpolnjevanje rokov) ali varčevanje materiala pri delu (nagrada za prihranke). Delovnopravna zakonodaja večine držav pozna tudi dodatke za nadure, nočno delo ter delo ob nedeljah in praznikih ali delo v nevarnih pogojih. Nagrade ali

[58] Ibidem, str. 83- 85.

dodatki se razlikujejo glede na sektor, v katerem delavec opravlja delo. Kadar se na določenem delovnem mestu zahteva intelekutalno delo in ne določen izdelek kot posledica fizičnega dela, so možna plačila proizvajalca v odstotkih od dobička, plačilo odstotka licenčnine, če so pravice prodane tretji osebi, fiksno enkratno plačilo v pavšalnem znesku oz. pavšalno nadomestilo, akontacija in zajamčena najnižja pristojbina ali kombinacija različnih alternativ.

Za oboje, tako fizično kot intelektualno delu, je v sistemu plač v zvezi z uspešnostjo, smiselno vnaprej natančno določi osnovo, povezovalni faktor za prožno plačilo. To je lahko doseganje določenih „mehkih" ciljev (npr. izboljšanje kupca zadovoljstvo) ali doseganje nekaterih oprijemljivejših kazalnikov uspešnosti (npr. doseganje pragov prometa). Nadalje, je potrebno razlikovati med posameznim prihodkom, ki ga doseže en sam zaposleni, prometom, ki ga je dosegel določen oddelek v družbi, prometom, ki ga doseglo podjetje, in prometom ki ga je dosegla družba na sploh. V primerih, ki vključujejo mejne vrednosti prometa, je razmeroma enostavno oceniti, ali je zaposleni dosegel določen cilj, saj rezultat temelji na objektivnih merilih. Če se delovna uspešnost meri na podlagi subjektivnih meril, je dosežek in posledično plačilo odvisno od mnenja delodajalca.

To ne pomeni, da so subjektivna merila neprimerna za oceno uspešnosti na delovnem mestu, a je bistvenega pomena dopolnjevanje subjektivnih meril z objektivnimi in posledično preprečitev izkoriščanja delovne sile oz. kršitev temeljnih ustavnih in delovnopravnih pravic in načel.

Nasprotno, obstajajo situacije, v katerih bi bil ustreznejši trenutno prevladujoč sistem minimalne plače. Ti modeli zagotavljajo stalne osnovne plače z nizkimi dodatki in so značilni za evropske države, kjer prevladujejo potrebe zaposlenih po ustrezni finančni varnosti, medtem ko so modeli v ZDA bolj znani kot sistemi plačil z dodatki za uspešnost in nižjimi osnovnimi plačami. Na prvi pogled ima sistem fiksnih plač več prednosti kot slabosti, a temu ni nujno vedno tako. Ker delavci niso roboti oz. niso programirani opravljati dela v enakem času in z enako kakovostjo, se pogosto zgodi, da je zelo produktiven delavec plačan enako kot delavec, ki je za isto opravilo porabil ogromno časa; in obratno, nekomu, ki v delo vloži ogromno svojega časa pripada enako plačilo kot drugemu na enakem delovnem mestu, ki mu za delo ni preveč mar. Povezovalni dejavnik za minimalno plačo v večini držav je še vedno "čas je zlato (time is money)".

Glede na zapisano je moč predvidevati, da bodo v prihodnosti stranke pogodb o zaposlitvi vse bolj podrejene sistemu delovne uspešnosti in ne sistemu minimalne osnovne plače. Tako bo delavec, ki opravlja delo učinkovito, prejel višjo plačo od manj produktivnega delavca, kar bo delodajalca stalo manj. Delavec, ki ima raje več časa zase, ima lahko koristi od tega, ker podjetje prihrani denar. Teoretično bi v nesebičnem svetu to vodilo k pravičnejši porazdelitvi plače v podjetju med vrhunskimi in manj uspešnimi. Prepričanje, da delavec, ki dela največ ur, naredi največ podjetje, ne bo več obveljalo.[59] Ne glede na sistem plač pa je moč pritrditi, da je obveznost vsakega delodajalca poskrbeti, da bodo delavci za svoje opravljeno delo ustrezno plačani.

7.4.2 Zaključek

Temeljne pravice in načela delovnega prava, kot so načelo enakega plačila za enako delo, svoboda dela, socialnovarstvene pravice, svobodna gospodarska pobuda izhajajo iz ustavnih pravic in so po navadi operacionalizacija načela prepovedi diskriminacije. V luči temeljnih načel je večina delavcev in sindikatov proti uvedbi nestalnega oz. spremenljivega prejemka in prožnega delovnega časa. Trdno stojijo za načelom enakega plačila za enako delo in se borijo za najvišje možne minimalne plače. Prilagodljiv delovni čas in stalna razpoložljivost vodita do večjega stresa in izgorelosti. Mnoge skrbi, da bi digitalizacija med delavci povzročila borbo za nadure in večji pritisk za posameznega zaposlenega, ki včasih ne more doseči ambicioznih ciljev delodajalca.

Zaradi uvedbe vedno več digitalnih inovacij se zdi, da bodo ljudje postali vse bolj nepomembni za delovne procese. To bi lahko kot strah pred brezposelnostjo in vrzel med bogati in revni vodilo v družbene konflikte. UI hkrati odpira nove priložnosti za posameznike in podjetja. Ljudje smo prilagodljivi in ustvarila bodo nova delovna mesta. Uporaba pametnih sistemov na delovnem mestu bo le pomagala zmanjšati čas, potreben za izdelek oz. opravljanje storitev in s tem povezanih stroškov. Prihranjeni čas, predvsem za nevarno delo, bo lahko posameznik izkoristil za drugo delo ali za prosti čas. Poleg tega bo tehnični razvoj omogočil vključitev starejših delavcev in invalidov v delovni proces, medtem ko bodo stroji opravljali nekatera opravila namesto njih. S tem ima UI za posledico rast

[59] Povzeto po: ibidem, str. 83-92.

blaginje. Tudi če bo nekaj teh novih delovnih mest pomenilo žrtvovanje davčnih prihodkov in socialne varnosti, se bo vsaj skušala preprečiti brezposelnost.

Jasno je, da je digitalizacija globalni pojav in da bo potrebna prilagoditev tako modrih kot belih ovratnikov. Z vidika pravic, ki izhajajo iz delovnega prava je zaželjeno, da bi v prihodnosti regulacija potekala v smeri enotne ureditve na mednarodni ravni po standardih, ki bodo prilagojeni tehnološkemu razvoju in upoštevali povečano potrebo po prilagodljivosti. Prilagajanje ali uvedba minimalne plače se naj vrši sorazmerno in odvisno od obstoječega varstva delavcev. Nedvomno pa je, da bi morale države članice izbrati najustreznejši instrument za reševanje naraščajoče nevarnosti neenakosti v dobi UI in zagotoviti minimalne standarde varstva delavcev, ki bodo prinesli daljnosežne koristi in ne zgolj trenutnih.
[60]

7.5 Sodstvo in umetna inteligenca

Mnogokrat se sprašujemo, ali bodo roboti res nekega dne nadomestili posameznike v opravljanju sodniške funkcije in ali je pri tem zares moč zagotoviti **neodvisnost in nepristranskost sodstva,** zagotovljene v 23., 125. členu Ustave RS, 3. členu Zakona o sodiščih, 6. členu EKČP, 10. členu Deklaracije ZN o človekovih pravicah in drugih glede na to, da algoritem sistemsko prilagodi in sestavi čustven človek z izkušnjami in prepričanji, ki ga robot kasneje le uporabi, upoštevajoč znane podatke iz podatkovnih baz. Temeljna pravica posameznika, ki se znajde v pravnem postopku je, da o njegovih pravicah in obveznostih odloča pristojni organ brez navodil, pritiska in prejudiciranja s strani države, zasebnih institucij, medijev, družbenih omrežij, ter v današnjem dobi digitalizacije, brez vpliva algoritmov.

Nasproti instituciji sodstva, človeškega ali digitalnega, vselej stoji posameznik, ki skozi sodni sistem uveljavlja svoje temeljne pravice, kot so pravica do poštenega sojenja, pravica do pravnega sredstva, pravica do sojenja v razumnem roku ipd. V nadaljevanju bom v povezavi s prejšnjim poglavjem o delu in UI najprej opisala poklice, za katere je v sodnem in pravosodnem sistemu moč pričakovati spremembe v strukturi dela, nato pa predstavila posameznikove temeljne pravice, ki tvorijo temelj ustavnega reda in pravne države v okviru sodnega varstva pravic.

[60] Ibidem, str. 117-119.

7.5.1 Poklici

Splošna sprejemljivost in večja dostopnost digitalnih storitev lahko prinese številne koristi na področju prava in v družbi na sploh. UI že danes omogoča analizo in pregled obsežnih podatkovnih baz in prepoznava vzorce, ki jih človek kot opazovalec nezavedno mnogokrat spregleda. Programske aplikacije za pravno analitiko lahko obdelujejo milijone sodnih dokumentov in ponudijo odvetnikom vpogled v potencialne strategije pravdanja ter celo simulirajo, kako se določen sodnik odzove na različne možnosti in argumente. UI lahko vsem izboljša tudi dostop do pravnih vsebin, ne le pravnikom, na hitrejši in cenejši način ter s tem premaga pretekle kritike nepreglednega in nezadostnega zagotavljanja informacij. V luči pravičnega in enakopravnega dostopa do spletnih vsebin, bi bilo smiselno sprejeti programe usposabljanja in ponuditi tečaje, ki bi pravnikom omogočili boljše razumevanje spletnih domen in programov, npr. *blockchain*, pametnih pogodb, podatkovnih baz, orodij za spletno reševanje sporov *(Online Dispute Resolution, ODR*) ipd., ter spletne novosti pridoma vključiti v delovni proces tako, da bi prepoznali potrebe strank in našli najboljšo rešitev zanje.[61]

Pravniki bi lahko v tem procesu sodelovali z drugimi poklici in zainteresiranimi strankami ter izboljšali zasnovo orodij za strojno učenje na področjih njihovega dela. K temu bi pripomogla ustanovitev pravnih raziskovalnih laboratorijev UI in informacijske tehnologije, kar bi lahko privedlo do oblikovanja novih specializacij za pravnike ali celo pojav novih poklicev. Glavne težave, ki se pri tem pojavijo so, da narašča količina in raznolikost podatkov, spisi sodišč postajajo daljši, večina teh podatkov je razpršenih, če pa že so zbrani, so oblikovani v različnih digitalnih formatih, ki jih vsaka digitalna domena ni zmožna prebrati. Prefinjenejši algoritmi, ki to zmorejo, so (vsaj v tem trenutku) tako dragi, da so zunaj finančnega dosega večine odvetniških družb, kar bi lahko ustvarilo **neenakost orožij**, npr. v kazenskih postopkih med državnimi tožilci z boljšimi kapacitetami pri uporabi napredne tehnologije in odvetniki, ki so pri tem omejeni. To postavlja obdolženca v veliko prikrajšanje. [62]

7.5.2 Pravni postopek

[61] Buocz, T. J.: Artificial Intelligence in Court: Legitimacy Problems of AI Assistance in the Judiciary, v: Retskraft- Copenhagen Journal of Legal Studies, 2 (2018) 1, str. 41.
[62] Council of Bars & Law Societies of Europe: CCBE CONSIDERATIONS ON THE LEGAL ASPECTS OF ARTIFICIAL INTELLIGENCE, Bruselj, 2020, str. 33, 34.

UI in njeni dosežki v zadnjih letih vidno posegajo tudi na področje sojenja in spreminjajo način delovanja sodišč ter sodnega in pravosodnega sistema na sploh. Digitalna tehnologija se uporablja v upravnih postopkih, obračunu davka in v delovnih sporih, pogumnejši korak v smeri digitalizacije pa predstavljajo spletna sodišča, zasnovana za objavo in dostop do sodnih odločb v sporih majhne vrednosti.[63] **CNN**[64] je poročal o odločitvi britanskega ministrstva za pravosodje, ki pozdravlja idejo o prenosu obravnav v družinskih in zakonskih sporih na spletu, pri čemer bi naj zagotovili, da nekateri podatki ostanejo javnosti nedostopni**.** Drugi primer je **Algoritem *CaseCruncher Alpha,*[65]** *ki* se je pomeril v tekmovanju s sto pravniki najbolj slovečih londonskih odvetniških pisarn. Ti so imeli na voljo osnovne podatke o več sto zahtevkih v zvezi z zavajanjem pri prodaji zavarovanja plačil v primeru kreditojemalčeve brezposelnosti, o katerih so pristojni že odločili, kar pa udeležencem ni bilo znano. Udeleženi pravniki so morali opraviti oceno verjetnosti uspeha (da/ne), pri tem pa so bile njihove ocene za več kot četrtino manj natančne (62,30 odstotka) kot ocene algoritma (86,60 odstotka).[66] Uporabnost UI se kaže tudi pri vodenju postopkov, ki spremljajo sodne obravnave. **Policija v Durhamu** (Velika Britanija) je leta 2018 začela, po vzoru represivnih organov iz ZDA (in odmevne sodbe **Loomis**[67]) poskusno uporabljati sisteme UI pri podaji ocene, ali naj oseba ostane v priporu ali na sojenje čaka na prostosti. Ustanovili so program **Hart (*Harm Assessment Risk Tool),*** ki klasificira posameznike glede na nizko, srednjo in visoko stopnjo verjetnosti ponovitve kaznivega dejanja. Policija se je za testiranje odločila v primerih, ko se ne more zanesti le na človeški dejavnik. Testi, ki so jih izvajali leta 2013, pri čemer so dve leti spremljali osumljenčevo vedenje, so pokazali, da je Hart pravilno odločitev pri majhnem tveganju sprejel v 98, pri velikem tveganju pa v 88 odstotkih.[68]

Vendar pa mnogi od teh sistemov, čeprav so vpeti v sistem UI, ne predstavljajo digitalizacije sodišč v polnem pomenu besede. Temeljijo namreč na podlagi logičnih

---

[63] Zuckerman, A.: Artificial Intelligence – Implications for the Legal Profession, Adversarial Process and the Rule of Law, UK Constitutional Law Association, 2020.
[64] Lights, camera, legal action! Courts to livestream divorce proceedings
< https://edition.cnn.com/2020/03/13/uk/livestream-divorces-intl-scli-gbr/index.html> (17.5.2020)
[65] Sourdin, T.: JUDGE V ROBOT? ARTIFICIAL INTELLIGENCE AND JUDICIAL DECISION-MAKING, v: UNSW Law Journal. 41 (2018) 4, str. 1116.
[66] Podpečan, M.: Umetna inteligenca in sojenje, v: Odvetnik, (2018) 88, str. 26.
[67] Loomis v. Wisconsin, 881 N.W.2d 749 (2016)
[68] Durham Police AI to help with custody decisions < https://www.bbc.co.uk/news/technology-39857645> (17.5.2020).

pravil, *če je x, potem y*, katerim sledijo rezultati *da ali ne*, in ne na sistemih UI. Do sedaj je imel razvoj UI torej omejen vpliv na sojenje. Ker napovedi kažejo na bistvene spremembe v obstoju in strukturi pravniških poklicev, željo po obvladovanju digitalizacije v pravnih postopkih in odpravi neenakosti med udeleženci, bo potrebno zagotoviti, da razvoj UI in sojenja poteka z roko v roki, v korist družbi in ob upoštevanju dosedanjih dognanj pravne teorije in temeljnih človekovih pravic.

Omenjena sodna odločba *Loomis* zahteva dodatno obrazložitev. Potem ko se je sodišče deloma oprlo na rezultate algoritma *Compas*, ki ga je zasnovalo zasebno podjetje Nortpointe Inc., je bil obtoženi Eric Loomis, s kriminalno kartoteko, obsojen na šestletno zaporno kazen, pri čemer v postopku ni imel pravice pregledati njegovega delovanja. Omenjeni algoritem je obtoženega ocenil za potencialnega povratnika, sodniki pa so oceno, da je Loomis *»nevaren, da pomeni grožnjo in da je nagnjen k ponavljanju kaznivih dejanj«,* upoštevali. Loomisu bi bila po presoji sodišč izrečena enaka sankcija tudi na podlagi drugih obstoječih okoliščin, zato so bila njegova pravna sredstva zavrnjena.[69] Kasneje se je izkazalo, da algoritem ki je bil uporabljen, tveganje za povratništvo v večji meri pripisuje obtožencem s temnejšo barvo kože, tisti s svetlejšo kožo pa so v primerjavi z nekaznovanimi temnopoltimi storilci predstavljali manjše tveganje za ponovitev kaznivega ravnanja.[70]

7.5.3 Temeljne pravice

7.5.3.1 Pravica do poštenega sodnega varstva

»Pravico vsakogar do poštenega sodnega varstva njegovih pravic, dolžnosti ali pravnih interesov v širšem pomenu varuje vrsta ustavnih določb: 4. odst.15. člena (pravica do sodnega varstva), 20. člen (odreditev in trajanje pripora), 21. člen (varstvo osebnosti in dostojanstva v sodnih postopkih), 22. člen (enako varstvo pravic), 23. člen (pravica do sodnega varstva), 24. člen (javnost sojenja), 25. člen (pravno sredstvo), 27. člen (domneva nedolžnosti), 28. člen (načelo zakonitosti v kazenskem pravu), 29. člen (pravna jamstva v kazenskem postopku), 30. člen (pravica do rehabilitacije in odškodnine), 31. člen (prepoved ponovnega sojenja), 3. odst. 120. člena (sodno varstvo proti odločitvam in dejanjem upravnih organov), 156. člen (prekinitev postopka pred sodiščem zaradi postopka za oceno ustavnosti), 157. člen (upravni spor) in 158. člen (pravnomočnost). Sedes

[69] Council of Bars & Law Societies of Europe: CCBE CONSIDERATIONS ON THE LEGAL ASPECTS OF ARTIFICIAL INTELLIGENCE. Bruselj, 2020, str. 18-19.

[70] Ti. strukturna nepristranskost, ki lahko izhaja iz vzorčnih podatkov, uporabljenih za treniranje umetne inteligence, ali pa iz samega algoritma.

materiae se nahaja v členih 22 in 23, ki skupaj določata bistvo pravice do sodišča in do poštenega sojenja (fair trial) in sta po vsebini primerljiva s ključnim prvim stavkom 1. odst. 6. člena EKČP[71].«[72]

Vloga, ki jo ima pravica do poštenega sojenja v demokratičnih družbah, ne sme biti zanemarjena pri presoji dopustnosti uporabe UI v sodstvu. To je še posebej pomembno v krizi vladavine prava v mnogih evropskih državah. Temeljna zahteva pravne države, pravna gotovost, se ne nanaša zgolj na materialno pravo, ampak jo je potrebno upoštevati tudi v samem postopku, v katerem se pravice materialnega prava uveljavljajo. Namen „procesne pravne varnosti" je zagotoviti pravično sojenje strankam v postopku, torej zagotavljanje možnosti, da vzpostavijo določen pravni položaj in da stranka, ki se počuti ogroženo prepreči kršitev pravic.

V zadevi **Kraska v. Švica**[73] je ESČP ugotovilo, da je namen člena 6 EKČP *»zadolžiti tribunal, da izvede pravilno analizo izjav, argumentov in dokazov, ki jih predložijo stranke, ne da bi se pri tem opiralo na lastno oceno, ali so slednje za njegovo odločitev relevantne.«* Podobno, v zadevi **Golder v. Združeno kraljestvo**[74] ugotavlja, da si je zelo težko zamisliti vladavino prava brez možnosti dostopa do sodišč. Pri tem se je sklicevalo na Preambulo EKČP, ki opozarja, da predstavlja vladavina prava eno izmed prvin skupnega duhovnega izročila članic Sveta Evrope in na statut Sveta Evrope, ki v 3. členu zavezuje *»vsako članico Sveta Evrope, da sprejema načelo vladavine prava […]«.* Tri leta kasneje je ESČP v zadevi **Klass**[75] razložilo razmerje med načelom vladavine prava in poštenim sojenjem: *»Vladavina prava pomeni, inter alia, da mora biti poseg izvršnih oblasti v posameznikove pravice podrejen učinkovitemu nadzoru, ki naj ga normalno zagotavlja sodstvo vsaj kot zadnje poroštvo, upoštevaje, da sodna kontrola nudi najboljša jamstva neodvisnosti, nepristranskosti in dobrega postopka.«*

Velik pomen daje pravici do poštenega sojenja tudi Evropska etična listina o uporabi UI v pravosodnih sistemih in njihovem okolju[76], ki določa: "Kadar se orodja UI uporabljajo za reševanje spora ali kot orodje za pomoč pri odločanju sodišča, je treba

[71] »Vsakdo ima pravico, da o njegovih civilnih pravicah in obveznostih ali o kakršnihkoli kazenskih obtožbah proti njemu pravično in javno ter v razumnem roku odloča neodvisno in nepristransko, z zakonom ustanovljeno sodišče.«
[72] Komentar Ustave RS e-Kurs: Pravica do poštenega sodnega varstva > https://e-kurs.si/komentar/pravica-do-postenega-sodnega-varstva/< (25.6.2020)
[73] Kraska v. Switzerland, 19. 4. 1993, A 254-B, s. 49.
[74] Golder v. The United Kingdom, 21. 2. 1975, A 18, §§ 34–36
[75] Klass in drugi v. Nemčija, 6. 9. 1978, A 28, s. 17.
[76] EUROPEAN COMMISSION FOR THE EFFICIENCY OF JUSTICE (CEPEJ): European Ethical Charter on the Use of Artificial Intelligence in Judicial Systems and their environment, Strasbourg, 3-4 December 2018.

zagotoviti da ta ne spodkopavajo pravice do poštenega sojenja."[77] To pomeni, da naj bodo jamstva, ki izhajajo iz Ustave, EKČP, Listine EU o temeljnih pravicah in drugih zagotovljena tudi v dobi digitalizacije, v kateri se srečujemo s socialnimi in ekonomskimi spremembami, ki se kažejo tudi v poteku pravnega postopka.

7.5.3.2 Dostop do sodišča

Ustava RS v 22. členu zagotavlja enako varstvo pravic in s tem operacionalizira prepoved diskriminacije iz 14. člena ter dopolnjuje temeljno garancijo demokratične države in načela delitve oblasti, pravico do pravnega sredstva iz 25. člena. Enako varstvo pravic je opredeljeno tudi v 7. členu Deklaracije o človekovih pravicah, 14. členu MPDPP in 20. členu Listine EU o temeljnih pravicah. V odprtih demokracijah mora biti vsakomur zagotovljeno enako varstvo njegovih pravic v postopku pred sodiščem in pred drugimi državnimi organi, organi lokalnih skupnosti in nosilci javnih pooblastil, ki odločajo o njegovih pravicah, dolžnostih ali pravnih interesih.

V dobi digitalizacije se v povezavi z dostopom do sodišča postavljata predvsem dve vprašanji. Prvo se nanaša na vzpostavitev in organizacijo sodišč, drugo pa na pravno urejanje dostopa do njih. Obema je skupno, da o pravicah in dolžnostih ter o obtožbah proti posamezniku brez nepotrebnega odlašanja odloča neodvisno, nepristransko in z zakonom ustanovljeno sodišče (23. člen Ustave RS in 3. člen Zakona o sodiščih). Pomemben vidik tega je tudi **načelo neposrednosti**, uveljavljeno tako v civilnem kot kazenskem postopku. Čeprav je danes še nepredstavljivo, da na sodišču o pravnih vprašanjih odloča robot, še manj pa so predstavljivi primeri, ko posameznik 'od doma' sodeluje v spletni obravnavi in prejme odločitev zgolj na podlagi računalniku posredovanih podatkov, menim, da morajo že trenutni zakonodajalci ujeti korak z hitro razvijajočim spletom in zagotoviti enak dostop do pravnega varstva tako, da z zakonom predpišejo, v katerih primerih in v kakšnem obsegu se UI uporablja v pravnem postopku. Le z jasnimi določbami in vnaprej predvidenimi primeri bo lahko država zagotovila enak dostop do sodišča vsem, ki potrebujejo sodno varstvo pravic v takšnih primerih in v takšnem obsegu. Vsakomur mora biti znana prisotnost oz. uporaba UI v postopku, čemur mora imeti vsak pravico tudi ugovarjati.

---

[77] "*When AI tools are used to resolve a dispute or as a tool to assist in judicial decision-making or to give guidance to the public, it is essential to ensure that they do not undermine the guarantees of the right of access to the judge and the right to a fair trial (equality of arms and respect for the adversarial process)*."

7.5.3.3 Sojenje v razumnem roku

Pravica do sojenja brez nepotrebnega odlašanja je urejena v 23. členu Ustave RS, 2. členu Zakona o varstvu pravice do sojenja brez nepotrebnega odlašanja, 6. členu EKČP in 47. členu Listine EU o temeljnih pravicah ter izhaja iz krovnega pojma pravice do poštenega sojenja. Računalniški sistem, ki je odporen na monotonost, izčrpanost in druge biološke in psihološke 'omejitve' človeka nedvomno natančneje in neprimerljivo hitreje opravi analizo sodne prakse in doktrine kot katerikoli človeški sodnik. Skladno s tem lahko ddigitlizacija pozitivno vpliva na hitrost sojenja, odpravi sodne zaostanke ter ponovno vzpostavi zaupanje v pravno državo. O tem pričajo tudi podatki, da se je število kršitev pravice do sojenja v razumnem roku močno zmanjšalo, saj je bila v letih 2012 in 2013 ta drugi od 24 vzrokov kršitve EKČP, v naslednjih letih (2014-2016) pa šele na 5. mestu.[78] Kljub dobrim stranem digitalizacije, ki omogoča hitro odločanje o pravnih vprašanjih, pa je pomembno ohraniti zavest o funkciji prava in sodišč v državi. ESČP je v tej luči poudarilo, da EKČP sicer zagotavlja pravico do sojenja brez nepotrebnega odlašanja, a jo je treba razlagati tako, da se ne ogrozi učinkovitost prava in verodostojnost sodnih odločb.[79]

7.5.3.4 Domneva nedolžnosti

V dobi digitalizacije, za katero je značilno hitro in neobvladljivo širjenje podatkov je pomemben vidik varstva človekovih pravic v preprečevanju *fake news* in drugih lažnih prirejanj realnosti ter ohranjanje zaupanja v pravno državo. Pri tem je potrebno upoštevati, da je posameznik v svojem zasebnem in družinskem življenju svoboden in uživa polno varstvo pravic na eni strani oz. da se prepreči stigmatizacija in socialna osamljenost kot posledici hitrega širjenja lažnih informacij na drugi. Kdor je obdolžen kaznivega ravnanja, velja za nedolžnega, dokler njegova krivda ni ugotovljena s pravnomočno sodbo. **Domnevo o nedolžnosti** posameznika kot temeljno človekovo pravico v pravnem postopku zagotavlja Ustava RS v 27. členu, 11. člen Deklaracije o človekovih pravicah, 6. člen EKČP in 48. člen Listine EU o temeljnih pravicah.

---

[78] Calvez, F. in Regis, N.: Length of court proceedings in the member states of the Council of Europe based on the case law of the European Court of Human Rights. Council of Europe Publishing, 3rd ed. (2018), str. 5.
[79] H. v. France, št. 10073/82, ECLI:CE:ECHR:1989:1024JUD001007382, §58; Vernillo v. France, št. 11889/85, ECLI:CE:ECHR:1991:0220JUD001188985, §38.

7.5.3.5 Obrazložitev odločitve

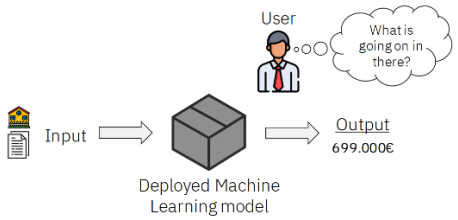
Pravica do poštenega sojenja vključuje tudi možnost spoznanja razlogov odločitve sodišča. Pravičnost ukrepov sodišča se odraža v utemeljitvi sodnih odločb, ki jih pripravijo sodniki, v katerih opisujejo dejanske in pravne okoliščine primera, način razlage in navajajo argumente, ki sta jih stranki predstavili med sojenjem. Pravica do utemeljene odločitve torej posameznika ščiti pred samovoljnostjo.[80]

Obrazložitev sodne odločbe zagotavlja preglednost sodstva in posledično poveča zaupanje javnosti v sodno vejo oblasti in pravno državo. Po drugi strani pa utemeljitev služi realizaciji pravnega interesa stranke v postopku. Pomanjkanje utemeljitve sodne odločbe bi povzročilo, da bi bila pravica do pritožbe zoper končno odločitev iluzorna. Poleg tega obrazložitev strankam dokazuje, da so bile zaslišane in upoštevane njihove trditve in dokazi zanje. Torej, pravica do obrazložene odločitve pomeni jamstvo, da bodo med postopkom pravice stranke spoštovane in omogoča javni nadzor nad pravosodjem.[81]

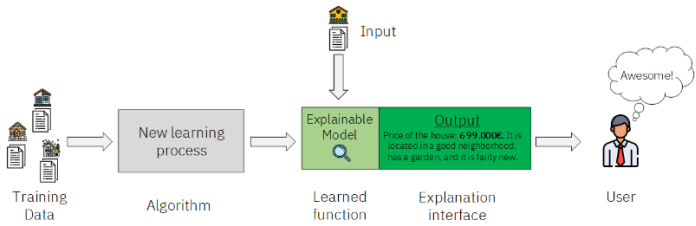
Če sistem UI ne bo mogel razložiti svojega delovanja, bo lahko predstavljal potencialno nevarnost za pravico do poštenega sojenja. Nekateri sodobni sistemi UI, zlasti tisti, ki temeljijo na strojnem učenju, niso dovolj transparentni ali pa je njihovo delovanje preveč zapleteno, da bi lahko podalo razlage o tem, zakaj je bila sprejeta določena odločitev.[82] Nekateri vidijo rešitev v konceptu 'razložljive UI' (*'explainable AI', 'XAI'*), ki se nanaša na metode in tehnike uporabe tehnologije UI, tako da lahko rezultate rešitve razumejo človeški strokovnjaki v nasprotju s konceptom "črne skrinjice" (black box) pri strojnem učenju, kjer niti njeni oblikovalci ne znajo razložiti, zakaj je sistem sprejel konkretno odločitev.[83]

---

[80] Ruiz Torija v. Spain, št. 18390/91, ECLI:CE:ECHR:1994:1209JUD001839091, §§29–30.
[81] Suominen v. Finland, št. 37801/97, ECLI:CE:ECHR:2003:0701JUD003780197, §37.
[82] Sileno, G., Boer, A. and van Engers, T.: The Role of Normware in Trustworthy and Explainable AI, CEUR Workshop Proceedings, 2381 (2019), str. 9-16.
[83] Computer says no: why making Ais fair, accountable and transparent is crucial <https://www.theguardian.com/science/2017/nov/05/computer-says-no-why-making-ais-fair-accountable-and-transparent-is-crucial > (25.5.2020).



Slika 8: Modeli strojnega učenja kot črna škatla.
Vir: lasten, ikone s Flaticon, 2023



Slika 9: Modeli strojnega učenja kot črna škatla.
Vir: lasten, ikone s Flaticon, 2023

EU prav tako poudarja, da je potrebno za povečanje transparentnosti in odpravljanje tveganja za pristranskost ali napake sisteme UI razvijati tako, da ljudje lahko razumejo njihova dejanja (podlago zanje).[84] Tudi v pravico do varstva podatkov (GDPR) je uvedla pravico do razlage kot poskus spoprijemanja s potencialnimi težavami, ki izhajajo iz naraščajočega pomena algoritmov.[85]

Obrazložitev odločitve je pogoj za izvrševanje pravice do pritožbe.[86]

[84] Sporočilo Komisije Evropskemu parlamentu, Evropskemu svetu, Svetu, Evropskemu ekonomsko-socialnemu odboru in Odboru regij, Umetna inteligenca za Evropo, COM (2018) 237 final.
[85] Več o konceptu XAI: Adadi, A. and Berrada, M.: Peeking Inside the Black-Box: A Survey on Explainable Artificial Intelligence (XAI), IEEE Access, 6 (2017), str. 52145.
[86] Hadjianastassiou v. Greece, št. 12945/87, ECLI:CE:ECHR:1992:1216JUD001294587, § 33.

7.5.3.6 Pritožba

Že v zadevi Golder je ESČP ugotovilo, da je treba šteti načelo, da ima vsakdo pravico pritožiti se v civilni zadevi na sodišče, tudi za enega od splošno priznanih temeljnih pravnih načel; isto velja za princip mednarodnega prava, ki prepoveduje, da bi se komurkoli odreklo pravico do sojenja.

Pravica do pritožbe iz 25. člena Ustave RS je temeljna pravica posameznika, ki izhajajoč iz načela zakonitosti (2. člen Ustave RS) in načela enakega varstva pravic (22. člen Ustave) karakterizira pravno državo. Vsakomur je zagotovljena pravica do pritožbe ali drugega pravnega sredstva proti odločbam sodišč in drugih državnih organov, organov lokalnih skupnosti in nosilcev javnih pooblastil, s katerimi ti odločajo o njegovih pravicah, dolžnostih ali pravnih interesih. V zvezi s pravico do pravnega sredstva je Ustavno sodišče RS v odločbi U-I-309/94 z dne 16. 2. 1996 obrazložilo, da ta ustavna določba zagotavlja spoštovanje načela inštančnosti pri odločanju sodišč, prav tako pa tudi pri odločanju drugih državnih organov, kadar ti odločajo o pravicah, obveznostih ali pravnih interesih.[87]

Skladno s členom 22 GDPR[88] ima posameznik, na katerega se odločanje nanaša, že danes pravico nasprotovati odločitvi, ki temelji zgolj na avtomatizirani obdelavi podatkov. V primeru, da bi se UI uporabljala pri odločanju v pravnem postopku na prvi stopnji, je smiselno upoštevati UI tudi v pritožbenem postopku. Nekateri menijo, da bi vložitev pritožbe samodejno razveljavila odločbo in postopek bi se nadaljeval tako, da bi človeški sodnik ponovno odločal o zadevi. Predvideva se tudi uzakonitev novega pritožbenega razloga: napake v sistemu/ tehnične napake/ napake algoritma in podobno. Toda v tem primeru bi moralo sodišče pritožniku predložiti tudi t.i. 'drevo odločitve', po katerem je sistem UI postopal, tako da se lahko ta seznani s postopkom sprejemanja odločitve in vloži pritožbo. Sistemi UI, ki jih premoremo danes, niso dovolj pregledni, da bi omogočali vpogled v postopek odločanja, mnoge vsebine, predvsem zaradi varstva osebnih podatkov, pa niso dostopne. Poleg tega tudi morebitni pritožniki nimajo dovolj znanja o branju algoritmov in razumevanju šifriranega odločanja.

---

[87] Višje sodišče v Mariboru, sodba IV Kp 31496/2012 z dne 01.12.2016.

[88] Uredba (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES (Splošna uredba o varstvu podatkov) (Besedilo velja za EGP), Uradni list Evropske unije, L 119, 4.5.2016, str. 1–88.

Poseben problem v okviru pritožbenega postopka je vprašanje devolutivnosti. Kako naj v primeru, ko robot odloči o določeni zadevi, njegovo odločanje razloži človeški sodnik, kot je predlagano zgoraj? Vprašanje se povezuje tudi s prvo temo, Izobraževanje in UI, saj bi se šolski sistem oz. študijski program prava moral prilagoditi in uvesti dodatne predmete, ki bi pripravili na takšno obrazlaganje. Ali bi bilo bolje, da je drugostopenjsko sodišče prav tako sestavljeno iz robotov? Ampak, kakšen algoritem naj vsebuje ta, drugostopenjski, sistem in zakaj ga ni, v skladu s pravico do sojenja brez nepotrebnega odlašanja, vseboval že prvostopenjski?

Vsebina načela inštančnosti je prav v tem, da lahko organ druge stopnje presoja odločitev prvostopnega organa z vidika vseh vprašanj, ki so pomembna za odločitev o pravici oziroma obveznosti. Smisel pravice do pritožbe je v tem, da se pritožniku zagotovi, da pritožbeno sodišče vsebinsko presodi utemeljenost pritožbenih navedb (odločba Ustavnega sodišča RS Up-258/03, Up-I-74/05 z dne 22. 9. 2005). Prav tako je smisel 25. člena Ustave, da lahko posameznik z vložitvijo pravnega sredstva učinkovito brani in varuje svoje pravne interese, kar pomeni, da mora pritožbeno sodišče pritožbo, če je dopustna, vsebinsko obravnavati in se do tistih pritožbenih navedb, ki so za odločitev bistvenega pomena, v obrazložitvi svoje odločbe tudi opredeliti (odločba Ustavnega sodišča RS Up-353/02 z dne 20. 5. 2004).[89]

Tudi 28. člen Deklaracije o človekovih pravicah, 47. člen Listine EU o temeljnih pravicah, 13. člen EKČP in 3. člen Zakona o varstvu pravice do sojenja brez nepotrebnega odlašanja določajo, da ima vsakdo, kateremu pravice so bile kršene, pravico do pravnega sredstva pred nacionalnim organom. Razpoložljivo pravno sredstvo bi moralo biti učinkovito tudi v praksi. Pri tem pa velja upoštevati tudi prakso, ki nas čaka v prihodnosti, povezano s prisotnostjo sistemov UI na vsaj nekaterih, če ne vseh korakih pravnega postopka.

Kot zaključek naj povzamem misel: *»Umetna inteligenca še dolgo ne bo mogla nadomestiti sodnika, ampak bo lahko samo orodje, ki je v pomoč pri odločanju. Stanje tehnike ne omogoča, da bi ena naprava osvojila nabor znanj in izkušenj, ki krasijo sodnika. Sodnik mora obvladati socialne veščine, psihologijo, raziskovanje, jezik, logiko, s pomočjo izvedenca mora razumeti stroko, kot tudi znati znotraj pravnega sistema kreativno reševati probleme, medtem ko lahko umetna inteligenca danes ponudi asistenco le v zvezi s posamezno od navedenih veščin«.*[90]

[89] Višje sodišče v Mariboru, sodba IV Kp 31496/2012 z dne 01.12.2016.
[90] Podpečan, M.:Umetna inteligenca in sojenje, v: Odvetnik, (2018) 88, str. 26.

7.6 Zaključek

Ne glede na to, kako napredne so digitalne tehnologije je moč ugotoviti, da so le orodje človeku. Vseh naših težav ne morejo rešiti, omogočajo pa stvari, ki so bile še pred eno generacijo nezamisljive. Dobro poznavanje sistemov UI in njihova uporaba na delovnem mestu ob hkratnem spoštovanju človekovih pravic in ravnoteženju posameznih vrednot in dobrin, omogoča večjo svobodo in preprečuje socialno izključenost posameznika v digitalnem svetu ter povečuje blaginjo družbe. Sistemi UI morajo zato biti osredotočeni na človeka in v službi človeštva in skupnega dobra.[91]

Da bi bila ta digitalna preobrazba v celoti uspešna, je potrebno ustvariti pravne okvire za zagotavljanje zaupanja vredne tehnologije ter podjetjem vliti zaupanje, omogočiti kompetence in dati sredstva za digitalizacijo. Usklajevanje prizadevanj med EU, državami članicami, regijami, civilno družbo in zasebnim sektorjem je ključnega pomena za doseganje tega in krepitev evropske digitalne vodilne vloge. Še pomembneje pa je, da to lahko stori ob hkratnem vključevanju in spoštovanju vsakogar. S tem lahko digitalna družba, ki temelji na evropskih vrednotah in evropskih pravilih resnično navdihne preostali svet.[92]

Seznam uporabnih povezav

Institut Jožef Štefan, Odsek za umetno inteligenco (https://www.ijs.si/ijsw/E3)
Slovensko društvo za umetno inteligenco (http://slais.ijs.si/)
CAHAI- Ad hoc Committee on Artificial Intelligence (https://www.coe.int/en/web/artificial-intelligence/cahai)
EU, Shaping Europe's Digital Future (https://ec.europa.eu/digital-single-market/en/artificial-intelligence)
OECD AI Policy Observatory(https://oecd.ai/)
International Research Centre on AI under the auspices of UNESCO (https://ircai.org/)
Human-centered AI (https://www.humane-ai.eu/)
EU AI Excellence Centres (https://ai-excellence.b2match.io/)
European Trade Union Institute, Digitalisation (https://www.etui.org/outils/keywords/digitalisation)
ILO, Future of Work (https://www.ilo.org/global/topics/future-of-work/lang--en/index.htm)
WIPO (https://www.wipo.int/portal/en/)

[91] Strokovna skupina na visoki ravni za umetno inteligenco: Etične smernice za zaupanja vredno umetno inteligenco, 2019, str. 5.
[92] Sporočilo Komisije Evropskemu parlamentu, Svetu, Evropskemu ekonomsko-socialnemu odboru in Odboru regij, Oblikovanje digitalne prihodnosti Evrope, COM(2020) 67 final, str. 13.

Seznam literature in virov

Monografije

Andersen, L. in drugi: HUMAN RIGHTS IN THE AGE OF ARTIFICIAL INTELLIGENCE, Access Now, November 2018.

Calvez, F. in Regis, N.: Length of court proceedings in the member states of the Council of Europe based on the case law of the European Court of Human Rights. Council of Europe Publishing, 3rd ed. 2018.

Council of Bars & Law Societies of Europe: CCBE CONSIDERATIONS ON THE LEGAL ASPECTS OF ARTIFICIAL INTELLIGENCE, Bruselj, 2020.

EUROPEAN COMMISSION FOR THE EFFICIENCY OF JUSTICE (CEPEJ): European Ethical Charter on the Use of Artificial Intelligence in Judicial Systems and their environment, Strasbourg, 3-4 December 2018.

European Commission: Inspirational practises for tomorrow's inclusive digital world: Technical Dossier No. 10, May 2019.

Evropska komisija, Evropska unija in enotni digitalni trg, 2017.

Evropska Unija: Živeti bolje v EU: Kaj pomeni enotni trg za vas. Luxembourg: Urad za uradne publikacije Evropskih skupnosti, 2006.

Ojanperä, S., O'Clery, N. in Graham, M.: Data science, artificial intelligence and the futures of work, The Alan Turing Institute, 2018.

Servoz, M.: AI, The future of work? Work of the future! On how artificial intelligence, robotics and automation are transforming jobs and the economy in Europe, Evropska komisija, 2019.

Skok, T.: IZČRPANJE PRAVIC INTELEKTUALNE LASTNINE V DIGITALNI DOBI (magistrsko delo), Ljubljana: Pravna fakulteta Univerze v Ljubljani, 2019.

Strokovna skupina na visoki ravni za umetno inteligenco: Etične smernice za zaupanja vredno umetno inteligenco, Bruselj, 2019.

UNESCO: Artificial Intelligence in Education: Challenges and Opportunities for Sustainable Development, Francija: Paris, 2019.

Wisskirschen, G. in drugi: Artificial Intelligence and Robotics and Their Impact on the Workplace, IBA Global Employment Institute, 2017.

World Economic Forum (WEF): The Future of Jobs Employment, Skills and Workforce Strategy for the Fourth Industrial Revolution, 2016.

Članki in poglavja iz knjig

Adadi, A. and Berrada, M.: Peeking Inside the Black-Box: A Survey on Explainable Artificial Intelligence (XAI), IEEE Access, 6 (2017), str. 52145.

Buocz, T. J.: Artificial Intelligence in Court: Legitimacy Problems of AI Assistance in the Judiciary, v: Retskraft- Copenhagen Journal of Legal Studies, 2 (2018) 1, str. 41.

Ducorps-Prouvost, E.: Labor Law And The Challenges Of Artificial Intelligence : 1st Part Of A Trilogy, Soulier Avocats, 2018.

Fleischmann, E.: The Impact of Digital Technology on Copyright Law, 8 (1987) 1, str. 2-5.

Jakšić, J.: Ali je pravo pripravljeno na izzive umetne inteligence?, v: Pravna praksa, 43 (2017), str. 17-19.

Kraljić, S. in Ivanc, T.: Pravni izzivi uporabe robotov v medicini, v: 28. posvetovanje Medicina, pravo & družba: Globalizacija medicine v 21. stoletju, 28.-30. marec 2019, Univerzitetna založba Univerze v Mariboru, 2019, str. 31-48.

Lahe, M.: Ohranjanje in krepite v zdravja predšolskih otrok, v: Metodicki obzori 12, 6 (2011) 2, str. 157.

Livingston, S., in Risse, M.: The Future Impact of Artificial Intelligence on Humans and Human Rights, v: Ethics & International Affairs, 33 (2019) 2, str. 143, 144.

Marguč, K.: Trajnostna evolucijska etika kot odgovor na problem vrzeli racionalnosti med umetno inteligenco in potrošnikom, v: Res novae, celovita revija za znanost, 2 (2017) 2, str. 78.

Podpečan, M.: Umetna inteligenca in sojenje, v: Odvetnik, (2018) 88, str. 26.
Bogataj Jančič, M.: Velika pričakovanja in še večja razočaranja: Predlog direktive o avtorski pravici na digitalnem trgu, v: IX. Posvet Pravo in ekonomija: Avtorska dela na univerzi 2. decembra 2016 (konferenčni zbornik), str. 51-56.
Samothrakis, S.: Viewpoint: Artificial Intelligence and Labour, Proceedings of the Twenty-Seventh International Joint Conference on Artificial Intelligence, v: Proceedings of the Twenty-Seventh International Joint Conference on Artificial Intelligence, IJCAI-18, str. 5653.
Sileno, G., Boer, A. and van Engers, T.: The Role of Normware in Trustworthy and Explainable AI, v: CEUR Workshop Proceedings, 2381 (2019), str. 9-16.
Sourdin, T.: JUDGE V ROBOT? ARTIFICIAL INTELLIGENCE AND JUDICIAL DECISION-MAKING, v: UNSW Law Journal. 41 (2018) 4, str. 1116.
Timms, M.: Letting Artificial Intelligence in Education Out of the Box: Educational Cobots and Smart Classrooms, v: International Journal of Artificial Intelligence in Education, 26 (2016), str. 701–712.
Turšek, T.: Avtorske pravice v elektronskem okolju v Sloveniji in EU, v: Organizacija znanja, 16 (2011) 1-2, str. 43.
Zuckerman, A.: Artificial Intelligence – Implications for the Legal Profession, Adversarial Process and the Rule of Law. UK Constitutional Law Association, 2020.

Pravni viri

Ustava Republike Slovenije (Uradni list RS, št. 33/91-I, 42/97 – UZS68, 66/00 – UZ80, 24/03 – UZ3a, 47, 68, 69/04 – UZ14, 69/04 – UZ43, 69/04 – UZ50, 68/06 – UZ121,140,143, 47/13 – UZ148, 47/13 – UZ90,97,99 in 75/16 – UZ70a).
Zakon o avtorski in sorodnih pravicah (Uradni list RS, št. 16/07 – uradno prečiščeno besedilo, 68/08, 110/13, 56/15, 63/16 – ZKUASP in 59/19).
Zakon o delovnih razmerjih (Uradni list RS, št. 21/13, 78/13 – popr., 47/15 – ZZSDT, 33/16 – PZ-F, 52/16, 15/17 – odl. US, 22/19 – ZPosS in 81/19).
Zakon o industrijski lastnini (Uradni list RS, št. 51/06 – uradno prečiščeno besedilo, 100/13 in 23/20).
Listina Evropske Unije o človekovih pravicah, Uradni list Evropske unije, C 83/389, str. 391–407.
Direktiva (EU) 2017/1564 Evropskega Sveta in Parlamenta z dne 13. septembra 2017 o določenih dovoljenih uporabah določenih del in drugih predmetov urejanja, zaščitenih z avtorsko pravico in sorodnimi pravicami, za slepe in slabovidne osebe ter osebe z drugimi motnjami branja ter o spremembi Direktive 2001/29/ES o usklajevanju določenih vidikov avtorske pravice in sorodnih pravic v informacijski družbi, Uradni list Evropske unije, L 242, 20.9.2017, str. 6–13.
Direktiva (EU) 2019/1152 Evropskega Sveta in Parlamenta z dne 20. junija 2019 o preglednih in predvidljivih delovnih pogojih v Evropski uniji, Uradni list Evropske unije, L 186, 11.7.2019, str. 105–121.
Direktiva (EU) 2019/789 Evropskega Sveta in Parlamenta z dne 17. aprila 2019 o določitvi pravil glede izvrševanja avtorske in sorodnih pravic, ki se uporabljajo za določene spletne prenose radiodifuznih organizacij in retransmisije televizijskih ter radijskih programov, in spremembi Direktive Sveta 93/83/EGS, Uradni list Evropske unije, L 130, 17.5.2019, str. 82–91.
Direktiva (EU) 2019/790 Evropskega Sveta in Parlamenta z dne 17. aprila 2019 o avtorski in sorodnih pravicah na enotnem digitalnem trgu in spremembi direktiv 96/9/ES in 2001/29/ES, Uradni list Evropske unije, L 130, 17.5.2019, str. 92–125.
DIREKTIVA 2003/88/ES EVROPSKEGA PARLAMENTA IN SVETA z dne 4. novembra 2003 o določenih vidikih organizacije delovnega časa, Uradni list Evropske unije, L 299, 18.11.2003, str. 9–19.
Direktiva 2006/42/ES Evropskega Sveta in Parlamenta z dne 17. maja 2006 o strojih in spremembah Direktive 95/16/ES, Uradni list Evropske unije, L 157, 9.6.2006, str. 24–86.
Direktiva 2011/83/EU Evropskega parlamenta in Sveta z dne 25. oktobra 2011 o pravicah potrošnikov, spremembi Direktive Sveta 93/13/EGS in Direktive 1999/44/ES Evropskega parlamenta in Sveta ter razveljavitvi Direktive Sveta 85/577/EGS in Direktive 97/7/ES Evropskega parlamenta in Sveta Besedilo velja za EGP, UL L 304, 22.11.2011, str. 64–88.

European Commission: Green Paper on Copyright and the Challenge of Technology - Copyright Issues Requiring Immediate Action. COM (88) 172 final, 7 June 1988.

European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14, 4 November 1950, ETS 5.

Evropska komisija: BELA KNJIGA o umetni inteligenci - evropski pristop k odličnosti in zaupanju, COM(2020) 65 final, str. 11.

International Covenant on Civil and Political Rights, UN General Assembly, Treaty Series, vol. 999, 16 December 1966, str. 171.

International Covenant on Economic, Social and Cultural Rights, UN General Assembly, Treaty Series, vol. 993, 16 December 1966, p. 3.

Mnenje Evropskega odbora regij- Digitalna Evropa za vse: uvajanje pametnih in vključujočih rešitev na terenu, 2020/C 39/18, str. 2.

Prečiščena različica Pogodbe o delovanju Evropske unije, UL C 326, 26.10.2012, str. 47–390.

PRIPOROČILO SVETA z dne 8. novembra 2019 o dostopu delavcev in samozaposlenih oseb do socialne zaščite, 2019/C 387/01.

SPOROČILO KOMISIJE EVROPSKEMU PARLAMENTU, EVROPSKEMU SVETU, SVETU, EVROPSKEMU EKONOMSKO-SOCIALNEMU ODBORU IN ODBORU REGIJ Umetna inteligenca za Evropo, COM (2018) 237 final.

SPOROČILO KOMISIJE EVROPSKEMU PARLAMENTU, SVETU, EVROPSKEMU EKONOMSKO-SOCIALNEMU ODBORU IN ODBORU REGIJ o vmesnem pregledu izvajanja strategije za enotni digitalni trg Povezani enotni digitalni trg za vse, COM(2017) 228 final.

SPOROČILO KOMISIJE EVROPSKEMU PARLAMENTU, SVETU, EVROPSKEMU EKONOMSKO-SOCIALNEMU ODBORU IN ODBORU REGIJ Oblikovanje digitalne prihodnosti Evrope, COM(2020) 67 final, str. 1.

SPOROČILO KOMISIJE EVROPSKEMU PARLAMENTU, SVETU, EVROPSKEMU EKONOMSKO-SOCIALNEMU ODBORU IN ODBORU REGIJ o akcijskem načrtu za digitalno izobraževanje, COM(2018) 22 final, str. 4-12.

SPOROČILO KOMISIJE EVROPSKEMU PARLAMENTU, SVETU, EVROPSKEMU EKONOMSKO-SOCIALNEMU ODBORU IN ODBORU REGIJ Spodbujanje pravičnega, učinkovitega in konkurenčnega evropskega gospodarstva, ki temelji na avtorskih pravicah, na enotnem digitalnem trgu, COM (2016) 592 final, str. 7.

SPOROČILO KOMISIJE EVROPSKEMU PARLAMENTU, SVETU, EVROPSKEMU EKONOMSKO-SOCIALNEMU ODBORU IN ODBORU REGIJ Oblikovanje digitalne prihodnosti Evrope, COM(2020) 67 final str. 13.

Universal Declaration of Human Rights, UN General Assembly, 217 A (III), 10 December 1948.

UREDBA (EU) 2016/679 EVROPSKEGA PARLAMENTA IN SVETA z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES (Splošna uredba o varstvu podatkov), L 119/1.

UREDBA (EU) 2017/1563 EVROPSKEGA PARLAMENTA IN SVETA z dne 13. septembra 2017 o čezmejni izmenjavi med Unijo in tretjimi državami izvodov v dostopnem formatu določenih del in drugih predmetov urejanja, zaščitenih z avtorsko pravico in sorodnimi pravicami, v korist slepih in slabovidnih oseb ter oseb z drugimi motnjami branja, Uradni list Evropske unije, L 242, 20.9.2017, p. 1–5.

Sodna praksa

C-403/08 in C-429/08, *Football Association Premier League Ltd and Others proti QC Leisure and Others,* ECLI:EU:C:2011:631.

C-78/70, *DEUTSCHE GRAMMOPHON GESELLSCHAFT MBH, HAMBURG, AND METRO-SB-GROSSMAERKTE GMBH AND COMPANY KG, REPRESENTED BY THE COMPANY METRO-SB-GROSSMAERKTE GMBH*, ECLI:EU:C:1971:59.

C-479/04, *Laserdisken ApS v. Kulturministeriet*, ECLI:EU:C:2006:549.

C-60/84 in 61/84, *Cinéthèque SA and others v Fédération nationale des cinémas français*, ECLI:EU:C:1985:329.

C-128/11, *UsedSoft GmbH v. Oracle International Corp.,* ECLI:EU:C:2012:407.
SKLEPNI PREDLOGI GENERALNEGA PRAVOBRANILCA YVESA BOTA, predstavljeni 24. aprila 2012(1), Zadeva C-128/11, *Axel W. Bierbach, stečajni upravitelj družbe UsedSoft GmbH, proti Oracle International Corp*., ECLI:EU:C:2012:234.
Golder v. The United Kingdom, 21. 2. 1975, A 18, §§ 34–36
H. v. France (1989) No. 10073/82, § 58; Vernillo v. France (1991) No. 11889/85, § 38; Katte Klitsche de la Grande v. Italy (1994) No. 12539/86, § 61.
Hadjianastassiou v. Greece, no. 12945/87,16.12.1992, § 33.
Klass in drugi v. Nemčija**,** 6. 9. 1978, A 28, s. 17.
Kraska v. Switzerland, 19. 4. 1993, A 254-B, s. 49; glej tudi sodbo Barberà, Messegué in Jabardo v. Španija**,** 6. 12. 1988, A 146, s. 31
Loomis v. Wisconsin, 881 N.W.2d 749 (2016)
Ruiz Torija v. Spain (1994) No. 18390/91, §§ 29–30.
Sodba VSM IV Kp 31496/2012 z dne 01.12.2016.
Suominen v. Finland (2003) No. 37801/97, § 37.

Spletni viri

Computer says no: why making Ais fair, accountable and transparent is crucial <https://www.theguardian.com/science/2017/nov/05/computer-says-no-why-making-ais-fair-accountable-and-transparent-is-crucial > (25.5.2020).
Durham Police AI to help with custody decisions < https://www.bbc.co.uk/news/technology-39857645> (17.5.2020).
Israel to track mobile phones of suspected corona virus cases 17.3.2020 < https://www.theguardian.com/world/2020/mar/17/israel-to-track-mobile-phones-of-suspected-coronavirus-cases> (17.3.2020)
Komentar Ustave RS e-Kurs: Pravica do poštenega sodnega varstva > https://e-kurs.si/komentar/pravica-do-postenega-sodnega-varstva/< (25.6.2020)
Lights, camera, legal action! Courts to livestream divorce proceedings < https://edition.cnn.com/2020/03/13/uk/livestream-divorces-intl-scli-gbr/index.html> (17.5.2020)
Slovar slovenskega knjižnega jezika, Splet <https://fran.si/131/snb-slovar-novejsega-besedja/3623770/T4MVC_System_Web_Mvc_ActionResult> (20.4.2020).
Urad RS za intelektualno lastnino: Avtor in avtorsko delo, <https://www.gov.si/teme/avtorska-in-sorodne-pravice/>. (15.5.2020)

Raziskave

Cedefop: 'The great divide: Digitalisation and digital skill gaps in the EU workforce', #ESJsurvey Insights. Thessaloniki: Greece. No 9, 2016.
UNICEF: Technical Guidance: Guide for Including Disability in Education Management Information Systems, 2016.

Priloga

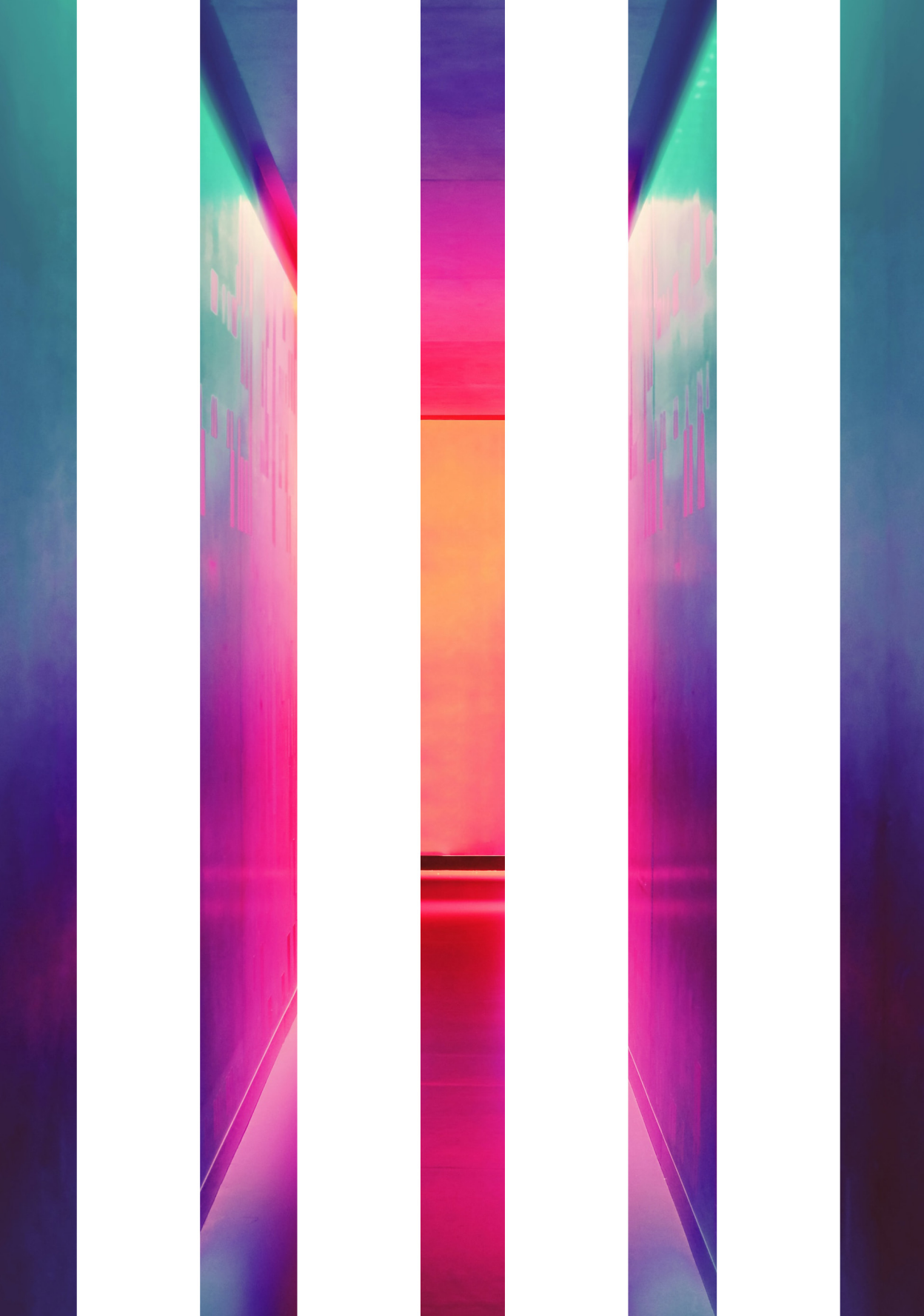
PRAVNI AKT	ČLEN	VSEBINA
Mednarodno pravo		
Deklaracija OZN o človekovih pravicah	2	Prepoved diskriminacije
	7	Enakost pred zakonom
	8	Pravica do učinkovitega pravnega sredstva
	10	Neodvisnost in nepristranskost sodišč
	11	Domneva nedolžnosti
	12	Varstvo zasebnosti
	22	Pravica do socialne varnosti
	23	Pravica do dela
	24	Pravica do počitka in prostega časa
	25	Pravica do življenjske ravni
	26	Pravica do izobraževanja
	30	Omejitev pravic
Mednarodni pakt o državljanskih in političnih pravicah	5	Omejitev pravic
	8	Prepoved suženjstva in prisilnega dela
	14	Enakost pred zakonom
	17	Varstvo zasebnosti
	26	Prepoved diskriminacije
Mednarodni pakt o ekonomskih, socialnih in kulturnih pravicah	4	Omejitev pravic
	5	Omejitev ali razveljavitev pravic
	6	Pravica do dela
	7	Pravica do pravičnih in ugodnih delovnih pogojev
	9	Pravica do socialne varnosti
	11	Pravica do življenskega standarda
	13	Pravica do izobraževanja
Konvencija o otrokovih pravicah	29	Pravica do izobraževanja
Konvencija proti diskriminaciji v izobraževanju	1	Prepoved disrkiminacije
	2	Opredelitev diskriminacije
	5	Prepoved diskriminacije v izobraževanju
Pravo EU		
Pogodba o Evropski uniji	2	Vrednote
	3	Cilji
	6	Priznavanje Listine EU in pristopk EU k EKČP
Pogodba o delovanju Evropske unije	6	Podporne pristojnosti
	9	Opredeljevanje in izvajanje politik in dejavnosti EU z upoštevanjem visoke stopnje zaposlenosti, zagotavljanjem ustrezne socialne zaščite, bojem proti socialni izključenosti in visoko stopnjo

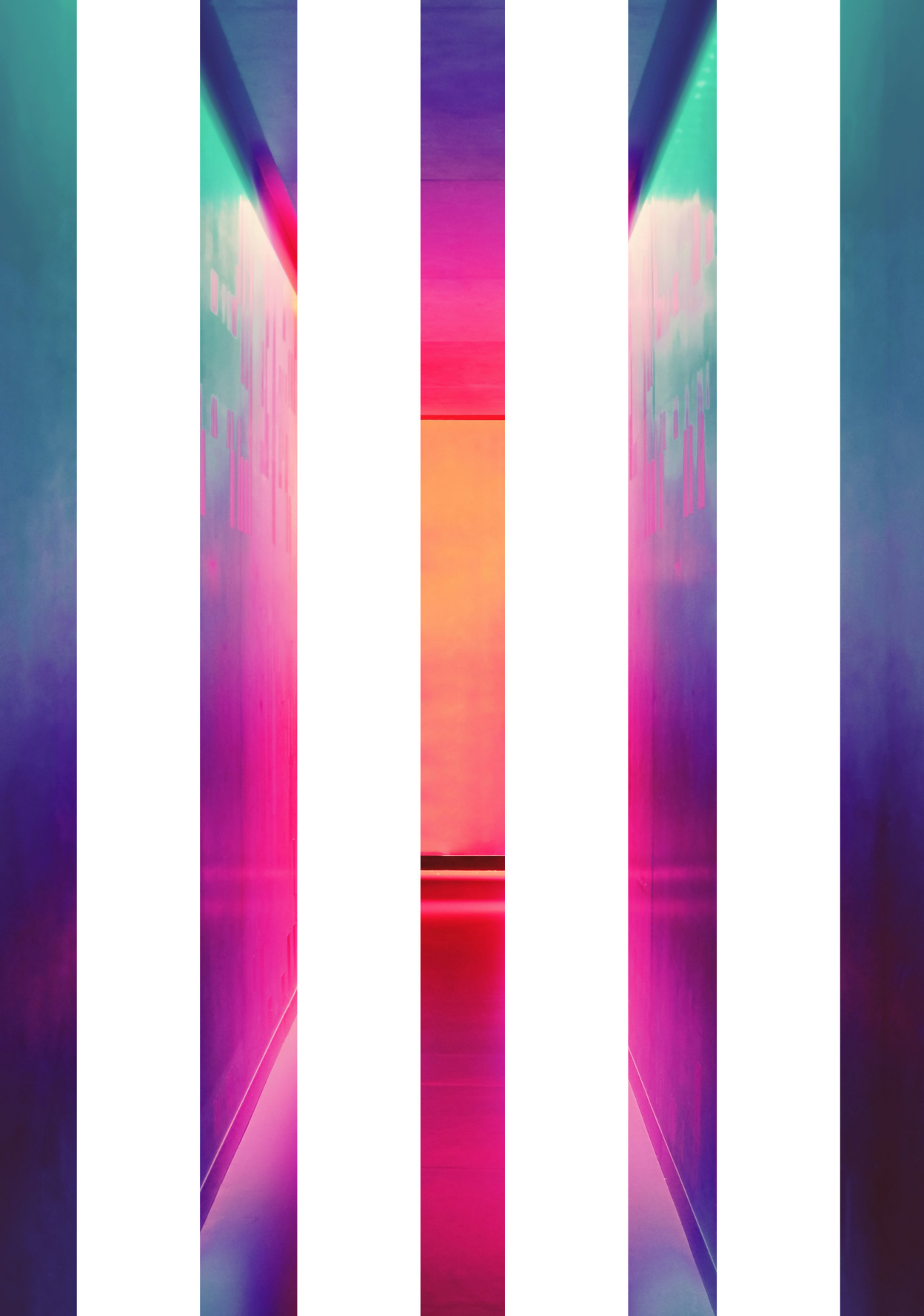
PRAVNI AKT	ČLEN	VSEBINA
		izobraževanja in usposabljanja ter varovanjem človekovega zdravja
	18	Prepoved diskriminacije
	19	Ukrepi za boj proti diskriminaciji
	151	Socialna politika
	153	Cilji socialne politike
	156	Doseganje ciljev socialne politike
	157	Enako plačilo brez diskriminacije glede na spol
	158	Enakovrednost sistemov plačanih dopustov
	165	Izobraževanje, poklicno usposabljanje, mladina in šport
	166	Cilji izobraževanja, poklicnega usposabljanja, mladine in športa
	176	Evropski socialni sklad za odpravljanje razvojnih neravnovesij v regijah unije
Listina Evropske unije o temeljnih pravicah	4. odstavek Preambule	Okrepitev pravic
	5	Prepoved suženjstva in prisilnega dela
	7	Spoštovanje zasebnega in družinskega življenja
	14	Pravica do izobraževanja
	15	Svoboda izbire poklica in pravica do dela
	20	Enakost pred zakonom
	21	Prepoved diskriminacije
	27	Pravica delavcev do obveščenosti in posvetovanja v podjetju
	30	Varstvo v primeru neupravičene odpustitve
	31	Pošteni in pravični delovni pogoji
	33	Družinsko in poklicno življenje
	34	Socialna varnost in socialna pomoč
	35	Varovanje zdravja
	47	Pravica do učinkovitega pravnega sredstva in nepristranskega sodišča
	48	Domneva nedolžnosti
	52	Obseg pravic in načel ter njihova razlaga
	53	Raven varstva
	54	Prepoved zlorabe pravic
Direktiva o preglednih in predvidljivih delovnih pogojih	4	Obveznost zagotavljanja informacij
	8	Najdaljše trajanje poskusne dobe
	10	Minimalna predvidljivost dela
	11	Dopolnilni ukrepi za pogodbe za delo na zahtevo
	12	Prehod na drugo obliko zaposlitve
	13	Obvezno usposabljanje

PRAVNI AKT	ČLEN	VSEBINA
	15	Pravne domneve in mehanizem zgodnjega reševanja sporov
	16	Pravica do pravnega sredstva
	17	Varstvo pred manj ugodno obravnavo ali neugodnimi posledicami
	18	Varstvo pred odpovedjo in dokazno breme
Direktiva EU o določenih vidikih organizacije delovnega časa	2	Koncept delovnega časa in počitkov
	3	Dnevni počitek
	4	Odmori
	5	Tedenski počitek
	6	Najdaljši tedenski delovni čas
	7	Letni dopust
	8	Trajanje nočnega dela
	12	Varnost in varovanje zdravja
Direktiva EU o splošnih okvirih enakega obravnavanja pri zaposlovanju in delu	2	Koncept diskriminacije
	6	Upravičenost različnega obravnavanja zaradi starosti
	9	Pravno varstvo
Pravo Sveta Evrope		
Evropska konvencija o varstvu človekovih pravic	1	Obveznost spoštovanja človekovih pravic
	4	Prepoved suženjstva in prisilnega dela
	6	Pravica do poštenega sojenja
	13	Pravica do učinkovitega pravnega sredstva
	14	Prepoved diskriminacije
	17	Prepoved zlorabe pravic
	18	Omejitev restrikcij pravic
	53	Varstvo priznanih človekovih pravic
Dodatni protokol h Konvenciji o varstvu človekovih pravic in temeljnih svoboščin	2	Pravica do izobraževanja
Protokol št. 12 h Konvenciji o varstvu človekovih pravic in temeljnih svoboščin	1	Splošna prepoved diskriminacije
Evropska socialna listina	1	Pravica do dela
	2	Pravica do pravičnih delovnih pogojev
	3	Pravica do varnih in zdravih delovnih pogojev
	4	Pravica do poštenega plačila
	9	Pravica do poklicnega usmerjanja
	10	Pravica do poklicnega usposabljanja
	12	Pravica do socialne varnosti
	13	Pravica do socialne in zdravstvene pomoči
	14	Pravica do socialnega varstva

PRAVNI AKT	ČLEN	VSEBINA
	20	Prepoved diskriminacije pri zaposlitvi in delu
	22	Pravica do sodelovanja pri določanju in izboljšanju delovnih pogojev in delovnega okolja
	23	Pravica starejših do socialne zaščite
	24	Pravica do varstva v primerih prenehanja delovnega razmerja
	26	Pravica do dostojanstva na delovnem mestu
	27	Pravica delavcev z družinami do enakih možnosti in enake obravnave
	30	Pravica do zaščite pred revščino in socialno izključenostjo
	E	Nediskriminacija
	G	Omejitve
Pravo RS		
Ustava Republike Slovenije	14	Enakost pred zakonom
	15	Uresničevanje in omejevanje pravic
	22	Enako varstvo pravic
	23	Pravica do sodnega varstva
	24	Javnost sojenja
	25	Pravica do pravnega sredstva
	27	Domneva nedolžnosti
	49	Svoboda dela
	50	Pravica do socialne varnosti
	57	Izobrazba in šolanje
	66	Varstvo dela
	125	Neodvisnost sodnikov
Zakon o delovnih razmerjih	6	Prepoved diskriminacije
	27	Enaka obravnava glede na spol
	35	Spoštovanje predpisov o varnosti in zdravju pri delu
	44	Obveznost plačila
	45	Varne delovne razmere
	47	Varovanje dostojanstva delavca pri delu
	68-72	Pogodba o zaposlitvi za opravljanje dela na domu
	133	Enako plačilo žensk in moških
	146	Prepoved opravljanja dela preko polnega delovnega časa
	148	Razporejanje delovnega časa
	154-156	Odmori in počitki
	159	Pridobitev pravice in minimalno trajanje letnega dopusta
	170, 171	Izobraževanje delavcev
	181-199	Varstvo nekaterih kategorij delavcev
Zakon o varstvu pravice do sojenja brez nepotrebnega odlašanja	2	Pravica do sojenja brez nepotrebnega odlašanja
	3	Pravna sredstva
Zakon o varstvu pred diskriminacijo	1	Namen in vsebina zakona

PRAVNI AKT	ČLEN	VSEBINA
	2	Uporaba zakona
	4	Diskriminacija
	5	Enako obravnavanje
	6	Neposredna in posredna diskriminacija
	7	Druge oblike diskriminacije
	13	Izjeme od prepovedi neposredne diskriminacije
	39	Pravno varstvo
	40	Obrnjeno dokazno breme
Zakon o sodiščih	3	Neodvisnost in nepristranskost sodnikov





TEMELJNE PRAVICE IN IZZIVI DIGITALIZACIJE: OD PRAVNE UREDITVE DO PRAKSE

PETRA WEINGERL (UR.)
Univerza v Mariboru, Pravna fakulteta, Maribor, Slovenija
petra.weingerl@um.si

DOI
https://doi.org/10.18690/um.pf.4.2023

ISBN
978-961-286-774-4

Bliskovit razvoj digitalizacije vpliva na vsa področja našega življenja. Na ravni EU se v zadnjih letih že odvija široka etična in pravna razprava o umetni inteligenci, robotiki stvari, močnih komunikacijskih omrežjih in primernem regulativnem okvirju, ki mora spoštovati tudi temeljne pravice. O tem so leta 2020 v sklopu Študentskega inovativnega projekta za družbeno korist (ŠIPK) raziskovali na Pravni fakulteti UM skupaj s sodelovanjem partnerja iz negospodarstva, Zavoda PIP, in osmih študentov iz štirih fakultet Univerze v Mariboru, in sicer Pravne fakultete, Ekonomsko-poslovne fakultete, Fakultete za elektrotehniko, računalništvo in informatiko in Filozofske fakultete. Namen projekta in pričujoče monografije je ozaveščati vse družbene deležnike o vplivu digitalizacije na družbena razmerja in pripraviti podlago za smernice za bodoče urejanje digitalizacije.

Ključne besede:
digitalizacija,
umetna inteligenca,
etične dileme,
pravna država,
diskriminacija,
varstvo zasebnosti

Univerzitetna založba Univerze v Mariboru

DOI
https://doi.org/
10.18690/um.pf.4.2023

ISBN
978-961-286-774-4

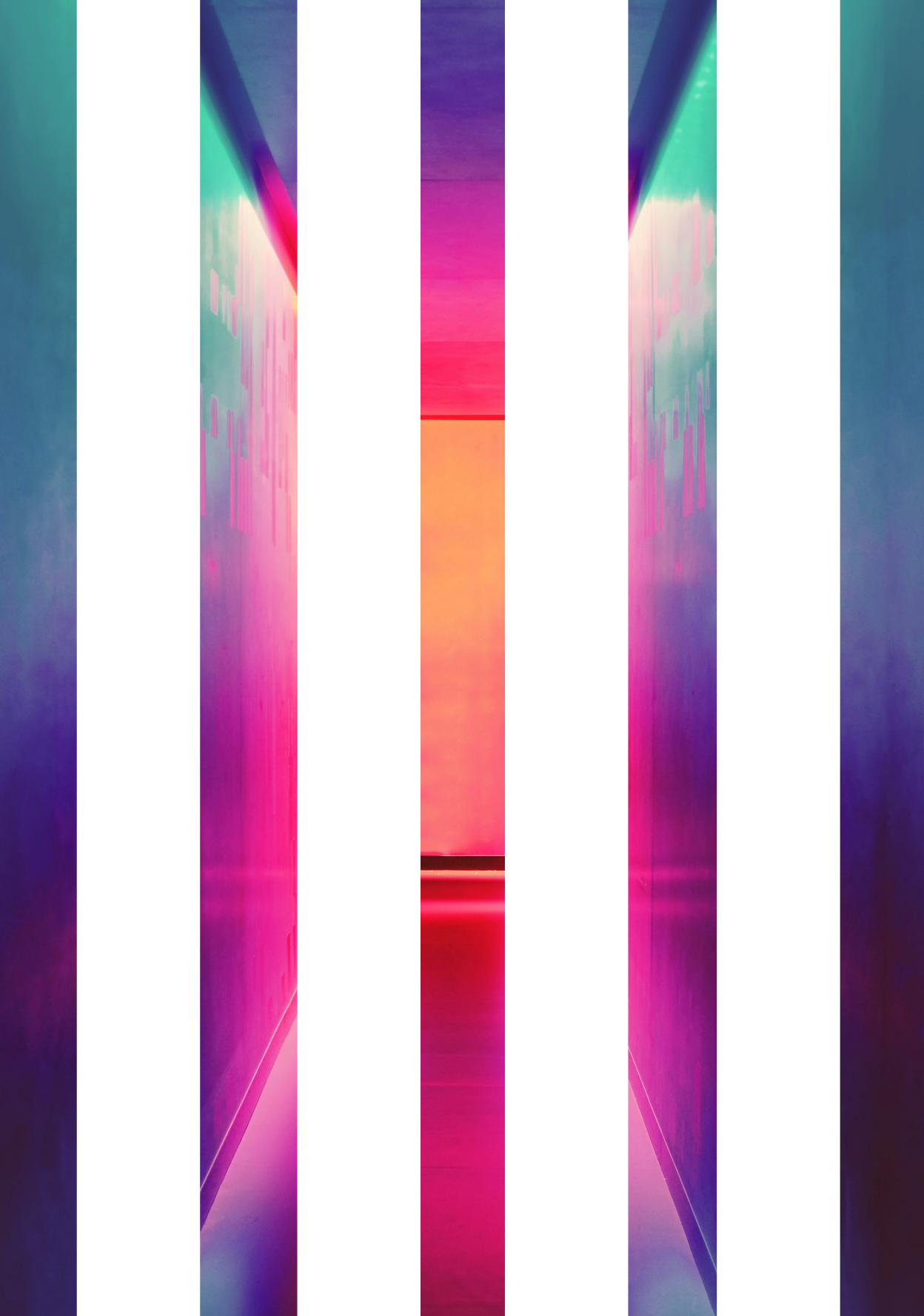
FUNDAMENTAL RIGHTS AND CHALLENGES OF DIGITIZATION: FROM LEGAL REGULATION TO PRACTICE

PETRA WEINGERL (ED.)
University of Maribor, Faculty of Law, Maribor, Slovenia
petra.weingerl@um.si

Keywords:
digitization,
artificial intelligence,
ethical dilemmas,
rule of law,
discrimination,
privacy

The rapid development of digitization affects all areas of our lives. At EU level a broad ethical and legal debate has been taking place in the recent years, focusing particularly on artificial intelligence, internet of things, the role of tech giants and especially on appropriate regulatory framework that puts fundamental rights first. These questions were investigated closely as part of the Student Innovative Project for Social Benefit (ŠIPK) at the Faculty of Law University of Maribor with the cooperation of private non-profit institution, Zavod PIP, and eight students from the Faculty of Law, the Faculty of Economics and Business, the Faculty of Electrical Engineering, Computer Science and Informatics and the Faculty of Arts. The purpose of the project is to raise awareness among all social stakeholders about the impact of digitization on social relations and to prepare the basis for guidelines for the future regulation of digitization.

University of Maribor Press



Univerza v Mariboru

Pravna fakulteta