

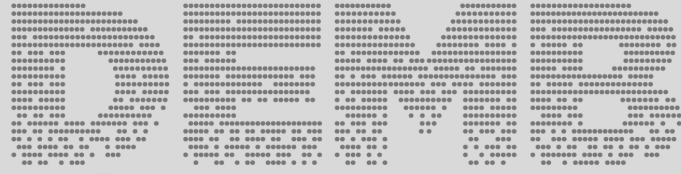
DIGITALNA EKONOMIJA IN PRAVO 2025
Študentsko posvetovanje o ekonomskih in pravnih izzivih
digitalne preobrazbe

ZBORNİK RECENZIRANIH ZNANSTVENIH PRISPEVKOV

Dejan Romih (ur.)

Nejc Fir (ur.)

0 1 0 1 0 0 1 1 1 0 0 1 0 1 1 0 0 1 1 1 0 1 1 0 0 1 1 1 0 0 1 0 1 0 1 0 1 0 0
1 1 1 0 0 1 0 1 1 0 0 1 1 1 0 1 1 0 1 1 1 0 0 1 0 1 0 1 0 0 1 1 1 0 0 1 0 1
1 0 0 1 1 1 0 1 1 0 1 1 1 0 0 1 0 1 0 0 1 1 1 0 0 1 0 1 1 0 0 1 1 1 0 1 1 0
1 1 1 0 0 1 0 1 0 0 1 1 1 0 0 1 0 1 1 0 0 1 1 1 0 1 1 0 1 1 1 0 0 1 0 1 0 0
1 1 1 0 0 1 0 1 1 0 0 1 1 1 0 1 1 0 1 1 1 0 0 1 1 1 1 0 1 0 0 1 1 1 0 0 1
0 1 1 0 0 1 1 1 0 1 1 0 1 1 1 0 0 0 1 0 1 0 1 1 1 0 0 1 1 1 1 0 0 0 1 0 1 0
0 1 0 1 0 0 1 1 1 0 0 1 0 1 1 0 0 1 1 1 0 1 1 0 1 1 1 0 0 1 0 1 0 1 0 1 0 0
1 1 1 0 0 1 0 1 1 0 0 1 1 1 0 1 1 0 1 1 0 1 0 1 0 1 0 0 1 1 1 0 0 1 0 1
1 0 0 1 1 1 0 1 1 0 1 1 1 0 0 1 0 1 0 0 1 1 1 0 0 1 0 1 1 0 0 1 1 1 0 1 1 0
1 1 1 0 0 1 0 1 0 0 1 1 1 0 0 1 0 1 1 0 0 1 1 1 0 1 1 1 0 0 1 0 1 0 0
1 1 1 0 0 1 0 1 1 0 0 1 1 1 0 1 1 0 1 1 1 0 0 1 1 1 1 0 1 0 0 1 1 1 0 0 1
0 1 1 0 0 1 1 1 0 1 1 0 1 1 1 0 0 0 1 0 1 0 1 1 1 0 0 1 1 1 1 0 0 0 1 0 1 0
0 1 0 1 0 0 1 1 1 0 0 1 0 1 1 0 0 1 1 1 0 1 1 0 1 1 1 0 0 1 1 1 1 0 0 1 0 0
1 1 1 0 0 1 0 1 1 0 0 1 1 1 0 1 1 0 1 1 1 0 0 1 0 1 0 0 1 1 1 0 0 1 0 1
1 0 0 1 1 1 0 1 1 0 1 1 1 0 0 1 0 1 0 0 1 1 1 0 0 1 0 1 1 0 0 1 1 1 0 1 1 0
1 1 1 0 0 1 0 1 0 0 1 1 1 0 0 1 0 1 1 0 0 1 1 1 0 1 1 1 0 0 1 0 1 0 0
1 1 1 0 0 1 0 1 1 0 0 1 1 1 0 1 1 0 1 1 1 0 0 1 1 1 1 0 1 0 0 1 1 1 0 0 1
0 1 1 0 0 1 1 1 0 1 1 0 1 1 1 0 0 0 1 0 1 0 1 1 1 0 0 1 1 1 1 0 0 0 1 0 1 0
0 1 0 0 1 1 1 0 0 1 0 1 1 0 0 1 1 1 0 1 1 0 1 1 1 0 0 1 1 1 1 1 0 1 0 0 1 1
1 0 0 1 0 1 1 0 0 1 1 1 0 1 1 0 1 1 1 0 0 0 1 0 1 0 1 1 1 0 0 1 1 1 1 0 0 0
1 0 1 0 0 1 0 1 0 0 1 1 1 0 0 1 0 1 1 0 0 1 1 1 0 1 1 0 1 1 1 0 0 1 0 1 0 1
0 1 0 0 1 1 1 0 0 1 0 1 1 0 0 1 1 1 0 1 1 0 1 1 1 0 0 1 0 1 0 1 0 0 1 1 1 0
0 1 0 1 1 0 0 1 1 1 0 1 1 0 1 1 1 0 0 1 0 1 0 0 1 1 1 0 0 1 0 1 1 0 0 1 1 1
0 1 1 0 1 1 1 0 0 1 0 1 0 0 1 1 1 0 0 1 0 1 1 0 0 1 1 1 0 1 1 0 1 1 1 0 0 1
0 1 0 0 1 1 1 0 0 1 0 1 1 0 0 1 1 1 0 1 1 0 1 1 1 0 0 1 1 1 1 1 0 1 0 0 1 1



DRUŠTVO EKONOMISTOV MARIBOR

MARIBOR SOCIETY OF ECONOMISTS

0 1 0 1 0 0 1 1 1 0 0 1 0 1 1 0 0 1 1 1 0 1 1 0 1 1 1 0 0 1 0 1 0 1 0 1 0 1 0 0
1 1 1 0 0 1 0 1 1 0 0 1 1 1 0 1 1 0 1 1 1 0 0 1 0 1 0 1 0 0 1 1 1 0 0 1 0 1
1 0 0 1 1 1 0 1 1 0 1 1 1 0 0 1 0 1 0 0 1 1 1 0 0 1 0 1 1 0 0 1 1 1 0 1 1 0
1 1 1 0 0 1 0 1 0 0 1 1 1 0 0 1 0 1 1 0 0 1 1 1 0 1 1 0 1 1 1 0 0 1 0 1 0 0
1 1 1 0 0 1 0 1 1 0 0 1 1 1 0 1 1 1 0 0 1 1 1 1 1 0 1 0 0 1 1 1 0 0 1 1 0 0 1
0 1 1 0 0 1 1 1 0 1 1 0 1 1 1 0 0 0 1 0 1 0 1 1 1 0 0 1 1 1 1 0 0 0 1 0 1 0
0 1 0 1 0 0 1 1 1 0 0 1 0 1 1 0 0 1 1 1 0 1 1 1 0 1 1 1 0 0 1 0 1 0 1 0 1 0 0
1 1 1 0 0 1 0 1 1 0 0 1 1 1 0 1 1 0 1 1 0 1 0 1 0 1 0 0 1 1 1 0 0 1 0 1 0 1
1 0 0 1 1 1 0 1 1 0 1 1 1 0 0 1 0 1 0 0 1 1 1 0 0 1 1 1 0 0 1 1 1 0 1 1 0
1 1 1 0 0 1 0 1 0 0 1 1 1 0 0 1 0 1 1 0 0 1 1 1 0 1 1 0 1 1 1 0 0 1 0 1 0 0
1 1 1 0 0 1 0 1 1 0 0 1 1 1 0 1 1 0 1 1 1 0 0 1 1 1 1 0 1 0 0 1 1 1 0 0 1
0 1 1 0 0 1 1 1 0 1 1 0 1 1 0 1 1 1 0 0 0 1 0 1 0 1 1 1 0 0 1 1 1 1 0 0 1 0 1 0
0 1 0 1 0 0 1 1 1 0 0 1 0 1 1 0 0 1 1 1 0 1 1 0 1 1 1 0 0 1 1 1 0 0 1 0 1 0 0
1 1 1 0 0 1 0 1 1 0 0 1 1 1 0 1 1 0 1 1 1 0 0 1 0 1 0 1 0 0 1 1 1 0 0 1 0 1
1 0 0 1 1 1 0 1 1 0 1 1 1 0 0 1 0 1 0 0 1 1 1 0 0 1 0 1 1 0 0 1 1 1 0 1 1 0
1 1 1 0 0 1 0 1 0 0 1 1 1 0 0 1 1 1 0 0 1 0 1 1 0 1 1 0 1 1 1 0 0 1 0 1 0 0
1 1 1 0 0 1 0 1 1 0 0 1 1 1 0 1 1 0 1 1 1 0 0 1 1 1 1 1 0 1 0 0 1 1 1 0 0 1
0 1 1 0 0 1 1 1 0 1 1 0 1 1 0 1 1 1 0 0 0 1 0 1 0 1 1 1 0 0 1 1 1 1 0 0 1 1 1
0 1 1 0 1 1 1 0 0 1 0 1 0 0 1 1 1 0 0 1 0 1 1 0 0 1 1 1 0 1 1 0 1 1 1 0 0 1
0 1 0 0 1 1 1 0 0 1 0 1 1 0 0 1 1 1 0 1 1 0 1 1 1 0 0 1 1 1 1 0 1 0 0 1 1 1
1 0 0 1 0 1 1 0 0 1 1 1 0 0 1 1 1 0 1 1 1 0 0 1 0 1 0 1 1 1 0 0 1 1 1 1 0 0 1
1 1 1 1 1 1 0 0 1 1 1 0 0 0 1 1 0 1 0 1 1 1 1 1 0 0 0 1 1 1 1 1 1 1 1 1 1 1 1

Maribor, september 2025

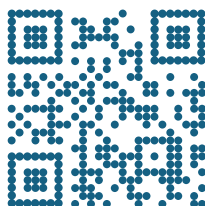
DIGITALNA EKONOMIJA IN PRAVO 2025

Študentsko posvetovanje o ekonomskih in pravnih izzivih
digitalne preobrazbe

0 1 0 1 0 0 1 1 1 0 0 1 0 1 1 0 0 1 1 1 0 1 1 0 1 1 1 0 0 1 0 1 0 1 0 1 0 1 0 0
1 1 1 0 0 1 0 1 1 0 0 1 1 1 0 1 1 0 1 1 1 0 0 1 0 1 0 1 0 0 1 1 1 0 0 1 0 1
1 0 0 1 1 1 0 1 1 0 1 1 1 0 0 1 0 1 0 0 1 1 1 0 0 1 0 1 1 0 0 1 1 1 0 1 1 0
1 1 1 0 0 1 0 1 0 0 1 1 1 0 0 1 0 1 1 0 0 1 1 1 0 1 1 0 1 1 1 0 0 1 0 1 0 0
1 1 1 0 0 1 0 1 1 0 0 1 1 1 0 1 1 0 1 1 1 0 0 1 1 1 1 1 0 1 0 0 1 1 1 0 0 1
0 1 1 0 0 1 1 1 0 1 1 0 1 1 1 0 0 0 1 1 1 0 0 1 1 1 1 1 0 0 1 1 1 0 0 0 1 0 1 0
0 1 0 1 0 0 1 1 1 0 0 1 0 1 1 0 0 1 1 1 0 1 1 0 1 1 1 0 0 1 0 1 0 1 0 1 0 0
1 1 1 0 0 1 0 1 1 0 0 1 1 0 1 1 0 1 1 1 0 0 1 0 1 0 1 0 0 1 1 1 0 0 1 0 1
1 0 0 1 1 1 0 1 1 0 1 1 1 1 1 0 0 1 1 1 0 0 1 0 1 1 0 0 1 1 1 0 1 1 0 1 1 0
1 1 1 0 0 1 0 1 0 0 1 1 0 0 0 1 1 0 0 0 1 1 1 0 1 1 0 1 1 1 0 0 1 0 1 0 0
1 1 1 0 0 1 0 1 1 0 0 1 1 1 1 1 0 1 1 1 0 0 1 1 1 1 0 1 0 0 1 1 1 0 0 1
0 1 1 0 0 1 1 1 0 1 1 0 1 1 1 0 0 0 0 0 1 1 1 1 1 0 0 0 1 0 1 0 1 0
0 1 0 1 0 0 1 1 1 0 0 1 0 1 1 0 0 1 1 0 1 1 0 1 1 1 0 0 1 0 1 0 1 0 0
1 1 1 0 0 1 0 1 1 0 0 1 0 1 1 0 0 1 0 1 0 1 0 1 0 0 1 1 1 0 0 1 0 1
0 0 1 1 1 0 1 1 0 1 1 1 0 0 1 0 1 0 0 0 0 1 0 1 1 0 0 1 1 1 0 1 1 0
1 1 1 0 0 1 0 1 0 0 1 1 1 0 0 1 0 1 1 0 1 1 1 0 1 1 1 0 0 1 0 1 0 0
1 1 1 0 0 1 0 1 1 0 0 1 1 1 0 1 1 0 1 1 1 0 0 1 1 1 1 0 1 0 0 1 1 1 0 0 1
0 1 1 0 0 1 1 1 0 1 1 0 1 1 1 0 0 0 1 0 1 0 1 1 1 0 0 1 1 1 1 0 0 0 1 0 1 0
0 1 1 0 1 1 1 0 0 1 0 1 0 0 1 1 1 0 0 1 0 1 1 0 0 1 1 1 0 1 1 0 1 1 1 0 0 1
0 1 0 0 1 1 1 0 0 1 0 1 1 0 0 1 1 1 0 1 1 0 1 1 1 0 0 1 1 1 1 0 1 0 0 1 1
1 0 0 1 0 1 1 0 0 1 1 1 0 1 1 0 1 1 1 0 0 0 1 0 1 0 1 1 1 0 0 1 1 1 1 0 0 0
1 0 1 0 0 1 0 1 0 0 1 1 1 0 0 1 0 1 1 0 0 1 1 1 0 1 1 1 0 0 1 0 1 0 1
0 1 0 0 1 1 1 0 0 1 0 1 1 0 0 1 1 1 0 1 1 0 1 1 1 0 0 1 0 1 0 0 1 1 1 0
0 1 0 1 1 0 0 1 1 1 0 1 1 0 1 1 1 0 0 1 0 1 0 0 1 1 1 0 0 1 0 1 1 0 0 1 1
0 1 1 0 1 1 1 0 0 1 0 1 0 0 1 1 1 0 0 1 0 1 1 0 0 1 1 1 0 1 1 0 1 1 1 0 0 1
0 1 0 0 1 1 1 0 0 1 0 1 1 0 0 1 1 1 0 1 1 0 1 1 1 0 0 1 1 1 1 0 1 0 0 1 1
1 0 0 1 0 1 1 0 0 1 1 1 0 1 1 0 1 1 1 0 0 0 1 0 1 0 1 1 1 0 0 1 1 1 1 0 0 1
1 1 1 1 1 1 0 0 1 1 1 0 0 0 1 1 0 1 0 1 1 1 1 0 0 0 1 1 1 1 1 1 1 1 1 1 1

<https://demb.si/>
<https://demb.si/digitalna-ekonomija-in-pravo-2025/>

DRUŠTVO EKONOMISTOV MARIBOR
Razlagova ulica 14, 2000 Maribor, Slovenija



SOORGANIZATORJI POSVETOVANJA



Univerza v Mariboru

Ekonomsko-poslovna fakulteta



Univerza v Mariboru

Pravna fakulteta



Univerza v Mariboru

Ekonomsko-poslovna fakulteta
Študentski svet



Univerza v Mariboru

Pravna fakulteta
Študentski svet

Zbornik recenziranih znanstvenih prispevkov
Digitalna ekonomija in pravo 2025

Maribor
Društvo ekonomistov Maribor
2025

<https://demb.si/>

Urednika: doc. dr. Dejan Romih (Univerza v Mariboru) in asist. Nejc Fir (Univerza v Mariboru)

Tehnična urednika: doc. dr. Dejan Romih (Univerza v Mariboru) in asist. Nejc Fir (Univerza v Mariboru)

Recenzenti: red. prof. dr. Darja Boršič (Univerza v Mariboru), red. prof. dr. Borut Bratina (Univerza v Mariboru), red. prof. dr. Silvo Dajčman (Univerza v Mariboru), red. prof. dr. Suzana Kraljić (Univerza v Mariboru), red. prof. dr. Darja Senčur Peček (Univerza v Mariboru), red. prof. dr. Bojan Tičar (Univerza v Mariboru), izr. prof. dr. Gregor Polančič (Univerza v Mariboru), izr. prof. dr. Miha Šepec (Univerza v Mariboru), doc. dr. Denis Baghrizabehi (Univerza v Mariboru), doc. dr. Rok Dacar (Univerza v Mariboru), doc. dr. Blaž Frešer (Univerza v Mariboru), doc. dr. Cocou Marius Mensah (Univerza v Mariboru), doc. dr. Maja Rožman (Univerza v Mariboru) in doc. dr. Daniel Zdolšek (Univerza v Mariboru)
Lektor: Mitja Brünec

Izdajalec in založnik: Društvo ekonomistov Maribor



© 2025, Društvo ekonomistov Maribor
Besedilo © 2025, avtorji

To delo je licencirano z licenco Creative Commons Priznanje avtorstva-Nekomercialno-Deljenje pod enakimi pogoji 4.0 Mednarodna (CC BY-NC-SA 4.0)
<https://creativecommons.org/licenses/by-nc-sa/4.0/>

Katalogni zapis o publikaciji (CIP) pripravili v Narodni in univerzitetni knjižnici v Ljubljani
COBISS.SI-ID 248285443
ISBN 978-961-6059-29-9 (PDF)

PREDGOVOR

Društvo ekonomistov Maribor je skupaj z Ekonomsko-poslovno fakulteto Univerze v Mariboru, Pravno fakulteto Univerze v Mariboru, Študentskim svetom Ekonomsko-poslovne fakultete Univerze v Mariboru in Študentskim svetom Pravne fakultete Univerze v Mariboru organiziralo študentsko posvetovanje Digitalna ekonomija in pravo 2025, posvetovanje o ekonomskih in pravnih izzivih digitalne preobrazbe, ki je potekalo 30. maja 2025 na daljavo s pomočjo aplikacije Microsoft Teams. Na študentskem posvetovanju je sodelovalo trinajst študentov Univerze v Ljubljani in Univerze v Mariboru. Ti so predstavili dvanajst znanstvenih prispevkov s področja digitalne ekonomije in prava, ki so jih napisali skupaj z visokošolskimi učitelji in sodelavci.

Študentsko posvetovanje je potekalo od 8.00 do 11.15, pri čemer so njegove udeležence pozdravili doc. dr. Dejan Romih, podpredsednik Društva ekonomistov Maribor, red. prof. dr. Borut Milfelner, prodekan za raziskovalno dejavnost Ekonomsko-poslovne fakultete Univerze v Mariboru, red. prof. dr. Janja Hojnik, prodekanica za znanstvenoraziskovalno dejavnost Pravne fakultete Univerze v Mariboru, študentka Pina Slaček, prodekanica za študentska vprašanja Ekonomsko-poslovne fakultete Univerze v Mariboru, in študentka Asja Lešnik, prodekanica za študentska vprašanja Pravne fakultete Univerze v Mariboru, ki so študentom in njihovim mentorjem zaželeli uspešno predstavitev.

Vsem soorganizatorjem in udeležencem študentskega posvetovanja iskreno čestitava, študentom pa želiva uspešno nadaljevanje študija.

Doc. dr. Dejan Romih in asist. Nejc Fir, urednika

KAZALO VSEBINE

PRVI DEL: DIGITALNA EKONOMIJA

Uporaba umetne inteligence v slovenskih podjetjih

Ana Bandur & Nejc Fir 11

Konkurenčnost slovenskih podjetij pri uporabi umetne inteligence: primerjalna analiza na agregatni ravni z državami EU

Gal Detiček & Nejc Fir 32

Merjenje negotovosti kibernetске varnosti v Združenih državah Amerike s pomočjo aplikacije Stanford Cable TV News Analyzer

Kaja Gartner Jovanović, Marko Možina & Dejan Romih 54

Vloga umetne inteligence pri povečevanju produktivnosti in njeni učinki na gospodarstvo: sistematični pregled literature

Nina Knez & Nejc Fir 62

(Sistemska) kibernetско tveganje in stres v ameriškem finančnem sistemu

Marko Možina & Dejan Romih 77

Ekonomska presoja investiranja v kibernetско varnost v izbranem zdravstvenem domu

Maruša Volavšek, Feliks Možina & Andreja Primec 85

DRUGI DEL: DIGITALNO PRAVO

Odgovornost delavca za uporabo orodja ChatGPT pri delu

Matej Makoter Rožmarin & Asja Lešnik 100

Dedovanje kriptovalut: pravni izzivi in praktične rešitve digitalne zapuščine

Veronika Mikl & Katja Drnovšek 108

Uporabnost tehnologije blockchain v zemljiški knjigi

Jovana Pajkowska & Kristjan Zahrastnik 129

Pravni vidiki zaščite zdravstvenih sistemov in podatkov: slovenski in evropski pristop

Žiga Rodošek & Andreja Primec 140

Problematika diskriminacije v zvezi z uporabo umetne inteligence pri zaposlovanju

Lisa Elizabeth Strouken & Aljoša Polajžar 159

Pravna vprašanja tokenizacije nepremičnin

Matej Velichkovski & Nataša Samec Berghaus 184

PRVI DEL: DIGITALNA EKONOMIJA



UPORABA UMETNE INTELIGENCE V SLOVENSКИH PODJETJIH

Ana Bandur, Univerza v Mariboru, Ekonomsko-poslovna fakulteta, Slovenija 

Asist. Nejc Fir, Univerza v Mariboru, Ekonomsko-poslovna fakulteta, Slovenija 

Povzetek: Umetna inteligenca je vse bolj prisotna v vseh gospodarskih dejavnostih, zato se z njeno uporabo na vsaj nekem področju sooča večina podjetij. Umetno inteligenco lahko podjetja vključujejo v delovne procese na različne načine, npr. pri prepoznavanju slik, generiranju naravnega jezika, prepoznavanju govora, besedilnem rudarjenju in pri avtomatizaciji procesov. Kljub množičnemu sprejemanju novih tehnologij se 77 % podjetij v vseh gospodarskih dejavnostih skupaj še zmeraj izogiba, najpogostejši razlog je pomanjkanje podpore vodstva in usposabljanj za uporabo umetne inteligenca. Kljub temu pa trenutno stanje v Sloveniji kaže na naraščajoč trend uporabe umetne inteligenca, pri čemer je največje povečanje zabeleženo pri tehnologijah za generiranje naravnega jezika.

Ključne besede: Evropska unija, gospodarske dejavnosti, konkurenčnost, Slovenija, umetna inteligenca

1 Uvod

Uporaba izraza umetna inteligenca (v nadaljevanju UI) se je izrazito povečala v preteklih letih in postala prisotna na različnih področjih našega življenja, vendar raziskovalci ne uporabljajo enotne definicije za opredelitev UI (Wang, 2019, str. 3). Schuett (2019) je mnenja, da je verjetno najbolj znana definicija UI tista, ki jo je podal Allan Turing leta 1950 z »igro posnemanja« oz. Turingovim testom. Omenjena definicija se glasi, da je UI vsak računalnik, ki opravi Turingov test. Slednji pa je opravljen, ko človeški sodnik ne more učinkovito ločiti med človekom in računalnikom, komunikacija pa lahko poteka le skozi besedilo.

Na podlagi taksonomije AI Watch lahko UI razdelimo na več področij, ki pokrivajo različne vidike njenega delovanja, razvoja in uporabe. V splošnem UI delimo glede na njene ključne zmožljivosti. Prva kategorija je razmišljanje in odločanje, ki zajema pretvarjanje podatkov v uporabno znanje in uporabo simboličnih pravil za sklepanje in optimizacijo. Druga kategorija pa učenje in zaznavanje, ki temelji na pridobivanju informacij in reševanju problemov na podlagi strukturiranih in nestrukturiranih podatkov ter prilagajanju in odzivanju na spremembe. Na podlagi te osnovne delitve lahko UI razčlenimo na več domen, ki jih razvrstimo na osrednje in prečne domene. Osrednjih pet domen predstavlja temeljne cilje UI, ki pokrivajo njene ključne tehnične vidike. Ti so razmišljanje, ki zajema avtomatsko sklepanje, načrtovanje s ciljem optimizacije, učenje, ki zajema strojno učenje, komunikacija, ki jo opredeljujeta razumevanje in generiranje besedila, in zaznavanje, ki vključuje računalniški vid za prepoznavanje obrazov in objektov ter obdelavo zvoka, torej zaznavanje govora in analiza zvoka. Prečne domene predstavljajo specifično področje raziskav, ampak pokrivajo širšo integracijo in uporabo UI. Med prečne domene so navedene integracija in interakcija, kamor spadajo avtonomna vozila in robotika, storitve UI, primer katerih so virtualni asistenti, ter etika in filozofija, ki se ukvarjata s transparentnostjo, varnostjo, in vplivom UI na družbo (European Commission, 2020).

Prispevek je sestavljen iz petih poglavij. V drugem poglavju smo analizirali pomen UI v različnih gospodarskih dejavnostih in vpliv na gospodarsko rast ter opravili pregled empirične literature. V tretjem poglavju smo analizirali izbrane kazalce uporabe UI v Sloveniji in EU za leti 2023 in 2024 glede na gospodarske dejavnosti. Pri analizi kazalcev UI smo uporabili opisno in komparativno metodo ter pri pregledu empirične literature metodo kompilacije. Analizo kazalcev UI na ravni gospodarskih dejavnosti smo opravili za zadnje razpoložljivo leto. V četrtem poglavju smo opravili

Wardovo metodo, s katero smo države EU razvrstili v skupine glede na izbrane kazalce uporabe UI. V petem poglavju smo predstavili sklepne ugotovitve.

2 Pomen UI v različnih gospodarskih dejavnostih in njen vpliv na gospodarsko rast

V današnjem svetu UI vpliva na številne gospodarske dejavnosti – ne izboljšuje le proizvodnje in preoblikuje obstoječih delovnih procesov, temveč tudi spodbuja nastajanje novih poklicev. UI med drugim izboljšuje procese odločanja in izkušnje potrošnikov, omogoča avtomatizacijo delovnih procesov in poenostavlja poslovanje. Vsi novi procesi in tehnologije pa hkrati zahtevajo vse več nujno potrebnih specialistov na področju upravljanja UI, kar prinaša tako priložnosti kot nenehne izzive (Ejjami, 2024).

UI je pomemben del širšega procesa digitalizacije in koncepta Industrija 4.0, ki predstavljata ključni gonili gospodarske rasti in konkurenčnosti. Inovacije na področju digitalizacije, vključno z UI, spodbujajo razvoj podjetij, držav in regij. EU prepoznava strateško vlogo UI za prihodnji gospodarski razvoj, kar se odraža v finančni podpori preko programov, kot je »The Digital Europe Programme«. Implementacija rešitev Industrija 4.0, ki vključuje UI, prinaša priložnosti za trajnostni razvoj in povečanje učinkovitosti proizvodnje, kar posledično prispeva h gospodarski rasti in širitvi trgov. UI je zato kot del digitalne transformacije ključna za izboljšanje konkurenčnosti, spodbujanje inovativnosti in zagotavljanje dolgoročnega gospodarskega razvoja v EU (Brodny, 2022). Tehnološki napredek in posledično UI povečujeta produktivnost s tem, ko omogočata večjo učinkovitost in natančnost ter manj zamud, zlasti v predelovalni gospodarski dejavnosti. Ena izmed razlag, zakaj uporaba UI v podjetjih povečuje gospodarsko rast, je njena široka uporabnost v vseh gospodarskih dejavnostih (Gonzales, 2023).

Aghion idr. (2017) so proučevali vpliv UI na gospodarsko rast. UI omogoča avtomatizacijo številnih intelektualnih nalog, ki so bile do nedavnega izvedljive samo s človeškim delom. Avtorji se sprašujejo, ali lahko UI povzroči hitrejšo gospodarsko rast. Prav tako jih zanima, ali bo gospodarska rast ostala stabilna, kot je bil zabeležen zgodovinski trend do sedaj. Eksponentna rast se bo zgodila, če UI omogoči avtomatizacijo raziskovalnih procesov, kot je generiranje novih idej, in ne zgolj avtomatizacijo proizvodnje. To lahko vodi v t. i. singularnost oz. eksplozivno rast, ki povzroča rast dohodka brez omejitev. Drugi scenarij omenja, da bo gospodarska rast ostala relativno konstantna oz. stabilna, saj jo omejuje Baumolov učinek, ki ga literatura imenuje tudi kot t. i. Baumolova stroškovna bolezen (angl. *Baumol's cost disease*). Baumolov učinek (Baumol, 1967, povzeto

po Aghion idr., 2017, str. 3) opisuje, da gospodarska rast ni omejena na tiste gospodarske dejavnosti, ki beležijo največjo rast produktivnosti, ampak jo je mogoče prenesti tudi na tiste gospodarske dejavnosti, pri katerih je produktivnost najtežje povečati. Če UI avtomatizira večino proizvodnje in nekatere storitve, bodo gospodarske dejavnosti, kjer UI ni najučinkovitejša, zavirale gospodarsko rast. Sklepamo lahko, da UI lahko poveča gospodarsko rast, če ji uspe avtomatizirati tudi gospodarske dejavnosti z nizko rastjo produktivnosti.

3 Uporaba UI v gospodarskih dejavnostih

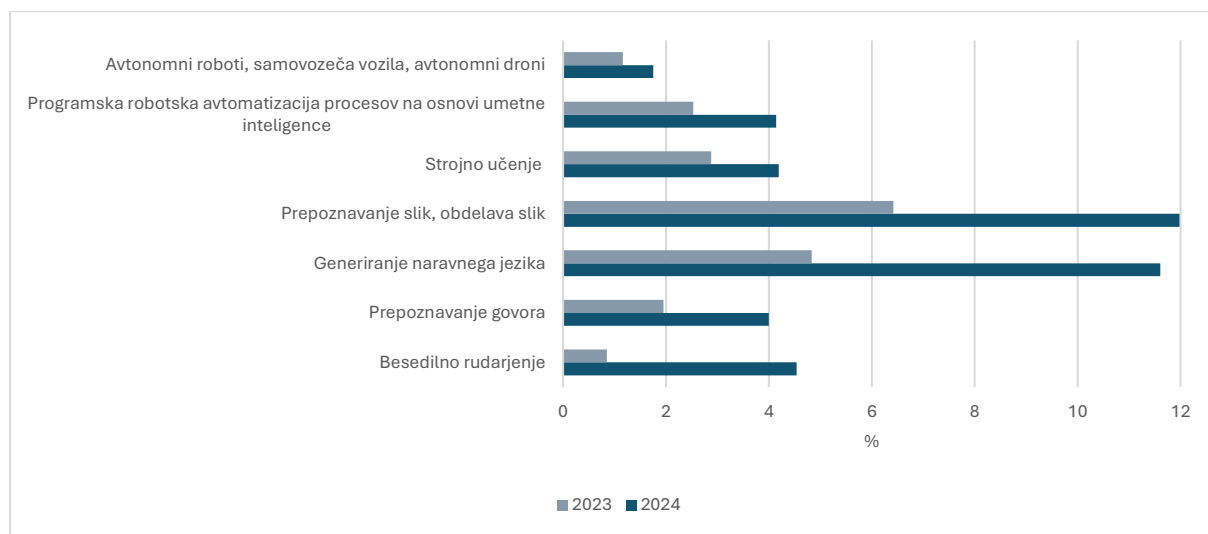
V analizi smo upoštevali podjetja z desetimi ali več zaposlenimi, pri čemer smo se zaradi obsežnega nabora možnih kazalcev omejili na izbrane kazalce uporabe UI. Omejitve se nanašajo tudi na leti 2023 in 2024, saj ni na voljo dovolj podatkov za analizo časovnih serij. Proučevali smo kazalce za Slovenijo in povprečje EU. Podatke smo analizirali na ravni gospodarskih dejavnosti, in sicer po kvalifikaciji Nace Rev. 2¹. Vse podatke za primerjavo kazalcev UI po gospodarskih dejavnostih smo pridobili v podatkovni bazi Eurostat. Podatki o uporabi informacijsko-komunikacijske tehnologije in e-poslovanju v podjetjih se zbirajo letno s pomočjo anket, ki jih izvajajo nacionalni statistični uradi na podlagi letnih modelnih vprašalnikov Eurostata. Ciljna populacija zajema podjetja z desetimi ali več zaposlenimi in samozaposlenimi osebami, medtem ko so manjša podjetja vključena prostovoljno. Za zagotovitev reprezentativnosti se običajno uporablja stratificirano naključno vzorčenje, zbrane podatke pa podrobno validira Eurostat (Eurostat, 2024a).

Na sliki 1 smo primerjali delež slovenskih podjetij iz leta 2023, ki so uporabljala tehnologije UI, z deležem podjetij iz leta 2024. Opazimo lahko, da se je delež podjetij, ki uporabljajo tehnologijo UI za analizo pisnega jezika oz. t. i. besedilno rudarjenje, iz leta 2023 v leto 2024 povečal za 3,6 odstotne točke. Največje povečanje uporabe se opazi pri tehnologiji za generiranje pisnega ali govornega jezika oz. t. i. generiranje naravnega jezika, ki je beležilo povečanje za 6,8 odstotne točke. Najmanjšo spremembo lahko opazimo pri tehnologijah za omogočanje fizičnega gibanja strojev preko avtonomnih odločitev na podlagi opazovanja okolice oz. t. i. avtonomnih robotih, samovozečih vozilih in avtonomnih dronih. Leta 2023 je to tehnologijo UI uporabljalo 1,2 % slovenskih

¹ Omenjena delitev gospodarskih dejavnosti po Nace Rev. 2. je naslednja (Braunsberger, 2010): C – predelovalna dejavnost, E - oskrba z vodo; ravnanje z odpadki in odpadki; saniranje okolja, F – gradbeništvo, G - trgovina; vzdrževanje in popravila motornih vozil, H - promet in skladiščenje, I – gostinstvo, J - informacijske in komunikacijske dejavnosti, M – strokovne, znanstvene in tehnične dejavnosti, N – druge raznovrstne poslovne dejavnosti.

podjetij, leta 2024 pa za 0,6 odstotne točke več podjetij oz. 1,8 % slovenskih podjetij. Pri večjem delu tehnologij UI opazimo podoben trend naraščanja, in sicer je med letoma 2023 in 2024 bilo zabeleženo dvakratno povečanje deleža podjetij, ki te tehnologije uporabljajo. Podobne ugotovitve navaja SURS (2024), ki je zabeležil, da je tehnologije UI leta 2024 uporabljalo 21 % podjetij, kar predstavlja skoraj dvakrat večji delež kot v predhodnem letu, ko jih je uporabljalo 11 % podjetij.

Slika 1: Delež slovenskih podjetij, ki v svoj proces implementira posamezne tehnologije UI



Vir podatkov: (Eurostat, 2025a).

Konkurenčnost slovenskih podjetij smo merili z različnimi kazalci UI. Opravili smo primerjavo gospodarskih dejavnosti po klasifikaciji Nace Rev. 2. Za vsako proučevano gospodarsko dejavnost smo najprej predstavili podatke za Slovenijo in nato za povprečje EU. Ob posameznih gospodarskih dejavnostih smo proučevali tudi skupne vrednosti za proučevane gospodarske dejavnosti².

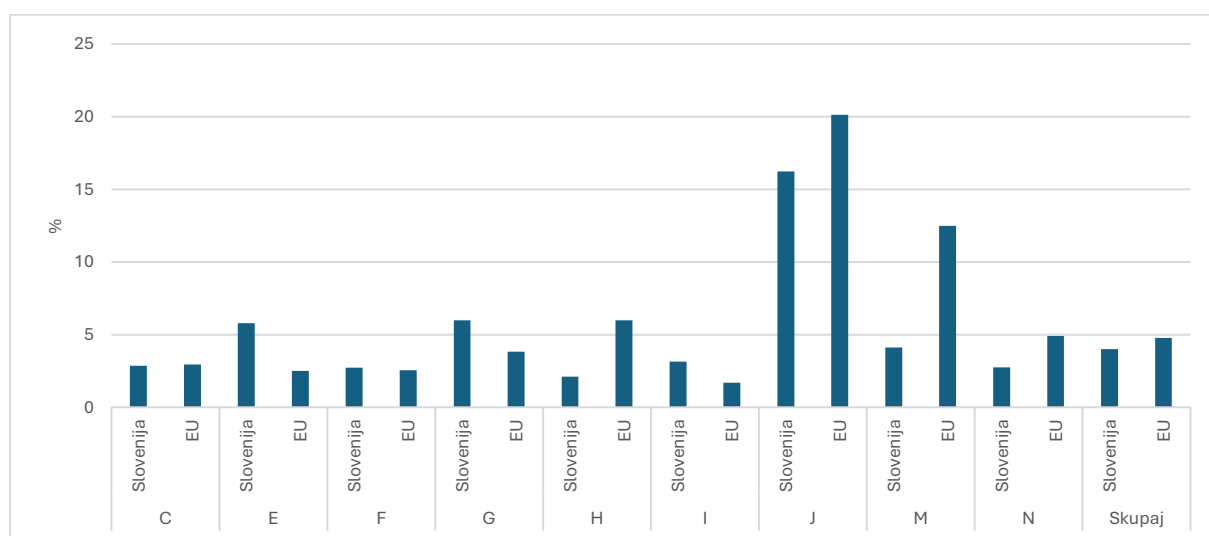
Na slikah 2, 3, 4 in 5 smo podrobneje prikazali nekatere izmed kazalcev UI s slike 1. Na sliki 2 je prikazan delež podjetij, ki uporablja tehnologijo UI za prepoznavanje govora v posameznih gospodarskih dejavnostih v Sloveniji in EU. Izstopa gospodarska dejavnost J (informacijske in komunikacijske dejavnosti), v kateri 16,2 % slovenskih podjetij uporablja tehnologijo UI za prepoznavanje govora. V Sloveniji ima gospodarska dejavnost J največji delež podjetij, ki uporablja to tehnologijo UI. Nemčija je s 30 % podjetij z uporabo UI za prepoznavanje govora vodilna država v gospodarski

² Izpustili smo gospodarske dejavnosti kmetijstvo, gozdarstvo, ribolov, rudarstvo, kamnolom in finančne gospodarske dejavnosti, za katere podatki niso bili dostopni.

dejavnosti J. V ostalih gospodarskih dejavnostih v Sloveniji se delež podjetij, ki uporabljajo to tehnologijo UI, giblje med 2 in 5 %. Od povprečja EU Slovenija najbolj navzdol odstopa v gospodarski dejavnosti M (strokovne, znanstvene in tehnične dejavnosti), in sicer zaostaja za 8,4 odstotne točke za povprečjem EU.

Zelo pogost trend v večjih korporacijah, kot so Amazon, Google in Microsoft, je uporaba tehnologij UI za prepoznavanje govora. Te tehnologije uporabljajo pri oblikovanju digitalnih asistentov, primeri teh so Amazon Echo, Google Home in Siri. Za izboljšanje uporabniške izkušnje morajo oblikovalci teh digitalnih asistentov nadgraditi zaznavanje različnih naglasov in blokiranje šumov iz ozadja. Digitalni asistent, integriran v mobilni telefon, kot je npr. Siri, uporabniku omogoča predvajanje glasbe, nastavljanje opomnikov, iskanje informacij po spletu in mnogo drugih spletnih aktivnosti (Mohammad, 2020).

Slika 2: Podjetja, ki uporabljajo tehnologije UI za pretvorbo govornega jezika v strojno berljiv format (prepoznavanje govora) v gospodarskih dejavnostih po klasifikaciji Nace Rev. 2 za leto 2024



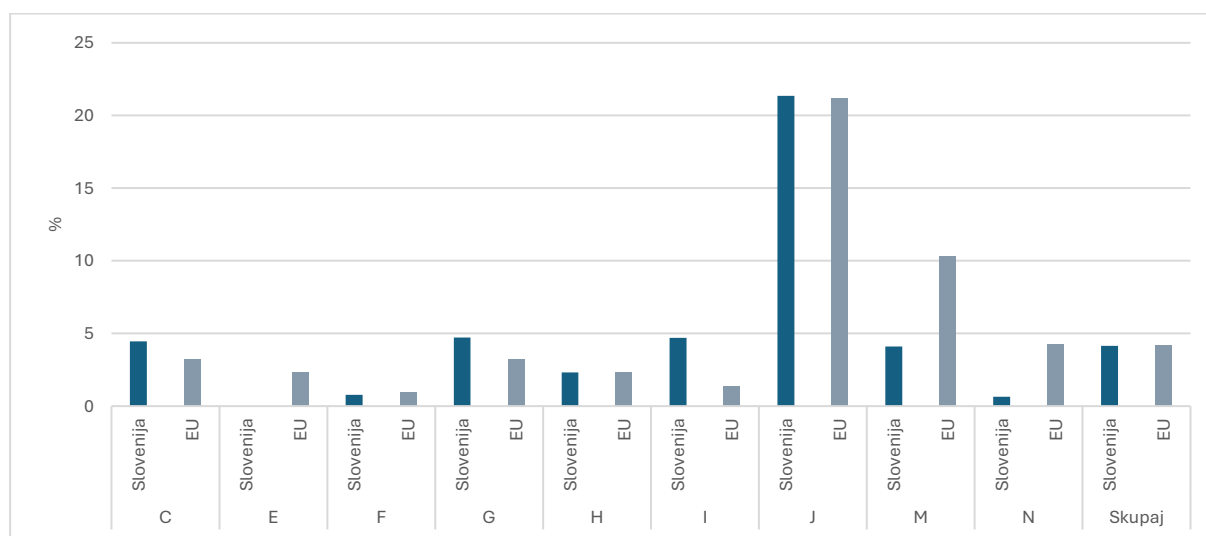
Vir podatkov: (Eurostat, 2025b).

Eden izmed kazalcev konkurenčnosti podjetij pri uporabi UI, ki je prikazan na sliki 3, je programska robotska avtomatizacija procesov. V Sloveniji je po podatkih za leto 2024 največji delež podjetij, ki so uporabljala to tehnologijo UI, v gospodarski dejavnosti J. Naslednja gospodarska dejavnost z največjim deležem podjetij, ki uporabljajo UI za programsko robotsko avtomatizacijo procesov, je gospodarska dejavnost G (trgovina; vzdrževanje in popravila motornih vozil) s 4,7 % podjetij. V gospodarski dejavnosti E (oskrba z vodo; ravnanje z odplakami in odpadki; saniranje okolja) pa

slovenska podjetja ne uporabljajo te tehnologije UI, medtem ko je delež podjetij, ki implementirajo to tehnologijo UI, v EU 2,3-odstoten. V gospodarski dejavnosti M je vodilna država Finska z 21-odstotnim deležem podjetij, kar je za 17 odstotnih točk večji delež podjetij kot v Sloveniji.

Alam idr. (2025, str. 30) omenjajo, da se povečuje avtomatizacija delovnih mest, kjer delavci opravljajo ponavljajoča se opravila ali vnašajo vhodne podatke. UI predvsem v predelovalni dejavnosti povečuje učinkovitost in natančnost dela. Brez delovnih mest bodo ostali nizko kvalificirani delavci, ki so do zdaj opravljali delo, ki ga bo v prihodnje popolnoma nadomestila UI, povečalo pa se bo povpraševanje po visoko kvalificirani delovni sili. Nove priložnosti bodo na področju vzdrževanja strojev, robotov in programske opreme. Avtor navaja, da druge raziskave kažejo, da bo tehnologija UI nadomestila človeka tudi v skladiščih in logističnih centrih, kjer se bodo uporabljala samovozeča vozila in bodo zaloge nadzorovane prav tako s pomočjo UI.

Slika 3: Podjetja, ki uporabljajo tehnologije UI za avtomatizacijo različnih delovnih procesov ali pomoč pri odločanju (programska robotska avtomatizacija procesov) v gospodarskih dejavnostih po klasifikaciji Nace Rev. 2 za leto 2024



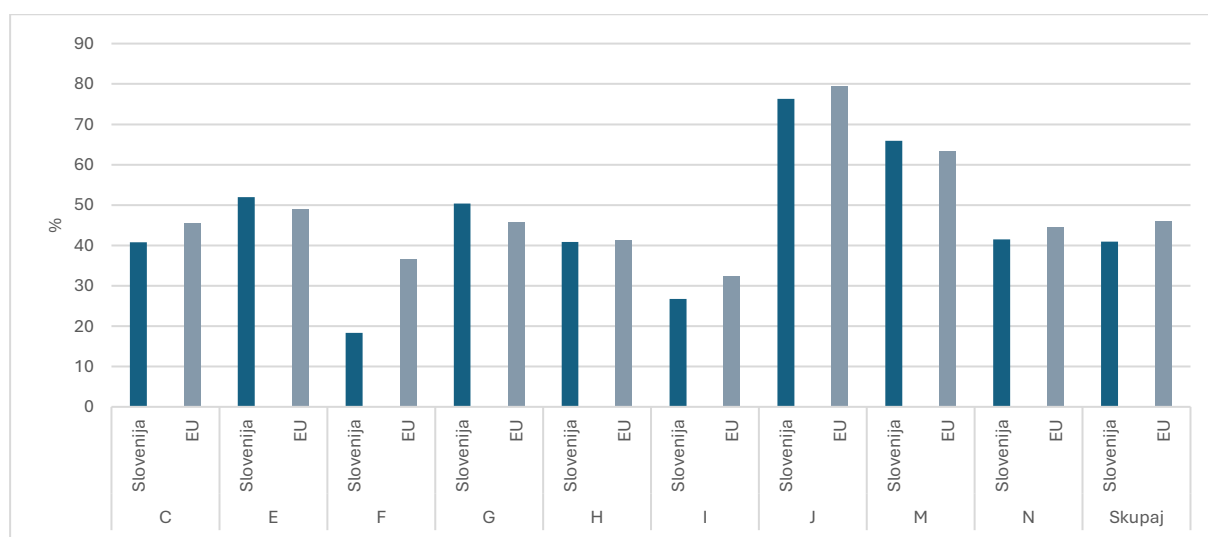
Vir podatkov: (Eurostat, 2025b).

V Sloveniji ponovno izstopa gospodarska dejavnost J, ki beleži 76,3 % podjetij, ki uporabljajo tehnologije UI ali kupujejo napredne ali vmesne storitve računalništva v oblaku ali izvajajo analitiko podatkov (slika 4). V vseh gospodarskih dejavnostih skupaj delež podjetij, ki uporabljajo to tehnologijo UI, znaša 40,9 %. Pri primerjavi deležev podjetij, ki uporabljajo to tehnologijo UI (slika 4) z ostalimi proučevanimi kazalci (sliki 2 in 3), opazimo, da je delež podjetij pri tem kazalcu v vseh

gospodarskih dejavnostih skupaj za desetkrat večji. Če vzamemo za primer gospodarsko dejavnost J na sliki 3 in 4, je na sliki 4 delež slovenskih podjetij, ki uporabljajo to tehnologijo UI za kar 3,6-krat večji kot na sliki 3. V gospodarski dejavnosti J je od vseh držav EU najuspešnejša Finska s 97-odstotnim deležem podjetij. Slovenija je beležila večji delež podjetij od povprečja EU le v gospodarskih dejavnostih E, G in M.

Vse pogostejše na tem področju tehnologij UI so pametne tovarne z arhitekturo CaSF (Cloud and AI-based Smart Factory), ki je razdeljena na več slojev. Arhitektura CaSF omogoča prepletanje pametnih naprav, kot so robotske roke, uporabo brezžičnega omrežja za prenos podatkov med pametnimi napravami in oblakom, uporabo oblaka za shranjevanje podatkov, pridobljenih iz naprav, in nadziranje procesov, kot so vzdrževanje, optimizacija in načrtovanje. Pametne tovarne uvajajo temeljite spremembe v tradicionalni proizvodni industriji, kar jim omogoča prilagajanje spreminjajočim se tržnim zahtevam (Hua, 2018).

Slika 4: Podjetja uporabljajo tehnologije UI ali kupujejo napredne ali vmesne storitve računalništva v oblaku ali izvajajo analitiko podatkov iz katerega koli vira med naslednjimi – E_DASWEB, E_DASLOC, E_DASSDS, E_DASGOV in E_DASSAT – v gospodarskih dejavnostih po klasifikaciji Nace Rev. 2 leta 2023



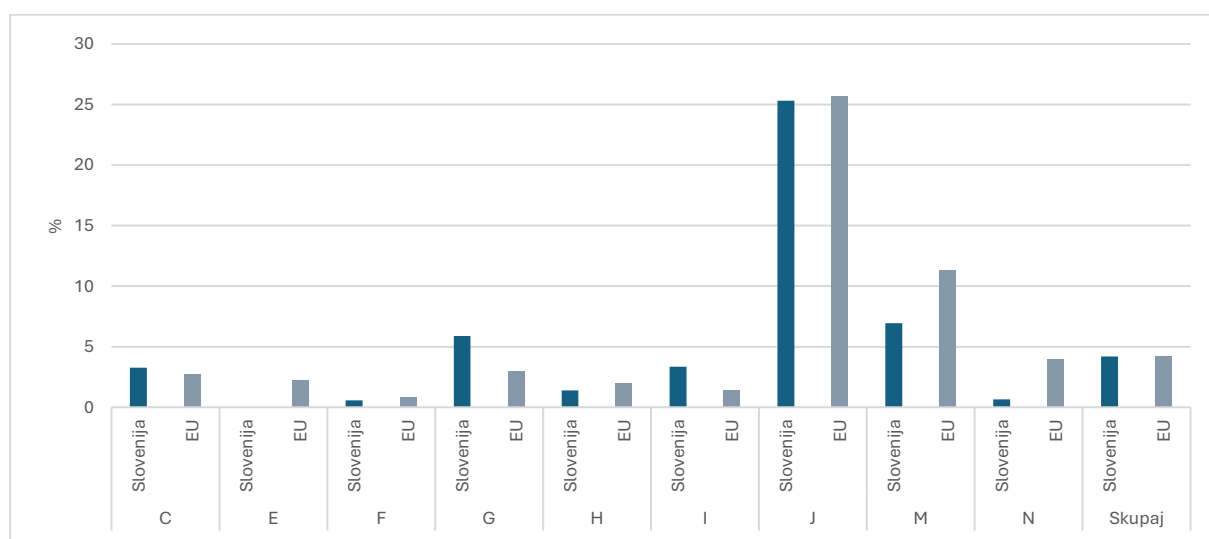
Vir podatkov: (Eurostat, 2025b).

Na sliki 5 smo analizirali uporabo strojnega učenja v slovenskih in evropskih podjetjih. Izmed vseh gospodarskih dejavnosti najbolj izstopa J, v kateri 25,3 % podjetij v Sloveniji in 25,7 % podjetij v EU implementira strojno učenje v svoje poslovne procese, največji delež v tej gospodarski dejavnosti

ima Hrvaška z 39-odstotnim deležem podjetij, ki uporabljajo strojno učenje. Podjetja v gospodarski dejavnosti E v Sloveniji te tehnologije UI ne uporabljajo. Relativno nizke deleže podjetij, ki uporabljajo strojno učenje v svojih poslovnih procesih, lahko opazimo v gospodarski dejavnosti F (gradbeništvo) z 0,57 % podjetij in v gospodarski dejavnosti N (druge raznovrstne poslovne dejavnosti) z 0,64 % podjetij. Delež podjetij, ki uporablja strojno učenje, je v vseh treh gospodarskih dejavnostih pod povprečjem EU, pri čemer za povprečjem EU najbolj zaostaja gospodarska dejavnost N za 3,3 odstotne točke.

Soleman (2024) navaja, da strojno učenje pomembno prispeva h gospodarski dejavnosti H (promet in skladiščenje), saj pomaga pri prepoznavanju objektov v avtonomnih vozilih in omogoča hitro in natančno zaznavanje cestnih razmer ter ustrezno odzivanje. S tem globoko učenje ne izboljšuje le operativne učinkovitosti, temveč tudi povečuje varnost in udobje uporabnikov tehnologije.

Slika 5: Podjetja, ki uporabljajo strojno učenje (globoko učenje) za analizo podatkov v gospodarskih dejavnostih po klasifikaciji Nace Rev. 2 za leto 2024



Vir podatkov: (Eurostat, 2025b).

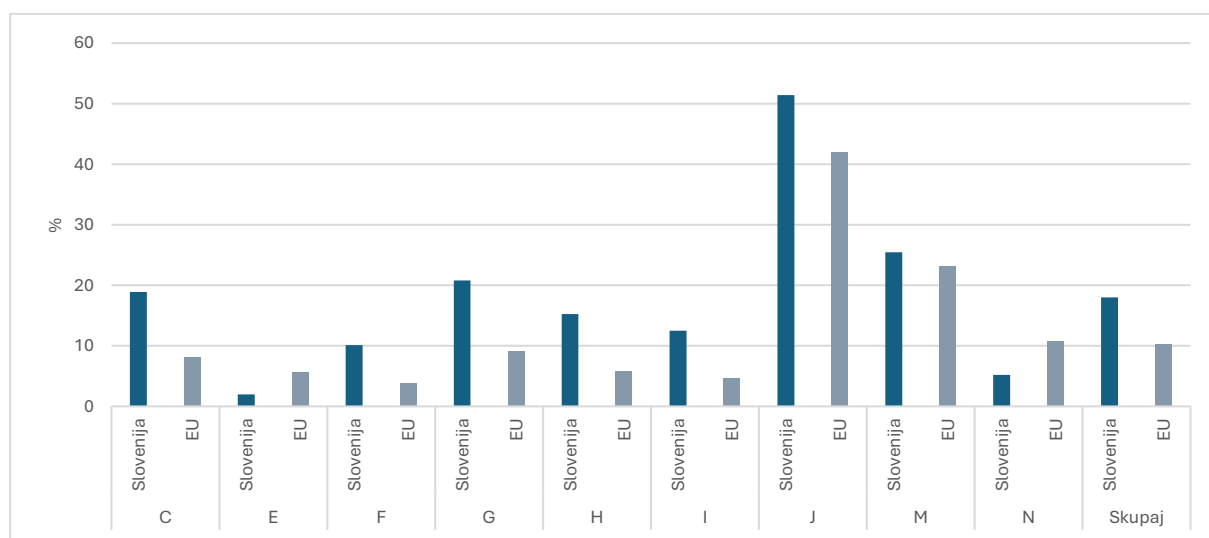
Slike 6, 7 in 8 prikazujejo delež podjetij leta 2024, ki so uporabljala tehnologijo UI zaradi vsaj enega, dveh ali treh namenov³. Po raziskavah McKinsey & Company podjetja največ uporabljajo tehnologijo UI pri trženju in prodaji, kar lahko povežemo z namenom AI_PBAM (podjetja, ki uporabljajo

³ Ti nameni pa so: AI_PMS – podjetja, ki uporabljajo UI za trženje ali prodajo; AI_PPP – podjetja, ki uporabljajo UI za proizvodni proces; AI_PBAM – podjetja, ki uporabljajo UI za upravljanje ali administracijo; AI_PLOG – podjetja, ki uporabljajo UI za logistiko; AI_PITS – podjetja, ki uporabljajo UI za varnost informacijsko-komunikacijske tehnologije;

UI za upravljanje ali administracijo), in pri razvoju izdelkov in storitev. To sta dve funkciji uporabe, pri katerih so prejšnje raziskave pokazale, da lahko uvajanje tehnologije UI prinese največ dodane vrednosti (Singla, 2024).

Mohammad (2020) opisuje obstoj novih tehnologij UI, kot so globoko učenje, tehnologija za prepoznavanje govorenja, tehnologija za generiranje naravnega jezika in mehansko učenje. Predstavi tudi razloge uporabe teh tehnologij v podjetjih v najrazličnejših gospodarskih dejavnostih. Omenjeni so personalizirano oglaševanje (AI_PBAM), komunikacija s strankami in izboljšanje storitev (AI_PITS), odkrivanje in preprečevanje prevar (AI_PFIN) in avtomatsko pakiranje z robotskimi napravami (AI_PMS). Vse nove tehnologije UI so izjemno pomembne pri poslovanju, izobraževanju in komunikaciji.

Slika 6: Podjetja, ki uporabljajo tehnologije UI zaradi vsaj enega od naslednjih namenov – AI_PMS, AI_PPP, AI_PBAM, AI_PLOG, AI_PITS, AI_PFIN, AI_PRDI – v gospodarskih dejavnostih po klasifikaciji Nace Rev. 2 za leto 2024



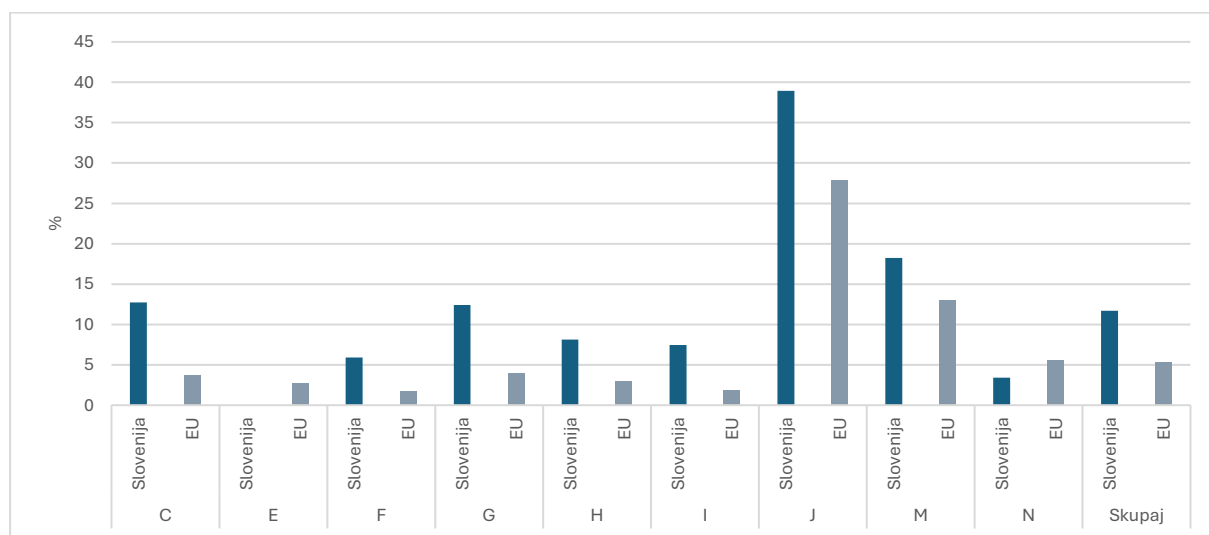
Vir podatkov: (Eurostat, 2025b).

Delež podjetij, ki uporabljajo tehnologije UI zaradi vsaj dveh od namenov v vseh gospodarskih dejavnostih, se zmanjšuje v primerjavi s podjetji, ki uporabljajo tehnologije UI zaradi vsaj enega od namenov. Na sliki 7 lahko opazimo podoben trend kot na sliki 6, največji delež podjetij, ki uporabljajo tehnologije UI zaradi vsaj enega ali vsaj dveh namenov, je v gospodarski dejavnosti J. Delež

AI_PFIN – podjetja, ki uporabljajo UI za računovodstvo, kontroling, finančno upravljanje; AI_PRDI – podjetja, ki uporabljajo UI za raziskave in razvoj, inovacije (Eurostat, 2024c).

podjetij v tej dejavnosti znaša skoraj 40 %, medtem ko v dejavnosti E slovenska podjetja ne uporabljajo tehnologij UI zaradi vsaj dveh od naštetih namenov.

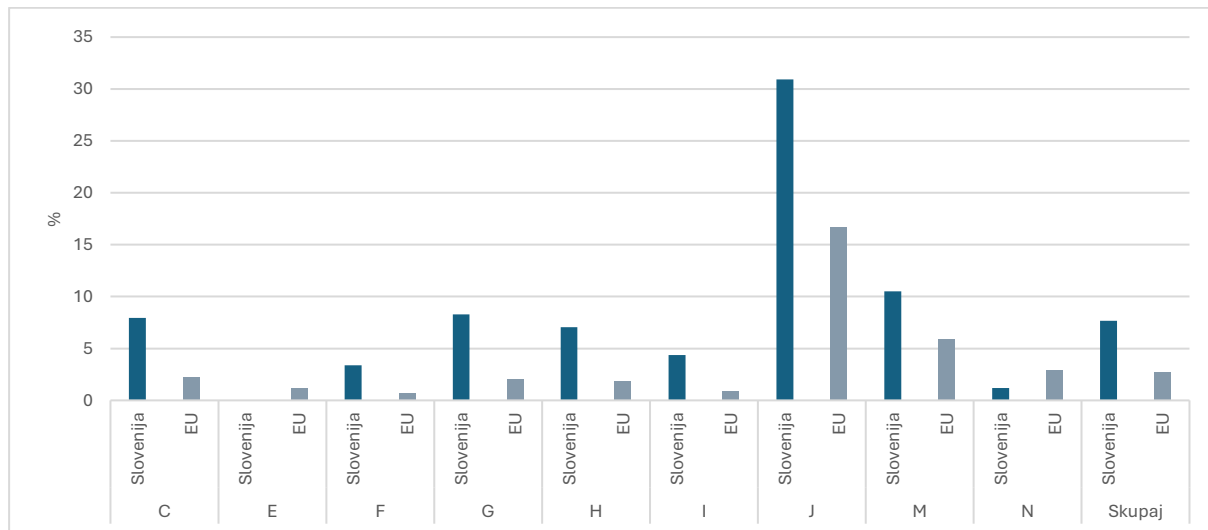
Slika 7: Podjetja, ki uporabljajo tehnologije UI zaradi vsaj dveh od naslednjih namenov – AI_PMS, AI_PPP, AI_PBAM, AI_PLOG, AI_PITS, AI_PFIN, AI_PRDI – v gospodarskih dejavnostih po klasifikaciji Nace Rev. 2 za leto 2024



Vir podatkov: (Eurostat, 2025b).

Največ podjetij v Sloveniji in EU, ki uporabljajo UI zaradi vsaj treh od naštetih namenov (slika 8), je v gospodarski dejavnosti J s 30,9-odstotnim deležem podjetij v Sloveniji in 16,7-odstotnim deležem podjetij v EU. V Sloveniji so najslabše zastopana podjetja v gospodarski dejavnosti E, v kateri sploh nobeno podjetje ne uporablja UI zaradi vsaj treh ali več namenov. Enako je razvidno s slike 7, kjer prav tako v gospodarski dejavnosti E nobeno podjetje ne uporablja UI zaradi vsaj dveh namenov. 1,97 % slovenskih podjetij v gospodarski dejavnosti J pa uporablja UI zaradi vsaj enega namena (slika 6). Slovenija je bila leta 2024 država z največjim deležem podjetij, in sicer 7,68-odstotnim, ki uporabljajo tehnologije UI zaradi vsaj treh od namenov gledano v vseh gospodarskih dejavnostih, sledila ji je Belgija s 7,34 % in nato Finska s 6,44 % podjetij.

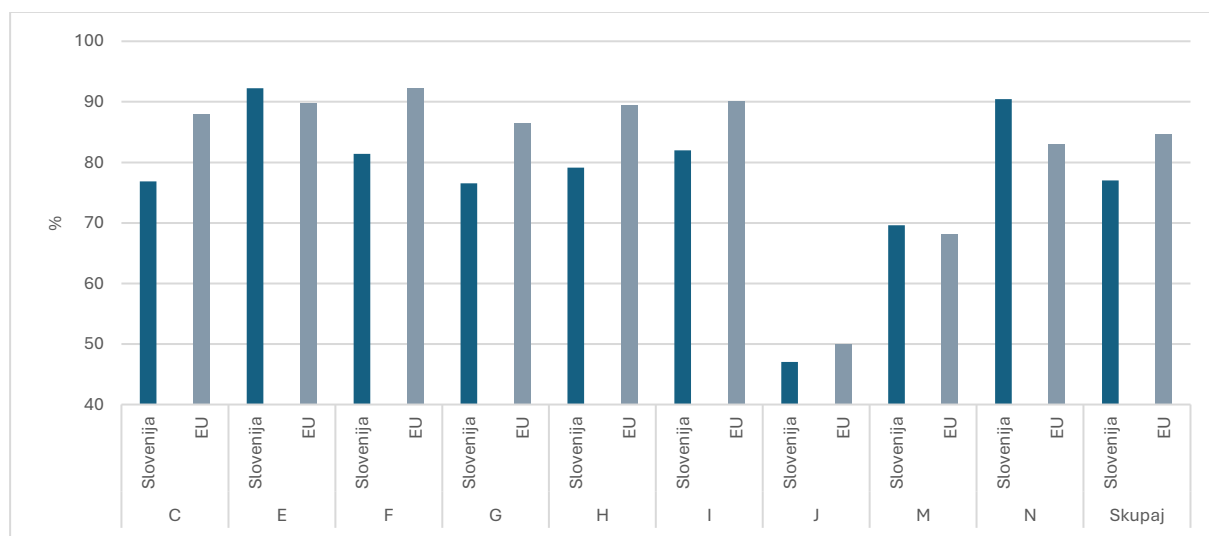
Slika 8: Podjetja, ki uporabljajo tehnologije UI zaradi vsaj treh od naslednjih namenov – AI_PMS, AI_PPP, AI_PBAM, AI_PLOG, AI_PITS, AI_PFIN, AI_PRDI – v gospodarskih dejavnostih po klasifikaciji Nace Rev. 2 za leto 2024



Vir podatkov: (Eurostat, 2025b).

S slike 9 je razvidno, da v Sloveniji 77 % vseh podjetij ne uporablja nobene izmed tehnologij UI. Najmanjši delež slovenskih podjetij je v gospodarski dejavnosti J s 47 % podjetij, kar je še vedno za 15,5 odstotne točke več podjetij kot na Švedskem, kjer UI ne uporablja 31,5 % podjetij. Najmanj pa se tehnologije UI uporabljajo v sektorju E, in sicer 92,2 % podjetij v Sloveniji ne uporablja nobene izmed tehnologij UI, medtem ko na Cipru nobeno podjetje v tej gospodarski dejavnosti ne uporablja nobene izmed tehnologij UI.

Slika 9: Delež podjetij, ki ne uporabljajo nobene izmed tehnologij UI (AI_TTM, AI_TSR, AI_TNLG, AI_TIR, AI_TML, AI_TPA, AI_TAR4) v gospodarskih dejavnostih po klasifikaciji Nace Rev. 2 za leto 2024



Vir podatkov: (Eurostat, 2025b).

Razlogov za izogibanje UI v podjetjih je veliko, Ivchyk (2024) navaja kot glavne ovire psihološke, organizacijske in etične. Pogosta vidika psiholoških ovir sta strah pred izgubo delovnih mest in nezaupanje v sisteme UI. Med organizacijskimi ovirami navaja pomanjkanje podpore vodstva in premalo usposabljanj za pripravo zaposlenih na uporabo UI. Kot tretje področje omenja etične ovire. Primeri etične ovire so pomisleki glede pristranskosti informacij, problematika glede zasebnosti podatkov in vprašanje, kdo je odgovoren za napake, ki jih naredi UI.

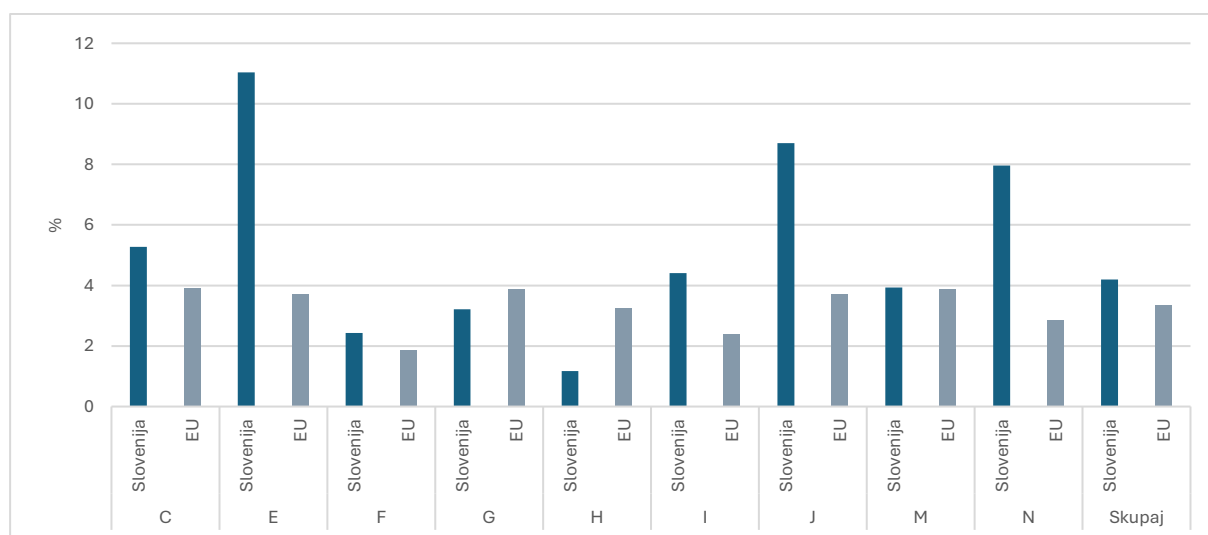
S slike 10 je razvidno, da so deleži podjetij, ki ne uporabljajo tehnologije UI zaradi prevelikih stroškov, v Sloveniji po večini gospodarskih dejavnostih majhni, izstopa le gospodarska dejavnost E z

⁴ Omenjene tehnologije UI so AI_TTM – podjetja, ki uporabljajo tehnologije UI za analizo pisanega jezika (rudarjenje besedil), AI_TSR – podjetja, ki uporabljajo tehnologije UI za pretvorbo govornega jezika v strojno berljivo obliko (prepoznavanje govora), AI_TNLG – podjetja, ki uporabljajo tehnologije UI za generiranje pisanega ali govornega jezika (generiranje naravnega jezika), AI_TIR – podjetja, ki uporabljajo tehnologije UI za prepoznavanje objektov ali oseb na podlagi slik (prepoznavanje slik, obdelava slik), AI_TML – podjetja, ki uporabljajo strojno učenje (npr. globoko učenje) za analizo podatkov, AI_TPA – podjetja, ki uporabljajo tehnologije UI za avtomatizacijo različnih delovnih tokov ali pomoč pri odločanju (robotska avtomatizacija procesov na osnovi UI), AI_TAR – podjetja, ki uporabljajo tehnologije UI, ki omogočajo fizično gibanje strojev prek avtonomnih odločitev na podlagi opazovanja okolice (avtonomni roboti, samovozeča vozila, avtonomni droni) (Eurostat, 2024c).

11 % podjetij, sledi gospodarska dejavnost J z 8,7 % podjetij in N z 8 % podjetij, ki sploh ne uporabljajo tehnologij UI zaradi prevelikih stroškov. Sklepamo lahko, da primarni razlog za neuporabo tehnologij UI ni v prevelikih stroških, saj so odstotki podjetij, ki ne uporabljajo tehnologij UI zaradi prevelikih stroškov relativno nizki.

Statistični urad Republike Slovenije (2024) navaja še druge razloge za neuporabo tehnologij UI v podjetjih z desetimi ali več zaposlenimi in samozaposlenimi. Kot najpogostejši razlog je omenjeno primanjkovanje ustreznega strokovnega znanja v podjetju, pri čemer je za leto 2024 65 % podjetij, ki navajajo omenjeno oviro. Ostali pomembni razlogi so še pomisleki glede kršitve varstva osebnih podatkov in zasebnosti, nejasnih pravnih posledic, med katere sodi npr. odgovornost za škodo, in nezdružljivost tehnologij z obstoječo programsko opremo.

Slika 10: Delež podjetij, ki ne uporabljajo nobene izmed tehnologij UI zaradi prevelikih stroškov v gospodarskih dejavnostih po klasifikaciji Nace Rev. 2 za leto 2024

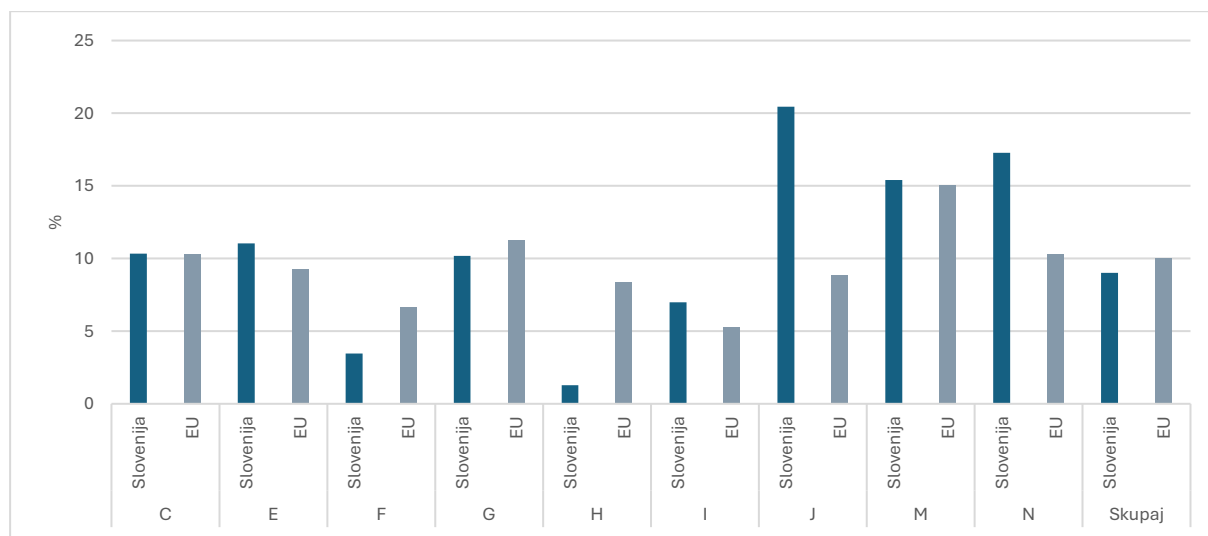


Vir podatkov: (Eurostat, 2025b).

S slike 11 je razvidno, da je v gospodarski dejavnosti J v Sloveniji največji delež podjetij, ki so že razmišljala o uporabi ene izmed tehnologij UI, in sicer 20,4 % podjetij, najmanjši delež podjetij, ki je razmišljalo o uvedbi tehnologij UI pa je v gospodarski dejavnosti H, in sicer 1,3 % podjetij. V gospodarski dejavnosti M je 15,4 % slovenskih podjetij že razmišljalo o uvedbi tehnologije UI, kar je za 0,4 odstotne točke več kot v povprečju EU in 5,6 odstotne točke manj kot na Danskem, kjer je o uvedbi razmišljalo 21 % podjetij.

1. avgusta 2024 je vstopil v veljavo Akt o umetni inteligenci, ki se bo v celoti začel uporabljati 2. avgusta 2026. Cilj Akta je izboljšanje delovanja notranjega trga z določitvijo enotnega pravnega okvira za uporabo UI v EU. Akt želi spodbuditi slovenska podjetja k uporabi UI, s tem ko poskuša vplivati na zaupanje v tehnologije UI (Vlade Republike Slovenije, 2024).

Slika 11: Podjetja, ki so kadar koli že razmišljala o uporabi ene izmed tehnologij UI (AI_TTM, AI_TSR, AI_TNLG, AI_TIR, AI_TML, AI_TPA, AI_TAR) v gospodarskih dejavnostih po klasifikaciji Nace Rev. 2 za leto 2024

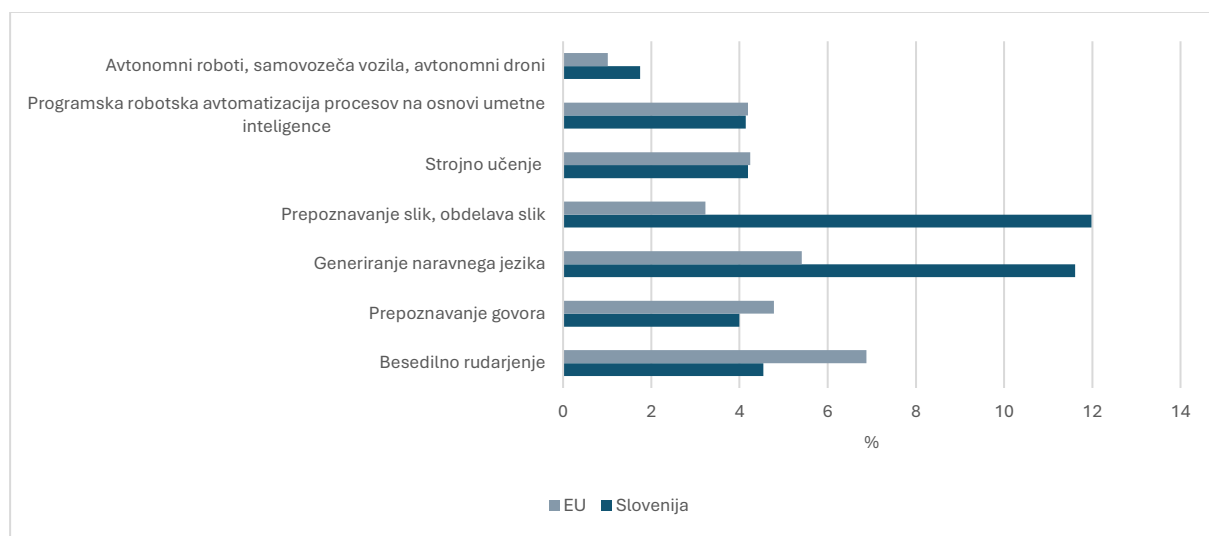


Vir podatkov: (Eurostat, 2025b).

Na sliki 12 smo primerjali podatke o tem, katere tehnologije UI uporabljata Slovenija in EU in kako se razlikujejo deleži podjetij, ki te tehnologije UI uporabljajo. Slovenija ima večje deleže od EU pri treh kazalcih, in sicer pri uporabi avtonomnih robotov, samovozečih vozil in avtonomnih dronov ter pri prepoznavanju slik, obdelavi slik in generiranju naravnega jezika. Največjo razliko lahko opazimo pri uporabi tehnologije UI za prepoznavanje in obdelavo slik, pri kateri ima Slovenija za 8,8 odstotne točke večji delež podjetij, ki implementirajo to tehnologijo UI. Slovenija najbolj zaostaja za EU pri uporabi tehnologij UI za besedilno rudarjenje, in sicer za 2,3 odstotne točke od povprečja EU.

V Sloveniji največ podjetij uporablja UI za prepoznavanje in obdelavo slik. Primer takšne tehnologije UI je model, imenovan NutriNet, ki povezuje tehnologije globokega učenja in prepoznavanja slik. To je prvi avtomatski sistem za prepoznavanje slik lažne hrane in pijače s kar 92,18-odstotno natančnostjo. Kot merilo natančnosti je uporabljena natančnost na ravni slikovnih točk (pixel accuracy), ki šteje število pravilno klasificiranih slikovnih točk (Mezgec & Koroušić Seljak, 2019).

Slika 12: Primerjava Slovenije in Evropske unije po deležu podjetij z destimi ali več zaposlenimi, ki uporabljajo različne tehnologije UI za leto 2024



Vir podatkov: (Eurostat, 2025b).

4 Združevanje držav v skupine glede na izbrane kazalce uporabe UI

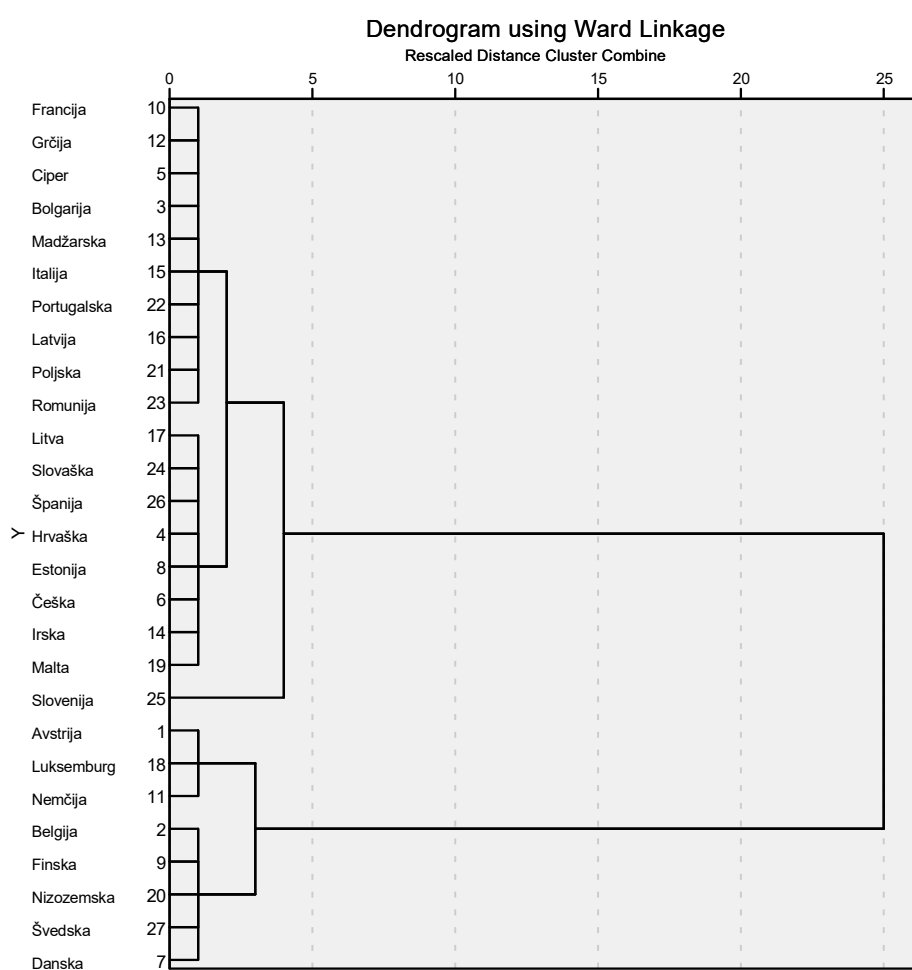
Prikaz podatkov o uporabi UI v slovenskih podjetjih glede na različne gospodarske dejavnosti razkriva različna odstopanja od povprečja EU. Zanimalo nas je, v katero skupino držav je Slovenija uvrščena glede na izbrane kazalce uporabe UI. Za namen takšne analize smo uporabili Wardovo metodo, ki sodi v skupino metod združevanja podatkov (Majerova & Nevima, 2017). Wardova metoda omogoča izoblikovanje homogenih skupin z minimiziranjem variance skupin, pri čemer v drevesnem razvrščanju enot znotraj skupin maksimizira evklidsko razdaljo. Z dendrogramom je mogoče prikazati razvrstitev držav v različne skupine glede na njihovo podobnost (Bastič, 2006, str. 40–41).

V analizo smo vključili podatke za vrednosti vseh gospodarskih sektorjev 27 držav EU za leto 2024, pri čemer smo upoštevali sedem izbranih proučevanih kazalcev uporabe UI, ki smo jih predhodno analizirali. Izbrani kazalci so v tem primeru izraženi na agregatni ravni in ne po gospodarskih dejavnostih⁵ (Eurostat, 2025b). Z Wardovo metodo, ki je prikazana na sliki 13, smo lahko države razvrstili v dve večji skupini, medtem ko je seznam članstva posamezne države v pripadajoči skupini

⁵ Uporabljeni kazalci v analizi so bili: delež podjetij, ki uporabljajo UI za besedilno rudarjenje; delež podjetij, ki uporabljajo UI za prepoznavanje govora; delež podjetij, ki uporabljajo UI za naravno generiranje jezika (NGL); delež podjetij, ki

držav prikazan v tabeli 1. V prvo skupino držav uvrščamo Bolgarijo, Hrvaško, Ciper, Češko, Estonijo, Francijo, Grčijo, Madžarsko, Irsko, Italijo, Latvijo, Litvo, Malto, Poljsko, Portugalsko, Romunijo, Slovaško, Slovenijo in Španijo. V drugo skupino držav uvrščamo Avstrijo, Belgijo, Dansko, Finsko, Nemčijo, Luksemburg, Nizozemsko in Švedsko. Druga skupina držav ima pri vseh proučevanih kazalcih relativno večjo povprečno vrednost uporabe UI kot prva skupina, kar je razvidno tudi iz tabele 2.

Slika 13: Dendrogram združevanja držav v skupine glede na izbrane kazalce uporabe UI v podjetjih po Wardovi metodi



Opomba: Izvirni izpis iz SPSS 28.0.

uporabljajo UI za obdelavo slik; delež podjetij, ki uporabljajo strojno učenje; delež podjetij, ki uporabljajo UI za programsko robotsko avtomatizacijo procesov; delež podjetij, ki uporabljajo UI za avtonomne robote, samovozeča vozila in avtonomne drone.

Tabela 1: Članstvo držav v skupinah glede na uporabo UI v podjetjih po Wardovi metodi

Skupina 1	Skupina 2
Bolgarija	Avstrija
Hrvaška	Belgija
Ciper	Danska
Češka	Finska
Estonija	Nemčija
Francija	Luksemburg
Grčija	Nizozemska
Madžarska	Švedska
Irska	
Italija	
Latvija	
Litva	
Malta	
Poljska	
Portugalska	
Romunija	
Slovaška	
Slovenija	
Španija	

Vir: Lastni.

Tabela 2: Povprečne vrednosti kazalcev uporabe UI v podjetjih glede na razvrščene skupine po Wardovi metodi

	Skupina 1	Skupina 2
Delež podjetij, ki uporabljajo UI za besedilno rudarjenje	4,90	14,66
Delež podjetij, ki uporabljajo UI za prepoznavanje govora	2,76	7,35
Delež podjetij, ki uporabljajo UI za naravno generiranje jezika (NGL)	4,08	11,54
Delež podjetij, ki uporabljajo UI za obdelavo slik	3,06	4,93
Delež podjetij, ki uporabljajo strojno učenje	3,44	7,69
Delež podjetij, ki uporabljajo UI za programsko robotsko avtomatizacijo procesov	3,41	7,79
Delež podjetij, ki uporabljajo UI za avtonomne robote, samovozeča vozila in avtonomne drone	0,85	1,89

Vir: Lastni.

5 Sklep

UI se ne razlikuje le v definicijah, ampak tudi glede načina in pogostosti uporabe v gospodarskih dejavnostih. V nekaterih gospodarskih dejavnostih smo ugotovili, da je UI bolj uporabna in nujno potrebna kot v drugih. Primer take gospodarske dejavnosti, kjer je nadpovprečno velik delež podjetij, tako v Sloveniji kot EU, ki uporabljajo tehnologije UI, je gospodarska dejavnost J (informacijske in komunikacijske dejavnosti). UI poleg avtomatizacije proizvodnih procesov, prepoznavanja in obdelave slik, strojnega učenja in podobnih funkcij prav tako ves čas ustvarja nove poklice, kar poleg priložnosti prinaša tudi nenehne izzive.

Analiza kazalcev UI v Sloveniji za leto 2023 in 2024 kaže na naraščajoč trend uporabe večine tehnologij UI, še posebej tehnologije za generiranje naravnega jezika. Gospodarska dejavnost J (informacijske in komunikacijske dejavnosti) izstopa po največjem deležu podjetij, ki uporabljajo različne tehnologije UI, kot so prepoznavanje govora, programska robotska avtomatizacija procesov, uporaba računalništva v oblaku in analitika podatkov ter strojno učenje. Kljub temu 77 % slovenskih podjetij v vseh gospodarskih dejavnostih skupaj še ne uporablja nobene tehnologije UI. Razlogov za neuporabo je več, primarni pa je predvsem pomanjkanje ustreznega strokovnega znanja. Kljub temu je 20,4 % podjetij v dejavnosti J že razmišljalo o uporabi UI. Slovenija ima v primerjavi z EU večji delež podjetij, ki uporabljajo UI za prepoznavanje in obdelavo slik, generiranje naravnega jezika in uporabo avtonomnih robotov, samovozečih vozil in avtonomnih dronov, medtem ko

zaostaja pri uporabi UI pri besedilnem rudarjenju, prepoznavanju govora, strojnem učenju in programsko-robotski avtomatizaciji procesov na osnovi UI. Glede na Wardovo metodo združevanja podatkov se je Slovenija uvrstila v prvo skupino, ki ima relativno manjše povprečne vrednosti kazalcev v primerjavi z drugo skupino.

Literatura in viri

1. Aghion, P. J., Jones, B., & Jones, C. (2017). *Artificial intelligence and economic growth* (NBER Working Paper No. 23928). National Bureau of Economic Research. <https://doi.org/10.3386/w23928>
2. Alam, M. S., Rahman, M. A., & Mrida, M. S. H. (2025). AI-driven data analytics and automation: A systematic literature. *Strategic Data Management and Innovation*, 2(1), 21–40. <https://doi.org/10.71292/sdmi.v2i01.9>
3. Bastič, M. (2006). *Metode raziskovanja*. Univerza v Mariboru Ekonomsko-poslovna fakulteta.
4. Baumol, W. J. (1967). Macroeconomics of unbalanced growth: The anatomy of urban crisis. *American Economic Review*, 57(3), 415–426.
5. Braunsberger, F., Hlavaty, M., Schlamburger, N., & Stevanovič, S. (2010). *Standardna klasifikacija dejavnosti 2008*. SURS. <https://www.stat.si/doc/pub/skd.pdf>
6. Brodny, J., & Tutak, M. (2022). Digitalization of small and medium-sized enterprises and economic growth: Evidence for the EU-27 countries. *Journal of Open Innovation: Technology, Market, and Complexity*, 8(2), 67. <http://doi.org/10.3390/joitmc8020067>
7. DBnomics. (2024). *Artificial intelligence by NACE Rev.2 activity*. DBnomics: https://db.nomics.world/Eurostat/isoc_eb_ain2?tab=list
8. Ejjami, R. (2024). Emerging professions in the age of AI across multiple sectors. *International Journal for Multidisciplinary Research*, 6(5), 1–32. <http://doi.org/10.36948/ijfmr.2024.v06i05.28762>
9. European Commission. (2020). *AI Watch: Defining artificial intelligence*. Joint Research Centre. <https://www.sipotra.it/wp-content/uploads/2020/10/AI-Watch-Defining-Artificial-Intelligence-1.pdf>
10. Eurostat. (2024a). *ICT usage in enterprises (isoc_e)*. Eurostat. https://ec.europa.eu/eurostat/cache/metadata/en/isoc_e_esms.htm
11. Eurostat. (2024b). *Data analytics by size class of enterprise*. Eurostat. https://ec.europa.eu/eurostat/data-browser/view/isoc_eb_das/default/table?lang=en
12. Eurostat. (2025a). *Artificial intelligence by size class of enterprise*. Eurostat. https://ec.europa.eu/eurostat/data-browser/view/isoc_eb_ai_custom_15700263/default/table?lang=en
13. Eurostat. (2025b). *Artificial intelligence by NACE Rev. 2 activity*. Eurostat. https://ec.europa.eu/eurostat/data-browser/view/isoc_eb_ain2_custom_15700284/default/table?lang=en
14. Gonzales, J. (2023). Implications of AI innovation on economic growth: A panel data study. *Journal of Economic Structures*, 12(13), 1–37. <http://doi.org/10.1186/s40008-023-00307-w>
15. Hua, Q., Wan, J., Wang, Z., & Yang, J. (2018). *Artificial intelligence for cloud-assisted smart factory*. V *IEEE Access*, 6 (str. 55419–55430). IEEE. <http://doi.org/10.1109/ACCESS.2018.2871724>
16. Ivchik, V. (2024). Overcoming barriers to artificial intelligence adoption. *Three Seas Economic Journal*, 5(4), 14–20. <https://doi.org/10.30525/2661-5150/2024-4-3>

17. Majerova, I., & Nevima, J. (2017). The measurement of human development using the Ward method of cluster analysis. *Journal of International Studies*, 10(2), 239–257. <http://doi.org/10.14254/2071-8330.2017/10-2/17>
18. Mezgec, S., & Seljak, B. K. (2019). *Using deep learning for food and beverage image recognition*. V 2019 IEEE International Conference on Big Data (str. 5149–5151). IEEE. <https://doi.org/10.1109/BigData47090.2019.9006181>
19. Mohammad, S. M. (2020). *Artificial intelligence in information technology*. Wilmington University. <http://doi.org/10.2139/ssrn.3625444>
20. Schuett, J. (2019). A legal definition of AI. *Law, Innovation and Technology*, 15(1), 60–82. <http://doi.org/10.1080/17579961.2023.2184135>
21. Singla, A. S. (2024). *The state of AI in early 2024: Gen AI adoption spikes and starts to generate value*. Pridobljeno 7. marec 2025 iz Quantum Black AI by McKinsey: <https://www.mckinsey.com/capabilities/quantumblack/our-insights/the-state-of-ai>
22. Soleman, S. (2024). Deep learning techniques for image and speech recognition: Current trends and future directions. *Escience Humanity Journal*, 5(1), 277–288. <http://doi.org/10.37296/esci.v5i1.212>
23. SURS. (2024). *Digitalno podjetništvo, podrobni podatki, 2024*. Statistični urad Republike Slovenije. <https://www.stat.si/StatWeb/News/Index/13267>
24. Vlada Republike Slovenije. (2024). *Danes je začela veljati evropska uredba o umetni inteligenci – prva taka celovita zakonodaja na svetu*. Vlada Republike Slovenije. <https://www.gov.si/novice/2024-08-01-danes-je-zacela-veljati-evropska-uredba-o-umetni-inteligenci-prva-taka-celovita-zakonodaja-na-svetu/>
25. Wang, P. (2019). On defining artificial intelligence. *Journal of Artificial General Intelligence*, 10(2), 1–37. <https://doi.org/10.2478/jagi-2019-0002>

KONKURENČNOST SLOVENSКИH PODJETIJ PRI UPORABI UMETNE INTELIGENCE: PRIMERJALNA ANALIZA NA AGREGATNI RAVNI Z DRŽAVAMI EU

Gal Detiček, Univerza v Mariboru, Ekonomsko-poslovna fakulteta, Slovenija 

Asist. Nejc Fir, Univerza v Mariboru, Ekonomsko-poslovna fakulteta, Slovenija 

Povzetek: V času porasta računalništva, procesiranja, podatkov in telekomunikacije osrednjo vlogo prevzema umetna inteligenca (UI), ki je prepoznana kot ključna tehnologija v okviru Slovenske strategije pametne specializacije. Uporaba UI v slovenskih podjetjih je glede na proučevane kazalce uporabe UI nadpovprečna, pri čemer Slovenija izstopa predvsem pri uporabi UI za IKT varnost in pri uporabi UI za prepoznavanje stvari ali oseb na slikah ter za njihovo obdelavo, zaostaja pa pri uporabi UI za rudarjenje besedil. Proučili smo različne kazalnike uporabe UI v slovenskih podjetjih in jih primerjali s povprečjem Evropske unije in najuspešnejšimi državami pri posameznih kazalcih. Slovenska podjetja izkazujejo nadpovprečno stopnjo digitalne intenzivnosti, uporaba UI pa je nadpovprečna na vseh proučevanih ravneh digitalizacije. Kljub temu se Slovenija sooča z izzivi, kot so beg možganov, premajhno financiranje temeljnih raziskav in potreba po regulaciji UI, zato je za nadaljnji razvoj ključnega pomena vlaganje v raziskave, izobraževanje in sodelovanje med deležniki.

Ključne besede: digitalna intenzivnost, Evropska unija, podjetje, Slovenija, umetna inteligenca

1 Uvod

Skozi zgodovino je družba doživela velik tehnološki napredek, s katerim so se pogosto premikale meje zmožnega, kar je družbi omogočilo številne koristi. V treh primerih so ti napredki bili tako znatni, da jih označujemo kot industrijske revolucije. Prvo industrijsko revolucijo sta zaznamovali mehanizacija in uporaba parnega stroja, drugo sta omogočili električna energija in masovna proizvodnja (tekoči trak), tretjo pa digitalizacija in informacijska tehnologija. V 21. stoletju je tako s porastom računalništva, procesiranja, podatkov in telekomunikacije osrednjo vlogo (predvsem v zadnjem desetletju) prevzela umetna inteligenca (v nadaljevanju UI), ki ob omrežju 5G in blockchainu predstavlja pomembno prelomnico, ki jo lahko označimo za četrto industrijsko revolucijo (French idr., 2021).

UI lahko s svojim delovanjem olajša življenje skozi povečanje produktivnosti ter izboljšano zdravstvo z natančnejšimi diagnozami bolezni in potrebno preventivo ter ponuja inovativne rešitve za podnebne spremembe. V hitro spreminjajočem se svetu ima EU številne priložnosti in izzive na področju UI. Za naslavljanje omenjenih izzivov je Evropska unija skupaj z Norveško aprila 2018 podpisala Deklaracijo o sodelovanju na področju UI s ciljem, da postane svetovno središče za UI. Pristopi k integraciji UI se med članicami razlikujejo v strategiji, prioritetah, proračunu, namenjenemu za to področje, časovnem okviru in implementaciji. Vsem državam pa je skupen cilj, da spodbujajo razvoj UI (Jorge Ricart idr., 2022). Vloga UI se v vsakdanjiku in ekonomskih aktivnostih z njenim razvojem povečuje. V Sloveniji je UI prepoznana kot ključna tehnologija za gospodarsko rast in razvoj v okviru Slovenske strategije pametne specializacije (S4), ki na eni strani izhaja iz realnih potencialov in trenutnega stanja raziskav in razvoja, na drugi strani pa tudi iz dejanskih potreb uporabe v gospodarstvu in družbi. Slovenska prizadevanja so usklajena z načrti EU in OECD ter v okviru Deklaracije o sodelovanju na področju UI (Gospodarska zbornica Slovenije, 2021).

V kvantitativnem delu raziskave smo z Wardovo metodo združili države v skupine glede na uporabo podjetij na področju UI, da smo lahko pridobili pregled nad skupnimi lastnostmi med državami in jih razvrstili v skupine. Raziskava je temeljila na statični analizi s proučevanjem zadnjih razpoložljivih podatkov iz leta 2023. Pri analizi kazalcev konkurenčnosti na področju UI smo uporabili tako deskriptivno kot tudi komparativno metodo, medtem ko je pregled empirične literature temeljil na metodi kompilacije.

Prispevek je sestavljen iz šestih poglavij. V drugem poglavju smo proučili stanje UI v Sloveniji in EU, v tretjem smo analizirali njen vpliv na slovenski podjetniški ekosistem ter nekatere kazalnike njene uporabe v podjetjih, v četrtem smo obravnavali rabo UI v podjetjih z različnimi stopnjami digitalizacije, v petem smo z Wardovo metodo razvrstili države v skupine glede na uporabo UI v podjetjih, medtem ko so v šestem poglavju navedene sklepne ugotovitve.

2 Umetna inteligenca v Sloveniji in EU

Slovenija je, podobno kot mnoge druge zahodne države, precej vpletena v razvoj UI in tovrstne tehnologije ter inovacije raziskav na tem področju. Kljub temu da Slovenija glede na določene podatke zaostaja za zahodnimi državami, je količina raziskav UI na prebivalca manjša le pri Švici. Po navedbah Požun idr. (2023) je Slovenija na drugem mestu po sofinanciranju projektov, povezanih z UI, ki se merijo na milijon prebivalcev. Ti projekti omogočajo spodbujanje digitalne transformacije, saj se UI omenja kot poglobljen dejavnik digitalne preobrazbe gospodarstev. Slovenija ima več kot 40-letno tradicijo raziskovanja na področju UI in sorodnih naprednejših tehnologij, saj so se raziskave na področju UI začele leta 1972 v Ljubljani. Del financiranja tovrstnih raziskovalnih dejavnosti prihaja od Javne agencije za raziskovalno dejavnost RS s financiranjem raziskovalnih programov, vendar je zaradi omejenosti (ker so sredstva namenjena celotnemu področju računalništva) izrednega pomena tudi pridobivanje sredstev iz razpisov EU.

Na področju izobraževanja ima Slovenija na visokošolski izobraževalni ravni dolgoletne izkušnje, vendar zaostaja pri vključevanju tem v povezavi z UI v srednješolske in osnovnošolske programe. UI danes npr. velja za eno glavnih področij študija na Fakulteti za računalništvo in informatiko Univerze v Ljubljani, in sicer na vseh treh ravneh, močno pa je zastopana tudi na Fakulteti za elektrotehniko, računalništvo in informatiko na Univerzi v Mariboru. Z rastočim pomenom na raznovrstnih področjih je vključena tudi v predmetnik Fakultete za matematiko in fiziko ter Fakultete za strojništvo Univerze v Ljubljani, Fakultete za informacijske študije in Fakultete za organizacijske vede Univerze v Mariboru ter tudi na Fakultete za matematiko, naravoslovje in informacijske tehnologije Univerze na Primorskem. UI je pomembna tematika tudi na drugih slovenskih fakultetah in v raziskovalnih organizacijah, vendar se ne pojavlja kot samostojni predmet. Na drugi strani pa v osnovnih in srednjih šolah predmet s tega področja ne obstaja (Evropska komisija, 2025a). V Sloveniji je prepoznana tudi potreba po umestitvi temeljnih znanj računalništva in informatike v kurikulum vrtcev ter učne načrte osnovnih in srednjih šol. Med te vsebine sodijo tudi veščine in znanja o UI, podatkovni znanosti in kibernetiki varnosti (MIZŠ, 2022).

Slovenija ima obsežno skupnost strokovnjakov, ki se ukvarja z UI na različnih področjih, od strojnega učenja in jezikovnih tehnologij do računalniške inteligence in mnogih drugih. S približno 250 raziskovalci na tem področju jih je v državi glede na velikost prebivalstva razmeroma veliko, na področju robotike pa deluje en raziskovalec na 7000 prebivalcev, kar Slovenijo uvršča na prvo mesto ne le v EU, temveč tudi na svetu. Kljub temu se Slovenija podobno kot druge države sooča z izzivom, saj ne izobrazi zadosti potrebnega kadra s področja računalništva in še ožjega področja UI, da bi lahko zadostila nenehno naraščajoči potrebi na področju izobraževanja, industrije in raziskovanja. Kljub temu je slovenska mreža strokovnjakov s področja UI dobro povezana, saj se ti združujejo v mnogih društvih in neuradnih skupinah ter se povezujejo na družbenih omrežjih. Nacionalni program za UI navaja tudi vizijo in temeljne cilje. Za uresničitev vizije, ki se glasi »nadgraditi več kot 40-letne raziskovalne dosežke na področju UI v Sloveniji ter postati mednarodno prepoznavni po kompetencah prenosa znanja in vrhunskih, etičnih in varnih tehnologij s področja UI v človeku prijazne in zaupanja vredne storitve in proizvode ob zagotavljanju nacionalne kulturne identitete,« je zastavljenih 10 strateških ciljev¹ (Evropska komisija, 2025a).

Slovenija ima splošni cilj implementacije UI, da bi v okviru in z upoštevanjem evropskih vrednot in pravic postali svetovno središče UI, kjer bi bila slednja osredotočena na človeka, ta pa bi ji lahko zaupal. Povezovanje na tem področju se je začelo aprila 2018 z Deklaracijo o sodelovanju na področju UI, junija 2018 pa je Evropska komisija predlagala tudi strategijo o UI. Decembra istega leta je z namenom povečanja sinergije Evropska komisija sprejela tudi t. i. *Usklajeni načrt za umetno inteligenco*, s čimer je spodbudila tesnejšo in učinkovitejšo sodelovanje po celotni EU, v Švici in na Norveškem. Eden izmed ključnih ukrepov je bila spodbuda, da vse države članice razvijejo svoj načrt in strategije na področju UI. Februarja 2020 je bil nato izdan dokument *Bela knjiga o umetni inteligenci – evropski pristop k odličnosti in zaupanju*, ki je posodobil prej omenjeni *Usklajeni načrt*

¹ SC1: Vzpostavitev dinamičnega ekosistema deležnikov za raziskave, inovacije in uvajanje UI

SC2: Izobraževanje in krepitev človeških virov

SC3: Podpora raziskavam in inovacijam na področju UI

SC4: Uvedba referenčnih rešitev UI v gospodarstvo, javni sektor, javno in državno upravo ter družbo

SC5: Vzpostavitev tehnološke infrastrukture za raziskave, razvoj in uporabo UI

SC6: Okrepitev varnosti z uporabo UI

SC7: Povečanje zaupanja javnosti v UI

SC8: Zagotovitev ustreznega pravnega in etičnega okvira

SC9: Okrepitev mednarodnega sodelovanja

SC10: Vzpostavitev nacionalnega observatorija za UI v Sloveniji

za umetno inteligenco, aprila 2021 pa je Evropska komisija izdala poročilo z naslovom »Pregled usklajenega načrta za umetno inteligenco za leto 2021 (Jorge Ricart idr., 2022). 1. avgusta 2024 je v veljavo vstopil tudi t. i. *Akt o umetni inteligenci*, ki je prvi pravni okvir o UI, ki določa jasen nabor pravil za razvijalce in uvajalce teh tehnologij z namenom omogočanja vodilne vloge evropskih držav na področju UI v svetu (Evropska komisija, 2025b).

3 Umetna inteligenca v slovenskem podjetniškem ekosistemu

Slovenija si prizadeva vzpostaviti dinamičen podjetniški ekosistem, ki je ključnega pomena za nadaljnji razvoj in uvajanje UI v državi. Po podatkih Eurostata (2025a) je leta 2023 UI uporabljalo 11,37 % vseh podjetij, leta 2024 pa se je delež teh podjetij povečal na 20,89 %. Slovenija se uvršča na 7. mesto v EU po deležu podjetij z uporabo UI in je nadpovprečna po omenjenem kazalniku, saj povprečje znaša 13,48 % podjetij. Med gospodarskimi panogami se delež uporabe UI v podjetjih relativno najbolj povečuje v sektorju informacijsko-komunikacijske tehnologije (v nadaljevanju IKT), prav tako pa se beleži naraščajoča vloga UI med zagonskimi podjetji. Kljub naraščajoči vlogi UI zaostajamo za vodilnimi državami pri podjetniških aktivnostih zagonskih podjetij in razvoju podjetij na področju UI. Leta 2020 je bilo 156 podjetij specializiranih za uporabo UI, pri čemer lahko ta podjetja razvrstimo v štiri skupine. Prvo skupino sestavlja 29 podjetij, ki na trgu ponujajo splošne storitve, povezane z implementacijami sistemov UI po naročilu, ki pa jih lahko dalje razdelimo na tiste, ki so ožje specializirane v UI (14 podjetij), in tiste, ki storitve UI ponujajo kot dopolnitev širšega nabora storitev (preostalih 15 podjetij). Drugo skupino sestavljajo multinacionalke, ki ponujajo raznolike storitve in izdelke, med njimi tudi take, ki so povezani z UI. Tovrstnih podjetij je bilo sedem. Tretjo skupino sestavljajo podjetja, ki se s svojimi izdelki ali storitvami osredotočajo na specifično področje uporabe UI. Teh podjetij je 71, od tega večina zagonskih podjetij, med katerimi jih je največ na področju zdravstva (deset podjetij). V četrti skupini je 49 podjetij, ki neposredno ne ponujajo izdelka ali storitve, ki temelji na uporabi UI, ampak imajo interno ekipo podatkovnih znanstvenikov, ki s svojim delom podpirajo poslovne naloge podjetja. Večinoma so to tehnološka podjetja ter podjetja s področja bančništva, trgovine in proizvodnje (Evropska komisija, 2025a).

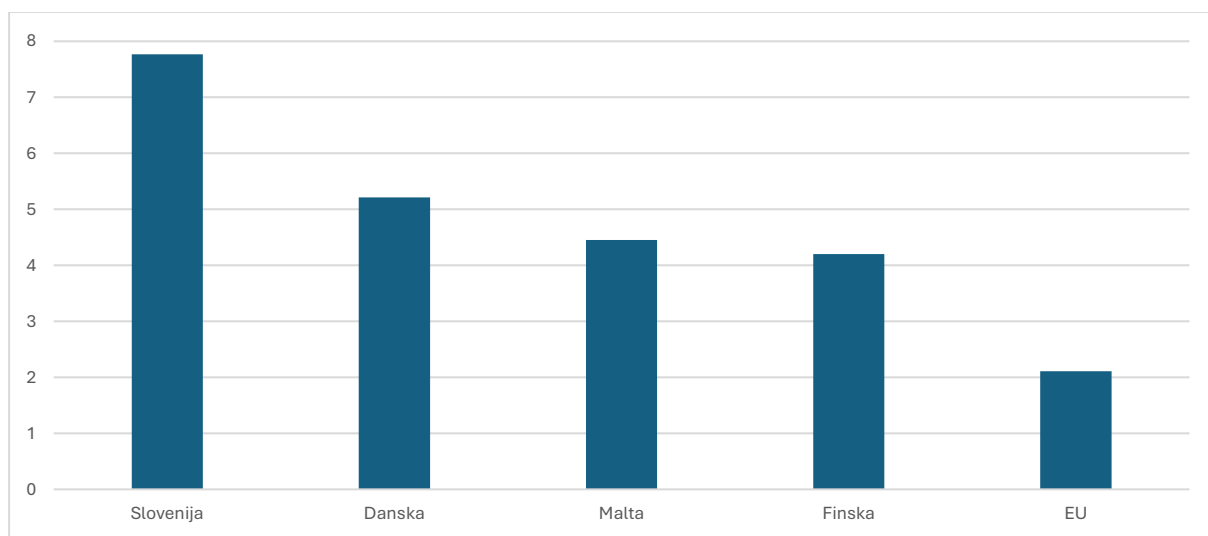
Podjetja lahko uporabijo UI za svoje delovanje in poslovne procese na različne načine, in sicer od rudarjenja podatkov do odnosov s strankami in optimizacije logistike, omogoča pa tudi zmanjševanje porabe pesticidov v kmetijstvu. Vister (2024) navaja, da UI podjetjem omogoča razvoj novih izdelkov in storitev, izboljša vzdrževanje strojev, poveča proizvodne zmogljivosti in prihrani energijo. Tako lahko podjetja povečujejo produktivnost, inovativnost in konkurenčnost v poslovnem

svetu, saj jim omogoča avtomatizacijo procesov, analizo obsežnih podatkov in napovedovanje trendov. Kljub vsem koristim pa se ob implementaciji UI v podjetje pojavljajo izzivi, zato se podjetjem svetuje vzpostavitev štirih osnovnih stebrov UI, in sicer: kultura podjetja, človeški viri, podatki in infrastruktura (Trampuž, 2023).

Podjetja lahko v svoj sistem implementirajo UI na različne načine, kot so tehnologije, ki analizirajo besedila, pretvarjajo govorjeni jezik v strojno berljiv format, z generiranjem naravnega jezika, prepoznavanjem in obdelavo slik, strojnim učenjem, z avtonomnimi roboti in droni ter samovozečimi vozili (Mihai idr., 2023). V nadaljevanju raziskave smo analizirali, v kolikšni meri so leta 2023 nekatere izmed teh tehnologij slovenska podjetja in podjetja treh vodilnih držav v EU, ki imajo deset ali več zaposlenih, implementirala v svoje delovanje, in vse primerjali s povprečjem EU ter na podlagi tega ugotavljali konkurenčnost slovenskih podjetij glede na uporabo UI. V primeru uvrstitve Slovenije med vodilne tri države v EU pri posameznem kazalniku uporabe UI smo v analizo vključili še četrto državo. Za proučevanje uporabe UI je mogoče upoštevati številne kazalnike, zato smo se v raziskavi omejili na deset kazalnikov.

Najprej smo se osredotočili na proučevanje uporabe UI za IKT varnost, kar je prikazano na sliki 1. Opazimo lahko, da je Slovenija na tem področju na prvem mestu s 7,8-odstotnim deležem podjetij, kar je za 2,6 odstotne točke več od drugouvrščene Danske, ki UI za ta namen uporablja v 5,2 % podjetij. Sledita ji Malta s 4,5-odstotnim deležem podjetij in Finska s 4,2-odstotnim deležem podjetij. Slovenija je torej vodilna država v EU na področju uporabe UI za namene IKT varnosti, pri čemer presega povprečje EU za skoraj štirikrat, saj povprečje EU znaša 2,1 % podjetij. Razloge za vodilni položaj Slovenije je mogoče razložiti, da je UI že več kot 30 let prisotna v študijskih izobraževalnih programih s področja IKT, ki posebno pozornost posvečajo tudi kibernetiki varnosti. Visoka raven znanja je podprta s preteklimi raziskavami in na dolgi rok omogoča, da je področje IKT varnosti in uporabe UI za te namene med prioritetskimi področji. Slovenija se uvršča med uspešnejše članice EU glede na pridobivanje sredstev in število projektov na tem področju (Evropska komisija, 2025a).

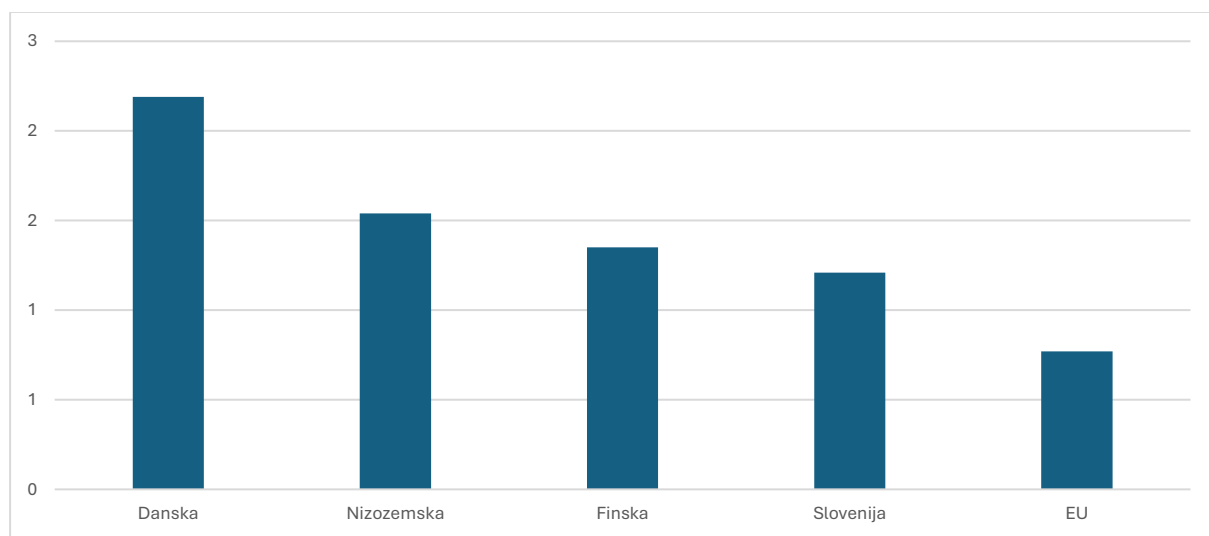
Slika 1: Delež podjetij z desetimi ali več zaposlenimi, ki uporabljajo UI za IKT varnost, v Sloveniji, naslednjih treh vodilnih državah in povprečju EU za leto 2023



Vir podatkov: Eurostat (2025b).

Na sliki 2 lahko opazimo delež podjetij, ki uporablja UI za logistične namene. Integracija UI na področju logistike v podjetjih izrazito pridobiva na pomenu, zlasti na področju trajnostnosti, saj omogoča sprejemanje ustrežnejših odločitev ter učinkovitejšo uporabo virov in proizvodnih dejavnikov. Skupek omenjenih dejavnikov vpliva na zmanjševanje negativnega vpliva na okolje skozi zmanjševanje ogljikovih emisij in količino odpadkov ter ekološko optimizacijo transportnih poti. Uravnoteženost med trajnostnostjo in učinkovitostjo je mogoče doseči z uporabo UI, ki z natančnejšim napovedovanjem povpraševanja, upravljanjem z zalogo in izboljšanjem transportnih poti na eni strani zmanjšuje stroške ter izboljšuje učinkovitost in produktivnost podjetij, na drugi strani pa omogoča lažje doseganje okoljevarstvenih in trajnostnih ciljev. Omenjeni rezultati uporabe UI na področju logistike vplivajo na naraščajoči obseg raziskav.

Slika 1: Delež podjetij, ki uporabljajo UI za logistične namene, v Sloveniji, vodilnih treh državah in povprečju EU za leto 2023



Vir podatkov: Eurostat (2025b).

Pojavljajo se štirje glavni izzivi pri soočanju z uvedbo trajnostne logistike. Prvi izziv predstavlja negotovost, ki je povezana z volatilnostjo povpraševanja, kompleksnostjo ponudbe, nepredvidljivostjo tehnološkega napredka in spremembami regulativ ter političnih usmeritev. Drugi izziv je kompleksnost omrežja, ki je zaznamovana s pomanjkanjem indikatorjev za ocenjevanje socialnih kazalnikov, nezadostnim upoštevanjem tveganj in regionalnimi tehnološkimi razlikami. Tretji izziv predstavlja logistično sodelovanje, ki pomeni zasebnost in varnost podatkov, raznolikost logističnih sistemov in variabilnost logističnih inovacij. Četrti izziv predstavlja potreba po tehnoloških inovacijah, ki zajema uporabo t. i. zelene embalaže, optimizacije transportnih poti, podpiranja električnih in hibridnih vozil ter skupne logistične platforme (Chen idr., 2024).

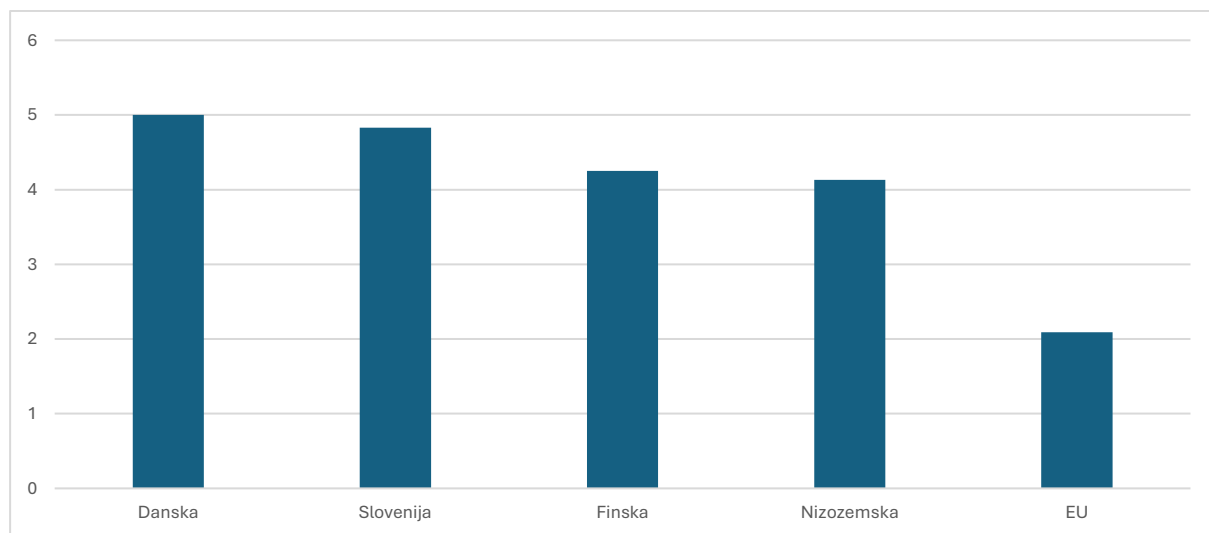
Abduljabbar idr. (2019) izpostavljajo tri pogloblitve trende na področju uporabe UI v logistiki, in sicer: uporaba UI pri sprejemanju odločitev, načrtovanju in upravljanju na korporativni ravni; izboljšanje javnega prevoza; razvoj avtonomnih vozil, ki bi povečala produktivnost in zmanjšala število nesreč na avtocestah. Med pomembne trende na tem področju Chen idr. (2024) označujejo tudi uporabo t. i. tehnologij blockchain, povratno logistiko in podatkovno analizo. V Sloveniji 1,2 % podjetij UI uporablja za logistične namene, kar jo uvršča nad povprečje EU. Slednje znaša 0,8 % podjetij oz. 0,4 odstotne točke manj od Slovenije. Vidno izstopa Danska, kjer UI za transport uporablja 2,2 % podjetij, kar je za eno odstotno točko več od Slovenije. Danski sledita Nizozemska in Finska

z 1,5 % in 1,4 % podjetij, ki imata izrazito manjši delež podjetij od vodilne Danske. Slovenija se po proučevanem kazalniku uvršča na 5. mesto v EU.

Podjetja uporabljajo tudi tehnologije, ki generirajo pisni ali govorni jezik, t. i. naravno generiranje jezika (v nadaljevanju NGL). Tovrstne tehnologije omogočajo prepoznavanje govora in prevajanje iz enega jezika v drugega (npr. Google Prevajalnik) in se uporabljajo za avtomatizirano pisanje dokumentov, v kombinaciji s strojnim učenjem pa tudi za komunikacijo s strankami preko sporočil (npr. chatbot) (SiStat, 2025). Trenutno je ta tehnologija UI ključnega pomena v sektorju financ in IKT (Redek idr., 2023).

V Sloveniji je po podatkih SiStata (2025) leta 2023 UI za NGL od 8576 podjetij z desetimi ali več zaposlenimi uporabljalo 414 podjetij. Na sliki 3 lahko vidimo, da delež takšnih podjetij znaša 4,83 %. V primerjavi z državami EU se Slovenija uvršča na drugo mesto in zaostaja za vodilno Dansko, katere delež podjetij, ki uporabljajo tehnologijo za NGL, znaša 5 %. Sloveniji sledita Finska s 4,25 % podjetij in Nizozemska s 4,13 % podjetij. Razlika med vodilnimi štirimi državami na tem področju in povprečjem vseh 27 držav EU je izrazita, saj je v EU v povprečju 2,09 % podjetij uporabljalo UI za NGL.

Slika 2: Delež podjetij, ki uporabljajo UI za naravno generiranje jezika (NGL), v Sloveniji, preostalih treh državah in povprečju EU za leto 2023



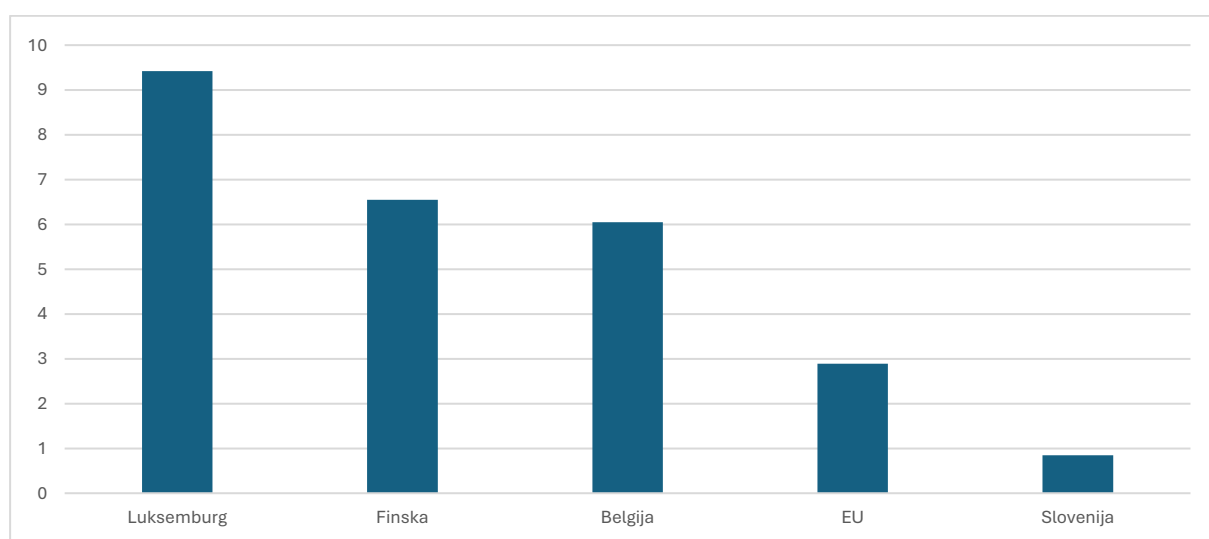
Vir podatkov: Eurostat (2025b).

Naslednje orodje UI, ki se pogosto uporablja v podjetjih, je rudarjenje besedil (angl. text mining). Podjetja se soočajo z obdelavo velikih količin podatkov, zato si lahko z rudarjenjem besedil

olajšajo poslovanje, ki omogoča izluščitev besedila in pridobitev relevantnih podatkov. Rudarjenje besedil sodi v podpodročje podatkovnega rudarjenja. Uporabno je predvsem na področju strateškega načrtovanja, z njegovo implementacijo pa lahko avtomatiziramo in zmanjšamo čas procesiranja informacij pri izdelavi strateških načrtov. Proces rudarjenja besedil lahko razdelimo v štiri korake. Prvi korak je pridobivanje besedila, ki se nanaša na iskanje besedila. Sledi predhodna obdelava, katere namen je nestrukturirano ali na pol strukturirano besedilo preoblikovati v strukturirano. Naslednji korak je obdelava besedila, kjer se vključijo t. i. algoritmi podatkovnega rudarjenja, s katerimi se lahko najdejo povezave v besedilu. Zadnji korak vključuje vrednotenje rezultatov, kjer se preveri, ali so bile pridobljene potrebne informacije, ter se izmeri uspešnost (Vasquez Rojas idr., 2018).

S slike 4 je razvidno, da Slovenija na področju uporabe UI za rudarjenje besedil zaostaja za povprečjem EU, kjer so tovrstne tehnologije relativno bolj razširjene. V Sloveniji uporablja UI za rudarjenje besedil 0,85 % podjetij, kar jih uvršča na predzadnje mesto v EU in zgolj pred Poljsko z 0,54 % podjetij. Povprečje EU znaša 2,89 % podjetij, ki uporabljajo UI za rudarjenje besedil, kar je približno trikrat več od Slovenije. Vodilne tri države v EU z največjim deležem podjetij, ki uporabljajo UI za rudarjenje besedil, so na prvem mestu Luksemburg z 9,42 % podjetij (kar je za 8,57 odstotne točke več kot Slovenija) in na drugem mestu Finska s 6,55 % podjetij, medtem ko je na tretjem mestu Belgija s 6,05 % podjetij.

Slika 3: Delež podjetij, ki uporabljajo UI za rudarjenje besedil, v Sloveniji, vodilnih treh državah in povprečju EU za leto 2023

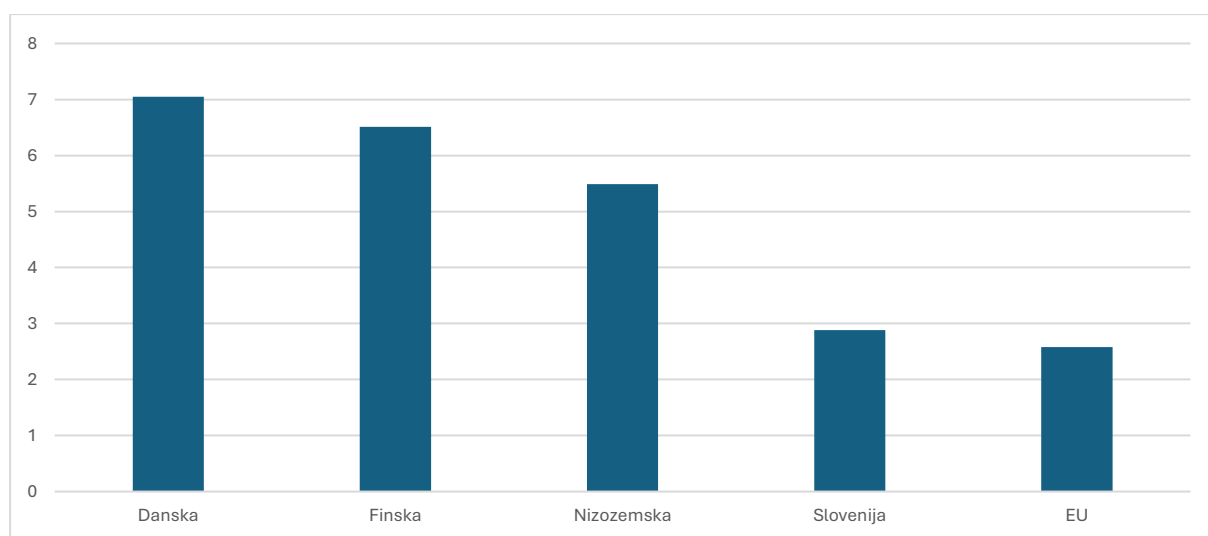


Vir podatkov: Eurostat (2025b).

Strojno učenje je metoda, pri kateri z algoritmi ustvarimo model za analizo ali napoved podatkov. Ti algoritmi so lahko nadzorovani, nenadzorovani, delno nadzorovani ali pa okrepijo in izboljšajo učenje (Lee & Shin, 2020). Zhou idr. (2020) navajajo, da podjetja uporabljajo strojno učenje za učinkovitejše reševanje problemov in optimizacijo upravljanja znanja. Uporablja se predvsem za (napredno) analizo podatkov in prepoznavanje glasu, slik in besedila, dinamično prilagajanje cen in napovedovanje prodaje. To področje UI je najbolj implementirano v rudarskem, proizvodnem in gradbenem sektorju, financah, IKT in v trgovinah na drobno (Redek idr., 2023).

Slika 5 prikazuje delež podjetij, ki uporabljajo strojno učenje za podatkovno analizo. Slovenija se v tem pogledu uvršča nekoliko nad povprečje EU in zaseda 12. mesto. Strojno učenje uporablja 2,88 % slovenskih podjetij, medtem ko ga v povprečju v EU uporablja 2,58 % podjetij. Na vrhu je ponovno Danska s 7,07 % podjetij, kar je za 4,17 odstotne točke več od Slovenije. Sledi ji Finska, ki za njo s 6,51 % podjetij zaostaja za 0,54 odstotne točke, tretje mesto pa zaseda Nizozemska s 5,49 % podjetij.

Slika 4: Delež podjetij, ki uporabljajo strojno učenje za podatkovno analizo, v Sloveniji, vodilnih treh državah in povprečju EU za leto 2023

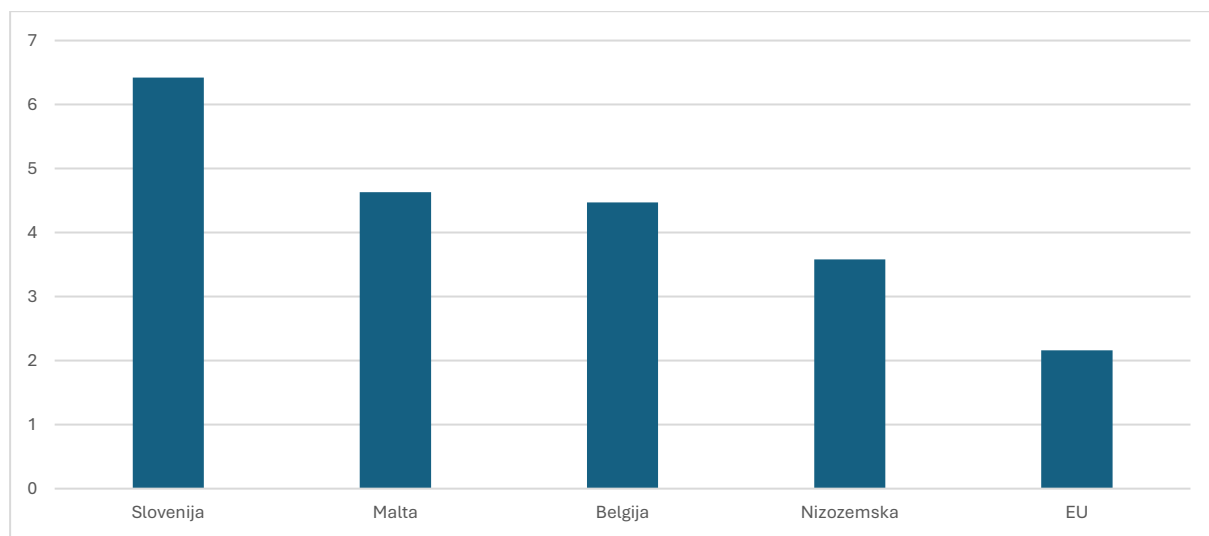


Vir podatkov: Eurostat (2025b).

Ena izmed oblik, ki temelji na algoritmih strojnega in globokega učenja, je prepoznavanje stvari ali oseb na slikah ter njihova obdelava (angl. image recognition and processing). Ta se lahko uporablja za varnost in nadzor, fotografiranje in digitalni marketing (Mihai idr., 2023). Po podatkih SiStata (2025) je leta 2023 UI za prepoznavanje objektov in oseb uporabljajo 551 podjetij. Na sliki 6 je

razvidno, da ima Slovenija s 6,42 % podjetij na tem področju največji delež v celotni EU. Sledijo ji Malta s 4,63 % podjetij, kar je za 1,79 odstotne točke manj od Slovenije; Belgija s 4,47 % podjetij in Nizozemska s 3,58 % podjetij. Povprečje v EU je skoraj trikrat manjše kot v Sloveniji in znaša 2,16 %.

Slika 5: Delež podjetij, ki uporabljajo UI za prepoznavanje stvari ali oseb na slikah ter za njihovo obdelavo, v Sloveniji, naslednjih treh vodilnih državah in povprečju EU za leto 2023



Vir podatkov: Eurostat (2025b).

4 Digitalna intenzivnost podjetij v Sloveniji in EU

Indeks digitalne intenzivnosti (v nadaljevanju DII) je kompozitni indeks, ki temelji na raziskavi EU o informacijsko-komunikacijski tehnologiji in e-poslovanju v podjetju. Gre za indikator, ki meri uporabo različnih tehnologij v podjetjih in se uporablja za ugotavljanje obsega digitalizacije podjetij (Evropska komisija, 2025c). Izračunan je na podlagi dvanajstih dejavnikov, kjer vsak predstavlja eno točko². Obstajajo štiri različice uporabljenih dejavnikov za določanje digitalne intenzivnosti, pri čemer se je leta 2023 upoštevala tretja (Eurostat, 2024a).

² Podjetje dobi točko, ko ima več kot 50 % zaposlenih dostop do interneta za poslovne namene, omogoča maksimalno hitrost nalaganja internetne povezave v vsaj 30 Mb/s, e-poslovanje podjetja predstavlja vsaj 1 % prometa, spletna prodaja predstavlja več kot 1 % prometa, spletna prodaja B2C predstavlja več kot 10 % vseh spletnih prodaj, uporablja storitve v oblaku, uporablja sofisticirane računalniške storitve, uporablja katero koli družbeno omrežje, in še dodatno točko, če uporablja dve ali več družbenih omrežij, opravlja analizo podatkov znotraj lastnega podjetja ali z

Na podlagi števila točk jih razdelimo v štiri skupine. Podjetja z zelo nizkim DII so tista, ki zberejo od nič do tri točke. V kolikor ima podjetje od štiri do šest točk, se uvrsti med podjetja z nizkim DII. Podjetja z visokim DII imajo od sedem do devet točk, medtem ko imajo podjetja z zelo visokim DII od deset do dvanajst točk (Evropska komisija, 2025c).

Po podatkih Sursa (2024) za leto 2023 v Sloveniji zelo nizek DII izkazuje 31 % podjetij. Nizek DII ima 35 % podjetij, kar predstavlja največji delež podjetij. 26 % podjetij ima visok DII, medtem ko ima 8 % zelo visok DII. Če podjetja izpolnjujejo vsaj štiri pogoje oz. imajo vsaj štiri točke v DII, dosegajo osnovno stopnjo digitalne zrelosti. V Sloveniji je leta 2023 bilo 69 % digitalno zrelih podjetij, pri čemer je bilo med malimi in srednje velikimi podjetji takšnih 68 % podjetij. Za primerjavo: v EU je osnovno stopnjo digitalne zrelosti doseglo 59 % podjetij, pri čemer je bilo med malimi in srednjimi podjetji takšnih 58 % podjetij. Glede na opisane podatke Slovenija izkazuje relativno visoko stopnjo digitalizacije podjetij (Eurostat, 2024b).

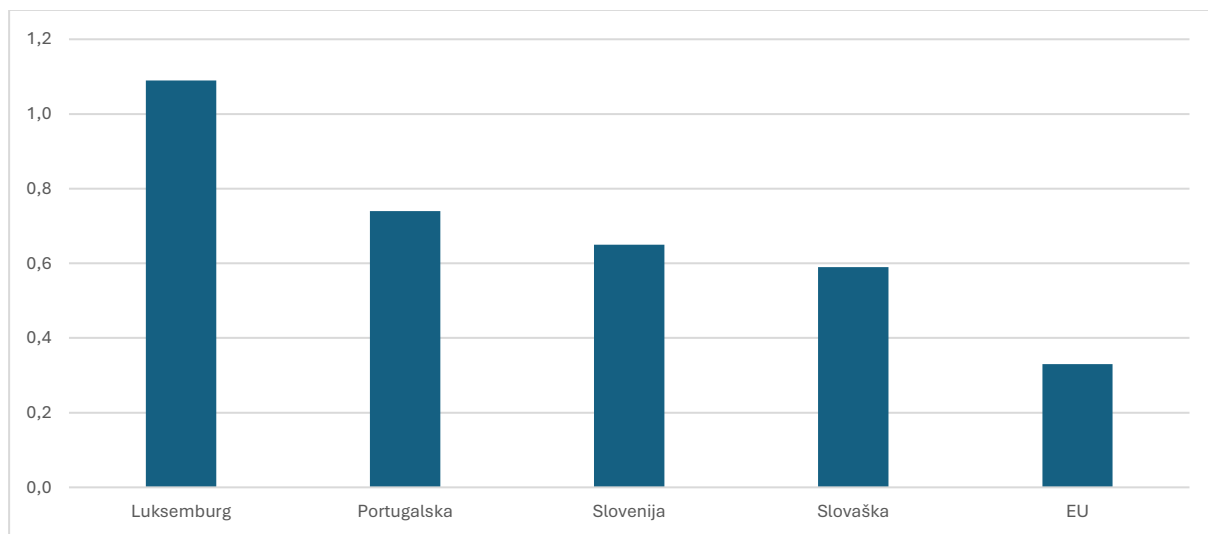
Cilj na ravni EU je do leta 2030 doseči 90-odstoten delež osnovne digitalne zrelosti med malimi in srednje velikimi podjetji (Evropska komisija, 2025d). Po podatkih Eurostata (2024b) je leta 2023 v povprečju EU imelo 42,2 % malih in srednje velikih podjetij zelo nizek DII. Takšnih podjetij je bilo največ v Romuniji, Bolgariji in Grčiji. V povprečju EU je leta 2023 imelo 33,8 % podjetij nizek DII, 19,6 % podjetij je imelo visok DII in 4,4 % podjetij je imelo zelo visok DII.

Ena izmed komponent DII je tudi uporaba UI, zato smo se osredotočili na komponento obravnavanega indeksa. Slike 7, 8, 9 in 10 prikazujejo uporabo UI v podjetjih glede na njihovo digitalno intenzivnost. Leta 2023 je UI uporabljalo 11 % podjetij, leta 2024 pa 21 % podjetij (Eurostat, 2025a).

S slike 7 lahko razberemo, da 0,65 % slovenskih podjetij z zelo nizko digitalno intenzivnostjo uporablja UI, kar jo uvršča na tretje mesto v EU. Pred Slovenijo sta vodilni Luksemburg, kjer UI uporablja 1,09 % podjetij z zelo nizkim DII, in Portugalska z 0,74 % podjetij z zelo nizkim DII. Četrto mesto zaseda Slovaška z 0,59 % podjetij z zelo nizkim DII, povprečje EU pa znaša 0,33 % podjetij z zelo nizko digitalno intenzivnostjo, kar je približno dvakrat manj kot v Sloveniji.

zunanjim ponudnikom, uporablja UI, ima programske pakete ERP za deljenje informacij med različnimi področji in uporablja CRM (Customer Relationship Management) (Eurostat, 2024a).

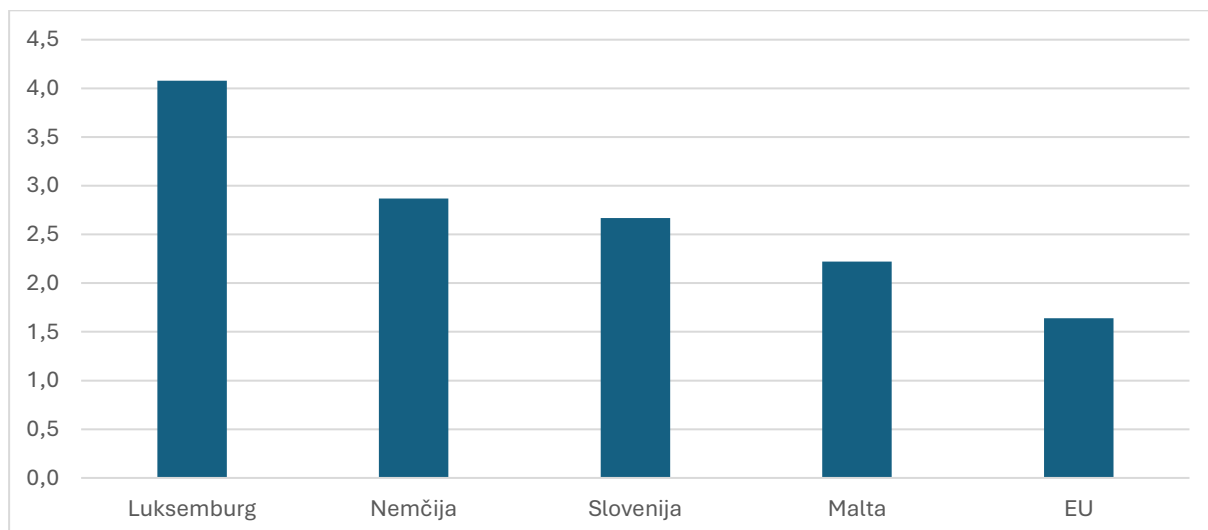
Slika 6: Delež podjetij z zelo nizkim digitalnim indeksom, ki uporabljajo UI, v Sloveniji, preostalih treh državah in povprečju EU za leto 2023



Vir podatkov: Eurostat (2025b).

Podobno velja tudi za podjetja z nizko digitalno intenzivnostjo, kar prikazuje slika 8. Prvo mesto ponovno zaseda Luksemburg, kjer UI uporablja 4,08 % podjetij z nizkim DII, sledi Nemčija z 2,87 % podjetij z nizkim DII. Slovenija je z 2,67 % podjetij na tretjem mestu, za njo pa je Malta z 2,22 % podjetij z nizkim DII. Povprečje EU v tej kategoriji znaša 1,64 % podjetij z nizkim DII.

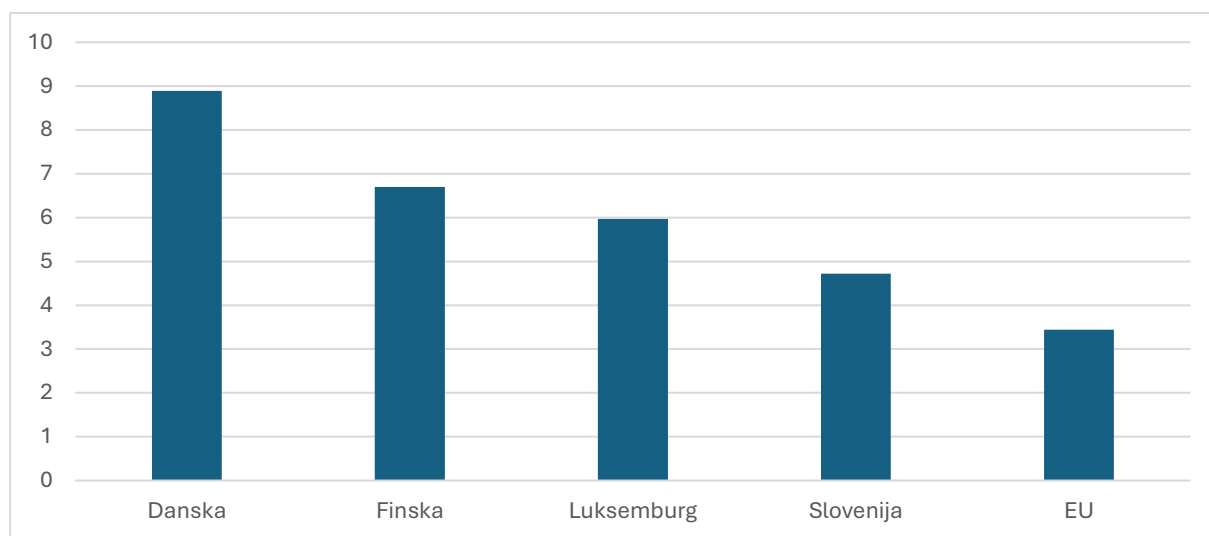
Slika 7: Delež podjetij z nizkim digitalnim indeksom, ki uporabljajo UI, v Sloveniji, preostalih treh državah in povprečju EU za leto 2023



Vir podatkov: Eurostat (2025b).

Slika 9 prikazuje delež podjetij z visokim DII, ki uporabljajo UI. V primerjavi s sliko 8 lahko opazimo, da Slovenija zaostaja za vodilnimi tremi državami. Slovenija se s 4,27 % podjetij v tej kategoriji uvršča na deseto mesto in za 1,28 odstotne točke presega povprečje EU, ki znaša 3,44 % podjetij. Vodilna država v tej kategoriji je Danska, kjer UI uporablja 8,89 % podjetij z visokim DII. Sledita ji Finska s 6,70 % podjetij in Luksemburg s 5,97 % podjetij z visoko stopnjo digitalizacije.

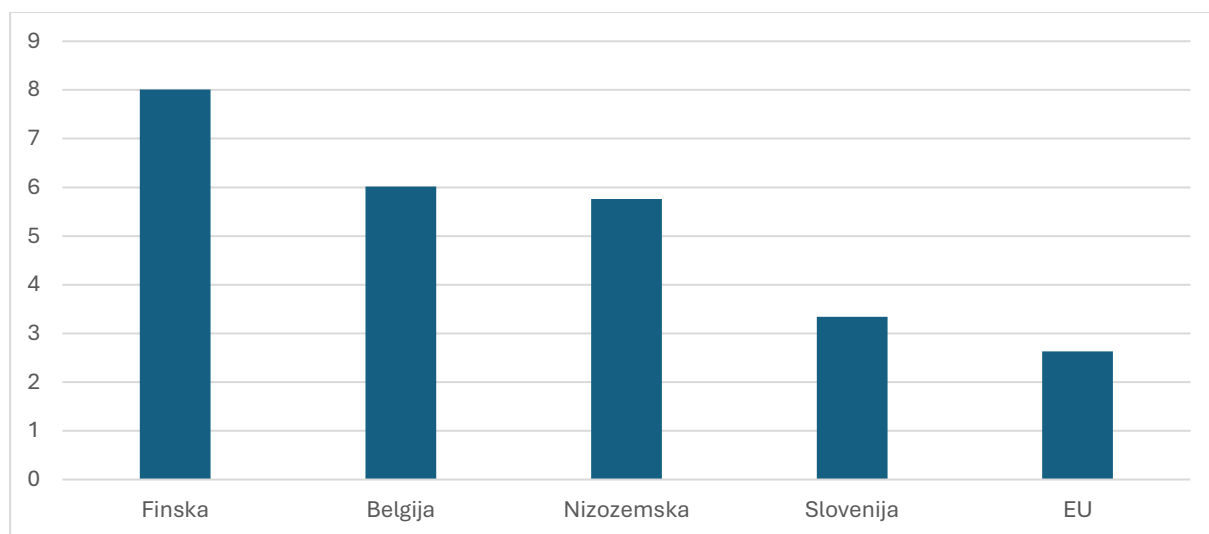
Slika 8: Delež podjetij z visokim digitalnim indeksom, ki uporabljajo UI, v Sloveniji, vodilnih treh državah in povprečju EU za leto 2023



Vir podatkov: Eurostat (2025b).

Slika 10 prikazuje podjetja z zelo visokim DII, ki uporabljajo UI. Slovenija s 3,34 % podjetij z zelo visokim DII, ki uporabljajo UI, zaseda osmo mesto. Za vodilno Finsko zaostaja za 4,67 odstotne točke, kjer UI uporablja 8,01 % podjetij z zelo visokim DII. Kljub temu se Slovenija uvršča nad povprečje EU, ki znaša 2,63 %. Za Finsko sta Belgija s 6,01 % podjetij in Nizozemska s 5,76 % podjetij z zelo visokim DII, ki pri svojem poslovanju uporablja UI. Sklenemo lahko, da se UI v slovenskih podjetjih uporablja nadpovprečno na vseh ravneh digitalne intenzivnosti.

Slika 9: Delež podjetij z zelo visokim digitalnim indeksom, ki uporabljajo UI, v Sloveniji, vodilnih treh državah in povprečju EU za leto 2023



Vir podatkov: Eurostat (2025b).

Kljub temu da podatki nakazujejo na nadpovprečno rabo UI v slovenskih podjetjih na vseh ravneh digitalne intenzivnosti, se Slovenija sooča z nekaterimi izzivi. Eden aktualnih na tem področju je beg možganov visoko izobražene mlajše delovne sile, ki je med drugim lahko posledica plačnega sistema v javnem sektorju. Slovenski raziskovalci pogosto odhajajo v tujino, kjer imajo boljše priložnosti na univerzah ali v gospodarstvu. Zaradi nestimulativnega sistema javnih plač je omejeno tudi zaposlovanje strokovnega kadra v javnem sektorju, posledično pa primanjkuje znanja za uvažanje UI v javni sektor (Evropska komisija, 2025a).

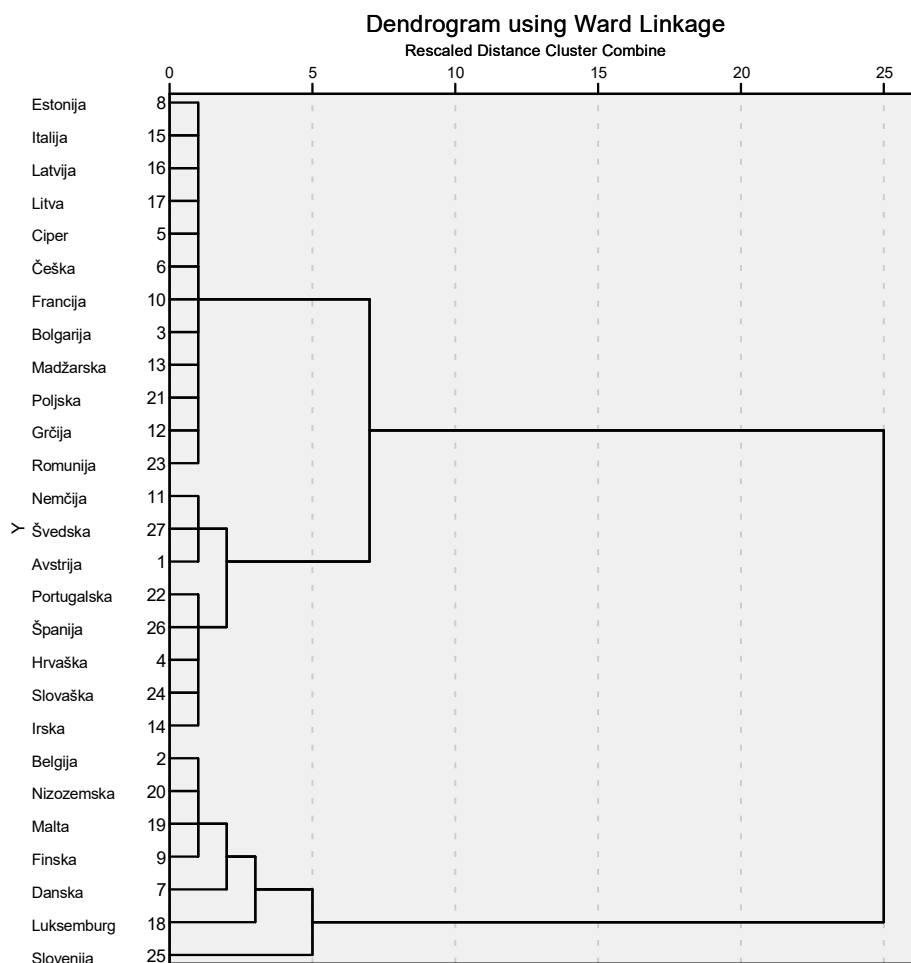
Dodaten izziv predstavlja premajhno financiranje temeljnih raziskav, kar vodi do pomanjkanja kadra v raziskovalnem sektorju. Rast tehnoloških podjetij dodatno ogroža in poslabšuje težave z odlivom raziskovalcev. Pomemben izziv je tudi potreba po regulaciji UI za preprečitev širjenja lažnih novic in vsebine ali kakršne koli druge škodljive rabe. Na drugi strani ima Slovenija nekatere ključne prednosti, ki ji omogočajo nadpovprečno pozicijo in konkurenčnost na področju UI. Druga prednost Slovenije je relativna majhnost države, ki omogoča učinkovito združevanje razvojnih in uporabniških kompetenc. Slovenija aktivno sodeluje v organizacijah, kot so OECD, Svet Evrope in UNESCO, ter uživa politično podporo za nadaljnji razvoj na področju UI (Evropska komisija, 2025a).

5 Združevanje držav v skupine na področju uporabe UI v podjetjih

Proučevanje konkurenčnosti slovenskih podjetij pri uporabi umetne inteligence v primerjavi z državami EU je temeljilo na izbranih kazalcih, ki smo jih analizirali glede na odstopanje od posameznih vrednosti držav in povprečja EU. Razširitev analize nam omogoča metoda združevanja podatkov, ki lahko glede na podobnosti podatkov razvrsti države v skupine. V omenjeno skupino metod sodi Wardova metoda, ki minimizira varianco znotraj skupin in z uporabo kvadrirane evklidske razdalje maksimizira homogenost znotraj skupin (Großwendt idr., 2019). Rezultat Wardove metode je dendrogram, ki prikazuje razvrstitev enot oz. držav v skupine (Bastič, 2006, str. 40–41).

Z Wardovo metodo smo analizirali vseh deset kazalcev uporabe umetne inteligence v podjetjih z desetimi ali več zaposlenimi, ki smo jih predhodno analizirali v prispevku, za 27 držav EU za leto 2023. Slika 11 prikazuje dendrogram, s katerim lahko z drevesnim razvrščanjem razvrstimo države v tri večje skupine.

Slika 10: Dendrogram združevanja držav v skupine glede na uporabo UI v podjetjih po Wardovi metodi



Opomba: Izvirni izpis iz SPSS 28.0.

V prvo skupino držav uvrščamo Bolgarijo, Ciper, Češko, Estonijo, Francijo, Grčijo, Madžarsko, Italijo, Latvijo, Litvo, Poljsko in Romunijo. Pri večini proučevanih kazalcev ima ta skupina držav relativno najmanjše povprečne vrednosti kazalca uporabe umetne inteligence. V drugo skupino držav uvrščamo Avstrijo, Hrvaško, Nemčijo, Irsko, Portugalsko, Slovaško, Španijo in Švedsko. Glede na proučevane kazalce se ta skupina držav uvršča okrog povprečja EU, prav tako so povprečne vrednosti večine proučevanih kazalcev države te skupine relativno večje od prve skupine in relativno manjše od tretje skupine. Drevesna razvrstitev držav prikazuje relativno večjo podobnost med državami prve in druge skupine v primerjavi s tretjo skupino držav, ki ima pri večini kazalcev relativno največje vrednosti uporabe umetne inteligence. V tretjo skupino držav uvrščamo Belgijo, Dansko, Finsko, Luksemburg, Malto, Nizozemsko in Slovenijo. Države iz omenjene skupine držav so bile pogosto navedene kot vodilne države pri proučevanih kazalcih uporabe umetne inteligence.

Omenjeni seznam držav v posamezni skupini je prikazan v tabeli 1, medtem ko je povprečna vrednost posameznega kazalca za pripadajočo skupino razvidna v tabeli 2.

Tabela 1: Članstvo držav v skupinah glede na uporabo UI v podjetjih po Wardovi metodi

Skupina 1	Skupina 2	Skupina 3
Bolgarija	Avstrija	Belgija
Ciper	Hrvaška	Danska
Češka	Nemčija	Finska
Estonija	Irska	Luksemburg
Francija	Portugalska	Malta
Grčija	Slovaška	Nizozemska
Madžarska	Španija	Slovenija
Italija	Švedska	
Latvija		
Litva		
Poljska		
Romunija		

Vir: Lastni.

Tabela 2: Povprečne vrednosti kazalcev uporabe UI v podjetjih glede na razvrščene skupine po Wardovi metodi

	Skupina 1	Skupina 2	Skupina 3
Delež podjetij, ki uporabljajo UI za IKT varnost	0,49	0,85	1,36
Delež podjetij, ki uporabljajo UI za logistične namene	1,23	2,20	4,58
Delež podjetij, ki uporabljajo UI za naravno generiranje jezika (NGL)	1,03	2,40	4,17
Delež podjetij, ki uporabljajo UI za rudarjenje besedil	1,27	2,43	4,17
Delež podjetij, ki uporabljajo strojno učenje za podatkovno analizo v Sloveniji	1,71	3,75	5,52
Delež podjetij, ki uporabljajo UI za prepoznavanje stvari ali oseb na slikah ter za njihovo obdelavo	1,43	2,95	5,05
Podjetja z zelo nizkim digitalnim indeksom, ki uporabljajo UI	1,82	3,98	6,06
Delež podjetij z nizkim indeksom, ki uporabljajo UI	0,85	1,65	2,13
Delež podjetij z visokim digitalnim indeksom, ki	1,49	3,03	5,21

uporabljajo UI			
Delež podjetij z zelo visokim digitalnim indeksom, ki uporabljajo UI	0,22	0,43	0,38

Vir: Lastni.

6 Sklep

Slovenija ima več kot 40-letno zgodovino raziskovanja UI ter je aktivno vpeta v njen razvoj in implementacijo na različnih področjih. Kljub temu da nekoliko zaostaja za največjimi zahodnimi državami, izkazuje visoko stopnjo vlaganja v raziskave UI na prebivalca ter močno akademsko in strokovno skupnost. Ključni izzivi ostajajo pomanjkanje kadrov in vključevanje vsebin o UI v izobraževalni sistem, zlasti na osnovno- in srednješolski ravni. Nacionalna strategija in mednarodno sodelovanje omogočata Sloveniji, da ohrani konkurenčnost ter prispeva k razvoju zaupanja vrednih in etičnih rešitev UI v skladu z evropskimi vrednotami.

Na podlagi analize uporabe UI v slovenskih podjetjih lahko ugotovimo, da Slovenija na določenih področjih presega povprečje EU in se uvršča med vodilne države v Uniji. Posebej izstopa pri uporabi UI za IKT varnost in prepoznavanje slik, kjer je med najboljšimi v Evropi. Prav tako je nadpovprečna pri implementaciji UI v logistiko, NGL in strojnem učenju za analizo podatkov. Kljub temu obstajajo področja, kjer Slovenija zaostaja, zlasti pri uporabi UI za rudarjenje besedil, kjer je skoraj na dnu evropske lestvice.

Povečevanje uporabe UI prinaša številne prednosti, kot so avtomatizacija procesov, optimizacija delovanja podjetij, večja konkurenčnost in izboljšanje trajnosti poslovanja. Vendar pa ostajajo tudi izzivi, kot so tehnološka infrastruktura, usposobljenost kadra in varnost podatkov. Za nadaljnji razvoj slovenskega podjetniškega ekosistema na področju UI bo ključno vlaganje v raziskave, izobraževanje in sodelovanje med zasebnim in javnim sektorjem. Čeprav Slovenija na določenih področjih dosega nadpovprečne rezultate, ostaja prostor za izboljšave in krepitev vloge UI v gospodarstvu, kar bo prispevalo k večji konkurenčnosti in trajnostnemu razvoju države. Z Wardovo metodo združevanja podatkov smo razdelili države EU v tri skupine, pri čemer se je Slovenija uvrstila v tretjo skupino držav, ki ima pri večini kazalcev največje povprečne vrednosti uporabe UI v podjetjih.

Slovenija izkazuje nadpovprečno stopnjo digitalizacije podjetij v primerjavi s povprečjem EU, kar dokazuje tudi visoka stopnja uporabe UI v podjetjih z različnimi ravni digitalne intenzivnosti.

Kljub temu pa obstajajo izzivi, kot so beg možganov, omejeno financiranje raziskav in potreba po regulaciji UI. Slovenija ima pomembne prednosti, kot so močna akademska tradicija, majhnost, ki omogoča hitrejšo prilagoditev, ter dobro vzpostavljena mednarodna sodelovanja. Za nadaljnji razvoj bo ključnega pomena vlaganje v raziskave, privabljanje in zadrževanje (mladih) talentov ter strateška regulacija UI, ki bo omogočala njen varnejši in učinkovitejši razvoj.

Literatura in viri

1. Abduljabbar, R., Dia, H., Liyanage, S., & Bagloee, S. A. (2019). Applications of artificial intelligence in transport: An overview. *Sustainability*, 11(1), 189. <http://doi.org/10.3390/su11010189>
2. Bastič, M. (2006). Metode raziskovanja. Univerza v Mariboru Ekonomsko-poslovna fakulteta.
3. Chen, W., Men, Y., Fuster, N., Osorio, C., & Juan, A. A. (2024). Artificial intelligence in logistics optimization with sustainable criteria: A review. *Sustainability*, 16(21), 9145. <https://doi.org/10.3390/su16219145>
4. Eurostat. (2024a). *Digital Intensity Index (DII) composition overview 2015–2024*. Eurostat. https://ec.europa.eu/eurostat/cache/metadata/Annexes/isoc_e_dii_esmsip2_an_1.pdf
5. Eurostat. (2024b). *How digitalised have the EU's enterprises become?* Eurostat. <https://ec.europa.eu/eurostat/web/products-eurostat-news/w/ddn-20240829-1>
6. Eurostat. (2025a). *Use of artificial intelligence in enterprises*. Eurostat. https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Use_of_artificial_intelligence_in_enterprises
7. Eurostat. (2025b). *Artificial intelligence by size class of enterprise*. Eurostat. https://ec.europa.eu/eurostat/data-browser/view/isoc_eb_ai__custom_15887300/default/table?lang=en
8. Evropska komisija. (2025a). *Slovenia AI Strategy Report*. Evropska komisija. https://ai-watch.ec.europa.eu/countries/slovenia/slovenia-ai-strategy-report_en
9. Evropska komisija. (2025b). *European approach to artificial intelligence*. Evropska komisija. <https://digital-strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence>
10. Evropska komisija. (2025c). *Glossary: Digital Intensity Index (DII)*. Evropska komisija. [https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Glossary:Digital_Intensity_Index_\(DII\)&curid=120437&ol-did=614292#:~:text=The%20digital%20intensity%20index%20\(DII,a%20score%20of%201%20point](https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Glossary:Digital_Intensity_Index_(DII)&curid=120437&ol-did=614292#:~:text=The%20digital%20intensity%20index%20(DII,a%20score%20of%201%20point)
11. Evropska komisija. (2025d). *Europe's digital decade: Digital targets for 2030*. Evropska komisija. https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_en
12. French, A., Shim, J. P., Risius, M., Larsen, K. R., & Jain, H. (2021). The 4th industrial revolution powered by the integration of AI, blockchain, and 5G AI. *Communications of the Association for Information Systems*, 49(1), 6. <http://doi.org/10.17705/1CAIS.04910>
13. Gospodarska zbornica Slovenije. (2021). *Nacionalni program spodbujanja razvoja in uporabe umetne inteligence v Republiki Sloveniji*. Gospodarska zbornica Slovenije. <https://www.gzs.si/Portals/Panoga-ZIT/Vsebine/novice-priponke/NpUI-SI-2025.pdf>

14. Großwendt, A., Röglin, H., & Schmidt, M. (2019). Analysis of Ward's method. V *Proceedings of the Thirtieth Annual ACM-SIAM Symposium on Discrete Algorithms* (str. 2939–2957). Society for Industrial and Applied Mathematics. <http://doi.org/10.1137/1.9781611975482.182>
15. Jorge Ricart, R., Van Roy, V., Rossetti, F., & Tangi, L. (2022). AI Watch. National strategies on Artificial Intelligence: A European perspective. 2022 edition. Evropska komisija. <http://doi.org/10.2760/385851>
16. Jorge Ricart, R., Van Roy, V., Rossetti, F., & Tangi, L. (2022). AI Watch. National strategies on Artificial Intelligence: A European perspective. 2022 edition. Evropska komisija. <http://doi.org/10.2760/385851>
17. Lee, I., & Shin, Y. J. (2020). Machine learning for enterprises: Applications, algorithm selection, and challenges. *Business Horizons*, 63(2), 157–170. <http://doi.org/10.1016/j.bushor.2019.10.005>
18. Mihaï, F., Aleca, O. E., & Gheorghe, M. (2023). Digital transformation based on AI technologies in European Union organizations. *Electronics*, 12(11), 2386. <https://doi.org/10.3390/electronics12112386>
19. MIŽŠ. (2022). *Okvir računalništva in informatike od vrtca do srednje šole. Poročilo strokovne delovne skupine za analizo prisotnosti vsebin računalništva in informatike v programih osnovnih in srednjih šol ter za pripravo študije o možnih spremembah (RINOS)*. Ministrstvo za izobraževanje, znanost in šport. https://www.racunalninstvo-in-informatika-za-vse.si/assets/img/fordownload/Porocilo_RINOS_10_1_22.pdf
20. Požun, R., Marinšek D., Jelenčič, J., Massri, M. B., Gošnak, I., Grm, T., & Korošec, T. (2023). Adoption of AI technologies in Slovenia. V Muren, P. D., Koman, M., & Redek, T. (Ured.), *Beyond bits and algorithms: Redefining businesses and future of work* (str. 73–86). Časnik Finance.
21. Redek, T., Koman, M., & Muren, P. D. (2023). The use of artificial intelligence in Slovenian companies: Main facts and research agenda. V Muren, P. D., Koman, M., & Redek, T. (Ured.), *Beyond bits and algorithms: Redefining businesses and future of work* (str. 103–118). Časnik Finance.
22. SiStat (2025). *Number of enterprises by usage of artificial intelligence technologies and size class, Slovenia, multiannually*. Statistični urad Republike Slovenije. <https://pxweb.stat.si/SiStatData/pxweb/en/Data/-/2984705S.px/table/tableViewLayout2/>
23. Trampuž, M. (2023). *Vodič uvajanja umetne inteligence v mala in srednja podjetja v Sloveniji*. Gospodarska zbornica Slovenije. https://www.gzs.si/Portals/Panoga-ElektroIndustrija/Vodic_uvajanja_umetne_inteligence_v_mala_in_srednja_podjetja_vSloveniji_WEB2.pdf
24. Vasquez Rojas, C., Roldan Reyes, E., Aguirre y Hernandez, F., & Cortes Robles, G. (2018). Integration of a text mining approach in the strategic planning process of small and medium-sized enterprises. *Industrial Management & Data Systems*, 118(4), 745–764. <http://doi.org/10.1108/IMDS-01-2017-0029>
25. Vister, A. (2024). *Umetna inteligenca v podjetjih: sodobni pogled na inovacijo in produktivnost*. Regijska razvojna agencija ROD Ajdovščina. <https://rra-rod.si/umetna-inteligenca-v-podjetjih-sodobni-pogled-na-inovacijo-in-produktivnost/>
26. Zhou, Z., Liu, Y., Yu, H., & Ren, L. (2020). The influence of machine learning-based knowledge management model on enterprise organizational capability innovation and industrial development. *Plos one*, 15(12), e0242253. <https://doi.org/10.1371/journal.pone.0242253>

MERJENJE NEGOTOVOSTI KIBERNETSKE VARNOSTI V ZDRUŽENIH DRŽAVAH AMERIKE S POMOČJO APLIKACIJE STANFORD CABLE TV NEWS ANALYZER

Kaja Gartner Jovanović, študentka, Univerza v Mariboru, Ekonomsko-poslovna fakulteta

Marko Možina, študent, Univerza v Ljubljani, Fakulteta za elektrotehniko

Doc. dr. Dejan Romih, Univerza v Mariboru, Ekonomsko-poslovna fakulteta 

Povzetek: V tem prispevku podajamo štiri merila negotovosti kibernetne varnosti, ki jih lahko oblikovalci politike in raziskovalci uporabljajo za merjenje negotovosti kibernetne varnosti v Združenih državah Amerike. Njihova posebnost je, da temeljijo na ameriških kabelskih novicah. Analiza kabelskih novic na televizijskih kanalih CNN, FOX in MSNBC je pokazala, da je bila po letu 2010 negotovost kibernetne varnosti v Združenih državah Amerike največja po hekerskem napadu na ameriško naftovodno omrežje Colonial Pipeline oz. ameriško podjetje Sony Pictures Entertainment. To ugotovitev moramo ublažiti z nekaterimi omejitvami. Upoštevali smo namreč samo kabelske novice (na največjih TV-postajah), pri čemer izkušnje učijo, da kabelske televizije ne poročajo o vseh kibernetnih incidentih, ampak samo o nekaterih (največjih). Poleg tega nismo upoštevali vseh ključnih besed, ampak samo nekatere (najpomembnejše). To pa ne pomeni, da merila niso koristno orodje za oblikovalce politike in raziskovalce, ampak samo, da moramo dobljene podatke jemati z rezervo.

Ključne besede: kabelska novica, negotovost, Stanford Cable TV News Analyzer

Cobiss: 1.08

1 Uvod

Negotovost kibernetске varnosti (angl. *cybersecurity uncertainty*) definiramo kot negotovost glede kibernetскеga incidenta (angl. *cyber incident*), tj. kibernetске grožnje (angl. *cyber threat*) ali njene uresničitve (OECD, 2024). Leta 2024 je Organizacija za gospodarsko sodelovanje in razvoj (OECD) podala dve merili negotovosti kibernetске varnosti: na časopisnih novicah temelječi indeks negotovosti kibernetске varnosti za Francijo, Nemčijo in Združene države Amerike (ZDA) ter na Google Trends temelječi indeks negotovosti kibernetске varnosti za Francijo, Nemčijo in ZDA, ki omogočata merjenje, opazovanje in spremljanje negotovosti kibernetске varnosti. Očitno je, da obstaja potreba po merjenju, opazovanju in spremljanju negotovosti kibernetске varnosti. Poleg tega je kibernetска varnost zelo aktualna tema (Florackis idr., 2020; Jamilov, Rey & Tahoun, 2021; Kotidis & Schreft, 2022). Izkazalo se je namreč, da so države, kot so Iran, Kitajska, Rusija in Severna Koreja, grožnja za kibernetсko varnost.

Proučevanje negotovosti kibernetске varnosti povzroča potrebo po interdisciplinarnosti. Eden izmed razlogov za to je, da negotovosti ni mogoče neposredno meriti, kar otežuje njeno opazovanje in spremljanje ter ugotavljanje njenih vzrokov in posledic, zato obstaja potreba po razvoju indeksov negotovosti, ki omogočajo njeno posredno merjenje. Pri njihovem razvoju si lahko pomagamo z znanjem in izkušnjami iz ekonomije, informatike, kibernetike, psihologije, sociologije ipd. Upoštevati pa moramo, da živimo in delamo v dobi umetne inteligence, ki spreminja razmere v družbi in gospodarstvu, zaradi česar moramo biti prilagodljivi. To vpliva tudi na merjenje, opazovanje in spremljanje negotovosti (ne glede na vrsto).

Namen tega prispevka je zapolniti vrzel v literaturi o kibernetски varnosti in dopolniti seznam meril negotovosti kibernetске varnosti, ki se uporabljajo v praksi. Izkušnje učijo, da je merjenje, opazovanje in spremljanje negotovosti kibernetске varnosti nujno potrebno za povečanje kibernetске odpornosti (angl. *cyber resilience*), tj. odpornosti proti kibernetским incidentom (Safitra idr., 2024; Stanik & Napiórkowski, 2023; Tzavara & Vassiliadis, 2024).

Prispevek je strukturiran tako, da ima še štiri poglavja. V drugem poglavju podajamo metode, v tretjem rezultate, v četrtem razpravo, v petem pa sklep.

2 Metode

V raziskavi smo uporabili aplikacijo Stanford Cable TV News Analyzer (<https://tvnews.stanford.edu/>) (Hong idr., 2021), ki so jo razvili raziskovalci na Univerzi Stanford. Aplikacija omogoča merjenje, opazovanje in spremljanje kabelskih novic (časa zaslona) na televizijskih kanalih CNN, FOX in MSNBC. Njena posebnost je, da temelji na uporabi umetne inteligence, ki omogoča analiziranje kabelskih novic. V raziskavi smo uporabili mesečne podatke od januarja 2010, ko je Univerza Stanford začela z merjenjem časa zaslona na ameriški kabelski televiziji, do septembra 2024. Na kabelskih novicah temelječe indekse negotovosti kibernetске varnosti smo dobili tako, da smo na spletni strani Cable TV News Analyzer vtipkali:

- text="cyber attack | cyber crime | cyber incident | cyber risk | cyber security | cyber war | cyber warfare | cyberattack | cybercrime | cyberincident | cyberrisk | cybersecurity | cyberwar | cyberwarfare | hacker | ransomware" (**cyber_1**);
- text="cyber attack | cyber attacks | cyber crime | cyber crimes | cyber incident | cyber incidents | cyber risk | cyber risks | cyber security | cyber war | cyber wars | cyber warfare | cyberattack | cyberattacks | cybercrime | cybercrimes | cyberincident | cyberincidents | cyberrisk | cyberrisks | cybersecurity | cyberwar | cyberwars | cyberwarfare | hacker | hackers | ransomware | ransomwares" (**cyber_2**);
- text="cyber" AND text="attack | attacks | crime | crimes | incident | incidents | risk | risks | security | war | wars | warfare | hacker | hackers | ransomware | ransomwares" AND textwindow="10" (**cyber_3**);
- text="cyber attack | cyber attacks | cyber crime | cyber crimes | cyber incident | cyber incidents | cyber risk | cyber risks | cyber security | cyber war | cyber wars | cyber warfare | cyberattack | cyberattacks | cybercrime | cybercrimes | cyberincident | cyberincidents | cyberrisk | cyberrisks | cybersecurity | cyberwar | cyberwars | cyberwarfare | hacker | hackers | ransomware | ransomwares | malware | phishing | data breach | data breaches | DDoS | denial of service | spyware | trojan | trojans | worm | worms | zero-day | backdoor | backdoors | social engineering" (**cyber_4**).

Na kabelskih novicah temelječi indeksi negotovosti kibernetске varnosti temeljijo na predpostavki, da je velikost negotovosti kibernetске varnosti odvisna od velikosti poročanja ameriških medijev o kibernetских incidentih. Izkušnje namreč učijo, da poročanje medijev vpliva na

oblikovanje javnega mnenja (Koné & Mullet, 1994; Public Health Institute, 2023), npr. o negotovosti. Problem je, da ni nujno, da večji indeks pomeni tudi večjo negotovost (v praksi).

Indeksi cyber_1, cyber_2, cyber_3 in cyber_4 se med seboj razlikujejo po številu ključnih besed ter uporabi operatorja AND in časovnega intervala. Indeks cyber_1 temelji na majhnem številu ključnih besed, indeks cyber_2 na srednje velikem številu ključnih besed, indeks cyber_4 na velikem številu ključnih besed, indeks cyber_3 pa na uporabi operatorja AND in časovnega intervala (textwindow="10"), kar v našem primeru pomeni, da se morata v časovnem intervalu 10 sekund v podnaslovu kabelskih novic pojaviti beseda cyber in vsaj ena od drugih ključnih besed.

3 Rezultati

V tem poglavju podajamo rezultate raziskave, v okviru katere nas je zanimalo, ali in kako lahko merimo, opazujemo in spremljamo negotovost kibernetike varnosti (v ZDA) s pomočjo spletne aplikacije Stanford Cable TV News Analyzer. Slika 1 kaže opisne statistike za spremenljivke, tj. indekse negotovosti kibernetike varnosti, cyber_1, cyber_2, cyber_3 in cyber_4.

Slika 1: Opisne statistike za spremenljivke cyber_1, cyber_2, cyber_3 in cyber_4

Variable	Obs	Mean	Std. dev.	Min	Max
cyber_1	178	211.842	321.9865	2	2539.23
cyber_2	178	392.6516	555.7585	5	4220.872
cyber_3	178	1604.755	2348.43	42.759	17524.82
cyber_4	178	4656.448	5312.869	310.236	40224.98

Vir podatkov: Hong idr. (2021), lastni izračuni.

S slike 1 je razvidno, da smo vse spremenljivke opazovali enako dolgo, tj. 178 mesecev. Spremenljivka cyber_1 ima najmanjše ($M = 211,84$ sekunde), spremenljivka cyber_4 pa največje povprečje ($M = 4656,45$ sekunde), kar smo pričakovali glede na kriterije izbora ključnih besed. To velja tudi za standardni odklon.

V okviru raziskave nas je zanimalo tudi, kakšna je korelacija med spremenljivkami cyber_1, cyber_2, cyber_3 in cyber_4.

Slika 2: Korelacija med spremenljivkami cyber_1, cyber_2, cyber_3 in cyber_4

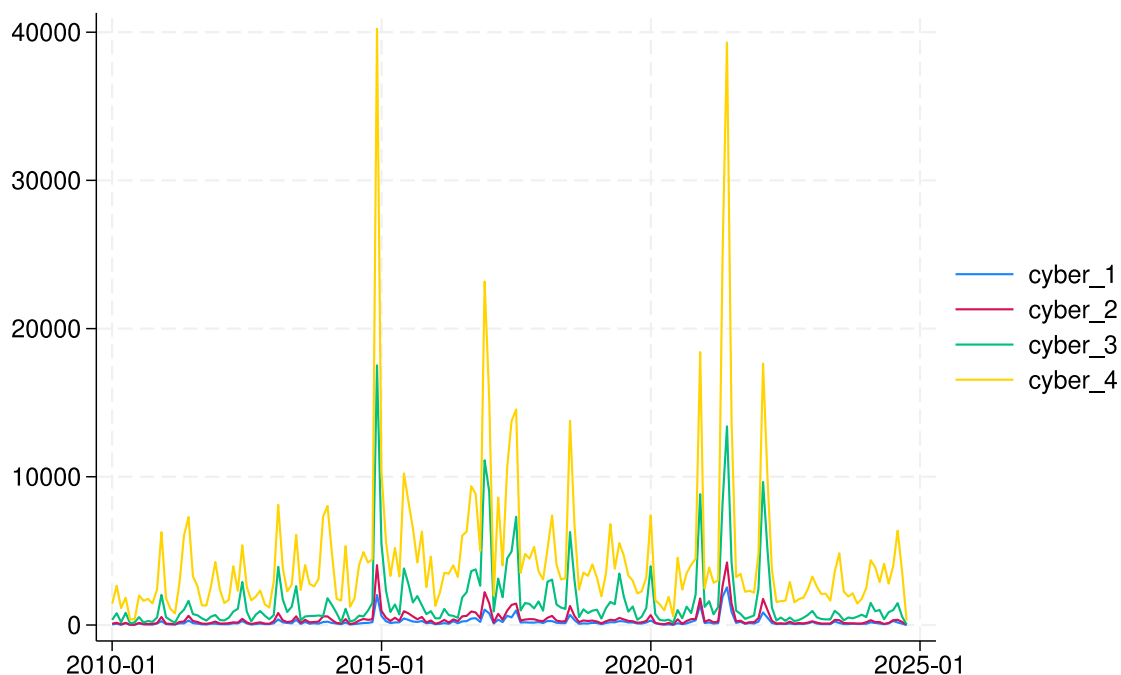
	cyber_1	cyber_2	cyber_3	cyber_4
cyber_1	1.0000			
cyber_2	0.9785	1.0000		
cyber_3	0.9290	0.9584	1.0000	
cyber_4	0.9672	0.9937	0.9593	1.0000

Vir podatkov: Hong idr. (2021), lastni izračuni.

S slike 2 je razvidno, da je najmočnejša korelacija med spremenljivkama cyber_1 in cyber_2 ($r = 0,98$), najšibkejša pa med spremenljivkama cyber_1 in cyber_3 ($r = 0,93$). Kljub temu so korelacije med spremenljivkami cyber_1, cyber_2, cyber_3 in cyber_4 zelo močne, saj so vrednosti korelacijskega koeficienta večje od 0,90. To je koristna informacija za druge raziskovalce, saj nakazuje na to, da je mogoče uporabiti tudi manj zahtevne indekse negotovosti kibernetске varnosti.

Slika 3 kaže gibanje spremenljivk cyber_1, cyber_2, cyber_3 in cyber_4.

Slika 3: Gibanje spremenljivk cyber_1, cyber_2, cyber_3 in cyber_4



Opomba: Os x kaže čas v mesecih, os y pa čas zaslona v sekundah.

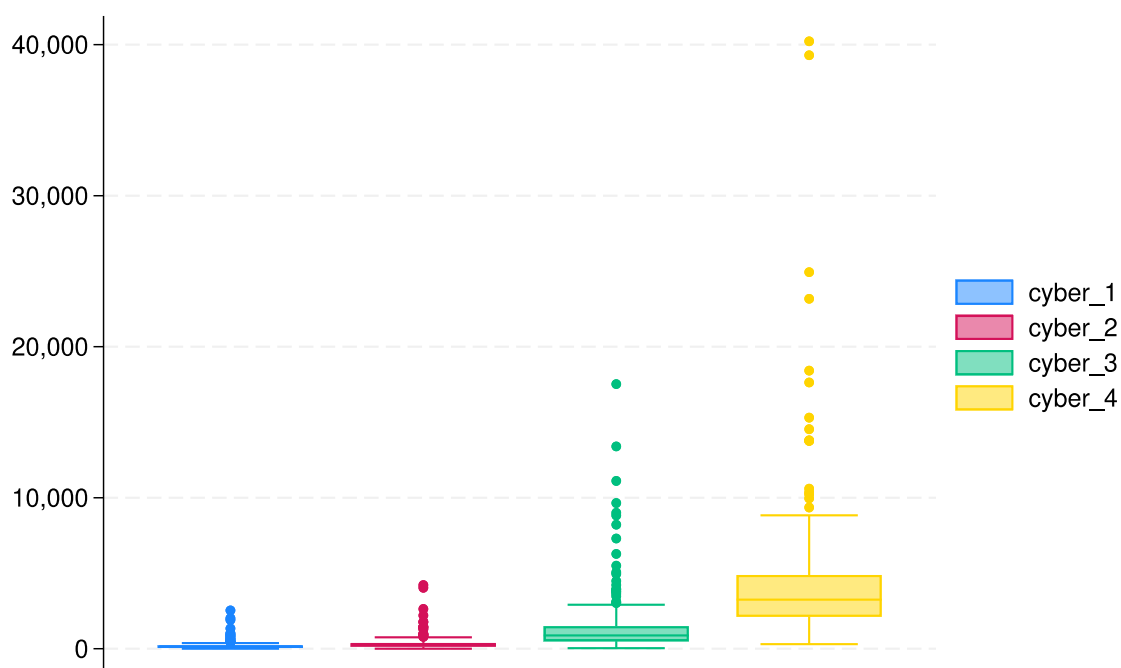
Vir podatkov: Hong idr. (2021), lastni izračuni.

S slike 3 je razvidno, da sta spremenljivki cyber_1 in cyber_2 največjo vrednost dosegli junija 2021 (2539,23 sekunde oz. 4222,87 sekunde), spremenljivki cyber_3 in cyber_4 pa decembra 2014

(17.524,82 sekunde oz. 40.225,98 sekunde). Analiza kabelskih novic kaže, da so junija 2021 ameriški mediji poročali o povečanem številu napadov z izsiljevalskim programjem v ZDA (zlasti pa o hekerskem napadu na naftovodno omrežje Colonial Pipeline, ki ga je maja 2021 izvedla /ruska/ hekerska skupina DarkSide¹), decembra 2014 pa o hekerskem napadu na Sony Pictures Entertainment Inc., ki ga je novembra 2014 izvedla (severnokorejska) hekerska skupina Guardians of Peace.

Poleg gibanja spremenljivk cyber_1, cyber_2, cyber_3 in cyber_4, nas je zanimala tudi njihova razpršenost. Slika 4 kaže grafikone kvartilov za spremenljivke cyber_1, cyber_2, cyber_3 in cyber_4.

Slika 4: Razpršenost spremenljivk cyber_1, cyber_2, cyber_3 in cyber_4



Opomba: Os y kaže čas zaslona v sekundah.

Vir podatkov: Hong idr. (2021), lastni izračuni.

S slike 4 je razvidno, da ima spremenljivka cyber_4 največjo, spremenljivka cyber_1 pa najmanjšo razpršenost, kar smo pričakovali glede na sestavo indeksov negotovosti kibernetске varnosti.

¹ Gl. Bradley, 2022.

4 Razprava

Rezultati kažejo, da aplikacija Stanford Cable TV News Analyzer omogoča merjenje, opazovanje in spremljanje negotovosti kibernetске varnosti, kar je koristna informacija za strokovnjake za kibernetско varnost. Izkazalo se je, da obstaja potreba po merjenju, opazovanju in spremljanju negotovosti kibernetске varnosti, na kar so opozorili tudi strokovnjaki za kibernetско varnost na OECD-ju. Merila negotovosti kibernetске varnosti, ki smo jih razvili za potrebe raziskave, kažejo, da je bila negotovost kibernetске varnosti v ZDA največja po hekerskem napadu na ameriško naftovodno omrežje oz. po hekerskem napadu na ameriški filmski studio Sony Pictures Entertainment. Ugotovili smo tudi, da sta od izbora ključnih besed in metode merjenja odvisni kakovost in uporabnost meril. Izziv pa je, kako njihovo kakovost in uporabnost še povečati.

5 Sklep

V tem prispevku smo podali štiri merila negotovosti kibernetске varnosti, ki temeljijo na uporabi (spletne) aplikacije Stanford Cable TV News Analyzer. Ugotovili smo, da lahko z njimi merimo, opazujemo in spremljamo negotovost kibernetске varnosti, kar potrjuje njihovo kakovost in uporabnost. Ugotovili smo tudi, kateri kibernetски incidenti so vplivali na njeno povečanje. Zavedamo pa se, da imajo merila negotovosti tudi svoje pomanjkljivosti, ki jih je treba odpraviti. Ena izmed njih je, da temeljijo na predpostavki, da je velikost negotovosti odvisna od velikosti poročanja, kar vedno ne velja.

Izkušnje učijo, da je analiza kabelskih novic učinkovita metoda raziskovanja, ki omogoča merjenje, opazovanje in spremljanje poročanja o kakem dogajanju ter ugotavljanje njegovih vzrokov in posledic. Toda to zahteva neodvisnost in nepristranskost medijev kot četrte veje oblasti (angl. *fourth branch of government*).

Glede na to, da smo se v prispevku omejili na t. i. velike tri, predlagamo, da se vzorec razširi tudi na druge ameriške televizijske postaje, saj so lahko tudi te vir informacij o negotovosti kibernetске varnosti.

Literatura in viri

1. Bradley, L. P. (2022). Was the Colonial cyberattack the first act of cyberwar against the U.S.? Finding the threshold of war for ransomware attacks. *St. John's Law Review*, 96(2), 487–515. <https://scholarship.law.stjohns.edu/lawreview/vol96/iss2/8/>

2. Florackis, C., Louca, C., Michaely, R., & Weber, M. (2020). *Cybersecurity risk* (NBER Working Paper No. 28196). National Bureau of Economic Research. <https://doi.org/10.3386/w28196>
3. Hong, J., Crichton, W., Zhang, H., Fu, D. Y., Ritchie, J., Barenholtz, J., Hannel, B., Yao, X., Murray, M., Moriba, G., Agrawala, M., & Fatahalian, K. (2021). *Analysis of faces in a decade of US cable TV news*. V *Proceedings of the 27th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining*. Association for Computing Machinery.
4. Jamilov, R., Rey, H., & Tahoun, A. (2021). *The anatomy of cyber risk* (NBER Working Paper No. 28906). National Bureau of Economic Research. <https://doi.org/10.3386/w28906>
5. Koné, D., & Mullet, E. (1994). Societal risk perception and media coverage. *Risk Analysis*, 14(1), 21–24. <https://doi.org/10.1111/j.1539-6924.1994.tb00024.x>
6. Kotidis, A., & Schreft, S. L. (2022). *Cyberattacks and financial stability: Evidence from a natural experiment* (Finance and Economics Discussion Series No. 2022–025). <https://doi.org/10.17016/feds.2022.025>
7. OECD. (2024). *New perspectives on measuring cybersecurity* (OECD Digital Economy Papers No. 366). OECD Publishing. <https://doi.org/10.1787/b1e31997-en>
8. Public Health Institute. (2023, 21. september). *How media coverage of crime shapes perception of public safety: PHI researcher in the SF Chronicle*. PHI. <https://www.phi.org/press/how-media-coverage-of-crime-shapes-perception-of-public-safety-phi-researcher-in-the-sf-chronicle/>
9. Safitra, M. F., Lubis, M., Fakhurroja, H., & Yekti, Y. N. D. (2024). Lessons from the past: A historical literature review on cyber resilience. V A. K. Nagar, D. S. Jat, D. K. Mishra, & A. Joshi (ur.), *Intelligent sustainable systems. WorldCIST 2023* (Lecture Notes in Networks and Systems, Vol. 828, str. 47–56). Springer. https://doi.org/10.1007/978-981-99-8111-3_5
10. Stanik, J., & Napiórkowski, J. (2023). Cyber resilience as a new strategy to reduce the impact of cyber threats. V A. Burduk, A. Batako, J. Machado, R. Wyczółkowski, K. Antosz, & A. Gola (ur.), *Advances in production. ISPEM 2023* (Lecture Notes in Networks and Systems, Vol. 790, str. 75–92). Springer. https://doi.org/10.1007/978-3-031-45021-1_6
11. Tzavara, V., & Vassiliadis, S. (2024). Tracing the evolution of cyber resilience: A historical and conceptual review. *International Journal of Information Security*, 23, 1695–1719. <https://doi.org/10.1007/s10207-023-00811-x>

VLOGA UMETNE INTELIGENCE PRI POVEČEVANJU PRODUKTIVNOSTI IN NJENI UČINKI NA GOSPODARSTVO: SISTEMATIČNI PREGLED LITERATURE

Nina Knez, Univerza v Mariboru, Ekonomsko-poslovna fakulteta, Slovenija 

Asist. Nejc Fir, Univerza v Mariboru, Ekonomsko-poslovna fakulteta, Slovenija 

Povzetek: Umetna inteligenca ima ključno vlogo pri povečevanju produktivnosti. V prispevku smo pregledali dosedanje raziskave in obstoječo literaturo ter obravnavali kompleksnost definiranja umetne inteligence in izpostavili različne načine merjenja produktivnosti. Analizirali smo tudi vpliv umetne inteligence na produktivnost delovne sile, kjer izpostavljamo potencial umetne inteligence za povečevanje učinkovitosti, zlasti v manjših podjetjih, kot tudi morebitno izgubo delovnih mest pri rutinskih opravilih. Raziskave prav tako proučujejo agregatne učinke umetne inteligence, vključno s potencialom za znižanje stroškov in povečanje globalnega BDP-ja, obenem pa opozarjajo na izzive, kot sta neenakomerna implementacija in poglobljanje neenakosti. Pojavlja se potreba po investicijah v človeški kapital in prilagoditvi izobraževalnih sistemov za uspešno integracijo umetne inteligence in izkoriščanje njenih prednosti.

Ključne besede: avtomatizacija, produktivnost, trg dela, umetna inteligenca

1 Uvod

EU obravnava umetno inteligenco (v nadaljevanju UI) kot eno izmed prednostnih nalog zaradi njene predvidene ključne vloge v digitalni preobrazbi gospodarstva in družbe. Evropski parlament (2020) navaja UI kot zmožnost stroja, da izkazuje človeške lastnosti, kot so mišljenje, učenje, načrtovanje in kreativnost. V vsakdanjem življenju pa lahko zasledimo uporabo UI na najrazličnejših področjih in v najrazličnejših oblikah. UI je preoblikovala praktično vsa področja življenja in gospodarstva, in sicer medicino, promet, proizvodnjo, hrano in kmetijstvo, javno upravo itd. Zaznamo jo lahko npr. pri spletnem nakupovanju in oglaševanju, iskanju na spletu, v obliki digitalnih osebnih asistentov, strojnih prevodih, v obliki pametnih domov, mest in infrastrukture, avtomobilih in pri kibernetiki varnosti.

Prispevek je razdeljen na osem poglavij in gre za sistematičen pregled literature. V drugem poglavju opredelimo UI, saj se pojavljajo njene različne definicije. V tretjem poglavju predstavimo različne mere produktivnosti. V četrtem poglavju obravnavamo vlogo UI pri povečevanju produktivnosti delovne sile in potrebo po investiranju v človeški kapital. V petem poglavju proučujemo vlogo UI pri zniževanju stroškov. V šestem poglavju proučujemo izpostavljenost različnih poklicev UI. V sedmem poglavju obravnavamo pričakovanja glede bodočega vpliva UI na gospodarstvo. V osmem poglavju so predstavljene sklepne ugotovitve.

2 Opredelitev UI

UI naglo pridobiva pomembno vlogo v modernem in hitro razvijajočem se okolju. Abbass (2021) je proučeval opredelitev UI, pri čemer je naletel na ovire, ali jo je mogoče definirati. UI je zaradi njene multidisciplinarnosti relativno težko opredeliti v okviru zgolj ene definicije. Abbas poudarja, da je univerzalna in nesporna definicija UI nemogoča, saj je v različnih disciplinah, kot so računalništvo, biologija, filozofija, matematika idr., prav tako so različni nazori o njej. Te različne discipline se osredotočajo na različne poudarke pri definiranju UI, ki so odvisne od njihovih interesov. Kljub izzivom pri postavljanju definicije pa obstaja potreba po njej, saj se s tem zagotovi določena stopnja doslednosti ter jasnosti pri uporabi izraza. Potrebna je jedrnata, jasna in hkrati dovolj fleksibilna definicija, ki ne omejuje razvoja področja in dovoljuje prostor za razvoj in rast koncepta. Pri definiranju UI je torej nujno treba upoštevati in se zavedati različnih perspektiv, ki so posledica njene multidisciplinarnosti narave.

Definiranje UI je izjemno kompleksen proces, kar Samoili idr. (2020) podobno kot Abbass (2021) v poročilu izpostavljajo dejstvo, da enotna in splošno dogovorjena definicija UI ne obstaja. Obstajajo različne disciplinarne perspektive, pri čemer je v poročilu izpostavljena operativna definicija UI, ki omogoča relativno visoko stopnjo celovitosti in vključenosti ključnih vidikov UI. Operativna definicija UI razlaga, da so sistemi UI programski (in morda tudi strojni) sistemi, ki so jih zasnovali ljudje, ki glede na kompleksen cilj delujejo v fizični ali digitalni dimenziji z zaznavanjem svojega okolja skozi pridobivanje podatkov, interpretacijo zbranih strukturiranih ali nestrukturiranih podatkov, razmišljanjem o znanju ali obdelavo informacij, pridobljenih iz teh podatkov, in odločanjem o najboljših ukrepih za doseg danega cilja. Sistemi UI lahko uporabljajo simbolna pravila ali se naučijo numeričnega modela, svoje vedenje pa lahko prilagodijo tudi z analizo, kako njihova prejšnja dejanja vplivajo na okolje. Poročilo omenja še druge definicije UI, ki se predvsem osredotočajo na definiranje UI preko njenih sposobnosti zaznavanja, razmišljanja, učenja, komuniciranja in delovanja v različnih okoljih.

V prispevku Abbass (2021) predlaga in opredeli dve možni definiciji UI za uredniške namene. Prva definicija opredeljuje, da je UI avtomatizacija kognicije. Abbass se v tem primeru predvsem osredotoča na definiranje UI s perspektive kognitivnih procesov, kar pomeni razmišljanje, predstavitev znanja, učenje in prilagajanje, podobno kot izpostavljajo Samoili idr. (2020). Druga definicija razlaga, da je UI družbeni in kognitivni pojav, ki stroju omogoča družbeno integracijo, da opravlja tekovalne naloge, ki zahtevajo kognitivne procese, in komunicira z drugimi entitetami v družbi z izmenjavo sporočil z visoko vsebnostjo informacij in krajšimi reprezentacijami. V tem primeru je izpostavljen družbeni in hkrati kognitivni vidik UI, ki presega zgolj tehnološke meje UI kot izdelka. Abbass prav tako poudarja, da sta ti dve definiciji zgolj odskočna deska za nadaljnje raziskovanje in razpravo o definiranju UI.

Martinez (2019) izpostavlja pomembnost definicije UI, saj je ta vedno bolj prisotna in vpletena v različnih sektorjih gospodarstva in vsakdanjega življenja posameznikov. Nujno je potrebna jasna definicija UI predvsem v pravnem smislu, da pri postavljanju in uporabi zakonov, povezanih z njo, ne povzroča zmede. Izpostavlja problematiko obstoječih definicij UI, ki so preveč splošne ali preveč omejene na specifične kontekste. V nadaljevanju Martinez omenja močno in šibko UI. Šibka UI naj bi simulirala inteligenco, medtem ko močna UI poseduje inteligenco. Takšno razlikovanje je izrednega pomena, da se v pravnem smislu lahko razrešijo vprašanja odgovornosti in regulacije uporabe. V definicijo je treba vključiti tudi ključen element UI, tj. avtonomnost. Ta pomeni, da je

sistem zmožen sprejemati odločitve, neodvisne od zunanjih vplivov, ampak zgolj iz svojega lastnega znanja in izkušenj. Avtor izpostavlja dva možna načina definiranja UI, in sicer deskriptivno in preskriptivno definicijo. Z deskriptivno definicijo naj bi UI definirali z navedbo različnih možnosti njene uporabe, s preskriptivno definicijo pa bi določili potrebne pogoje, ki jih mora nek sistem izpolnjevati, da ga lahko smatramo kot UI.

3 Merjenje produktivnosti

Doseganje gospodarske rasti in visokega standarda življenja je cilj vsake države, pri čemer je produktivnost ključni dejavnik za doseganje teh ciljev. Pri opredelitvi vloge UI pri povečevanju produktivnosti prav tako ne potrebujemo zgolj definicije UI, za katero smo ugotovili, da jo je zelo težko postaviti v meje zgolj ene. Pomembnejše je razumevanje vloge UI pri produktivnosti in potrebno je razumevanje vloge produktivnosti v ekonomskih procesih. Podobno kot pri UI lahko tudi produktivnost definiramo in merimo na različne načine (Steindl & Stroh, 2001). Avtorja na tem mestu navajata produktivnost dela in skupno faktorsko produktivnost (Total Factor Productivity, v nadaljevanju TFP). Produktivnost dela je najpogosteje uporabljena mera produktivnosti in se meri kot realni obseg proizvodnje na opravljeno delovno uro. Med recesijami je rast produktivnosti nizka ali celo negativna, medtem ko je visoka v času ekspanzije. Slednja dinamika nakazuje, da je produktivnost dela izrazito prociklična. Na rast produktivnosti dela vplivata kapitalna intenzivnost in kakovost dela. TFP je drug način merjenja produktivnosti, in sicer se meri kot realni obseg proizvodnje na enoto vseh inputov. To odraža splošno učinkovitost pretvorbe inputov v outpute. Metoda TFP odraža učinke tehnologije, ekonomije obsega, morebitnih neupoštevanih inputov, prerazporeditev virov idr. Na rast TFP pa vplivajo splošno znanje in izobrazba delovne sile, prednosti določenih organizacijskih struktur ali tehnik upravljanja, zmanjšanje neučinkovitosti ter prerazporeditev virov v bolj produktivne namene.

Syverson (2011) je prav tako izpostavil predhodno omenjeni vrsti produktivnosti. Opozoril je, da se pri merjenju produktivnosti pojavljajo določene težave v povezavi z merjenjem outputa v proizvodnji, saj podjetja pogosto proizvajajo več kot en izdelek. Naslednji dejavnik, ki povzroča težave pri merjenju produktivnosti, je spreminjanje cen. To pomeni, da lahko cene odražajo stanje lokalnega trga in ne opredeljujejo učinkovitosti trga. Prav tako združevanje različnih inputov v proizvodnem procesu otežuje merjenje produktivnosti, saj ta zahteva ustrezno utežitev inputov v proizvodni funkciji, pri čemer se pogosto uporablja Cobb-Douglasova proizvodna funkcija. Tudi ustrezno

merjenje elastičnosti proizvodnih dejavnikov in kakovost podatkov povzročata težave pri merjenju produktivnosti.

4 Vloga UI pri povečevanju produktivnosti in potreba po investicijah v človeški kapital

V tem poglavju smo se najprej osredotočili na vlogo UI pri povečevanju produktivnosti na ravni podjetja. Študija Damioli idr. (2021) analizira vpliv UI na produktivnost dela na vzorcu 5257 podjetij, ki so vpeljala UI v svoje poslovanje med letoma 2000 in 2016. Raziskava vključuje različne dejavnike, ki vplivajo na produktivnost, in sicer kapital, delo in znanje. Ugotovitve kažejo na pozitiven vpliv patentov UI na produktivnost dela, vendar je pomembno izpostaviti, da ta učinek velja zgolj za mala in srednja podjetja ter v storitvenih industrijah. Mala in srednja podjetja so se sposobna hitreje prilagoditi in vpeljati UI v svojo dejavnost. Avtorji omenjajo, da se je s podvojitvijo števila patentnih prijav UI produktivnost dela v povprečju povečala za okoli 3 %. V večjih podjetjih in proizvodnih sektorjih pa so učinki izrazito heterogeni. Pomembno je prav tako omeniti časovni vidik vloge UI pri povečevanju produktivnosti, saj je bil vpliv UI na produktivnost relativno večji v obdobju 2009–2016, kot je bil v obdobju 2000–2008.

Nurlia idr. (2023) so podobno kot Damioli idr. (2021) potrdili vpliv UI na povečanje produktivnosti delovne sile. Pri tem pa poudarjajo, da se morajo organizacije in podjetja primerno pripraviti na implementacijo UI. Vpeljava UI sama po sebi ni dovolj, ampak je nujno potrebno zaposlene izobraziti in usposobiti za delo z UI ter primerno prilagoditi svoje poslovne procese, da bodo ti lahko ustrezno uporabljali takšno tehnologijo. Usposabljanje zaposlenih je ključno, saj morajo ti najprej celostno razumeti nove tehnologije UI in kako jo uporabljati za izboljšanje svoje delovne učinkovitosti. V kolikor podjetja to uspešno izvedejo, lahko pričakujejo pozitiven vpliv UI pri povečevanju produktivnosti, saj razumevanje UI predstavlja predpogoj za povečevanje produktivnosti dela. Avtorji obeh študij izpostavljajo potencial UI na povečanje produktivnosti delovne sile, a hkrati opozarjajo na različne možne učinke glede na velikost podjetij in glede na sektor, v katerem se UI uporablja.

Proučevanje vloge UI pri povečevanju produktivnosti ima tudi izrazito makroekonomsko oz. agregatno perspektivo. Acemoglu (2024) se v raziskavi osredotoča na vlogo UI pri makroekonomski produktivnosti. Ugotavlja, da se lahko vpliv UI na agregatno produktivnost prenese preko štirih kanalov. Prvič, s povečanjem obsega nalog, ki jih je mogoče avtomatizirati. Drugič, s povečanjem mejne produktivnosti nalog, ki jih opravlja človeško delo. Tretjič, z zmanjšanjem stroškov

avtomatizacije nalog. Četrtyč, z ustvarjanjem novih nalog ali izdelkov. Pri prvem kanalu se avtomatizacija nanaša predvsem na širitev obsega nalog, ki jih lahko opravljajo kapitalna sredstva, kot so digitalna orodja in različni algoritmi. Drugi kanal se osredotoča na specializacijo ljudi za druge podnaloge, saj bi lahko UI določene naloge opravila namesto njih in na ta način povečala produktivnost. Tretji kanal deluje na način, da UI zmanjšuje stroške, povezane z nadomeščanjem človeškega dela s kapitalom, in se v proizvodne procese vpeljuje vedno več kapitalnih sredstev. Pri četrtem kanalu pa avtor izpostavlja priložnost ustvarjanja popolnoma novih aktivnosti in dobrin, povezanih z UI, ki pred tem niso obstajale, kar pa prispeva k agregatni produktivnosti.

Podrobneje je Acemoglu (2024) v nadaljevanju omenjal Hultenov izrek, ki pojasnjuje, kako se mikroekonomske izboljšave produktivnosti pretvorijo v makroekonomske spremembe. Osnovna ideja je, da UI izboljša produktivnost ali zmanjša stroške pri posameznih nalogah v podjetjih. Nato se meri seštetni vpliv UI v posameznih podjetjih na agregatno produktivnost, tako da pri tem upoštevamo delež gospodarstva, povezanega z nalogami pod vplivom UI. Hultenov izrek razlaga, da je TFP enaka vsoti sprememb produktivnosti pri posameznih nalogah ali dejavnostih, pri čemer so te spremembe utežene z deležem vsake naloge v gospodarstvu, merjenim z njenim prispevkom k BDP-ju. Jabbari in Azizi (2024) v svoji raziskavi izpostavljata pozitivne makroekonomske posledice vpliva UI na gospodarstvo. Podobno kot Acemoglu (2024) izpostavljata avtomatizacijo, obdelavo in analizo velikih količin podatkov, pa tudi večjo natančnost davčnih napovedi, napovedi obrestnih mer idr. Kljub temu obstajajo številni izzivi pri ocenitvi obsega vpliva UI na gospodarstvo in makroekonomsko okolje ter njene vloge pri povečevanju produktivnosti dela in kapitala.

V nadaljevanju tega poglavja opozarjamo na potrebo po investicijah v človeški kapital z vidika znanj in veščin UI. Potreba po vlaganju v človeški kapital in sposobnostih, povezanih z UI, se skozi čas povečuje. Pojavljajo se novi zaposlitveni trendi, in sicer se je leta 2023 povečalo število oglasov za delovna mesta, ki so zahtevala znanja s področja generativne UI. Naložbe v generativno UI pa so se skoraj osemkrat povečale med letoma 2022 in 2023 in dosegle 25,2 milijarde USD. Tudi več kot polovica organizacij je vpeljala uporabo UI na vsaj enem mestu v poslovnem procesu. Največkrat so to napovedne storitve, analitika za pomoč strankam in optimizacija servisnih operacij. Podobno na svojih delovnih mestih uporabljajo UI orodja, kot so GitHub, Copilot in ChatGPT, prav razvijalci programske opreme. Prav tako je moč porasta uporabe UI videti v industrijskem sektorju, kjer se nameščajo industrijski roboti za avtomatizacijo proizvodnje. Na tem področju je vodilna Kitajska. Mnoge države, kot so ZDA, ki so trenutno vodilna v zasebnih investicijah v UI, Kitajska,

države EU in Združeno kraljestvo, pričakujejo v prihodnosti pozitiven vpliv UI na produktivnost, zato povečujejo svoje naložbe v razvoj in implementacijo UI (Maslej idr., 2024).

UI ima zato pomembno vlogo pri pridobitvi znanj že med šolanjem. Uporaba UI pri izobraževanju je spremenila pristop tako učiteljev pri poučevanju kot učencev pri pridobivanju novih znanj. Harry (2023) v raziskavi ugotavlja, da uporaba UI pri učenju omogoča višjo stopnjo personalizacije in s tem učinkovito pripomore k produktivnejšemu učenju in povečevanju motivacije. UI se lahko prilagodi učnemu tempu posameznikov in jim pri tem nudi ustrezno literaturo. Tudi učiteljem lahko olajša delo s hitrejšo obdelavo podatkov, kar lahko omogoči vpeljavo ustrežnejših poučevalnih metod. Maslej idr. (2024) poudarjajo, da bosta dostop do UI in njena uporaba v izobraževalnem procesu omogočila zmanjšanje vrzeli v znanju med posamezniki in tako pripomogla k relativno bolj usposobljeni in produktivnejši delovni sili.

Med investicije v človeški kapital štejemo tudi investicije v zdravje, saj je zdrava delovna sila tudi produktivnejša. Ta tema je poglobljena v razvitih državah, ki se soočajo s problematiko staranja prebivalstva. Kirsten (2010) je preučeval vpliv zdravja zaposlenih tako na individualno produktivnost dela kot tudi na agregatni ravni. Slabo zdravje zaposlenih in porast kroničnih bolezni močno vplivata na povečanje stroškov podjetij in zmanjšanje njihove učinkovitosti. Prav tako se pojavljata absentizem in prezentizem. Absentizem pomeni, da pride v podjetju do izgube delovnih dni zaradi bolezni, prezentizem pa pomeni prisotnost na delovnem mestu z zmanjšano učinkovitostjo zaradi zdravstvenih težav. Prezentizem je izjemno pereč problem, saj je izguba produktivnosti v povprečju 7,5-krat večja od tiste, ki je izgubljena zaradi absentizma, in trikrat večja od neposrednih zdravstvenih stroškov. Študija omenja tudi povezavo med psihosocialnimi dejavniki in produktivnostjo, saj je stres eden izmed pogloblitvenih dejavnikov pri zmanjšanju produktivnosti zaposlenega. Povečuje se zavedanje o tej problematiki, zato se v ta namen promovira zdrav življenjski slog ter se raje osredotoča na preventivo kot kurativo.

Rajpurkar idr. (2022) so v svoji raziskavi proučevali vlogo UI v zdravstvu pri povečevanju produktivnosti. Uvajanje UI v zdravstvu omogoča napredek pri interpretaciji medicinskih slik, pri diagnostiki rakavih obolenj, v gastroenterologiji, oftalmologiji idr. Pojavljajo se tudi možnosti na področju obdelave podatkov kemičnih in genomskih zaporedij in njihovo večje razumevanje. S povečanjem produktivnosti v zdravstvu in hitrejšim ter natančnejšim zaznavanjem ter reševanjem zdravstvenih stanj lahko povečamo agregatno produktivnost dela.

5 Vloga UI pri zniževanju stroškov

V tem poglavju obravnavamo vlogo UI pri zniževanju stroškov. Acemoglu in Restrepo (2018) v raziskavi obravnavata možne posledice, ki bi jih lahko povzročila avtomatizacija in vpeljava UI v poslovne procese. Avtomatizacija vključuje tako vpeljava UI kot robotike, pri čemer vpeljava le-teh zamenja delavce za kapitalno intenzivnejšo proizvodnjo. Pojavi se učinek substitucije proizvodnih dejavnikov, ki bo izrazitejši v prihodnosti, ko bodo relativne cene kapitala vplivale na omenjeni proces ali pa bo prisotna relativno višja produktivnost kapitala v primerjavi z delom. V kolikor se zmanjšajo stroški proizvodnje, se lahko pojavi produktivnostni učinek. Ta predpostavlja, da se zaradi manjših proizvodnih stroškov poveča povpraševanje po delavcih pri nalogah, ki niso avtomatizirane. Povpraševanje po delu se lahko poveča v sektorjih, ki so se avtomatizirali, in tudi v tistih, ki niso bili zaznamovani s procesom avtomatizacije. Kljub temu pa bo avtomatizacija pogosto povzročila učinek substitucije proizvodnih dejavnikov, kar lahko vodi v heterogene posledice pri povpraševanju po delovni sili, plačah in zaposlenosti.

UI lahko stroške znižuje na različne načine, predvsem znotraj optimizacije dobavnih verig. Z napovedno analitiko lahko UI natančneje napove bodoče trende v povpraševanju, pri čemer so lahko napovedi natančnejše tudi do 50 %. Natančnejše napovedi lahko preprečujejo kopičenje zaloge ali pomanjkanje blaga v podjetjih. Shil idr. (2024) so v raziskavi ugotovili, da so podjetja, ki uporabljajo prediktivno analitiko, v povprečju zmanjšala svoje stroške za 18 %. UI lahko prav tako pripomore k zmanjšanju stroškov transporta do 25 % z optimizacijo načrtovanja poti in urnikov v logističnih operacijah. Hitrejše in natančnejše odločanje podjetjem omogoča sprejemanje stroškovno učinkovitejših odločitev.

Učinkovitost programske opreme in UI je tako izrednega pomena, saj lahko te tehnologije z avtomatizacijo ter natančnejšo in hitrejšo analizo znatno vplivajo na znižanje stroškov v poslovnih in proizvodnih procesih. Manjši proizvodni stroški posledično pomenijo tudi padec cen proizvodov in storitev in posledično vpliv na povečanje realnega dohodka gospodinjstev in njihovo povpraševanje po vsem blagu in storitvah (Acemoglu & Restrepo, 2018).

6 Izpostavljenost poklicev UI

Implementacija UI ima kompleksen vpliv na produktivnost in lahko celo vodi do sprememb v zaposlovanju. Nurlia idr. (2023) izpostavljajo možnost izgube delovnih mest zaradi vpeljave UI. Slednja povzroča avtomatizacijo rutinskih in ponavljajočih se del zlasti v proizvodnji in na delovnih

mestih, kjer se zahteva fizično ali ročno delo ter vzdržljivost. Pojavlja se zmanjšana potreba po delovni sili v proizvodnem sektorju. Te ugotovitve potrjuje študija Acemoglu & Restrepo (2020), ki je potrdila negativno korelacijo med uvedbo industrijskih robotov in zaposlovanjem ter plačami med letoma 1990 in 2007 na primeru ZDA. Ocenjena vrednost zmanjšanja zaposlenih je šest delavcev, v kolikor se v poslovni proces uvede en dodaten robot. Prav tako en dodaten robot na tisoč delavcev v povprečju zmanjša plače za približno 0,5 %. Takšno povezavo je mogoče opaziti v proizvodnji, rutinskih in fizičnih poklicih ter pri delavcih brez terciarne izobrazbe. Kljub temu pa implementacija UI ne pomeni nujno neto izgube delovnih mest, ampak morebitno preoblikovanje določenih poklicev.

Raziskava Munro idr. (2019), ki v vzorcu zajema 769 različnih poklicev in proučuje vpliv UI nanje, za razliko izpostavlja, da bo UI v relativno večji meri vplivala na delovna mesta z relativno večjimi dohodki in tista delovna mesta, ki zahtevajo visoko kvalificirano delovno silo. Takšni poklici so relativno bolj izpostavljeni vplivu UI iz več razlogov. Eden izmed pomembnejših izvira iz značilnosti dela in tehnoloških zmožnosti UI. Ti poklici pogosto vključujejo analizo podatkov, načrtovanje, odločanje in reševanje kompleksnejših problemov. V teh primerih se UI uporablja za kognitivne naloge in procese, ki jih relativno hitreje obdelava in analizira ter ponudi optimalne rešitve. Pri avtomatizaciji rutinskih nalog, kot je vnos podatkov ali priprava poročil, se lahko delavci v bolj plačanih in višje kvalificiranih poklicih osredotočijo na zahtevnejše in ustvarjalne naloge. UI predstavlja pomembno dopolnilno orodje na delovnem mestu, ki povečuje posameznikovo učinkovitost. Ob avtomatizaciji rutinskih nalog pa povzroča ustvarjanje novih delovnih mest, ki so povezana z razvojem, implementacijo in vzdrževanjem tehnoloških sistemov UI, kar pa zahteva nova znanja in spretnosti. UI zahteva spremembe potreb po spretnostnih in vodi do dodatnega izobraževanja in nujne prekvalifikacije delovne sile.

UI ima pomemben in znaten vpliv na trg dela. Med poklici, ki so relativno bolj izpostavljeni UI, so poslovni in administrativni poklici, znanstveniki, inženirji, vodje in podjetniki. Relativno najmanj izpostavljeni UI pa so poklici, kot so npr. čistilci, delavci v kmetijstvu, gozdarstvu in ribištvi, pomočniki pri pripravi hrane in ostali pomožni delavci. Delavci z relativno nižjimi dohodki so prav tako manj izpostavljeni vplivom UI, vendar so hkrati manj pripravljeni na prehod, ko se bo začela UI uvajati v njihovo stroko. Poleg tega se pojavljajo nova delovna mesta, povezana z razvojem in vzdrževanjem sistemov UI. S širitvijo UI se pri delodajalcih pojavljajo nove zahteve po spretnostih in veščinah. V državah OECD zaznavajo povečano potrebo po digitalni pismenosti, ustvarjalnosti

in socialnih spretnostih, saj je relativno težko usvojiti veščine UI (OECD, 2023).

7 Pričakovanja glede bodočega vpliva UI na gospodarstvo

Filippucci idr. (2024) so izvedli raziskavo v sklopu OECD na temo vpliva UI na produktivnost, distribucijo dohodka in gospodarsko rast. Avtorji UI obravnavajo kot bazično tehnologijo, ki ima velik potencial pri vplivu na gospodarstvo in družbeno blaginjo. V raziskavi avtorji izpostavljajo različne vidike vpliva UI na agregatno produktivnost, hkrati pa podobno kot Jabbari in Azizi (2024) opozarjajo na negotovost njenih dolgoročnih učinkov na produktivnost. Eden izmed vidikov vpliva UI na produktivnost je povezava UI z inoviranjem. UI ima lastnost avtonomije in s tem sposobnost samoizboljševanja, kar omogoča pospešitev inovacij in posledično povečanje gospodarske rasti. Še eden izmed pozitivnih vplivov UI je možnost zmanjšanja plačne neenakosti znotraj posameznih poklicev.

Poleg pozitivnih vidikov in velikega potenciala UI pa se pojavljajo določene negativne posledice, kot so neenakomerna stopnja uvajanja UI, geografska koncentracija razvoja UI, povečanje neenakosti med različnimi poklici ter posamezniki z različnimi ravnmi izobrazbe, širjenje dezinformacij, pristranskost in kršitve zasebnosti. Prav tako uvajanje UI pogloblja neenakost med državami. Države v razvoju zaostajajo z implementacijo UI v svoja gospodarstva iz več razlogov. Predpogoj za uvajanje UI je namreč dobro razvita digitalna infrastruktura, stabilna internetna povezava, digitalne spretnosti in pismenost, kar pa je v državah v razvoju manj prisotno. K razlikam med državami prispevajo še jezikovna pristranskost razvoja UI, ki je najpogostejše v angleščini, koncentracija znanja UI v nekaj velikih podjetjih in fiskalna zmogljivost držav. Vodilne države pri patentiranju UI so trenutno ZDA, Kitajska in EU (Filippucci idr., 2024).

Projekcije uporabe UI kažejo, da naj bi okoli 70 % podjetij na svetu v svoje delovanje implementiralo UI in da bi skupna stopnja uporabe UI v podjetjih do leta 2030 znašala približno 50 %. Leta 2023 je UI uporabljalo okoli 33 % vseh podjetij. Napovedi kažejo, da bi lahko avtomatizacija dela do leta 2030 povečala svetovni BDP za skoraj 9 %, inovacije izdelkov in storitev pa bi lahko prispevale k 7-odstotnemu povečanju potencialnega BDP-ja. Avtomatizacija dela in inovacije bi lahko tako do leta 2030 povečale svetovni BDP za 16 %. Glede na širše makroekonomske ocene pa ima UI do leta 2030 potencial povečati svetovni BDP do 26 %. Tudi na tem mestu pa se omenjajo negativne eksternalije implementacije UI, kot so stroški prehoda na uporabo UI v podjetjih, morebitna izguba delovnih mest ali potreba po prekvalifikaciji delavcev ter neenakomerna porazdelitev

prednosti uporabe UI med državami, panogami in podjetji (Banerjee idr., 2023).

8 Sklep

UI predstavlja pomemben dejavnik gospodarskega razvoja v sodobnem, hitro razvijajočem se svetu z značilnim potencialom za povečanje produktivnosti na različnih ravneh. Razumevanje njenega vpliva zahteva upoštevanje kompleksnosti definicije UI ter različnih načinov merjenja produktivnosti.

Definiranje UI je izziv zaradi njene multidisciplinarne narave, pri čemer različne discipline poudarjajo različne vidike. Kljub temu se pogosto uporablja operativna definicija UI, ki jo opisuje kot sisteme, zasnovane za zaznavanje okolja, interpretacijo podatkov, razmišljanje ali obdelavo informacij ter sprejemanje odločitev za doseg določenih ciljev. Podobno kot UI se tudi produktivnost definira in meri na različne načine, pri čemer sta ključni meri produktivnost dela in TFP.

Implementacija UI ima dvojen vpliv na trg dela. Na eni strani raziskave nakazujejo na možen pozitiven vpliv UI na povečevanje produktivnosti delovne sile, zlasti v manjših podjetjih in storitvenih dejavnostih, kjer se lažje prilagodijo novim tehnologijam, vendar pa je za uresničitev tega potenciala ključnega pomena usposabljanje zaposlenih in prilagoditev poslovnih procesov. Po drugi strani pa obstaja tudi možnost izgube delovnih mest, predvsem pri rutinskih in ponavljajočih se nalogah v proizvodnji. Kljub temu pa se z razvojem UI odpirajo nova delovna mesta, povezana z njenim razvojem, implementacijo in vzdrževanjem, kar zahteva nove spretnosti in prekvalifikacijo delovne sile. Pomembno je tudi, da UI ne vpliva le na manj zahtevna dela, ampak lahko znatno vpliva tudi na boljše plačana in visoko izobražena delovna mesta, saj je učinkovita pri analizi podatkov in reševanju kompleksnih problemov. Zaradi tega se povečuje potreba po digitalni pismenosti, ustvarjalnosti in socialnih spretnostih.

Z agregatnega vidika ima UI potencial za povečanje produktivnosti preko več kanalov, vključno z avtomatizacijo nalog, povečanjem produktivnosti človeškega dela pri preostalih nalogah, znižanjem stroškov avtomatizacije in ustvarjanjem novih dejavnosti in izdelkov. UI lahko prispeva k znižanju stroškov predvsem z optimizacijo dobavnih verig, natančnejšim napovedovanjem povpraševanja in optimizacijo transporta. Nižji proizvodni stroški lahko posledično povečajo realni dohodek gospodinjstev.

Napovedi kažejo na široko implementacijo UI v prihodnosti z ocenami, da bo do leta 2030 okoli 70

% podjetij uporabljalo UI, kar bi lahko svetovni BDP povečalo za 26 %. Kljub temu pa obstajajo tudi izzivi in potencialne negativne posledice, kot so neenakomerna stopnja uvajanja UI med državami in panogami, povečanje neenakosti med različnimi poklici in posamezniki ter širjenje dezinformacij. Države v razvoju se soočajo z večjimi ovirami pri implementaciji UI zaradi manj razvite digitalne infrastrukture in pomanjkanja digitalnih spretnosti. UI ima znaten potencial za povečanje produktivnosti na vseh ravneh gospodarstva. Za uspešno izkoriščanje teh priložnosti je nujno investirati v človeški kapital, prilagoditi izobraževalne sisteme, nasloviti morebitne negativne vplive na trg dela ter zmanjšati neenakosti pri dostopu do tehnologije in njenih prednosti.

Literatura in viri

1. Abbass, H. (2021). Editorial: What is artificial intelligence? *IEEE Transactions on Artificial Intelligence*, 2(2), 94–95. <http://doi.org/10.1109/TAI.2021.3096243>
2. Acemoglu, D., & Restrepo, P. (2018). *Artificial intelligence, automation, and work* (NBER Working Paper No. 24196). National Bureau of Economic Research. <http://doi.org/10.3386/w24196>
3. Acemoglu, D., & Restrepo, P. (2020). Robots and jobs: Evidence from US labor markets. *Journal of political economy*, 128(6), 2188–2244. <http://doi.org/10.1086/705716>
4. Acemoglu, D. (2024). The simple macroeconomics of AI. *Economic Policy*, 40(121), 13–58. <http://doi.org/10.1093/epolic/eiae042>
5. Banerjee, A., Kabadi, S., & Karimov, D. (2023). The transformative power of AI: Projected impacts on the global economy by 2030. *Review of Artificial Intelligence in Education*, 4 (00), 1–11. <http://doi.org/10.37497/rev.artif.intell.educ.v4i00.20>
6. Damioli, G., Van Roy, V., & Vertesy, D. (2021). The impact of artificial intelligence on labor productivity. *Eurasian Business Review*, 11(2), 1–25. <https://doi.org/10.1007/s40821-020-00172-8>
7. Evropski parlament. (2020). *Kaj je umetna inteligenca in kako se uporablja v praksi?* Evropski parlament. <https://www.europarl.europa.eu/topics/sl/article/20200827STO85804/kaj-je-umetna-inteligenca-in-kako-se-uporablja-v-praksi>
8. Filippucci, F., Gal, P., Jona-Lasinio, C., Leandro, A., & Nicoletti, G. (2024). *The impact of artificial intelligence on productivity, distribution and growth: Key mechanisms, initial evidence and policy challenges* (OECD Working Paper No. 15). OECD. <https://doi.org/10.1787/8d900037-en>
9. Harry, A. (2023). Role of AI in education. *Injury: Interdisciplinary Journal and Humanity*, 2 (3), 260–268. <http://doi.org/10.58631/injury.v2i3.52>
10. Jabbari, A., & Azizi, J. (2024). *The Role of artificial intelligence in macroeconomics*. SSRN. <http://doi.org/10.2139/ssrn.4854582>
11. Kirsten, W. (2010). Making the link between health and productivity at the workplace—A global perspective. *Industrial health*, 48(3), 251–255. <http://doi.org/10.2486/indhealth.48.251>
12. Martinez, R. (2019). Artificial intelligence: Distinguishing between types & definitions. *Nevada Law Journal*, 19(3).

13. Maslej, N., Fattorini, L., Perrault, R., Parli, V., Reuel, A., Brynjolfsson, E., Etchemendy, J., Ligett, K., Lyons, T., Manyika, J., Niebles, J. C., Shoham, Y., Wald, R., & Clark, J. (2024). *The AI Index 2024 Annual Report*. Stanford University. <https://hai.stanford.edu/ai-index/2024-ai-index-report>
14. Munro, M., Whiton, J., & Maxim, R. (2019). *What jobs are affected by AI?* Brookings. <https://apo.org.au/node/269216>
15. Nurlia, N., Daud, I., & Rosadi, M. E. (2023). AI implementation impact on workforce productivity: The role of AI training and organizational adaptation. *Escalate: Economics And Business Journal*, 1(1), 1–13. <http://doi.org/10.61536/escalate.v1i01.6>
16. OECD. (2023). *Employment outlook 2023: Artificial intelligence and the labour market*. OECD Publishing. https://www.oecd.org/en/publications/oecd-employment-outlook-2023_08785bba-en.html
17. Rajpurkar, P., Chen, E., Banerjee, O., & Topol, E. J. (2022). AI in health and medicine. *Nature medicine*, 28(1), 31–38. <http://doi.org/10.1038/s41591-021-01614-0>
18. Samoil, S., López Cobo, M., Gómez, E., De Prato, G., Martínez-Plumed, F., & Delipetrev, B. (2020). *AI watch. Defining artificial intelligence. Towards an operational definition and taxonomy of artificial intelligence*. Publications Office of the European Union. <https://doi.org/10.2760/382730>
19. Shil, S. K., Islam, M. R., & Pant, L. (2024). Optimizing US supply chains with AI: Reducing costs and improving efficiency. *International Journal of Advanced Engineering Technologies and Innovations*, 2(1), 223–247. <https://ija-eti.com/index.php/Journal/article/view/709/740>
20. Steindel, C., & Stiroh, K. J. (2001). *Productivity: What is it, and why do we care about it?* (FRB of New York Staff Report No. 122). Federal Reserve Bank of New York. <http://doi.org/10.2139/ssrn.923421>
21. Syverson, C. (2011). What determines productivity? *Journal of Economic Literature*, 49(2), 326–365. <http://doi.org/10.1257/jel.49.2.326>

Priloga

Tabela 1: Zbirna tabela ključnih ugotovitev dosedanjih raziskav s področja UI in njene vloge pri povečevanju produktivnosti

Avtorji	Ključne ugotovitve
Abbass (2021)	– Težavnost pri definiranju UI; potreba po definiciji zaradi doslednosti – UI kot avtomatizacija kognicije ali kot družbeni in kognitivni pojav
Acemoglu & Restrepo (2018)	– UI povzroča učinek substitucije – Manjši stroški zaradi implementacije UI lahko povečajo povpraševanje po delu; lahko vodijo do cenejših izdelkov in večje kupne moči gospodinjstev – Heterogenost učinkov na plače in zaposlenost
Acemoglu & Restrepo (2020)	– Negativen vpliv industrijskih robotov na zaposlovanje in plače; najizraziteje v proizvodnji, rutinskih in fizičnih poklicih, pri delavcih brez terciarne izobrazbe – Možnost preoblikovanja delovnih mest
Acemoglu (2024)	– Štirje kanali vpliva UI na produktivnost; avtomatizacija nalog, izboljšanje človeškega dela, zmanjšanje stroškov avtomatizacije ter ustvarjanje novih nalog in izdelkov – Učinki UI na posamezne naloge v podjetjih se prenašajo na agregatno produktivnost preko Hultenovega izreka
Banerjee idr. (2023)	– Do leta 2030 bo 70 % podjetij uporabljalo UI, kar bo povečalo globalni BDP za 26 % – Avtomatizacija poveča BDP za 9 %, inovacije pa za 7 % – Negativni učinki vključujejo stroške prehoda, izgubo delovnih mest, prekvalifikacijo in neenakomerno porazdelitev koristi
Damioli idr. (2021)	– Pozitiven vpliv patentov UI na produktivnost; mala in srednje velika podjetja; storitveni sektor – Znatni vpliv povečanja produktivnosti v obdobju 2009–2016; podvojitev števila patentnih prijav UI – Heterogeni učinki implementacije UI na produktivnost v večjih podjetjih in proizvodnih sektorjih
Evropski parlament (2020)	– Uporaba UI je ključna pri digitalni preobrazbi gospodarstva in družbe – UI kot zmogljivost stroja, da izkazuje človeške lastnosti; mišljenje, učenje, načrtovanje, kreativnost
Filippucci idr. (2024)	– Potencial UI za povečanje produktivnosti, inovacij, gospodarske rasti – Negativni učinki UI; neenakomerna implementacija UI, geografska koncentracija razvoja UI, širjenje neenakosti med državami in poklici – Vodilne države v patentiranju UI so ZDA, Kitajska in države EU; države v razvoju zaostajajo
Harry (2023)	– Personalizacija učenja z uporabo UI, prilagoditev učnemu tempu, podpora učiteljem pri poučevanju
Jabbari & Azizi (2024)	– Pozitiven agregatni učinek UI na produktivnost – Metodološki izzivi pri merjenju vpliva UI na produktivnost dela in kapitala
Kirsten (2010)	– Slabo zdravje zaposlenih negativno vpliva na njihovo produktivnost; pojav absentizma in prezentizma – Stres kot pomemben dejavnik pri zmanjšanju produktivnosti
Martinez (2019)	– Potreba po pravni definiciji UI – Močna UI poseduje inteligenco, šibka UI jo simulira; ključna je avtonomnost UI – Deskriptivna definicija opisuje uporabo, preskriptivna določa pogoje uporabe UI

Vir: Lastni.

Tabela 2: Zbirna tabela ključnih ugotovitev dosedanjih raziskav s področja UI in njene vloge pri povečevanju produktivnosti (nadaljevanje)

Avtorji	Ključne ugotovitve
Maslej idr. (2024)	– Povečanje naložb v generativno UI – Povečanje uporabe UI v podjetjih; napovedne storitve, analitika, optimizacija – ZDA, Kitajska, EU, Združeno kraljestvo vlagajo v UI; pričakovan pozitiven vpliv UI na produktivnost

	– Potencial zmanjšanja vrzeli v znanju med delovno silo
Munro idr. (2019)	– Vpliv UI na visoko kvalificirane poklice; avtomatizacija kognitivnih nalog, osredotočenost na zahtevnejše naloge; dopolnilna vloga UI – UI zahteva razvoj novih spretnosti in prekvalifikacijo delovne sile
Nurlia idr. (2023)	– Pozitiven vpliv UI na rast produktivnosti; treba je izobraziti zaposlene in prilagoditi poslovne procese – Avtomatizacija lahko vodi do izgube delovnih mest
OECD (2023)	– Administrativni poklici in poslovneži, znanstveniki, inženirji, vodje bolj izpostavljeni vplivu UI; fizična dela manj – Nova delovna mesta v razvoju in vzdrževanju sistemov UI – Naraščanje potrebe po digitalnih spretnostih
Rajpurkar idr. (2022)	– UI v zdravstvu vpliva na povečanje produktivnosti; interpretacija medicinskih slik, obdelava kemičnih in genomskih zaporedij, natančnejša in hitrejša diagnoza zdravstvenih stanj
Samoili idr. (2020)	– Enotna definicija UI ne obstaja; posledica različnih disciplinarnih perspektiv – Operativna definicija UI; zaznavanje, razmišljanje, učenje, odločanje
Shil idr. (2024)	– UI izboljša natančnost napovedne analitike, optimizira zaloge, zmanjšuje stroške podjetij in transporta, omogoča hitrejšo odločanje
Steindel & Stiroh (2001)	– Mere produktivnosti; produktivnost dela in skupna faktorska produktivnost (TFP) – Produktivnost dela je prociklična – TFP meri splošno učinkovitost proizvodnje in vključuje učinke tehnologije, ekonomije obsega ter izobraževanje delovne sile, organizacijske strukture in prerazporeditev virov
Syverson (2011)	– Težave pri merjenju produktivnosti; kompleksnost proizvodnje, spreminjanje cen, združevanje različnih inputov, merjenje elastičnosti proizvodnih dejavnikov, kakovost podatkov

Vir: Lastni.

(SISTEMSKO) KIBERNETSKO TVEGANJE IN STRES V AMERIŠKEM FINANČNEM SISTEMU

Marko Možina, študent, Univerza v Ljubljani, Fakulteta za elektrotehniko

Doc. dr. Dejan Romih, Univerza v Mariboru, Ekonomsko-poslovna fakulteta  

Povzetek: V tem prispevku obravnavamo (sistemsko) kibernetско tveganje in stres, ki sta aktualni temi v centralnem bančništvu, ter predstavljamo na kabelskih novicah temelječi indeks kibernetkega tveganja za Združene države Amerike, ki omogoča merjenje, opazovanje in spremljanje kibernetkega tveganja v ameriškem finančnem sistemu. S pomočjo aplikacije Stanford Cable TV News Analyzer smo analizirali kabelske novice in ugotovili, da je bilo kibernetско tveganje v ameriškem finančnem sistemu največje po eskalaciji rusko-ukrajinske vojne, ko je vladal strah pred kibernetскими napadi na ameriški finančni sistem. Toda upoštevati moramo, da TV-postaje ne poročajo o vseh kibernetских incidentih, kar zmanjšuje natančnost merjenja. Poleg tega večji indeks kibernetkega tveganja nujno ne pomeni tudi večjega kibernetkega tveganja v realnem svetu.

Ključne besede: kabelska novica, kibernetско tveganje, kibernetски stres, Stanford Cable TV News Analyzer, Združene države Amerike

Cobiss: 1.08

1 Uvod

Sistemsko tveganje (angl. *systemic risk*) v finančnem sistemu je aktualna tema v centralnem bančništvu. Po letu 2008 so centralni bančniki veliko govorili in pisali o vzrokih in posledicah sistemskega tveganja. To velja tudi za sistemski stres (angl. *systemic stress*) v finančnem sistemu, ki ga lahko definiramo kot sistemsko tveganje, ki se je uresničilo, kar pomeni, da so nastale motnje v delovanju finančnega sistema, kot se je pokazalo med finančno krizo leta 2008. V zadnjem času centralni bančniki veliko govorijo in pišejo o sistemskem kibernetiskem tveganju (angl. *systemic cyber risk*), ki je posebna vrsta sistemskega tveganja (Brando idr., 2022; Eisenbach, Kovner & Lee, 2022a, 2022b; Kotidis & Schreft, 2022; Panetta & Leo, 2025; Welburn & Strong, 2022). Definiramo ga lahko kot tveganje, da bo prišlo do kibernetkega incidenta (angl. *cyber incident*), ki bo povzročil motnje v delovanju finančnega sistema kot celote (Birindelli & Iannuzzi, 2025; Panetta & Leo, 2025). Po analogiji s sistemskim stresom lahko sistemski kibernetški stres (angl. *systemic cyber stress*) definiramo kot sistemsko kibernetško tveganje, ki se je uresničilo, kar pomeni, da so nastale motnje v delovanju finančnega sistema.

V tem prispevku se osredotočamo na merjenje, opazovanje in spremljanje (sistemskega) kibernetkega tveganja v ameriškem finančnem sistemu. Pretekli kibernetški incidenti so povzročili potrebo po merjenju, opazovanju in spremljanju (sistemskega) kibernetkega tveganja v finančnem sistemu ter ugotavljanju njegovih vzrokov in posledic (Board of Governors of the Federal Reserve System, 2021, 2022, 2023, 2024; Santucci, 2018). Literatura (Birindelli & Iannuzzi, 2025; Brando idr., 2022; Eisenbach, Kovner & Lee, 2022a, 2022b; Kotidis & Schreft, 2022; Panetta & Leo, 2025) kaže, da kibernetkega tveganja ne smemo podcenjevati, kar se je v Združenih državah Amerike (ZDA) pokazalo med kibernetškim napadom na ameriško banko JPMorgan Chase leta 2014. Eisenbach, Kovner in Lee (2025) so ugotovili, da so posledice kibernetških napadov na finančne institucije odvisne od faze finančnega ciklusa (finančnih pogojev), kar se je pokazalo med krizo covid-19. Kljub temu obstaja potreba po obvladovanju tveganja kibernetške varnosti ne glede na fazo finančnega ciklusa (Aldasoro idr., 2020a, 2020b). Finančni sistem je namreč hrbtenica gospodarskega sistema, zaradi česar je nemoteno delovanje finančnega sektorja pogoj za nemoteno delovanje gospodarskega sektorja. Motnje v delovanju finančnega sistema povzročajo motnje v delovanju gospodarskega sistema, kar stanje samo še poslabša (Eisenbach, Kovner & Lee, 2022a, 2022b), zato je v interesu države (zlasti centralne banke), da finančni sistem nemoteno deluje. Njegovo delovanje ogrožajo različni dejavniki, kot so kibernetški napadi (Gulyás & Kiss, 2023).

Upoštevati moramo, da je finančna infrastruktura (v najširšem pomenu besedne zveze) del strateške infrastrukture, ki je navadno tarča kibernetских napadov, zato ne preseneča izjava največje ameriške banke, da je pogosto tarča poskusov kibernetских napadov. Problem je, ker lahko (sistemski) kibernetски incidenti povzročijo (sistemski) kibernetски stres, ta pa (sistemski) finančni stres (gl. sliko P.1 v prilogi).

Dejstvo je, da (sistemskega) kibernetskega tveganja ni mogoče neposredno meriti, zato predlagamo uporabo posrednega merila. Gre za pristop, ki so ga v ekonomiji uporabili že drugi in za katerega se je izkazalo, da ima svoje prednosti in pomanjkljivosti, ki jih moramo vzeti v zakup.

Prispevek je strukturiran tako, da ima še štiri poglavja. V drugem poglavju podajamo metode, v tretjem rezultate, v četrtem razpravo, v petem pa sklep.

2 Metode

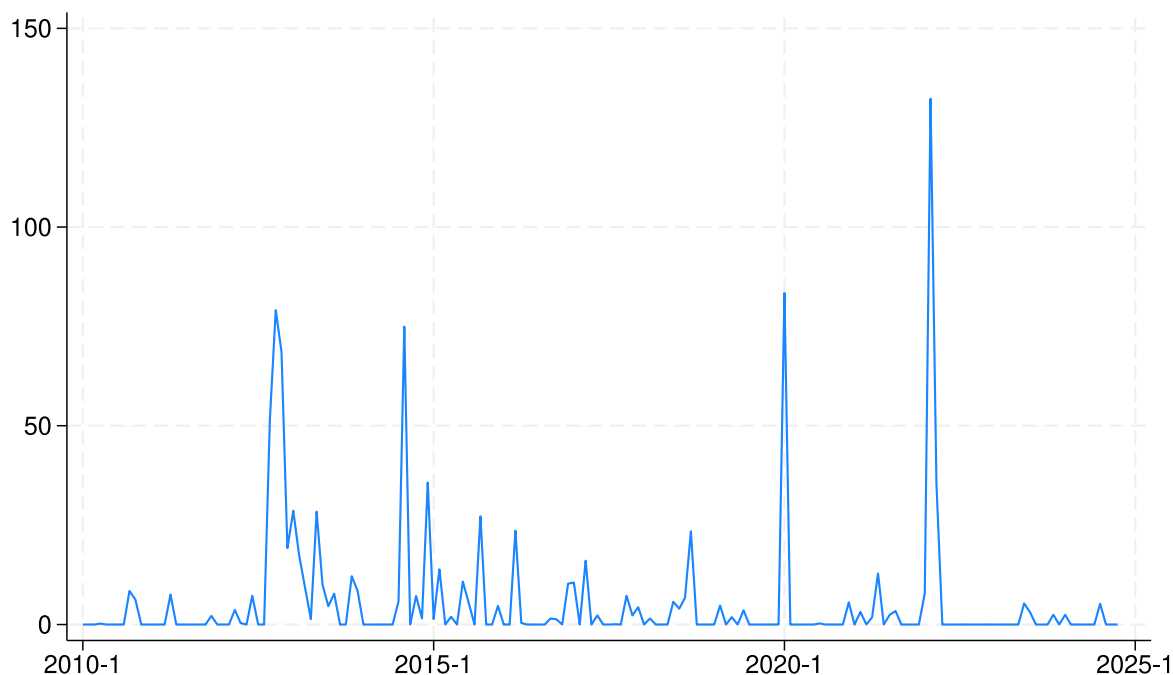
Za potrebe te raziskave smo razvili na kabelskih novicah temelječi indeks kibernetskega tveganja (angl. *cable news-based cyber risk index*) za ZDA, ki omogoča merjenje, opazovanje in spremljanje kibernetskega tveganja v ameriškem finančnem sistemu. Pri tem smo si pomagali z umetno inteligenco, saj smo uporabili spletno aplikacijo Stanford Cable TV News Analyzer (<https://tvnews.stanford.edu/>) (Hong idr., 2021), ki omogoča analiziranje kabelskih novic na CNN-u, FOX-u in MSNBC-ju. V našem primeru smo uporabili naslednji iskalni niz: `text="breach | cyber | [hack]" AND text="[bank] financial [institution] | stock [market] | stock [exchange] | Wall Street | Bank of America | Citybank | Goldman Sachs | JPMorgan Chase | Nasdaq | New York Stock Exchange | NYSE" AND text="United States | U.S." AND textwindow="10"`, lahko pa bi izbrali tudi druge ključne metode. To pomeni, da je indeks mogoče prilagajati času in razmeram.

Ideja indeksa je, daljši ko je čas zaslona (v sekundah) o kibernetškem tveganju, večje je kibernetško tveganje v realnem svetu.

3 Rezultati

V tem poglavju podajamo rezultate raziskave, v okviru katere smo razvili indeks kibernetskega tveganja, ki temelji na ideji, da je kibernetško tveganje v ameriškem finančnem sistemu največje takrat, ko ameriški mediji (CNN, FOX, MSNBC) o njem največ poročajo. Slika 1 kaže gibanje na kabelskih novicah temelječega indeksa kibernetskega tveganja za ZDA oz. čas zaslona o kibernetškem tveganju na ameriških kabelskih TV-postajah.

Slika 1: Gibanje časa zaslona o kibernetnem tveganju na ameriških kabelskih TV-postajah v sekundah



Opomba: Os x kaže čas v mesecih in letih, os y pa čas zaslona v sekundah. 2010-1 = januar 2010.

Vir podatkov: Hong idr. (2021), lastni izračuni.

S slike 1 je razvidno, da je bilo kibernetno tveganje v ameriškem finančnem sistemu največje februarja 2022, ko je skupni čas zaslona o kibernetnem tveganju v ameriškem finančnem sistemu na CNN-u, FOX-u in MSNBC-ju znašal 132,3 sekunde ali 2,2 minute. To ni veliko, vseeno pa indeks opozarja na povečano kibernetno tveganje v ameriškem finančnem sistemu. Vrh sovпада z eskalacijo rusko-ukrajinske vojne, ko je v ZDA vladal strah pred kibernetnimi napadi na ameriški finančni sistem. S slike 1 je razvidno tudi, da je bilo kibernetno tveganje v ameriškem finančnem sistemu sorazmerno veliko tudi oktobra 2012 (79,1 sekunde), avgusta 2014 (74,9 sekunde) in januarja 2020 (83,4 sekunde). Oktobra 2012 so ameriški mediji poročali o odkritju vohunske programske opreme Red October (slov. Rdeči oktober), ki se je širila po e-pošti in ogrožala ameriške sektorje kritične infrastrukture (med njimi tudi sektor finančnih storitev). Avgusta 2014 so ameriški mediji poročali o kibernetnem napadu na ameriško banko JPMorgan Chase (in nekatere druge), januarja 2020 pa o iranski grožnji s kibernetnim napadom na ameriške sektorje kritične infrastrukture. Čeprav so ti dogodki povečali kibernetno tveganje v ZDA, niso povzročili (večjih) motenj v delovanju ameriškega finančnega sistema. So pa povzročili potrebo po povečanju naložb v kibernetno varnost.

4 Razprava

Indeks, ki ga podajamo v tem prispevku, omogoča merjenje, opazovanje in spremljanje kibernet-skega tveganja (tudi tveganja kibernet-ske varnosti) v ZDA ter ugotavljanje njegovih vzrokov in po-sledic, zaradi česar ga lahko uporabljajo (ameriški) oblikovalci politike in raziskovalci. Njegova prednost je tudi, da ga je mogoče prilagoditi potrebam oblikovalcev politike in raziskovalcev, za-radi česar bi lahko bil zanimiv tudi za ameriško centralno banko (gl. npr. Board of Governors of the Federal Reserve System, 2021, 2022, 2023, 2024). Število kibernet-skih incidentov v ZDA se na-mreč povečuje, kar povzroča potrebo po ukrepanju (Brando idr., 2022). Toda upoštevati moramo, da mediji ne poročajo o vseh kibernet-skih incidentih (v finančnem sektorju), kar vpliva na rezul-tate. Kljub temu menimo, da je lahko predlagani indeks koristen pripomoček za oblikovalce poli-tike in raziskovalce, toda potrebne so dodatne raziskave, ki bi upravičile njegovo uporabo v praksi (ne glede na fazo finančnega ciklusa).

5 Sklep

Ta prispevek je izhodišče za široko in poglobljeno razpravo o merjenju (in obvladovanju) (sistem-skega) kibernet-skega tveganja (v ZDA). Očitno je, da je ta potrebna, zlasti glede na vlogo in pomen ameriškega finančnega (in gospodarskega) sistema (v svetu). Pa tudi zato, ker se zavedamo, da na kabelskih novicah temelječi indeks kibernet-skega tveganja za ZDA, ki smo ga predstavili v tem prispevku, ni brez pomanjkljivosti, zato predlagamo, da se jih odkrije in odpravi. Pri tem si lahko oblikovalci politike in raziskovalci pomagajo z umetno inteligenco. Glede na to, da smo se v razi-skavi omejili na kabelske novice in ZDA, predlagamo tudi, da se raziskava razširi na druge novice in države, pa tudi na druge sisteme, kot je pokojninski¹. Na koncu naj še enkrat opozorimo (na omejitve), da na kabelskih novicah temelječi indeks kibernet-skega tveganja upošteva samo

¹ Junija 2023 je CalPERS, največji javni pokojninski sklad v ZDA, razkril, da je bil prizadet v obsežnem kibernet-skem in-cidentu. Napadalci so izkoristili ranljivost v programski opremi MOVEit, ki jo je uporabljal njihov zunanji izvajalec PBI Research Services, in pridobili nepooblaščen dostop do osebnih podatkov približno 769.000 upokojencev. Med priza-detimi podatki so bili imena, datumi rojstva, številke socialnega zavarovanja ter podatki o družinskih članih. Napad je bil del širše kampanje, ki je prizadela več sto organizacij po svetu, v primeru CalPERS pa je incident vzbudil posebno zaskrbljenost zaradi občutljivosti osebnih podatkov starejših članov sklada. Organizacija je takoj po odkritju incidenta obvestila prizadete posameznike, jim ponudila dve leti brezplačnega spremljanja kreditne sposobnosti ter okrepila var-nostne ukrepe za zaščito svojih članov. Incident ni vplival na izplačila pokojnin ali delovanje notranjih sistemov Cal-PERS, vendar pa je sprožil dodatna preverjanja varnosti pri sodelovanju z zunanjimi izvajalci.

kibernetske incidente, o katerih so poročali CNN, FOX in MSNBC, ne pa tudi drugih. Zato bi bilo smiselno veljavnost rezultatov preveriti z drugimi metodami.

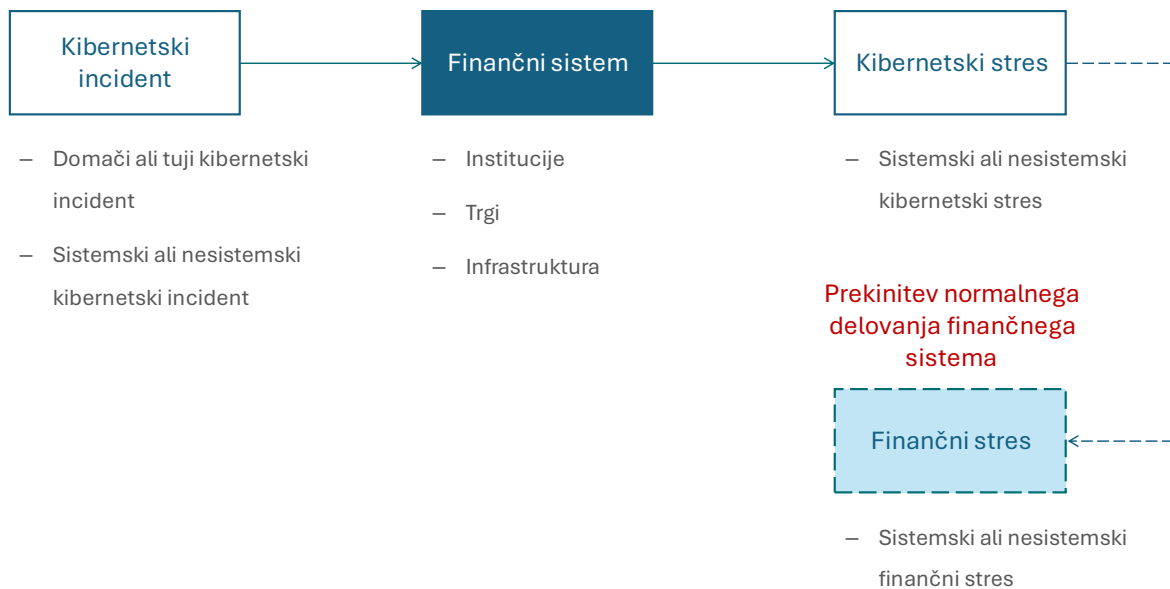
Literatura in viri

1. Aldasoro, I., Gambacorta, L., Giudici, P., & Leach, T. (2020a). *The drivers of cyber risk* (BIS Working Paper No. 865). Bank for International Settlements. <https://www.bis.org/publ/work865.htm>
2. Aldasoro, I., Gambacorta, L., Giudici, P., & Leach, T. (2020b). *Operational and cyber risks in the financial sector* (BIS Working Paper No. 840). Bank for International Settlements. <https://www.bis.org/publ/work840.htm>
3. Birindelli, G., & Iannuzzi, A. P. (2025). The systemic importance of cyber risk in banks. V V. Pacelli (ur.), *Systemic risk and complex networks in modern financial systems* (str. 301–321). Springer. https://doi.org/10.1007/978-3-031-64916-5_16
4. Board of Governors of the Federal Reserve System. (2021, september). *Cybersecurity and financial system resilience report*. <https://www.federalreserve.gov/publications/files/cybersecurity-report-202109.pdf>
5. Board of Governors of the Federal Reserve System. (2022, julij). *Cybersecurity and financial system resilience report*. <https://www.federalreserve.gov/publications/files/cybersecurity-report-202207.pdf>
6. Board of Governors of the Federal Reserve System. (2023, avgust). *Cybersecurity and financial system resilience report*. <https://www.federalreserve.gov/publications/files/cybersecurity-report-202308.pdf>
7. Board of Governors of the Federal Reserve System. (2024, julij). *Cybersecurity and financial system resilience report*. <https://www.federalreserve.gov/publications/files/cybersecurity-report-202407.pdf>
8. Brando, D., Kotidis, A., Kovner, A., Lee, M., & Schreft, S. L. (2022, 12. maj). *Implications of cyber risk for financial stability*. FEDS Notes. <https://doi.org/10.17016/2380-7172.3077>
9. Eisenbach, T. M., Kovner, A., & Lee, M. J. (2022, revised August 2023). *When it rains, it pours: Cyber risk and financial conditions* (Staff Report No. 1022). Federal Reserve Bank of New York. https://www.newyorkfed.org/research/staff_reports/sr1022.html
10. Eisenbach, T. M., Kovner, A., & Lee, M. J. (2022a). Cyber risk and the U.S. financial system: A pre-mortem analysis. *Journal of Financial Economics*, 145(3), 802–826. <https://doi.org/10.1016/j.jfineco.2021.10.007>
11. Eisenbach, T. M., Kovner, A., & Lee, M. J. (2022b). *When it rains, it pours: Cyber vulnerability and financial conditions* (Staff Report No. 1022). Federal Reserve Bank of New York. <https://doi.org/10.2139/ssrn.4173257>
12. Gulyás, O., & Kiss, G. (2023). Impact of cyber-attacks on the financial institutions. *Procedia Computer Science*, 219, 84–90. <https://doi.org/10.1016/j.procs.2023.01.267>
13. Hong, J., Crichton, W., Zhang, H., Fu, D. Y., Ritchie, J., Barenholtz, J., Hannel, B., Yao, X., Murray, M., Moriba, G., Agrawala, M., & Fatahalian, K. (2021). *Analysis of faces in a decade of US cable TV news*. V *Proceedings of the 27th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining*. Association for Computing Machinery.
14. Kotidis, A., & Schreft, S. L. (2022). *Cyberattacks and financial stability: Evidence from a natural experiment* (Finance and Economics Discussion Series No. 2022-025). Board of Governors of the Federal Reserve System. <https://doi.org/10.17016/FEDS.2022.025>

15. Panetta, I. C., & Leo, S. (2025). Systemic cyber risk in the financial sector: Can network analysis assist in identifying vulnerabilities and improving resilience? V V. Pacelli (ur.), *Systemic risk and complex networks in modern financial systems* (str. 133–153). Springer. https://doi.org/10.1007/978-3-031-64916-5_8
16. Romih, D., & Primec, A. (2025, 23. april). *Sistemska kibernetško tveganje in stres*. Posvetovanje Kibernetška varnost, pokojninski sistem in umetna inteligenca, Univerza v Mariboru, Ekonomsko-poslovna fakulteta.
17. Santucci, L. (2018). *Quantifying cyber risk in the financial services industry* (Discussion Paper No. 18-03). Federal Reserve Bank of Philadelphia. <https://doi.org/10.21799/frbp.dp.2018.03>
18. Welburn, J. W., & Strong, A. M. (2022). Systemic cyber risk and aggregate impacts. *Risk Analysis*, 42(8), 1606–1622. <https://doi.org/10.1111/risa.13715>

Priloga

Slika P.1: Diagram odnosa med kibernetским incidentom in finančnim stresom



Vir: Romih in Primec (2025).

EKONOMSKA PRESOJA INVESTIRANJA V KIBERNETSKO VARNOST V IZBRANEM ZDRAVSTVENEM DOMU

Maruša Volavšek, študentka, Univerza v Mariboru, Ekonomsko-poslovna fakulteta 

Feliks Možina, Univerza v Ljubljani, Ekonomska fakulteta

Izr. prof. dr. Andreja Primec, Univerza v Mariboru, Ekonomsko-poslovna fakulteta 

Povzetek: Digitalizacija zdravstvenega sektorja poleg koristi ustvarja tudi večjo izpostavljenost kibernetiskim tveganjem, ki lahko ogrozijo zaupnost podatkov in motijo delovanje ključnih storitev. Zdravstvene ustanove se vse pogosteje soočajo s kibernetiskimi napadi, ki lahko imajo resne organizacijske, finančne in pravne posledice. V prispevku obravnavamo vprašanje, ali je investicija v kibernetisko varnost v zdravstvu poleg zakonske obveznosti tudi ekonomsko upravičena odločitev. Uporabili smo metodo kvalitativne študije primera za analizo organizacijskih varnostnih ukrepov izbranega zdravstvenega doma z območja Štajerske, v okviru katere smo s pomočjo prilagojenega teoretičnega modela ocenili neto vrednost varnostne investicije. Ugotovili smo, da so vlaganja v kibernetisko varnost ekonomsko upravičena, saj koristi zaščitnih ukrepov presegajo stroške, tudi ob spremenjenih pogojih. Prispevek obravnava tudi pomen dolgoročno usmerjenega načrtovanja, ustreznega razporejanja sredstev in systemskega financiranja kot ključnih dejavnikov za večjo digitalno odpornost zdravstvenih ustanov.

Ključne besede: kibernetiska varnost, zdravstveni sektor, študija primera, upravičenost investicije, analiza stroškov in koristi

Cobiss: 1.08

1 Uvod

Kibernetska varnost je ključna aktivnost, ki zagotavlja zaščito računalniških sistemov, omrežij, podatkov in infrastrukture pred različnimi zlonamernimi napadi, nepooblaščenim dostopom in škodo. V svetu, kjer digitalizacija postaja vse bolj prepletena z vsakodnevnim življenjem, so kibernetske grožnje vse bolj prisotne in raznolike (Consilium, 2025).

Zdravstveni sistem, v katerem digitalizacija storitev prinaša številne prednosti za paciente (elektronski zdravstveni kartoni, telemedicina in diagnostika, podprta z umetno inteligenco (European Commission, 2025)), je obenem izrazito izpostavljen kibernetskim tveganjem. Le-ti ne ogrožajo le občutljivih podatkov pacientov, temveč lahko tudi motijo delovanje ključnih zdravstvenih storitev.

Potencialni kibernetski napadi predstavljajo resno grožnjo, saj lahko upočasnijo zdravstvene postopke, ohromijo delovanje urgentnih oddelkov ter motijo izvajanje ključnih zdravstvenih storitev. Število varnostnih napadov v zdravstvu se je v zadnjih letih povečalo bolj kot na katerem koli drugem kritičnem področju znotraj EU. O tem priča tudi 309 napadov, ki so leta 2023 znotraj EU prizadeli kibernetsko varnost v zdravstvenem sektorju (Evropska komisija, 2025).

Ne glede na dejstvo, da je zagotavljanje kibernetske varnosti v zdravstvu zakonita dolžnost izvajalcev zdravstvene dejavnosti, pa je cilj prispevka pokazati, da je to tudi ekonomsko upravičena odločitev. Namen je usmerjen k praktični implementaciji ugotovitev prispevka. Na primeru podatkov izbranega zdravstvenega doma bomo z uporabo modela neto vrednosti investicije v kibernetsko varnost poskušali oblikovati normativno sodbo.

V prispevku bomo uporabili kvalitativno metodo študije primera za analizo organizacijskih varnostnih ukrepov izbranega zdravstvenega doma z območja Štajerske. Osrednje analitično orodje bo prilagojeni teoretični model, ki omogoča oceno neto vrednosti investicije v kibernetsko varnost. V teoretičnem okviru prispevka bomo predstavili pomen kibernetske varnosti v zdravstvu in ključne izzive, povezane z velikimi stroški napadov, vrednostjo podatkov, pomanjkanjem virov ter napačnim dojemanjem varnosti v zdravstvenem sektorju. V nadaljevanju bomo opisali izbrani model za izračun neto vrednosti investicije v kibernetsko varnost, ki temelji na predpostavki omrežja brez zamejitev ter upošteva dejavnike, kot so verjetnost napada, dovzetnost sistema in potencialna izguba ob napadu. Model bomo aplikativno uporabili v okviru študije primera izbranega zdravstvenega doma, kjer bomo z analizo razpoložljivih podatkov ocenili smiselnost

konkretnih varnostnih vlaganj. V sklepnem delu bomo podali ključne ugotovitve in priporočila za izboljšanje varnostne strategije izbrane zdravstvene ustanove.

2 Teoretični okvir

Digitalna transformacija zdravstvenega sektorja, zlasti uvajanje sistemov za izmenjavo zdravstvenih informacij (angl. *HIE – Health Information Exchange*), prinaša številne prednosti za kakovost in učinkovitost oskrbe, hkrati pa tudi nove izzive na področju kibernetске varnosti. Zdravstvene ustanove, ki delujejo v okviru HIE, morajo zaščititi občutljive zdravstvene podatke, saj lahko kibernetски napadi povzročijo velike finančne izgube, regulatorne posledice ter izgubo zaupanja pacientov (Appari, A., & Johnson, M. E., 2010).

Zdravstvene ustanove so zaradi potreb po hitrejšem pretoku informacij in večji učinkovitosti informacijsko izrazito povezane. Ta povezanost pomeni, da so kibernetска tveganja razpršena med vse ustanove in niso omejena zgolj na posamezno enoto. Huang s sodelavci (2014) opozarja, da članice zdravstvenih informacijskih ekosistemov (HIE) delujejo v okolju, kjer so povezane organizacije medsebojno varnostno odvisne: ranljivost ene ustanove lahko predstavlja tveganje za celoten sistem. Takšna medsebojna povezanost ustvarja sistemsko tveganje in zahteva podrobno razumevanje topologije omrežja.

Vsako omrežje je sestavljeno iz vozlišč (npr. bolnišnic, zdravstvenih domov, zavarovalnic ...), njihove lastnosti pa izhajajo iz strukture medsebojnega deljenja informacij. Huang s sodelavci (2014) poudarja, da je omrežje zdravstvenega sistema najbolje opisati kot omrežje brez zamejitev (angl. *scale-free network*), za katerega so značilne lastnosti, ki jih opisujeta Barabási in Albert (1999). Večina organizacij (vozlišč) vzpostavi le nekaj povezav, medtem ko ima nekaj ključnih vozlišč – kot so velike bolnišnice ali regionalni zdravstveni domovi – zelo veliko število povezav in delujejo kot središča (angl. *hubs*). Za stabilnost sistema je ključna kibernetска varnost vozlišč, saj se lahko zaradi omrežnih učinkov vdor v eno ustanovo, zaradi že omenjenih povezav, prenese tudi na preostale. Za celovito razumevanje kibernetске varnosti v zdravstvenih sistemih je torej nujno poznavanje zaščite celotnega omrežja, ne zgolj posameznih ustanov.

Zdravstveni sektor pa na žalost nima celovitega pogleda na kibernetсko varnost. Raziskave so pokazale, da v zdravstvenih informacijskih izmenjavah pogosto obstajajo zaskrbljujoče vrzeli v varnosti in zaščiti zasebnosti. Študije, kot so AHIMA/HIMSS (2011), so opozorile, da HIE še vedno trpijo zaradi pomanjkljive usklajenosti standardov, kar potencialno vodi do varnostnih vrzeli,

nezdružljivosti sistemov ter večje možnosti za zlorabo podatkov. Sinhronizirani standardi namreč omogočajo varno, enotno in učinkovito izmenjavo zdravstvenih podatkov. Prav tako se je izkazalo, da številne ustanove nimajo specializiranega osebja za zagotavljanje varnosti, kar povečuje tveganje za kibernetiski napad. Vlaganja v varnost so pogosto razumljena kot strošek brez neposrednega doprinosa, saj koristi, kot sta manjše število napadov in večja odpornost sistema, ostanejo nedokumentirane v kratkoročnih finančnih izkazih (Huang et al., 2014).

Dodatna ovira za zagotavljanje ustrezne kibernetске zaštite so omejena finančna sredstva. Tovrstno financiranje temelji predvsem na pogodbah z Zavodom za zdravstveno zavarovanje Slovenije (ZZZS) in prihodkih iz samoplačniških storitev, vendar višina le-teh pogosto ne omogoča pokritja visokih izdatkov za uvedbo dodatnih varnostnih rešitev ter ustreznega kadra za upravljanje varnosti. Zadostna sredstva, obenem pa usmerjeno načrtovanje ter razporejanje teh sredstev glede na dejanska tveganja, so bistveni dejavniki za doseganje dolgoročne vzdržnosti in učinkovitosti varnostnih ukrepov (lasten vir, intervju 24. 3. 2025).

Pomanjkanje sistemskega financiranja za kibernetisko varnost se odraža tudi na primeru izbranega ZD. V intervjuju, ki smo ga izvedli s predstavniki ZD, so ti pojasnili, da so v zadnjih letih sicer uvedli določene ukrepe za izboljšanje kibernetiske varnosti, vendar so jih morali v celoti financirati iz lastnih sredstev. To kaže na odsotnost specifičnih subvencioniranih programov, ki bi podpirali kibernetisko varnost v zdravstvu. Glavni izziv pri zagotavljanju ustreznega financiranja ostaja finančna vzdržnost, saj trenutna sredstva ne zadoščajo za dolgoročne in pogosto drage varnostne ukrepe. Usposabljanja in delavnice, ki so ključni za ohranjanje informacijske varnosti, se prav tako financirajo znotraj omejenih virov, kar zmanjšuje njihovo pogostost in kakovost. Ob zaključku so predstavniki ZD izrazili potrebo po večjem vlaganju na nacionalni in evropski ravni ter po uvedbi specializiranih razpisov in subvencij za kibernetisko zaščito zdravstvenih ustanov (lasten vir, intervju 24. 3. 2025). Kot smo omenili, je ob financiranju pomembno tudi razporejanje teh sredstev. Neomejena višina izdatkov za kibernetisko varnost je navsezadnje lahko nerentabilna, ko so potencialne izgube v primeru napada manjše od izdatkov za kibernetisko zaščito. Ta prispevek naslavlja in opozarja predvsem na to »ožjo« ekonomsko presojo vlaganj v kibernetisko varnost.

Da bi to bolje doumeli, je potrebno poznavanje ekonomskega načrtovanja investicij. Temu se posveča študija Huanga, Behare in Gooja (2014), ki predstavlja enega temeljnih modelov za analizo optimalne investicije v informacijsko varnost v okviru zdravstvenega sistema. Avtorji izdatke za kibernetisko varnost v omrežnih sistemih obravnavajo kot ekonomsko odločitev. Njihov

zaključek je, da optimalna raven investicije v kibernetško varnost predstavlja zgolj določen delež pričakovane finančne izgube v primeru kibernetškega vdora. Pri izpeljavi in aplikaciji modela se bomo omejili zgolj na oceno neto vrednosti investicije v kibernetško varnost, ki pa ni enaka neto sedanji vrednosti investicije (NSV), ki jo v ekonomiji in financah prav tako poznamo. Medtem ko NSV vse prihodnje denarne tokove diskontira na določeni časovni trenutek, neto vrednost investicije ne uporablja diskontiranja, temveč temelji na razliki med stanjem brez investicije in stanjem z investicijo.

Model temelji na predhodnih delih o ekonomiki informacijske varnosti, zlasti na prispevkih Andersona in Moora (2006), ki sta izpostavila, da ustanove zaradi napačnih ekonomskih spodbud pogosto premalo vlagajo v kibernetško varnost. Tisti, ki sprejemajo odločitve o naložbah v varnostne ukrepe, namreč niso vedno pripravljeni investirati v meri, ki bi bila optimalna za celotno družbo, saj stroške nosijo sami in jih ne delijo z ostalimi deležniki. Gordon in Loeb (2002) sta razvila modele, ki tako kot prispevek Huanga s sodelavci (2014) kažejo, da optimalna investicija v kibernetško varnost običajno predstavlja le del pričakovane izgube.

Za ocenitev neto vrednosti investicije v kibernetško varnost zdravstvenega doma se bomo poslužili teoretičnega modela, ki sledi izpeljavi Huanga s sodelavci (2014). Na tem mestu poudarjamo, da empirična aplikacija teoretičnega modela na primeru ZD ni popolna. Teoretični model je namreč matematična abstrakcija, ki poskuša resničnost abstrahirati na računsko izvedljivost. Tako so nekatere spremenljivke v modelu praktično neizmerljive. Posledično smo se morali v določenih primerih zadovoljiti z ocenami in približki.

3 Rezultati

Model temelji na predpostavki omrežja brez zamejitev, kjer se napadi prek povezav med vozlišči širijo podobno kot epidemija. Prav tako se predpostavlja, da so napadi naključnega značaja in niso odvisni od dosedanje zaščite zdravstvene ustanove oz. celotnega omrežja.

Najprej bomo predstavili ključne spremenljivke in izpeljavo modela po vzoru Huanga s sodelavci (2014). Nato bomo v model vstavili pridobljene in ocenjene vrednosti ter končno ocenili neto vrednosti investicije v kibernetško varnost izbranega zdravstvenega doma.

Ključne spremenljivke modela so:

- η – verjetnost napada (neodvisna od dosedanjih vložkov v kibernetško varnost),

- θ – dovzetnost sistema (odvisna zgolj od povezanosti znotraj sistema),
- w – višina investicije v informacijsko varnost,
- ϕ – verjetnost uspešnega vdora,
- S – potencialna izguba zaradi uspešnega napada,
- q – faktor učinkovitosti investicij v kibernetsko varnost.

1. Opredelitev širjenja napada

Model uporablja pristop, ki temelji na dinamiki širjenja okužb v omrežjih. Po modelu je hitrost širjenja napada definirana kot:

$$\lambda = \frac{r}{\delta}, \quad (1)$$

kjer je:

- r stopnja okužbe, torej verjetnost, da se napad razširi na sosednje vozlišče;
- δ stopnja okrevanja oz. zaščite;
- λ hitrost širjenja napada.

Širjenje napada lahko nadalje opredelimo tudi kot funkcijo q in w . Večji ko sta učinkovitost vložene investicije (q) in investicija v kibernetsko varnost (w), manjša je hitrost širjenja napada:

$$\lambda \equiv \frac{1}{qw+1}, \quad (2)$$

kjer je:

- w investicija v kibernetsko varnost;
- $q \in (0,1]$ parameter, ki meri učinkovitost investicije.

2. Dovzetnost sistema

Dovzetnost sistema je povezana s številom povezav v omrežju (n). Ko se n približuje 0, je dovzetnost sistema blizu 0. V kolikor pa se n približuje ∞ , je dovzetnost sistema skoraj 1. Določena je kot:

$$\theta = e^{-1/n}, \quad (3)$$

kjer je:

- e konstanta,
- n število povezav določene ustanove z ostalimi zdravstvenimi institucijami.

3. Verjetnost vdora

Uporabimo znan rezultat iz teorije omrežij brez zamejitev (May in Lloyd (2001), Anderson in May (1991)), ki pravi, da je verjetnost vdora v ravnotežnem stanju (angl. *steady state*):

$$\varphi = \eta \cdot P = \eta \cdot c e^{\frac{-1}{(\lambda n)}}, \quad (5)$$

kjer je:

- η verjetnost napada;
- P verjetnost okužbe, normalizirana na interval vrednosti (0,1);
- c normalizacijska konstanta.

Če vstavimo enačbo (3), dobimo:

$$\varphi = \eta \cdot \theta^{1/\lambda}. \quad (6)$$

Če vstavimo še enačbo (2), dobimo:

$$\varphi = \eta \cdot \theta^{qw+1}. \quad (7)$$

4. Neto vrednost varnostne investicije

Neto vrednost varnostne investicije opredelimo kot razliko med začetnim tveganjem brez zaščite in tveganjem po investiciji v kibernetsko varnost, zmanjšano za omenjeno investicijo:

$$\Pi(w) = (\eta \cdot \theta - \varphi) \cdot S - w, \quad (8)$$

kjer je:

- Π neto vrednost investicije,
- S potencialna izguba v primeru vdora.

V enačbo vstavimo izraz (7) in končno dobimo:

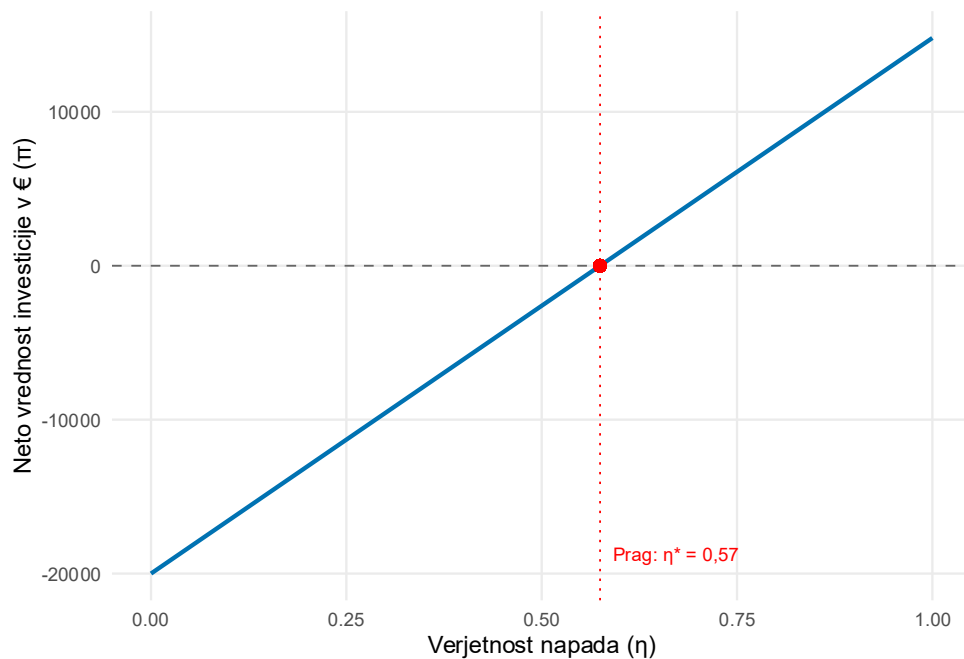
$$\Pi(w) = \eta \cdot \theta \cdot S(1 - \theta^{qw}) - w. \quad (9)$$

Ko v enačbo vstavimo parametre izbranega ZD (verjetnost napada (0,70), dovzetnost sistema (0,87), potencialna izguba (40.000 evrov), učinkovitost investicije (1) in izdatki za kibernetško varnost (20.000 evrov)), pridobimo pozitiven izid neto investicije. Ta vrednost nakazuje, da ZD privarčuje 4360 evrov, če se odloči za investicijo v kibernetško varnost. Na podlagi tega lahko rečemo, da so izdatki za kibernetško varnost učinkoviti, obenem pa ne pretirani, tj. takrat, ko so izdatki večji od potencialnih izgub.

Za opredelitev širšega intervala zaupanja pozitivne neto sedanje vrednosti investicije bomo izvedli analizo občutljivosti s simulacijami. Spreminjali bomo vrednosti ključnih vhodnih spremenljivk in iskali tiste kombinacije, pri katerih postane neto sedanja vrednost enaka nič. Tako bomo določili mejne vrednosti spremenljivk in jih primerjali z vrednostmi, uporabljenimi v osnovnem izračunu. Preizkušanja statističnih hipotez s p-vrednostmi v našem primeru žal ne moremo izvesti, saj bi to zahtevalo poznavanje porazdelitvene funkcije spremenljivk verjetnost napada, potencialna izguba in učinkovitost investicije. Omejili se bomo na navedene tri spremenljivke, saj sta spremenljivki izdatki za kibernetško varnost in dovzetnost sistema zadostno opredeljeni ter eksaktni.

Kot lahko razberemo s slike 1, znaša mejna vrednost verjetnosti napada 0,57 (*ceteris paribus*, tj. ob nespremenjenih drugih pogojih). To pomeni, da je neto vrednost investicije v kibernetško varnost enaka 0, ko znaša verjetnost napada 57 %. Pod to vrednostjo investicija ni upravičena. Ko pa se verjetnost napada povzpne nad mejno vrednost, kar pomeni, da je napad vse bolj verjeten, je neto vrednost investicije vse večja (*ceteris paribus*). Prihranki, ki jih z obstoječo varnostno infrastrukturo dosegamo, se torej linearno povečujejo z verjetnostjo napada.

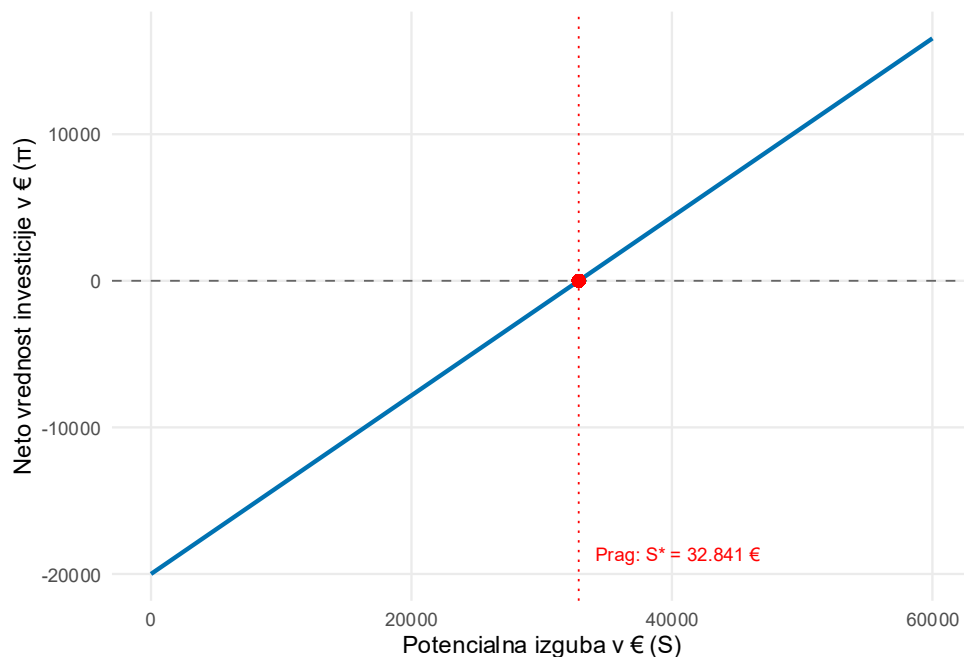
Slika 1: Neto vrednost investicije (os y) v primeru različnih verjetnosti napada (η) (os x)



Vir: Lastni.

Kot lahko razberemo s slike 2, znaša mejna vrednost potencialne izgube 32.841 evrov. To pomeni, da je neto vrednost investicije v kibernetiko varnost enaka 0, ko potencialna izguba znaša 32.841 evrov. Pod to vrednostjo investicija ni upravičena. Ko pa se potencialna izguba povzpne nad mejno vrednostj, se upravičenost investicije linearno povečuje. Poenostavljeno: več ko lahko izgubimo v primeru, da nismo varnostno zaščiteni, bolj se nam investicija v kibernetiko varnost izplača.

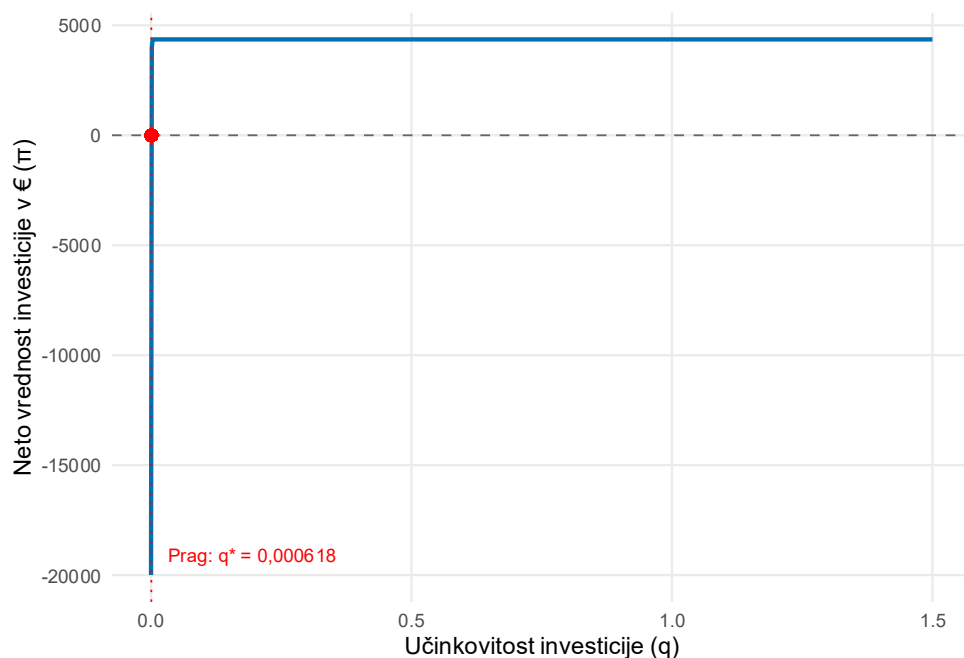
Slika 2: Neto vrednost investicije (os y) v primeru različnih potencialnih izgub (S) (os x)



Vir: Lastni.

Kot lahko razberemo s slike 3, znaša mejna vrednost učinkovitosti investicije 0,000618. To pomeni, da je neto vrednost investicije v kibernetško varnost enaka 0, ko učinkovitost investicije znaša 0,000618. Pod to vrednostjo investicija ni upravičena. Vrednost učinkovitosti investicije meri efektiven delež od izdatkov v kibernetško varnost. V našem primeru je ta enaka 1, kar pomeni, da so celotni izdatki v kibernetško varnost učinkoviti. Mejna vrednost 0,000618 bi pomenila, da je učinkovitost 0,06 % celotnih izdatkov v kibernetško varnost. S slike 3 lahko dodatno vidimo, da vrednost spremenljivke nad pribl. 0,000618 pravzaprav nima nikakršnega vpliva na neto vrednosti investicije. Problematiko te spremenljivke dodatno obravnavamo v razpravi.

Slika 3: Neto vrednost investicije (os y) v primeru različnih vrednosti učinkovitosti investicije (q) (os x)



Vir: Lastn.

4 Razprava

Večino vrednosti spremenljivk, potrebnih za izračun enačbe (9), smo pridobili neposredno od ZD. Vrednosti parametrov smo navedli že v poglavju Rezultati, tu pa bomo opredelili še težave pri iskanju teh vrednosti ter opisali ad hoc rešitve (tj. priložnostne rešitve, prilagojene konkretni situaciji), h katerim smo se zatekli.

Tako je bila npr. spremenljivka verjetnost kibernetkega napada praktično nedoločljiva. V kontekstu napada na zdravstveni dom namreč ni jasno, v okvirih katere igre je verjetnost opredeljena. Pri igri met kovanca je namreč verjetnost vsakega meta 50 %. Če dojemamo igro širše kot število kibernetkih napadov, razdeljeno glede na sektor, bi bila verjetnost za kibernetki napad na zdravstveno ustanovo zgolj 4 % (ENISA, 2024). Ker pa bi se v tem primeru soočali s problemom heterogenosti sektorjev (npr. velikost ipd.), smo to – tudi razumsko majhno verjetnost – opustili. Ustali smo se na 70-odstotni verjetnosti, ki smo jo pridobili iz poročil HIMSS 2020 in 2021, kjer je približno 70 % izmed vprašanih zdravstvenih ustanov beležilo vsaj en kibernetki napad. Kljub temu pa tudi ta vrednost ni neoporečna, saj ne zajame možnosti več napadov na ustanovo.

Kot lahko vidimo iz simulacij občutljivosti, je 70-odstotna verjetnost napada zmerno oddaljena od mejne vrednosti 57 %, kar pomeni, da je interval zaupanja za pozitiven izid neto vrednosti investicije v okviru te spremenljivke relativno velik.

Pri vseh ostalih spremenljivkah smo se morali zateči k ocenam oz. dejanskim številkam ZD. Najbolj groba ocena je bila verjetno podana za faktor učinkovitosti investicij v kibernetško varnost, ki po svoji vsebini spominja na težko merljive mejne vrednosti v ekonomiji. Kljub temu pa analiza občutljivosti s simulacijami prikazuje faktično neodvisnost neto vrednosti investicije od učinkovitosti investicije nad njeno mejno vrednostjo. To zagotavlja bolj ali manj enak rezultat (neto vrednost investicije) ob različnih nivojih učinkovitosti in nakazuje na dodatno vsebinsko pomanjkljivost teoretičnega modela.

Prav tako hipotetična je bila ocena dnevne izgube ob kibernetškem napadu. Ta časovno odvisna ocena je pravzaprav težko združljiva s statičnimi in časovno enkratnimi lastnostmi modela. Izguba je namreč tudi časovno odvisna (več dni trajajoč napad pomeni večjo izgubo), zato smo z analizo občutljivosti pokazali, da ob večjih potencialnih izgubah zaradi dlje trajajočega kibernetškega napada neto vrednost investicije zgolj raste.

Najnatančnejši in najbolj opredeljivi sta bili vrednosti izdatkov za kibernetško varnost in dovzetnost sistema. Prva je sicer prav tako časovno odvisna (izdatki v enem letu), obenem pa tudi časovno nezdružljiva z dnevno izgubo ob kibernetškem napadu (dan proti letu). Druga pa je časovno neodvisna in tako pravzaprav neproblematična. Spremenljivki sta natančno opredeljeni, zato se nam izvedba analize občutljivosti s simulacijami ni zdela smiselna.

Zaradi odsotnosti časovne komponente model ne zajema dinamike ponavljajočih se kibernetških napadov skozi daljše obdobje. Posledično namreč ni jasno (v matematičnem smislu), kakšen je izid modela v primeru, da se v določenem časovnem obdobju pripeti več kibernetških napadov, vendar pa se lahko z intuicijo dokoplremo do ugotovitve, da je neto vrednost investicije še toliko večja, če se z enako uspešnostjo ubranijo tudi naslednje grožnje, in ne zgolj prve in edine. Izdatki za varnost so namreč fiksni in ne variabilni strošek.

Kljub pomanjkljivostim se je model za oceno neto vrednosti investicije v kibernetško varnost izkazal kot pomenljivo orodje za odločanje v zdravstvenem sektorju. Model omogoča kvantitativno vrednotenje varnostnih ukrepov, kar Zdravstvenemu domu omogoča boljše načrtovanje njegovih vlaganj. Poudarja namreč pomen pametnega vlaganja glede na spreminjajoče se razmere v

zunanjem in notranjem okolju ZD. Zdravstveni dom naj izdatke za kibernetško varnost prilagaja verjetnosti napada, ocenjenim potencialnim izgubam ter drugim spremenljivkam, zajetim v modelu.

Obenem slabosti teoretičnega modela rodijo tudi prednosti – abstrahirana realnost v našem primeru doprinese k boljšemu razumevanju vpliva ključnih spremenljivk na stroškovno učinkovitost. Modelirana realnost je namreč okleščena vseh motečih dejavnikov, ki nimajo značilnega vpliva na odvisno spremenljivko. To je sicer mnogokrat nevarno početje, saj se lahko zgodi, da iz modela nevede izpustimo izjemno pomembno spremenljivko in tako popačimo končni rezultat. V ekonometriji to imenujemo pristranskost zaradi izpuščenih spremenljivk (angl. *omitted variable bias*).

K zaključku tega poglavja dodajamo, da bi lahko model neto vrednosti investicije v kibernetško varnost, ki ga predstavljamo v prispevku, z nekoliko več znanja in prostora razširili še na optimalno stopnjo izdatkov. A naj bo to vsebina za naslednji prispevek.

5 Sklep

Na podlagi rezultatov prispevka smo z uporabo teoretičnega modela neto vrednosti investicije na primeru izbranega zdravstvenega doma pokazali, da so vlaganja v kibernetško varnost ekonomsko upravičena. Pozitiven izračun neto vrednosti skupaj z analizo občutljivosti potrjujeta, da so koristi zaščitnih ukrepov tudi ob spremenjenih pogojih večje od izdatkov. Kljub metodološkim omejitvam model omogoča kvantitativno podporo odločanju o varnostnih vlaganjih v zdravstvenem sektorju.

Glede na predstavljene ugotovitve priporočamo, da izbrani ZD vzpostavi celovit varnostni načrt, ki bo vključeval oceno kibernetških tveganj, protokole za odzivanje na incidente ter strategijo postopnega nadgrajevanja obstoječih varnostnih ukrepov. V luči omejenih lastnih sredstev bi bilo smiselno, da se ustanova aktivno usmerja v pridobivanje dodatne finančne podpore preko nacionalnih in evropskih razpisov, namenjenih sofinanciranju kibernetške varnosti v javnem sektorju. Pomemben dejavnik za dolgoročno odpornost sistema predstavlja tudi redno usposabljanje zaposlenih, zato predlagamo vzpostavitev letnega cikla obveznih izobraževanj s poudarkom na osebju, ki upravlja z občutljivimi informacijami. Smiselna bi bila tudi uvedba postopkov za periodično ocenjevanje učinkovitosti sprejetih varnostnih ukrepov, denimo z interno simulacijo napadov in analizo izdatkov glede na potencialno preprečene izgube. Takšen pristop bi

omogočil boljše upravljanje tveganj in prispeval k večji stroškovni učinkovitosti varnostne politike ZD.

Literatura in viri

1. AHIMA/HIMSS. (2011). *The privacy and security gaps in health information exchanges*. White Paper by the AHIMA/HIMSS HIE Privacy and Security Joint Work group, 2011. https://fliphtml5.com/bppm/bsac/AHIMA%3A_The_Privacy_and_Security_Gaps_in_Health_Information_.../25/
2. Anderson, R. M., & May, R. M. (1991). *Infectious diseases of humans: Dynamics and control*. Oxford University Press.
3. Anderson, R.M., & Moore, T. (2006). The economics of information security. *Science*, 314(5799), 610–613. <https://www.science.org/doi/10.1126/science.1130992>
4. Appari, A., & Johnson, M. E. (2010). Information security and privacy in healthcare: Current state of research. *International journal of Internet and enterprise management*, 6(4), 279–314. <http://dx.doi.org/10.1504/IJIEEM.2010.035624>
5. Barabási, A. L., & Albert, R. (1999). Emergence in scaling in random networks. *Science*, 286(5439), 509–512. <https://www.science.org/doi/abs/10.1126/science.286.5439.509>
6. Consilium. (2025). *Kibernetska varnost*. Council of the European Union. <https://www.consilium.europa.eu/sl/topics/cybersecurity/>
7. European Comission. (2025, January 15). *Cybersecurity of hospitals and healthcare providers*. Evropska komisija. <https://digital-strategy.ec.europa.eu/en/factpages/cybersecurity-hospitals-and-healthcare-providers>
8. Evropska komisija. (2025). *Kibernetska varnost bolnišnic in izvajalcev zdravstvenih dejavnosti*. Evropska komisija. https://commission.europa.eu/cybersecurity-healthcare_sl
9. ENISA. (2024). *ENISA Threat Landscape 2024*. European Union Agency for Cybersecurity. <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024>
10. Gordon, L. A. & Loeb, M. P. (2002). The economics of information security investment. *ACM Transactions on Information and System Security (TISSEC)*, 5(4), 438–457. <https://dl.acm.org/doi/10.1145/581271.581274>
11. Healthcare Information and Management Systems Society. (2020). *2020 HIMSS Cybersecurity Survey*. HIMSS. https://www.himss.org/sites/hde/files/media/file/2020/11/16/2020_himss_cybersecurity_survey_final.pdf
12. Healthcare Information and Management Systems Society. (2021). *2021 HIMSS Cybersecurity Survey*. HIMSS. https://www.himss.org/sites/hde/files/media/file/2022/01/28/2021_himss_cybersecurity_survey.pdf
13. Huang, C. D., Behara, R. S., & Goo, J. (2014). Optimal information security investment in a healthcare information exchange: An economic analysis. *Decision Support Systems*, 61, 1–11. <https://doi.org/10.1016/j.dss.2013.10.011>
14. May, R. M., & Lloyd, A. L. (2001). Infection dynamics on scale-free networks. *Physical Review E*, 64(6), 066112. <https://doi.org/10.1103/PhysRevE.64.066112>
15. Portela, D., Nogueira-Leite, D., Almeida, R., & Cruz-Correia, R. (2023, June 30). Economic impact of a hospital cyberattack in a national health system: Descriptive case study. *JMIR Formative Research*, 7(1), e41738. <https://doi.org/10.2196/41738>
16. Wirth, A. (2017). The economics of cybersecurity. *Biomedical instrumentation & technology*, 51(s6), 52–59. <https://array.aami.org/doi/full/10.2345/0899-8205-51.s6.52>

DRUGI DEL: DIGITALNO PRAVO



ODGOVORNOST DELAVCA ZA UPORABO ORODJA CHATGPT PRI DELU

Asist. Matej Makoter Rožmarin, Univerza v Mariboru, Pravna fakulteta 

Asja Lešnik, Univerza v Mariboru, Pravna fakulteta 

Povzetek: Umetna inteligenca je čedalje bolj prisotna na vseh področjih, tudi v delovnem okolju. Eno izmed najpogostejše uporabljenih umetnointeligentnih orodij je orodje ChatGPT, ki ga delavci pogosto uporabljajo za iskanje informacij, kot pomoč pri generiranju besedil in pri analizi podatkov ter celo za avtomatizacijo določenih nalog. Vse to odpira vprašanje odgovornosti v primeru, ko se delavec pri opravljanju dela zanaša na informacije, ki mu jih ponudi ChatGPT, pri čemer zaradi napačnih, nepopolnih ali zavajajočih informacij delodajalcu povzroči škodo.

Prispevek obravnava vprašanje odškodninske in delovnopravne odgovornosti za škodo, povzročeno z uporabo orodja ChatGPT pri delu.

Ključne besede: umetna inteligenca, ChatGPT, škoda, delovno pravo, odškodninska odgovornost.

Cobiss: 1.08

1 Uvod

Delavci se v današnjem času pri delu vse bolj poslužujejo uporabe umetnointeligenčnih sistemov. Ena izmed najpogostejše uporabljenih oblik umetne inteligence danes so klepetalni roboti oz. t. i. *chatboti*. Med njimi je najbolj znan ChatGPT, prvi jezikovni model umetne inteligence, ki ga je razvilo podjetje OpenAI in je trgu postal dostopen dne 30. 11. 2022 (Pratiwie, 2023, str. 2297).¹

Uporaba ChatGPT-ja se je od leta 2022 hitro razširila po vsem svetu. Humlum in Vestergaard sta konec leta 2024 opravila raziskavo med 18.000 delavci iz enajstih različnih poklicev, pri kateri sta raziskovala uporabo ChatGPT-ja pri delu. Pri tem je kar 41 % delavcev odgovorilo, da pri svojem delu uporabljajo ChatGPT (Humlum in Vestergaard, 2025, str. 2). Raziskava, ki jo je novembra 2024 izvedel Google, je pokazala, da se uporaba umetne inteligence predvsem med mladimi delavci hitro povečuje. V raziskavi, izvedeni med 1005 ameriški delavci, starimi od 22 do 39 let, je 93 % anketirancev, starih od 22 do 27 let, povedalo, da uporablja ChatGPT vsaj enkrat na teden. Med anketiranci, starimi od 28 do 39 let, pa jih ChatGPT uporablja 79 % (Shibu, 2024).

Izraz Chat GPT pomeni »Chat Generative Pre-Trained Transformer«, to je jezikovni model umetne inteligence, ki temelji na ogromnih količinah podatkov, kot so knjige, članki, spletne strani, časopisi in druga literarna dela (Sharma in Kavia, 2023, str. 172). ChatGPT uporablja model globokega učenja in lahko na podlagi zbranih podatkov ustvari novo, izvirno vsebino na podlagi poziva uporabnika. Z njegovo pomočjo lahko z enostavnimi ukazi ustvarimo izvirno vsebino za osebno in poklicno rabo. S pomočjo ChatGPT-ja lahko v nekaj trenutkih sestavimo kompleksna elektronska sporočila, seminarske naloge, poročila, poslovne načrte, programske kode itd. (Perlman, 2023, str. 2).

Delavci lahko namreč ChatGPT uporabljajo za pridobivanje virov ali informacij pri delu ali pa za opravljanje delovnih nalog (Pratiwie, 2023, str. 2297). Raziskava Bahrinija in drugih ugotavlja, da se ChatGPT v delovnem okolju uporablja predvsem kot orodje za iskanje informacij, potrebnih za opravljanje dela (Bahrini in drugi, 2023). V raziskavi Googla so anketiranci navedli, da ChatGPT

¹ Čeprav je bil ChatGPT prvi veliki jezikovni model, pa ni bil zadnji. Tako na primer Google upravlja model Gemini (prej imenovan Bard), Meta upravlja model Llama-3, Amazon pa model Claude.AI 3 (Lorek, 2015, str. 515).

uporabljajo predvsem za pisanje elektronskih sporočil, ustvarjanje zapisnikov sestankov in premagovanje jezikovnih ovir (Shibu, 2024).

Pri tem pa je treba izpostaviti, da so informacije in odgovori, ki jih ustvari ChatGPT, v veliko primerih lahko napačni, nepopolni ali celo zavajajoči (Grant, 2024, str. 609), kar med drugim odpira vprašanje odgovornosti za škodo, ki bi jo delavci zaradi uporabe ChatGPT-ja delodajalcu povzročili pri delu.

Prispevek v drugem poglavju naslavlja vprašanje delovnopravne odgovornosti za uporabo orodja ChatGPT, v tretjem poglavju naslavlja vprašanje civilnopravne (odškodninske odgovornosti), v zadnjem delu pa prispevek na podlagi fiktivnega primera konkretizirano analizira obe vrsti odgovornosti.

2 Delovnopravna odgovornost

Zakon o delovnih razmerjih (v nadaljevanju ZDR-1) vse od 33. do 35. člena določa temeljno obveznost delavca – opravljanje dela. Delavec mora delo, za katero je sklenil pogodbo o zaposlitvi, opravljati vestno (33. člen ZDR-1), pri čemer mora upoštevati zahteve in navodila delodajalca (34. člen ZDR-1).

Delavec se je pri opravljanju dela dolžan vzdržati vseh ravnanj, ki glede na naravo dela, ki ga opravlja pri delodajalcu, materialno ali moralno škodujejo ali bi lahko škodovala poslovnim interesom delodajalca (37. člen ZDR-1).

Delavec ima po 38. členu ZDR-1 obveznost varovanja poslovne skrivnosti, kar pomeni, da ne sme izkoriščati za svojo osebno uporabo ali izdati tretjemu delodajalčevih poslovnih skrivnosti, ki jih kot take določi delodajalec, in ki so bile delavcu zaupane ali s katerimi je bil seznanjen na drug način.

Delavcu, ki krši pogodbene ali druge obveznosti iz delovnega razmerja, lahko delodajalec v primeru ugotovljene disciplinske odgovornosti izreče opomin ali druge disciplinske sankcije, kot so npr. denarna kazen ali odvzem bonitet, če so določene v kolektivni pogodbi na ravni dejavnosti (172. člen ZDR-1). Temeljni pogoj za disciplinsko odgovornost delavca je krivda delavca. Krivda je opredeljena z določeno stopnjo storilčeve vednosti oz. zavesti, da je njegovo ravnanje protipravno, ter z določeno stopnjo hotenja, da stori dejanje, s katerim povzroči nedopustno posledico (Sodba VIII Ips 202/98).

Kršitev pogodbene obveznosti ali druge obveznosti iz delovnega razmerja je lahko tudi razlog za redno odpoved pogodbe o zaposlitvi (3. alineja prvega odstavka 89. člena ZDR-1).

V kolikor gre za naklepno hujšo kršitev obveznosti iz delovnega razmerja ali kršitev iz hude malomarnosti, pa je lahko to tudi razlog za izredno odpoved pogodbe o zaposlitvi (2. alineja prvega odstavka 110. člena ZDR-1).

3 Odškodninska odgovornost

Delavec je delodajalcu za nastalo škodo lahko tudi odškodninsko odgovoren. 177. člen ZDR-1 določa, da je delavec, ki na delu ali v zvezi z delom namenoma ali iz hude malomarnosti povzroči škodo delodajalcu, škodo dolžan povrniti.

Odškodninska odgovornost delavca se presoja po splošnih načelih civilnega prava, in sicer po določbah Obligacijskega zakonika (v nadaljevanju OZ) (VDSS sodba Pdp 919/2008). Ta med drugim določa predpostavke odškodninske obveznosti, ki morajo biti kumulativno izpolnjene, da je podan temelj odškodninske obveznosti delavca: protipravno (nedopustno) ravnanje, škoda, vzročna zveza med protipravnim ravnanjem in škodo ter odškodninska odgovornost (VSL Sodba I Cpg 236/2021; VDSS Sodba Pdp 441/2022; VDSS Sodba Pdp 73/2023).

V našem pravnem redu je uveljavljeno načelo krivdne odgovornosti z obrnjenim dokaznim bremenom, kar pomeni, da v kolikor oškodovanec dokaže obstoj prvih treh predpostavk odškodninske obveznosti, se odškodninska odgovornost domneva (VSL sodba in sklep I Cpg 1054/2015),² kar pomeni, da povzročitelj škode velja za krivega, če ne dokaže, da je škoda nastala brez njegove krivde (VSM sodba I Cp 460/2008).

Vendar pa se domneva najlažja stopnja krivde, to je navadna malomarnost (*culpa levis*), kar pomeni, da velja obrnjeno dokazno breme le glede navadne malomarnosti. Glede hujših oblik krivde je dokazno breme na strani tistega, ki tako obliko krivde zatrjuje (VSM sodba I Cp 460/2008). 177. člen ZDR-1 določa, da je delavec odgovoren za škodo, ki jo na delu ali v zvezi z delom delodajalcu povzroči namenoma ali iz hude malomarnosti. Po določbah 131. in 135. člena OZ se torej hujša stopnja krivde ne domneva, zato je na delodajalcu dokazno breme, da mu je delavec

² Navedeno smiselno izhaja iz določbe prvega odstavka 131. člena OZ, ki določa, da kdor drugemu povzroči škodo, jo je dolžan povrniti, če ne dokaže, da je škoda nastala brez njegove krivde.

povzročil škodo namenoma ali iz hude malomarnosti. Delodajalec mora zato v postopku kumulativno dokazati vse štiri predpostavke odškodninske obveznosti, torej, da je delavec ravnal nedopustno, da je nastala škoda, da obstaja vzročna zveza med ravnanjem delavca in nastalo škodo ter da je delavec škodo povzročil namenoma ali iz hude malomarnosti (VDSS Sodba pdp 651/2021; VDSS Sodba Pdp 349/2020).

Pogoj za opredelitev ravnanja kot protipravnega oz. nedopustnega je nujno zatrjevanje in dokazovanje kršitve konkretnega dolžnega ravnanja delavca (VSM Sodba I Cp 999/2019). Sodna praksa je že večkrat zavzela stališče, da kršitev temeljne obveznosti vestnega opravljanja dela po 33. členu ZDR-1 pomeni tudi protipravno ravnanje v smislu elementa civilnega delikta (VDSS sodba Pdp 971/2013). V kolikor delodajalec uspe dokazati, da je delavec z uporabo orodja ChatGPT kršil delovnopravno obveznost po 33. členu ZDR-1, s tem dokaže tudi protipravnost kot predpostavko odškodninske odgovornosti.

Nadalje mora delodajalec dokazati, da mu je z ravnanjem delavca nastala škoda³ ter da je nastala škoda posledica konkretnega (protipravnega) ravnanja delavca (vzročna zveza) (VSRS Sklep II Ips 367/2004).

Kot že navedeno, se hujša stopnja krivde ne domneva, zato mora delodajalec za obstoj odškodninske odgovornosti delavca po 177. členu ZDR-1 dokazati tudi, da je delavec povzročil škodo namenoma ali iz hude malomarnosti. Pri vprašanju malomarnosti gre za vprašanje, ali je delavec ravnal s potrebno skrbnostjo. Huda malomarnost pomeni zanemarjanje tiste skrbnosti, ki se pričakuje od vsakega povprečnega delavca na istih ali podobnih delovnih mestih pri delodajalcu (VSRS Sodba VIII Ips 159/2017; VDSS Sodba Pdp 317/2017; VDSS Sodba in sklep Pdp 172/2023).

4 Analiza konkretnega primera

Zamislimo si fiktivni primer računovodje, ki bi uporabil ChatGPT za pripravo letnega poročila gospodarske družbe. Letnega poročila ne bi pregledal, temveč bi se zanašal na besedilo, ki ga je

³ Škoda je zmanjšanje premoženja (navadna škoda), preprečitev povečanja premoženja (izgubljeni dobiček), pa tudi povzročitev telesnih ali duševnih bolečin ali strahu drugemu ter okrnitev ugleda pravne osebe (nepremoženjska škoda) (132. člen OZ).

generiral ChatGPT. Zaradi napak v letnem poročilu bi bila gospodarska družba v davčnem prekršku, zaradi česar bi ji inšpekcija naložila plačilo visoke globe.

S tem, ko se je računovodja odločil da se bo zanašal na generirano besedilo ChatGPT brez dodatnega preverjanja in nadzora, je nedvomno kršil obveznost vestnega opravljanja dela po 33. členu ZDR-1. Poleg tega je delavec s svojim ravnanjem kršil tudi 37. člen ZDR-1, ki prepoveduje škodljivo ravnanje delavca. V obravnavanem primeru je namreč računovodja s svojo odločitvijo, da se popolnoma zanaša na ChatGPT brez ustreznega preverjanja informacij, povzročil škodo podjetju, saj so napake v letnem poročilu vodile do davčnega prekrška in obveznosti plačila globe. Poleg tega lahko nepravilno pripravljeno letno poročilo škodi tudi ugledu podjetja ter povzroči dodatne administrativne stroške za odpravo napak. Takšno ravnanje, ki vodi do nastanka škode podjetju, je torej v nasprotju z določbami 37. člena ZDR-1, saj predstavlja škodljivo ravnanje.

Poleg tega bi lahko delavec z vnosom podatkov v ChatGPT kršil tudi obveznost varovanja poslovnih skrivnosti delodajalca po 38. členu ZDR-1.

Zaradi svojega ravnanja bi lahko bil delavec za svoje ravnanje disciplinsko odgovoren. Prvi odstavek 172. člena ZDR-1 namreč določa, da lahko delavcu, ki krši pogodbene ali druge obveznosti iz delovnega razmerja, delodajalec v primeru ugotovljene disciplinske odgovornosti izreče opomin ali druge disciplinske sankcije, kot je npr. denarna kazen ali odvzem bonitet, če so določene v kolektivni pogodbi na ravni dejavnosti.

Poleg tega bi lahko bil delavec zaradi kršitve obveznosti iz delovnega razmerja podvržen tudi morebitnemu postopku redne odpovedi pogodbe o zaposlitvi iz krivdnega razloga po 3. alineji prvega odstavka 89. člena ZDR-1 oz., če bi se kršitev smatrala kot hujša kršitev obveznosti iz delovnega razmerja in je delavec ravnal naklepoma ali iz hude malomarnosti, tudi postopku izredne odpovedi pogodbe o zaposlitvi po 2. alineji prvega odstavka 110. člena ZDR-1.

Delavec bi skladno s 177. členom ZDR-1 lahko delodajalcu za nastalo škodo tudi odškodninsko odgoval. Z vidika odškodninske odgovornosti je treba dokazati vse predpostavke odškodninske obveznosti. Ker je v konkretnem primeru delavec kršil dolžnost vestnega opravljanja dela in prepovedi škodljivega ravnanja, je s tem ravnal tudi protipravno (VDSS sodba Pdp 971/2013). Delodajalcu je zaradi njegovega ravnanja nastala premoženjska škoda (plačilo globe za prekršek). Ravnanje delavca, ki se pri svojem delu zanaša na podatke, ki mu jih zagotovi ChatGPT, ne da bi informacije sploh preveril, nedvomno odstopa od ravnanja povprečno skrbnega računovodje.

Opustitev dolžne skrbnosti v tem primeru torej pomeni, da je delavec ravnal (najmanj) hudo malomarno (VDSS Sodba Pdp 257/2022). S tem so izpolnjene vse predpostavke odškodninske obveznosti, zaradi česar bi bil računovodja v obravnavanem primeru delodajalcu odškodninsko odgovoren.

5 Sklep

Uporaba orodja ChatGPT v delovnem okolju odpira številna pravna vprašanja, med drugim vprašanje odgovornosti delavcev za morebitno škodo, ki bi jo lahko povzročili zaradi napačnih, nepopolnih ali zavajajočih informacij, ki jih generira umetna inteligenca.

Delavci so dolžni svoje delo opravljati vestno, po navodilih delodajalca in se vzdržati vseh ravnanj, ki bi lahko škodovala poslovnim interesom delodajalca. Pri uporabi ChatGPT-ja v delovnem okolju je zato ključnega pomena, da delavci preverijo pravilnost in točnost informacij, ki jih orodje generira.

Analiza konkretnega primera je pokazala, da lahko slepo zaupanje informacijam in podatkom, ki jih generira ChatGPT, brez preverjanja vsebin, pomeni kršitev temeljnih delovnih obveznosti, kar lahko privede do disciplinskih sankcij, odpovedi pogodbe o zaposlitvi in tudi odškodninske odgovornosti delodajalcu.

Literatura in viri

1. Bahrini, A. & Khamoshifar, M. & Abbasimehr H. & Riggs, R. & Esmaeili, M. & Majdabadkohne, R. & Pasehvar, M. (2023). *ChatGPT: Applications, opportunities, and threats. Systems and Information Engineering Design Symposium (SIEDS)*, 274–279. <https://doi.org/10.48550/arXiv.2304.09103>
2. Grant M. G. (2024). Artificial intelligence and the practice of law: A chat with ChatGPT. *Saint Louis University Law Journal* 68(3), 609. <https://doi.org/10.35629/5252-0511396407>
3. Humlum A. & Vestergaard E. (2025). The unequal adoption of ChatGPT exacerbates existing inequalities among workers. *PNAS*, 122(1), 2. <https://doi.org/10.1073/pnas.2414972121>
4. Lorek A. L. (2023). AI legal innovations: The benefits and drawbacks of Chat-GPT and generative AI in the legal industry. *Ohio Northern University Law Review*, 50(3), 515. https://digitalcommons.onu.edu/onu_law_review/vol50/iss3/4
5. Obligacijski zakonik (OZ), Uradni list RS, št. 97/07 – uradno prečiščeno besedilo, 64/16 – odl. US in 20/18 – OROZ631.
6. Perlman, A. (2023). The implications of ChatGPT for legal services and society. *Michigan Technology Law Review*, 30(1), 1–2. <https://dx.doi.org/10.2139/ssrn.4294197>

7. Pratiwie S. N. (2023). Chatbots in the workplace: An interpretive phenomenological study of workers on the use of ChatGPT. *International Journal of Social Service and Research*, 3(9), 2297. <https://doi.org/10.46799/ijssr.v3i9.537>
8. Sharma K. S. & Kavia A. S. (2023). ChatGPT and copyright: Legal and ethical challenges. *Osmania University Journal of IPR* 1(1), 172–176. <https://dx.doi.org/10.2139/ssrn.4848807>
9. Shibu S. (2024). *Almost 100% of Gen Zers surveyed admitted to using AI tools at work*. Entrepreneur. <https://www.entrepreneur.com/business-news/gen-z-is-using-ai-chatgpt-at-work-and-proud-of-it-survey/483435>
10. VDSS Sodba in sklep Pdp 172/2023 z dne 23. 11. 2023, ECLI:SI:VDSS:2023:PDP.172.2023.
11. VDSS Sodba Pdp 73/2023 z dne 26. 7. 2023, ECLI:SI:VDSS:2023:PDP.73.2023.
12. VDSS Sodba Pdp 257/2022 z dne 10. 5. 2022, ECLI:SI:VDSS:2022:PDP.257.2022.
13. VDSS Sodba Pdp 317/2017 z dne 24. 8. 2017, ECLI:SI:VDSS:2017:PDP.317.2017.
14. VDSS Sodba Pdp 349/2020 z dne 5. 11. 2020, ECLI:SI:VDSS:2020:PDP.349.2020.
15. VDSS Sodba Pdp 441/2022 z dne 15. 12. 2022, ECLI:SI:VDSS:2022:PDP.441.2022.
16. VDSS Sodba Pdp 651/2021 z dne 14. 2. 2022, ECLI:SI:VDSS:2022:PDP.651.2021.
17. VDSS sodba Pdp 919/2008 z dne 30. 9. 2008, ECLI:SI:VDSS:2008:PDP.919.2008.
18. VDSS sodba Pdp 971/2013 z dne 16. 4. 2014, ECLI:SI:VDSS:2014:PDP.971.2013.
19. VSL Sodba I Cpg 236/2021 z dne 24. 1. 2023, ECLI:SI:VSLJ:2023:I.CPG.236.2021.
20. VSL sodba in sklep I Cpg 1054/2015 z dne 28. 10. 2015, ECLI:SI:VSLJ:2015:I.CPG.1054.2015.
21. VSM sodba I Cp 460/2008 z dne 8. 10. 2008, ECLI:SI:VSMB:2008:I.CP.460.2008.
22. VSM Sodba I Cp 999/2019 z dne 4. 2. 2020, ECLI:SI:VSMB:2020:I.CP.999.2019.
23. VSRS Sklep II Ips 367/2004 z dne 27. 10. 2005, ECLI:SI:VSRS:2005:II.IPS.367.2004.
24. VSRS Sodba VIII Ips 202/98 z dne 1. 12. 1998, ECLI:SI:VSRS:1998:VIII.IPS.202.98.
25. VSRS Sodba VIII Ips 159/2017 z dne 7. 11. 2017, ECLI:SI:VSRS:2017:VIII.IPS.159.2017.
26. Zakon o delovnih razmerjih (ZDR-1), 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, 81/19, 203/20 – ZIUPOPDVE, 119/21 – ZČmiS-A, 202/21 – odl. US, 15/22, 54/22 – ZUPŠ-1, 114/23 in 136/23 – ZIUZDS.

DEDOVANJE KRIPTOVALUT: PRAVNI IZZIVI IN PRAKTIČNE REŠITVE DIGITALNE ZAPUŠČINE

Veronika Mikl, študentka, Univerza v Mariboru, Pravna fakulteta, Slovenija 

Doc. dr. Katja Drnovšek, Univerza v Mariboru, Pravna fakulteta, Slovenija 

Povzetek: V digitalni dobi dedovanje sega onkraj tradicionalnih oblik premoženja in vključuje digitalna sredstva, med katerimi imajo kriptovalute posebno mesto zaradi svoje edinstvene decentralizirane narave. Prispevek se osredotoča na pravne in praktične izzive, povezane z dedovanjem kriptovalut, ter analizira ključne vidike, kot so pravna ureditev, varnost dostopa in tehnične ovire. Uvodoma sta pojasnjena pojem digitalne zapuščine in vse večji pomen slednje v sodobni družbi. Predstavljena je pravna ureditev dedovanja digitalnih sredstev v slovenskem in mednarodnem kontekstu ob upoštevanju obstoječih praks za zagotovitev varnega in učinkovitega dostopa dedičev do kriptodenarnic. Obravnavani so tudi varnostni ukrepi, kot so upravljanje zasebnih ključev, skrbniška gesla in digitalne oporoke, ki igrajo ključno vlogo pri ohranjanju digitalnega premoženja.

Ključne besede: digitalna zapuščina, kriptovalute, dedovanje, digitalna sredstva, dedovanje zapuščine.

Cobiss: 1.08

1 Uvod

Dedno pravo tradicionalno ni področje, ki bi bilo dramatično podvrženo družbenemu in tehnološkemu napredku, kar izkazuje tudi še zmeraj veljavni Zakon o dedovanju (ZD) iz leta 1976, ki je bil do danes le nekajkrat in le malenkostno spremenjen, hkrati pa še zmeraj v zadostni meri služi svojemu namenu. Kljub temu digitalizacija vsakdanjega življenja odpira nove pravne in praktične izzive tudi na tem področju. Digitalna sredstva predstavljajo vse večji del premoženja, s katerim posameznik upravlja skozi življenje, ob njegovi smrti pa kot del zapuščine preide na dediče. Ker ZD ne vsebuje določb, ki bi izrecno urejale dedovanje digitalnega premoženja, drugi področni zakoni pa se vprašanj, povezanih z digitalnimi sredstvi, le delno dotikajo z osamljeno definicijo ali omembo virtualnih sredstev, se pri odločanju o razdelitvi tovrstnega premoženja med dediče uporabljajo splošne določbe. Zaradi posebnih značilnosti digitalnih sredstev slednje ne nudijo vseh odgovorov in rešitev, ki bi učinkovito naslovile sodobne probleme. Vse pogostejše se tako pojavljajo primeri, v katerih je treba odločiti, kaj storiti z računi zapustnika na družbenih omrežjih in platformah (ki imajo lahko pri zapustnikih-vplivnejših tudi veliko premoženjsko vrednost) in z morebitno znamko, ki jo je pri tem ustvaril, z virtualnimi stvarmi, ki jih je kupil ali pridobil pri igranju spletnih videoiger, ter seveda z raznimi oblikami digitalnega premoženja, ki jih ni mogoče materializirati v fizični obliki.

Poseben izziv pri dedovanju digitalnih sredstev predstavljajo kriptovalute, ki s svojo decentralizirano naravo zahtevajo poseben pristop in presegajo klasično razumevanje premoženjskega dela zapuščine in položaja dedičev pri njegovi delitvi. Lastniki tega premoženja, sodniki v zapuščinskem postopku, pa tudi drugi pravni strokovnjaki, se tako srečujejo s ključnim vprašanjem, kako dedičem zagotoviti učinkovit dostop do teh sredstev, ki je lahko zaradi neinformiranosti, tehničnega neznanja, nedostopnosti zasebnih ključev, pa tudi zaradi pravne neurejenosti tega področja, hitro ogrožen.

Z namenom natančne obravnave pravnih in praktičnih izzivov, povezanih z dedovanjem kriptovalut, prispevek najprej pojasni ključne koncepte digitalne zapuščine in digitalnih sredstev, ter daje poseben poudarek kriptovalutam in blockchainu. V nadaljevanju analizira pravno ureditev dedovanja digitalnih sredstev v slovenskem in primerjalnopravnem okviru, s kritično presojo obstoječe zakonodaje in izpostavitvijo odprtih vprašanj. Struktura prispevka sledi tematski razdelitvi: uvodoma so predstavljene uporabljene raziskovalne metode, sledijo pravna opredelitev digitalnih sredstev, posebna obravnava kriptovalut, analiza zakonitega in

oporočnega dedovanja ter praktični izzivi dostopa do digitalnega premoženja. Prispevek se zaključi z ugotovitvami in predlogi za nadaljnji razvoj pravne ureditve.

2 Metode dela

Prispevek temelji na kombinaciji dogmatične, normative in primerjalnopravne metode, s katerimi se analizira trenutno veljavna pravna ureditev dedovanja kriptovalut v Sloveniji in širše. Na podlagi dogmatične metode so najprej obravnavane in interpretirane pravne norme s področja dednega prava, pri čemer je posebna pozornost namenjena določbam Zakona o dedovanju in drugim relevantnim predpisom. Pri raziskavi so bile uporabljene tudi metoda kompilacije za zbiranje teoretičnih in praktičnih stališč iz pravne literature, metoda deskripcije za predstavitev veljavnih pravnih rešitev in metoda analize, s katero so bile identificirane ključne težave pri dedovanju digitalnih sredstev. Ker gre za pravno področje, ki se hitro razvija, je bil v prispevku uporabljen tudi primerjalnopravni pristop, s katerim so analizirane tuje ureditve in njihova uporabnost pri reševanju vprašanj, povezanih z dedovanjem kriptovalut. S tem se izpostavijo možnosti za izboljšanje slovenske zakonodaje in ponudi vpogled v prihodnje trende urejanja digitalne zapuščine.

3 Pravna opredelitev digitalnih sredstev

Digitalna sredstva so digitalna oblika katere koli vrste sredstev, vrednostnih papirjev, pravic, valut ali obračunskih enot, registriranih v porazdeljeni knjigi transakcij, kot je blockchain (Allen, Rauches, Blanding, & Bear, 2020). V obstoječi pravni literaturi ni enotnega soglasja o tem, kaj natančno predstavlja digitalno sredstvo. Kot ključni značilnosti se pogosto izpostavljata obstoj v binarni obliki ter realna ali potencialna vrednost. Čeprav se ti lastnosti odražata v pojmu digitalna sredstva, sami po sebi nista zadostni za dokončno opredelitev vseh binarno zasnovanih objektov kot digitalnih sredstev (Abidin, 2025, str. 2). Digitalna sredstva ne zajemajo zgolj žetonov in kriptovalut, temveč tudi velike podatkovne zbirke (angl. *Big Data*), domenska imena, račune na družbenih omrežjih, virtualno premoženje v igrah ter digitalne vsebine, kot so informacije, shranjene v spletnih sistemih (npr. besedila, video in avdio datoteke, grafične podobe in animacije), vendar taka kategorizacija ni vedno obravnavana kot smiselna (Abidin, 2025, str. 2).

Obseg opredelitve digitalnega sredstva je pogosto odvisen od namena klasifikacije. Pri zaščiti pravic do digitalnih sredstev z omejevanjem dostopa je lahko koristno, da je definicija digitalnih

sredstev čim širša, saj to zagotavlja večjo varnost, vendar pravna ureditev sredstev, kot so žetoni in kriptovalute, zahteva natančnejše določbe, ki upoštevajo njihovo finančno naravo (Abidin, 2025, str. 3). Različni raziskovalci so predlagali različne klasifikacije digitalnih sredstev, odvisno od namena njihove opredelitve. Nekateri digitalna sredstva razvrščajo v kategorije, kot so sredstva omrežnih sistemov, programska sredstva, strojna sredstva, storitvena sredstva, robotska sredstva, podatkovna in metapodatkovna sredstva ter digitalno podprte naprave (Ruan, 2019). Ko konvencionalni predmeti civilnih pravic prevzamejo digitalno obliko, se pojavijo posebni pravni izzivi. V takih primerih je njihova opredelitev kot digitalna sredstva pogosto upravičena, vendar je ključno razlikovati med širokim in ozkim razumevanjem digitalnih sredstev:

- v širšem smislu se lahko za digitalno sredstvo šteje vsaka lastnina v digitalni obliki;
- v ožjem smislu pa digitalna sredstva predstavljajo nova ekonomska sredstva, ustvarjena s pomočjo digitalne tehnologije (Abidin, 2025, str. 3).

Za široko opredelitev digitalnega objekta kot sredstva so se npr. odločili v ZDA, kjer Revidirani enotni zakon o fiduciarnih pravicah dostopa do digitalnih sredstev (angl. *Revised Uniform Fiduciary Access to Digital Assets Act*, RUFADAA) (Uniform Law Commission, 2015), ki ga je leta 2015 sprejela konferenca komisij za poenotenje zakonodaje zveznih držav ZDA (angl. *Uniform Law Commission* – ULC), določa pravila glede dostopa pooblaščenih oseb (fiduciarjev), kot so izvršitelji oporok, skrbniki in pooblaščenci, do digitalnih sredstev pokojnika ali nesposobne osebe (The Law Office of Raymond E. Brown, 2023). Člen 870(h) tega zakona opredeljuje digitalno sredstvo kot elektronski zapis, v katerem ima posameznik pravico ali interes, pri čemer so izključena osnovna sredstva ali obveznosti, razen če so tudi sami elektronski zapisi. Pojem »zapis« se nanaša na informacije, shranjene na fizični napravi ali v elektronskem mediju, ki so dostopne v zaznavni obliki. Na podlagi te definicije lahko digitalno sredstvo široko razumemo kot vsak elektronsko shranjen in prenosljiv predmet, ki je lahko v lasti ter ima povezane lastniške in uporabniške pravice (Abidin, 2025, str. 2).

Ker enotnega sistema kategorizacije digitalnih sredstev ni, omenjeno predstavlja resno oviro pri njihovi regulaciji in upravljanju, saj pogosto obstajajo v mednarodnem in večpravnem okolju. Klasifikacija digitalnih sredstev mora temeljiti na njihovi naravi in bistvu, torej biti skladna s pravicami in obveznostmi, ki jih nalagajo lastniku, pa tudi z njihovim glavnim ekonomskim

namenom in funkcijo digitalnega sredstva. Sprememba oblike sredstva ne pomeni nujno spremembe njegove pravne narave, lahko pa privede do nastanka novih mehanizmov za ustvarjanje, shranjevanje, dostavo in prenos sredstva, kar ima pravne posledice. To je mogoče enostavno ponazoriti s primerom digitalne obveznice: čeprav se narava sredstva ohrani, lahko digitalna oblika vpliva na način njegovega prenosa in s tem povzroči drugačne pravne posledice (Allen, Rauches, Blanding, & Bear, 2020).

Izraz digitalno sredstvo (angl. *digital asset*) je tako širši od izraza kriptosredstvo¹ (angl. *cryptoassets*; glej spodaj). Izraz je dovolj širok in se uporablja že dolgo, da zajema vse od digitalnih predmetov, kot so predmeti v igrah, pa do tudi običajnih nematerializiranih delnic podjetij. V zadnjem času se uporablja za opis predmetov v sodobnih sistemih DLT.² Za razliko od drugih neopredmetenih sredstev, ki temeljijo na notranjih sistemih elektronskega evidentiranja (npr. nematerializirane delnice), so ključne značilnosti teh »novih« digitalnih sredstev:

- Izraznost: pravice in obveznosti je mogoče neposredno kodirati v premoženje in jih samodejno izvrševati.
- Obvladljivost s kriptografskimi ključi: za dostop do sredstev in transakcij so potrebni kriptografski ključi.
- Združljivost: digitalna sredstva se lahko (če ni umetnih omejitev) prosto gibljejo po sistemu, v katerem so bila izdana, in sodelujejo z drugimi digitalnimi sredstvi, ki obstajajo znotraj istih meja (Allen, Rauches, Blanding, & Bear, 2020, str. 13).

4 Kriptovalute kot digitalna sredstva

Kriptovalute so digitalna sredstva, ki temeljijo na decentraliziranem blockchainu (slov. tudi *verženje blokov*) in omogočajo izvedbo varnih, hitrih ter pogosto cenejših finančnih transakcij

¹ Uredba (EU) 2023/1114 Evropskega parlamenta in Sveta z dne 31. maja 2023 o trgih kriptosredstev in spremembi uredb (EU) št. 1093/2010 in (EU) št. 1095/2010 ter direktiv 2013/36/EU in (EU) 2019/1937 (Besedilo velja za EGP) je v členu 3 opredelila, da kriptosredstvo pomeni digitalno predstavitev vrednosti ali pravice, ki jo je mogoče elektronsko prenesti in shraniti z uporabo tehnologije razpršene evidence ali podobne tehnologije.

² Sistem DLT (*Distributed Ledger Technology*) je tehnologija porazdeljene evidence, ki omogoča shranjevanje, upravljanje in preverjanje podatkov na decentraliziran način. Namesto da bi se podatki hranili v eni centralizirani bazi, so razpršeni med več vozlišč (angl. *nodes*) v omrežju, kar zagotavlja večjo varnost, odpornost proti manipulaciji in transparentnost (Allen, Rauches, Blanding, & Bear, 2020, str. 13).

brez posredovanja centralnih bank ali državnih institucij. Za razliko od tradicionalnih valut, ki jih izdajajo centralne banke (t. i. fiat valute), se kriptovalute ustvarjajo s tehnološkimi procesi, kot je rudarjenje, in imajo pogosto vnaprej določeno omejeno skupno zalogo, kar zagotavlja večjo predvidljivost njihovega izdajanja (CoinDesk, 2025). Kriptovalute so nastale kot odziv na sistemske pomanjkljivosti obstoječega finančnega sistema. Gre za digitalno valuto, pri kateri transakcije preverja in evidence vodi decentraliziran sistem, ki za varen prenos digitalnih podatkov uporablja napredne kriptografske metode. Blockchain omogoča delovanje kriptovalut z ustvarjanjem digitalne, javne in nespremenljive evidence vseh povezanih transakcij, kar zagotavlja preglednost in varnost sistema. Decentralizacija tega sistema ne temelji na zaupanju v posamezni subjekt, temveč na tehnološki zasnovi, kar omogoča široko uporabo in vključevanje različnih deležnikov (Pantin, 2023, str. 647–648).

Blockchain lahko na kratko opredelimo kot porazdeljeno glavno knjigo ali seznam podatkovnih zapisov transakcij, ki lahko vključujejo kakršno koli vrednost, denar, blago, lastnino ali glasove. Blockchain se deli v decentraliziranem omrežju računalnikov ter temelji na matematiki in napredni kriptografiji, kjer lahko vsako transakcijo preveri celotno omrežje, ki je lahko javno ali zasebno. Na ta način blockchain postavlja pod vprašaj vse poslovne modele, ki se pri zaupanju in preverjanju zanašajo na tretje osebe, kot so zavarovalnice ali banke (Beck & Müller-Bloch, 2017, str. 5390). Pred sprejetjem blockchaina so stranke sklepale vrednostne transakcije na spletu tako, da so: (1) uporabljale valute, ki jih je izdala vlada, kot plačilno sredstvo, (2) sodelovale z zaupanja vrednimi tretjimi osebami za ublažitev tveganja nasprotne stranke in (3) z vzdrževanjem ločenih računovodskih sistemov za evidentiranje transakcij (Lacity, 2020, str. 364).

Ena od prednosti, ki jo uporabniki pripisujejo kriptovalutam v primerjavi z državnim denarjem, je njihova omejena ponudba, določena s programsko kodo. Za razliko od fiat valut, katerih količino uravnavajo monetarne oblasti in politični odločevalci, je izdajanje kriptovalut pogosto omejeno z vnaprej določenimi algoritmi, kar preprečuje neomejeno tiskanje in potencialno razvrednotenje valute (Ackerman & Kiernan, 2022). Vrednost kriptovalute temelji predvsem na razmerju med njeno ponudbo in skupnim povpraševanjem na trgu (Ciaian, Rajcaniova, & Kanacs, 2016). Glavna privlačnost kriptovalut je v tem, da predstavljajo alternativno pot do finančne svobode, neodvisno od nadzora vlad ali centralnih bank. Decentralizirani finančni instrumenti, kot so kriptovalute, delujejo na javnih omrežjih brez centraliziranega nadzora ali enotne regulativne oblasti. To pomeni, da pri transakcijah ni posrednikov, kot so banke, niti ni potrebnih kreditnih

preverjanj. V decentraliziranem omrežju blockchaina posamezniki za sodelovanje ne potrebujejo medsebojnega poznavanja ali zaupanja, saj varnost in verodostojnost transakcij zagotavlja tehnologija (Pantin, 2023, str. 652–653).

V kontekstu digitalne zapuščine predstavljajo kriptovalute poseben izziv pri dedovanju, saj so shranjene v digitalnih denarnicah, dostop do njih pa je zaščiten s kriptografskimi ključi. Zaradi njihove decentralizirane narave ni osrednjega upravitelja, ki bi omogočil prenos lastništva po smrti imetnika, kar pomeni, da lahko ob nepravilnem upravljanju postanejo nedostopne (CoinDesk, 2025).

5 Digitalna zapuščina v slovenskih in mednarodnih pravnih okvirih

Pojem »digitalna zapuščina« se uporablja za označevanje celote digitalnih sredstev in podatkov, ki ostanejo za posameznikom po njegovi smrti, hkrati pa se lahko nanaša tudi na obstoječe pravne norme, ki urejajo to področje. Med ključna pravna vprašanja sodijo določanje upravičencev do dostopa in pridobitve občutljivih podatkov, kot so gesla za bančne račune, zdravstvene informacije ali podatki o socialnem zavarovanju (Nemeth & Carvalho, 2017, str. 253). V tuji literaturi izraz digitalna zapuščina označuje univerzalno nasledstvo, ki zajema tako žetone in kriptovalute kot tudi e-poštna sporočila in sporočila v komunikacijskih aplikacijah, e-poštne račune v e-poštnih storitvah, elektronske bančne kartice, fotoalbume, objavljene na Instagramu in v oblračnih storitvah, ter glasbene zbirke v digitalnih storitvah in aplikacijah (Berlee, 2017, str. 256–260).

Slovenska dednopravna zakonodaja ne omenja ali opredeljuje digitalne zapuščine in njene vsebine, prav tako ne vzpostavlja posebnega režima, ki bi posebej in drugače urejal dedovanje tovrstnega premoženja. Enako velja za ostalo zakonodajo na področju slovenskega civilnega prava, ki pušča to področje v veliki meri pravno neurejeno. To ne pomeni, da je slovenski zakonodajalec obstoj digitalnega premoženja v celoti spregledal. Slovenija je npr. ena izmed prvih držav, ki je kriptovalute uredila v svoji zakonodaji s področja preprečevanja pranja denarja in financiranja terorizma. Zakon o preprečevanju pranja denarja in financiranja terorizma (v nadaljevanju: ZPPDFT-2) v 3. točki 56. člena opredeljuje virtualne valute kot digitalno obliko vrednosti, ki je ne izda ali za katero ne jamči ne centralna banka ne javni organ in ki ni nujno vezana na zakonito uvedeno valuto ter je brez pravnega statusa valute ali denarnega sredstva; fizične ali pravne osebe jo sprejemajo kot sredstvo menjave, ki se lahko elektronsko prenaša,

shranjuje in izmenjuje (Grlica, 2023). Tudi na področju davkov je bil že leta 2022 sprejet predlog novega zakona o davku od virtualnih valut, vendar do sprejetja zakona ni prišlo. Finančna uprava Republike Slovenije tako vsak primer obdavčitve kriptovalut presoja posebej in se opira na obstoječo ureditev, ki pa je dokaj nejasna (Uršič, 2025). Opisane rešitve pa imajo le omejeno vrednost pri obravnavi dedovanja kriptovalut in drugega digitalnega premoženja. V slovenskem pravnem redu tako ni posebnih določb, ki bi se nanašale neposredno na dedovanje podatkov, digitalnih vsebin ali digitalnih valut, zato se za ta vprašanja uporabljajo splošna načela, ki urejajo dedovanje. Na to opozarja tudi Skubic (2019, str. 28–29), ki pojasnjuje, da se digitalna sredstva v odsotnosti posebnih pravil dedujejo na podlagi splošnih dednopravnih določb. S sklicevanjem na nemško sodno prakso dodatno izpostavlja, da lahko dediči v primeru digitalnih vsebin, kot so računi na družbenih omrežjih, uveljavljajo pravico do dostopa do podatkov, ki jih je imel zapustnik. Dodaja tudi, da je mogoče smernice iz te tuje sodne prakse v bistvenem upoštevati tudi v slovenskem pravnem redu ter da velja dostop do takšnih vsebin – in posledično tudi njihovo dedovanje – šteti kot dopusten. Še posebej to velja za digitalne produkte, ki imajo ekonomsko vrednost, kot so kriptovalute ali v določenih primerih celo zamenljive trofeje v spletnih igrah.

Tudi na ravni Evropske unije še ni vzpostavljena zakonodaja, ki bi se neposredno ukvarjala s problemom digitalne zapuščine in s tem ponujala rešitve ali vsaj smernice za države članice. Te tematike se sicer posredno dotika Splošna uredba o varstvu podatkov (v nadaljevanju: GDPR)³, ki pa ne ureja posebej zaščite osebnih podatkov umrlih posameznikov, temveč prepušča državam članicam, da to področje uredijo z nacionalnimi pravili. GDPR, ki je začel veljati leta 2016, pokriva le osebne podatke živih posameznikov, države članice pa spodbuja, da sprejmejo nacionalne ukrepe glede ravnanja z osebnimi podatki umrlih oseb.

Primerjalnopravni pregled ureditve tega področja v drugih državah potrjuje, da se tudi drugod srečujejo s podobnimi pravnimi izzivi kot v Republiki Sloveniji. Ob pomanjkanju izrecnih določb, ki bi specialno urejale vprašanje dedovanja digitalnih sredstev, se uporabljajo splošne določbe, ki v večini pravnih sistemov pomenijo, da dediči avtomatično podedujejo vse prenosljive pravice in premoženje, ki ga je imel zapustnik v lasti, brez potrebe po posameznem prenosu sredstev ali

³ 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).

obveznosti. To pomeni, da dediči z dedovanjem vstopijo v pravni položaj zapustnika. Hrvaška zakonodaja, ki izhaja iz enake dednopravne podlage kot slovenska, npr. določa, da zapuščina predstavlja celoto pravic in obveznosti, ki so pripadale pokojniku ob njegovi smrti, če so dedne in proste za sukcesijo. Kaj pripada nekomu za čas njegovega življenja, je v hrvaškem civilnem pravu pojasnjeno skozi opredelitev lastnine, pri čemer lastnina pomeni vse, kar je pripadalo pokojniku v trenutku smrti, vključno z vsemi subjektivnimi dednimi pravicami in drugimi pravnimi entitetami (Vučković & Kanceljak, 2019, str. 724–725). Podobne določbe vsebujejo tudi drugi pravni sistemi, npr. 1922. člen nemškega civilnega zakonika (BGB) ali 1112. člen Civilnega zakonika Ruske federacije, po katerih dediščina zajema vsa sredstva, ki jih je imel zapustnik v lasti ob smrti, ter njegove premoženjske pravice in obveznosti, zato so v teh pravnih redih tudi digitalna sredstva, ki imajo prenosljivo vrednost in niso neločljivo vezana na osebno identiteto zapustnika, predmet dedovanja, razen če posebni predpisi določajo drugače (Abidin, 2025, str. 4). Iz tega sledi, da večina tujih držav trenutno k vprašanju dedovanja digitalnih sredstev pristopa na enak način – z uporabo splošnih dednopravnih pravil – kar kaže, da enostavnih in dokončnih rešitev na tem področju še ni.

To seveda pomeni, da se za dedovanje digitalnih sredstev uporabljajo splošne določbe dednopravne zakonodaje, ki niso posebej prilagojene posebnostim digitalnih sredstev in kriptovalut. V nekaterih primerih to ne predstavlja posebne težave, saj je tudi digitalno premoženje navsezadnje predmet premoženjskih pravic, ki nastajajo, se prenašajo in ugašajo na enak način kot pri tradicionalnih oblikah premoženja, vendar pa bi lahko v prihodnosti, če obstoječa ureditev ne bo zadostno naslovila posebnosti teh sredstev, pričakovali večje tveganje za nastanek pravnih negotovosti, sporov, zastojev v postopku, v skrajnih primerih pa celo otežen ali onemogočen dostop do zapustnikovega premoženja ter s tem povezano nezmožnost celovite in dokončne ureditve pravnih razmerij.

6 Zakonito dedovanje

V primerih, kadar zapustnik umre brez oporoke ali je bila ta preklicana ali spoznana za neveljavno, bila uničena, izgubljena, skrita ali založena in se zato obravnava kot neobstoječa, kadar zapustnik z oporoko ni razpolagal z vsem svojim premoženjem ali če je z oporoko postavljen dedič, ki je umrl pred zapustnikom ali se je odrekel dedovanju, zapustnik pa za te primere ni določil namestnika, se dedovanje izvede na podlagi zakona (Zupančič & Žnidaršič Skubic, 2009, str. 63, 75–78). Pri zakonitem dedovanju sta najpomembnejša kriterija za

dedovanje sorodstvena in zakonska zveza. Kot zakoniti dediči po ZD pridejo v poštev zapustnikovi potomci, njegovi posvojenci in njihovi potomci, njegov zakonec ali zunajzakonski partner, zapustnikovi starši in njihovi potomci (tudi zapustnikov posvojitelj in njegovi potomci), pa tudi zapustnikovi stari starši in njihovi potomci. Navedene osebe dedujejo po določenih dednih redih (Zupančič, 2005, str. 43).

Prvi dedni red, določen v 11., 12., 13. in 21. členu ZD, zajema zapustnikove otroke (zakonske, zunajzakonske in posvojene) ter njihove potomce, skupaj z zakoncem zapustnika. Ti dedujejo po enakih delih, po glavah. Zakonec deduje v prvem dednem redu, če obstaja vsaj en zapustnikov potomec, prav tako pa deduje celotno zapuščino, če se potomci dedovanju odpovejo. Drugi dedni red nastopi, če zapustnik nima potomcev. Po 14. členu ZD v tem primeru dedujejo njegovi starši in zakonec. Starša si delita polovico zapuščine (vsak $\frac{1}{4}$), zakonec pa prejme drugo polovico. Če zakonec ne deduje, starši podedujejo celotno zapuščino (vsak $\frac{1}{2}$). Če eden od staršev ne deduje, njegov delež pripade njegovim potomcem po enakih delih, kar imenujemo vstopna pravica. V nasprotnem primeru preide zapuščina k drugemu staršu, kot določa 16. člen ZD. Tretji dedni red, določen v 18., 19. in 20. členu ZD, nastopi, če ni dedičev iz prvega ali drugega dednega reda. V tem primeru dedujejo zapustnikovi stari starši, ki se delijo na materine in očetove starše. Vsakemu paru pripada polovica zapuščine, kar pomeni, da vsak stari starš podeduje $\frac{1}{4}$. Če kateri od starih staršev ne deduje, njegov delež po vstopni pravici pripade njegovim potomcem, torej stricem in tetam zapustnika. Če pa pokojni stari starš nima potomcev ali ti ne dedujejo, njegov delež preide na njegovega zakonca – drugega starega starša. Dediči bližnjega dednega reda izključujejo dediče bolj oddaljenega dednega reda (10. člen ZD). V primeru kriptovalut se torej pri zakonitem dedovanju uporabijo splošne določbe, opisane zgoraj. Dedič bo odvisno od dednega reda in števila dedičev prejel svoj idealni delež.

Preden se zapuščina razdeli, je treba po smrti zapustnika ugotoviti njeno vrednost. Popiše in oceni se vse premoženje, ki ga je imel zapustnik ob svoji smrti (to zajema vse nepremičnine, premičnine, denar in kriptovalute), tudi tisto, s katerim je razpolagal z oporoko, in vse njegove terjatve, tudi tiste, ki jih ima proti kakšnemu dediču, razen tistih, ki so očitno neizterljive. Od ugotovljene vrednosti premoženja se odbijejo zapustnikovi dolgovi, stroški za popis in ocenitev zapuščine ter stroški pogreba (28. člen ZD). Vrednost zapuščine vpliva na odmero sodne takse, ki jo ureja Zakon o sodnih taksah (v nadaljevanju: ZST-1). Ta v 25. členu določa, da se taksa plača od čiste vrednosti zapuščine, ki jo sodišče ugotavlja po prostem preudarku na podlagi izjav

dedičev in podatkov, s katerimi razpolaga. Vrednost čiste zapuščine se ugotovi po vrednosti, ki jo ima ob ceni.

Smiselno je izpostaviti, da vrednost kriptovalut ni pomembna z vidika določitve deležev posameznega dediča, saj vsak dobi svoj ustrezen del, ki pa ima zaradi svoje narave variabilno vrednost. Kot primer: zakonec zapustnika, ki je zapustil še enega otroka, po splošnih pravilih zakonitega dedovanja podeduje $\frac{1}{2}$ zapuščine, s tem pa tudi $\frac{1}{2}$ portfelja kriptovalut, ki so del te zapuščine (npr. 0,5 bitcoina (BTC), če je zapustnik zapustil 1 bitcoin, ali 10 ethereumov (ETH), če je zapustnik zapustil 20 ethereumov). Enako ni sporno, če se dediči glede delitve sporazumejo (in npr. en dedič prevzame vse kriptovalute, preostali pa si razdelijo druge oblike premoženja). Vrednotenje zapuščine, kot je opisano, ni zakonsko sporno ne glede na vrsto premoženja, ki sestavlja zapuščino. Pravna podlaga za ocenjevanje in obračun je jasna in enotna za vse oblike premoženja, vključno z digitalnimi sredstvi.

Vrednost zapuščine ima posledice tudi na davčnem področju. Tako kot vsako podedljivo premoženje so tudi kriptovalute v večini držav po svetu predmet obdavčitve z davkom na dediščino. V Sloveniji je njihova obdavčitev urejena predvsem v kontekstu njihove prodaje ali zamenjave, kjer se obravnavajo kot dohodek ali kapitalski dobiček (Kriptomat, 2024). Kadar govorimo o dedovanju premoženja, pa je osrednji zakon Zakon o davku na dediščino in darila (v nadaljevanju: ZDDD), ki določa obdavčitev glede na dedni red in sorodstveno razmerje med zapustnikom in dedičem. Prvi dedni red, kamor spadajo zapustnikovi otroci in zakonci, je davka oproščen, medtem ko se za drugi in tretji dedni red davčne stopnje določajo glede na vrednost podedovanega premoženja (8. člen ZDDD). Davčna obveznost nastane na dan pravnomočnosti sklepa o dedovanju oz. na dan sprejema darila (6. člen ZDDD). Glede na to, da kriptovalute nimajo posebne obravnave v dedni zakonodaji, se v tem kontekstu obravnavajo kot premoženje in so zato predmet davka na dediščino in darila v skladu z zgoraj omenjenimi določbami. Dedič kriptovalut bo obdavčen glede na dedni red, v katerem deduje, in vrednost podedovanega (davčne stopnje za dediče drugega dednega reda se gibljejo med 5 in 14 %, za dediče tretjega dednega reda med 8 in 17 %, za vse druge osebe – npr. oporočne dediče – pa med 12 in 39 %). Ker se vrednost kriptovalut lahko spreminja, je ključnega pomena, da se njihova vrednost pravilno oceni.

V Nemčiji se npr. davčne stopnje pri dedovanju gibljejo med 7 % in 50 %, odvisno od vrednosti podedovanega premoženja. Bitcoin in druge kriptovalute so sestavni del zapuščine, ki preide na

dediče. Enako velja recimo na Japonskem in v Združenem kraljestvu, kjer se bitcoini in druga digitalna sredstva obravnavajo kot premoženje za namene obdavčitve dediščine in so, z določenimi izjemami, predmet davka na dediščino v višini 40 %. Tudi v Združenih državah Amerike morajo dediči plačati davek na dediščino za podedovane kriptovalute v skladu s skupno vrednostjo zapuščine. V Franciji se davčne stopnje gibljejo med 5 % in 45 %, odvisno od vrednosti zapuščine (Carata & Chelaru, 2024, str. 8).

Določanje vrednosti premoženja zapustnika, plačilo davka in sodne takse sami po sebi niso sporni. Problem za dediče lahko nastane zaradi volatilnosti kriptovalut, kar lahko privede do znatnih finančnih izgub (Simasko, 2025). Carata & Chelaru (2024, str. 8) ugotavljata, da v skladu z uveljavljeno pravno doktrino tveganje volatilnosti nosijo dediči, saj se vrednost kriptovalut, preračunana v fiat valute, nenehno spreminja in ni vezana na uradno določeni tečaj. Obenem se postavlja vprašanje, kateri časovni trenutek je relevanten za določitev njihove vrednosti. Po njihnih navedbah se pri ugotavljanju vrednosti zapuščine za namene delitve med dediče (in izračuna nujnega deleža) upošteva vrednost kriptovalut na dan smrti zapustnika. Lastninska pravica se pridobi retroaktivno, z učinkom od dneva smrti zapustnika, zato je ta datum tudi ključen za določitev vrednosti kriptovalut. Njihova vrednost se izračuna na podlagi menjalnega razmerja s fiat valutami, ki je bilo na ta dan določeno na eni izmed borznih platform.

Ta časovni trenutek pa ni enak trenutku, ki se upošteva pri izračunu sodne takse ali davka na dediščino. Pri ugotavljanju vrednosti, ki je odločilna za odmero sodne takse v zapuščinskem postopku, se bo vrednost kriptovalut skladno z ZST-1 določila na podlagi menjalnega tečaja na dan, ko je sodišče odmerjalo takso v zapuščinskem postopku, pri računanju davka na dediščino pa skladno z ZDDD na dan, ko je izdalo sklep o dedovanju. Sodišče sicer lahko odmeri takso in izda sklep o dedovanju na isti dan, po naravi stvari pa tega ne more storiti na dan smrti zapustnika, kar pomeni, da se bo vrednost kriptovalut, izražena v fiat valuti, v teh časovnih trenutkih najpogosteje razlikovala. Predvsem je problematična situacija, ko je posamezna kriptovaluta ob smrti zapustnika vredna občutno več kot pa po trenutku, ko sta odmerjena sodna taksa in davek na dediščino in darila. Takšna dilema se pojavi tako pri zakonitem kot tudi oporočnem dedovanju.

7 Oporočno dedovanje

Oporočno dedovanje temelji na oporoki, ki predstavlja izraz svobode testiranja. Ta svoboda sicer ni absolutna, saj je zapustnik pri razpolaganju omejen (npr. z 8. in 62. členom ZD). Oporoka je enostranska, preklicna in strogo osebna izjava volje, podana za primer smrti. Gre za strogo formalni pravni posel, saj velja načelo obličnosti in je oporoka veljavna le, če je sestavljena v eni izmed oblik, določenih v ZD. Oporočitelj ima vselej pravico, da oporoko prekliče, kar mu omogočata prvi odstavek 99. člena in 105. člen ZD. Oporoka tako določi drugačno usodo premoženju, kot bi jo to imelo v primeru zakonitega dedovanja (Zupančič, 2005, str. 67–74).

Tudi kadar zapustnik sestavi oporoko, ne more priti do popolnega neupoštevanja zakonitega dednega reda, čemur služi institut nujnega deleža. Nujni dediči morajo dobiti del, ki jim pripada po zakonu, četudi jih je zapustnik v oporoki prezrl. Zapustnika takšna določba omejuje tudi pri razpolaganju s premoženjem za čas svojega življenja. Če je zapustnik z delom premoženja, ki predstavlja nujni delež, razpolagal bodisi z darili med živimi bodisi z oporoko, lahko prikrajšani nujni dediči po njegovi smrti zahtevajo, da se ta razpolaganja razveljavijo (Zupančič, 2005, str. 55–58). Izračunanje nujnega deleža in razpoložljivega dela zapuščine se ugotavlja po določbah 28. člena ZD. V kolikor bi zapustnik kriptovalute podaril že za čas svojega življenja in s tem prikrajšal nujni delež dedičev, se uporabita določbi 34. in 35. člena ZD, ki določata, da se v primeru takšnega prikrajšanja najprej zmanjšajo oporočna razpolaganja, če to ne zadostuje, pa se vrnejo tudi darila, kolikor je treba, da se dopolni nujni delež. Pri določanju vrednosti daril se upošteva vrednost darila ob zapustnikovi smrti in po stanju ob daritvi (30. člen ZD). Enako kot pri določanju vrednosti zapustnikovega premoženja in na ta znesek vezanem davku na dediščino in darila ter določitvi sodne takse, so lahko tudi v tem primeru kriptovalute ob zapustnikovi smrti vredne veliko več ali manj kot takrat, ko jih je dedič dobil v dar.

V Sloveniji so pravno priznane le oblike oporok, ki so izrecno navedene v ZD (lastnoročna oporoka, pisna oporoka pred pričami, sodna oporoka, oporoka, sestavljena v tujini, oporoka, sestavljena na slovenski ladji, oporoka, sestavljena med izrednim ali vojnim stanjem, mednarodna oporoka ter notarska oporoka, ki jo sicer ureja Zakon o notariatu), pri čemer digitalna (angl. *digital will*) in elektronska oporoka (angl. *electronic will*), ki se omenjata v strokovni literaturi, nista med njimi. Lamovec Hren (2024, str. 190–191) pojasnjuje, da izraza kljub podobnosti nista sopomenki. Ugotavlja, da so nekateri avtorji izraz digitalna oporoka uporabljali nedosledno – bodisi za opis elektronsko oblikovane in shranjene oporoke bodisi kot

zapis volje, ki se nanaša izključno na digitalno premoženje. V slednjem primeru digitalna oporoka pomeni neformalen dokument, v katerem zapustnik določi osebe, ki bodo po njegovi smrti imele dostop do njegovega digitalnega premoženja, pogosto skupaj z uporabniškimi imeni in gesli. Gre za občutljive osebne podatke, ki so pogosto varnostno kodirani, zato Lamovec Hren opozarja, da ni v interesu, da so javno dostopni. Tako je smiselno, da je tak zapis fizično ločen od klasične oporoke, ki ureja razpolaganje s premičnim in nepremičnim premoženjem. Elektronska oporoka pa po njenem mnenju zajema širši spekter – tako digitalne kot analogne zapise, nastale z uporabo elektronskih naprav, medtem ko digitalna oporoka zajema zgolj digitalno premoženje. Tudi Storow (2022, str. 828) elektronsko oporoko opredeljuje kot oporoko, ustvarjeno in shranjeno v digitalni obliki ter podpisano z elektronskim podpisom, s čimer potrdi razumevanje elektronske oporoke kot formaliziranega elektronskega dokumenta.

V večini držav, vključno s Slovenijo, elektronska oporoka ni priznana kot veljavna oblika razpolaganja za primer smrti. Slovenska zakonodaja tega izrecno ne ureja, vendar iz 62. in 76. člena ZD izhaja, da so veljavne le tiste oporoke, ki ustrezajo eni od zakonsko določenih oblik. Ob sprejetju ZD elektronski zapis še ni bil razširjen, zato je razumljivo, da se pisna oporoka obravnava izključno v klasični obliki. Čeprav bi se elektronski zapis lahko teoretično subsumiral pod pisno obliko, to preprečuje Zakon o elektronskem poslovanju in elektronskem podpisu (v nadaljevanju: ZEPEP), ki v 13. členu oporočne posle izrecno izključuje iz izenačevanja pisne in elektronske oblike. Popolna prepoved elektronske oporoke zagotavlja pravno gotovost, vendar lahko pretirano poudarjanje obličnosti vodi v situacije, kjer je dejanska volja oporočitelja spregledana (Lamovec Hren, 2024, str. 284–289).

8 Praktični izzivi pri dedovanju kriptovalut

Kriptovalute niso vidne v klasičnih finančnih evidencah, kot so bančni računi ali nepremičninski registri, kar pomeni, da dediči sploh ne vedo, da je pokojnik morebiti imel kriptovalute in kakšen je v tem primeru njihov obseg (Vučković & Kanceljak, 2019). Za razliko od tradicionalnih finančnih instrumentov ne obstaja osrednji organ, ki bi dedičem omogočal pridobitev informacij o premoženju zapustnika, kar je glavna značilnost decentralizacije. Kriptovalute so shranjene v digitalnih denarnicah, katerih lastniki so v blockchainu identificirani le s kombinacijo številčnih nizov, kar pomeni, da brez izrecne izjave ali dokumentacije zapustnika dediči nimajo pravnega ali tehničnega sredstva za ugotovitev lastništva (Carata & Chelaru, 2024). Visoka stopnja varnosti in anonimnosti je sicer ena največjih prednosti, a hkrati ravno to povzroča izzive, ko govorimo o

dedovanju (McClure, 2024). Varnostni mehanizmi, povezani z zasebnimi in javnimi ključi, ter kriptodenarnice še dodatno zapletejo situacijo. Zasebni ključ je ključni element kriptovalut in varuje uporabnike pred krajo in nepooblaščenim dostopom do njihovih sredstev. Če uporabnik izgubi svoj zasebni ključ, ne more več dostopati do svoje denarnice (The Investopedia Team, 2024). V tem primeru govorimo o premoženju, zato velja domneva, da je posestnik hkrati tudi lastnik (posest pomeni lastništvo). To pomeni, da morajo dediči za učinkovit dostop do kriptovalut v teh denarnicah pridobiti posest dostopnih ključev. Če oseba pridobi te ključe, samodejno postane lastnik in uporabnik denarnice ter sredstev v njej (Carata & Chelaru, 2024, str. 7). Iz omenjenih razlogov je dokumentiranje gesel in dostopnih podatkov nujno. Navodila za dostop do zasebnega ključa morajo biti na voljo osebi, ki bo skrbela za prenos premoženja. Brez teh podatkov lahko kriptosredstva postanejo nedostopna in se *de facto* izgubijo za vedno. Če oseba umre brez oporoke, se kriptovalute dedujejo v skladu z zakonom, vendar dedovanje samo po sebi ne zagotavlja njihovega dostopa (McClure, 2024).

Da bi zapustniki ustrezno postopali, je v tem kontekstu bistveno razlikovati med različnimi oblikami hrambe kriptovalut. V primeru, da so sredstva shranjena na določenih kriptoborzah, kot so Coinbase, Kraken ali Binance, lahko zapustnik določi upravičenca za primer smrti. Ta postopek je podoben imenovanju upravičenca pri bančnem računu ali pokojninskem načrtu. Za njegovo vzpostavitev se je treba prijaviti v svoj račun in poiskati možnost določitve upravičenca. Nekatere platforme to označujejo kot obrazec za prenos ob smrti (angl. *Transfer on Death – TOD*), kjer je treba navesti ime, datum rojstva in kontaktne podatke upravičenca. Priporočljivo je hraniti kopijo za lastne evidence. Zasebne denarnice (kjer se shranjujejo zasebni ključi), kot so Ledger, Trezor in MetaMask, običajno ne omogočajo neposredne določitve upravičencev, zato je nujno voditi evidenco dostopnih podatkov in zasebne ključe varno shraniti. Pri načrtovanju dedovanja je priporočljivo vključiti podrobna navodila za dostop do denarnice, vključno z gesli, obnovitvenimi frazami ali lokacijami fizičnih naprav. Za varno shranjevanje zasebnih ključev je smiselno uporabiti strojno denarnico ali šifrirano datoteko. V določenih primerih je lahko ustrezna tudi skrbniška rešitev, saj nekatere specializirane storitve za upravljanje digitalnih sredstev omogočajo enostavnejšo določitev upravičencev (Simasko, 2025).

Možnost tehnološke metode vključuje različne vnaprej določene načine prenosa ali programe, ki so del digitalnih denarnic, ter določene avtomatizirane sisteme prenosa, ki temeljijo na pametnih pogodbah in dokazilu o smrti imetnika. Ena izmed najnaprednejših metod prenosa

premoženja vključuje uporabo elektronskega sefa, podprtega z blockchainom. Lastnik v tem primeru zapusti tudi navodila za prenos podatkov dedičem, pri čemer se prenos lahko sproži npr. s predložitvijo izpiska iz matičnega registra o smrti. Kljub naprednosti te tehnologije popolna zaščita podatkov ni povsem zagotovljena. Številne kriptoborze omogočajo storitve prenosa digitalnih denarnic na dediče, vendar šele po tem, ko ti predložijo dokazilo o smrti zapustnika in upravičenosti do dedovanja (Carata & Chelaru, 2024, str. 7). Mešana metoda vključuje dedovanje digitalnih denarnic v fizični in elektronski obliki. Dostopni ključi so lahko shranjeni na varnih mestih, kot so bančni sefi ali arhivi, njihova lokacija pa je lahko navedena v besedilu oporoke (Morris, 2018).

Spodaj opisana primera jasno prikazujeta, kakšno razliko lahko naredi ustrezno načrtovanje usode digitalnega premoženja. Gerald Cotten, ustanovitelj kanadske kriptoborze QuadrigaCX, je decembra 2018 nenadoma preminil pri 30 letih. Bil je edini, ki je imel dostop do ključev za digitalne denarnice s približno 190 milijonov kanadskih dolarjev vrednimi sredstvi strank. Ker ni pustil navodil za dostop, vlagateljem niso mogli povrniti njihovega denarja. Njegova smrt je sprožila preiskavo, saj je okoli 115.000 ljudi utrpelo izgube, mnogi pa so sumili goljufijo. Strokovnjaki so analizirali njegove naprave in dokumente, a večina sredstev je ostala nedostopna. Oblasti so zaključile, da je šlo za Ponzijevo shemo – Cotten naj bi stranke zavajal s fiktivnimi zneski ali vlagal v kriptovalute, ki so izgubile vrednost. Primer razkriva tveganja centralizacije nadzora nad kriptovalutami in pomen načrtovanja prenosa digitalnega premoženja v primeru nepričakovanih dogodkov (CoinDesk, 2024). Nasprotni primer je Hal Finney, pionir kriptovalut in prvi prejemnik bitcoina, ki je zaradi degenerativne bolezni pravočasno uredil dostop do svojih sredstev. Ključe in navodila je varno shranil, kar je njegovim dedičem omogočilo nemoten prevzem premoženja. Ta primera poudarjata ključno vlogo premišljenega načrtovanja pri dedovanju digitalnih sredstev in tveganja, ki nastanejo, če tega ni (Kaur, 2024).

Kriptovalute ponujajo privlačne priložnosti za ustvarjanje premoženja, vendar zahtevajo skrbno načrtovanje za vključitev v dedni načrt. Bistveno je upoštevati naslednje vidike:

- Varnost shranjevanja dostopnih podatkov: Priporočljivo je hraniti zasebne ključe v strojni denarnici ali šifriranem digitalnem arhivu, pri čemer je treba zagotoviti, da izvršitelj oporoke ali skrbnik razpolagata z ustreznimi navodili za varen dostop.

- Redno posodabljanje evidence kriptometja: Nujno je vzdrževati ažuren popis digitalnih sredstev, ki vključuje naslove denarnic, vrste kriptovalut in njihovo približno vrednost, ter ga periodično posodablja skladno s spremembami v portfelju.
- Določitev jasnih smernic v dednih dokumentih: Čeprav je varnost dostopa prednostnega pomena, morajo dedni dokumenti vsebovati dovolj informacij, ki omogočajo zakonitim dedičem identifikacijo in dostop do kriptometja.
- Upoštevanje manj uveljavljenih digitalnih sredstev: V primeru razpršenega portfelja, ki vključuje altcoine ali žetone, ki niso podprti na večjih borzah, je pomembno, da so ta sredstva ustrezno dokumentirana, s čimer se prepreči njihova morebitna izguba ali spregled v postopku dedovanja (Simasko, 2025).

Da bi se izognili zgoraj opisanim izzivom pri dedovanju kriptovalut, je bistveno, da zapustniki pravočasno premislijo, kaj želijo, da se zgodi z njihovim digitalnim premoženjem, in komu ga nameravajo zapustiti. Kriptovalute zaradi svoje decentralizirane narave ne omogočajo enostavnega prenosa na dediče, zato lahko neustrezno načrtovanje vodi v trajno izgubo sredstev. Za zagotovitev učinkovitega prenosa kriptopremoženja so še vedno relevantne tradicionalne oporoke, veljavne po ZD, ki omogočajo razpolaganje s premoženjem za primer smrti. Skrbno načrtovanje in izbira ustreznega instrumenta dedovanja sta zato ključna za varen in nemoten prenos kriptovalut na dediče.

9 Sklep

Razvoj digitalnih tehnologij in decentraliziranih financ predstavlja pomembne pravne in praktične izzive za področje dednega prava, ki sicer ni znano po pretirano dinamičnem pristopu k naslavljanju družbenih sprememb. Dejstvo, da ureditev dedovanja v ZD desetletja ni zahtevala bistvenih sprememb in je z zadostno učinkovitostjo pokrivala različne oblike premoženja, ne glede na njihov nosilec ali obliko, priča o njegovi odpornosti na tehnološki razvoj. Tradicionalni koncepti univerzalne sukcesije v veliki večini primerov zadoščajo za razdelitev premoženja med dediče, kar velja tako za klasične oblike premoženja (premičnine, nepremičnine, terjatve itd.) kot tudi za razne inovacije in digitalne oblike premoženja, ki jih je s pomočjo metod razlage in analogije običajno mogoče finančno ovrednotiti in obravnavati na enak način kot klasične oblike. Kot opozarjajo nekatere težave, ki se že pojavljajo v praksi, pa veljavna ureditev vendarle

spregleda tehnološke posebnosti kriptovalut, katerih decentralizirana narava lahko bistveno oteži ali celo prepreči prenos digitalnega premoženja na dediče.

Analiza slovenskega pravnega okvira kaže, da trenutno uveljavljeni pristop, ki se pri reševanju dednopравnih vprašanj zanaša na uporabo splošnih določb ZD, ne zagotavlja celovite zaščite interesov dedičev v zapuščinskem postopku, kadar del zapuščine predstavljajo kriptovalute. Tako pri zakonitem kot tudi oporočnem dedovanju se odpirajo pomembne pravne dileme, ki so povezane predvsem z vrednotenjem in volatilnostjo kriptovalut. Nenehne spremembe v njihovi vrednosti ne predstavljajo bistvene težave pri določitvi idealnega deleža zapuščine, ki pripade posameznemu dediču (»en bitcoin je en bitcoin«), lahko pa drastično zapletejo postopek, ko pride do razdelitve premoženja v naravi določanja nujnega deleža ter vračunavanja in vračanja daril. V naštetih primerih se vrednost kriptovalut, preračunana v fiat valuto, namreč oceni po časovnem trenutku v bolj ali manj oddaljeni preteklosti, kar lahko v praksi predstavlja veliko negotovost za dediče (ki navsezadnje ne morejo pravno razpolagati s kriptovalutami, dokler zapuščinski postopek ni pravnomočno zaključen), včasih pa tudi nesorazmerno obremenitev (npr. vračanje darila pri dediču, ki je bil obdarjen s kriptovalutami, katerih vrednost se je v vmesnem času bistveno spremenila). Do dodatnega zapleta lahko privedejo razhajanja med ureditvijo v ZD, ZST-1 in ZDDD, ki časovni trenutek, po katerem se ocenjuje vrednost zapuščine, vežejo na različne pravnorelevantne okoliščine (trenutek smrti, čas cenitve, izdaja sklepa o dedovanju), kar ima lahko za posledico nesorazmerno visoko sodno takso ali odmero davka.

Tudi v primerih, ko zakonska neurejenost dedovanja digitalnih sredstev ne predstavlja pravnih ovir za prehod tovrstne zapuščine na dediče, je njihova pravna gotovost pogosto ogrožena zaradi praktičnih izzivov. Nedostopnost podatkov o imetništvu decentraliziranih valut, odsotnost institucionalnega nadzora in upravljanja ter nepoznavanje zasebnih ključev lahko privedejo do situacije, kjer je zapuščina na podlagi sklepa o dedovanju pravnomočno prešla na dediče, ti pa do nje ne morejo dostopati. Decentralizirani sistemi že po svoji naravi ne vsebujejo institucionalnih mehanizmov, ki bi tretjim osebam omogočali dostop do podatkov o digitalnih sredstvih ali do digitalnih sredstev kot takih po smrti njihovega imetnika, zato lahko takšna situacija vodi v trajno izgubo premoženja. Možnosti državnih organov so – po smrti zapustnika, pa tudi dedičev – na tem področju izrazito omejene, zato je prav zapustnik tisti, ki mora prevzeti odgovornost za usodo lastnega digitalnega premoženja po svoji smrti. Pri tem je v prvi vrsti ključno ozaveščanje imetnikov kriptovalut o pravnem položaju njihovega digitalnega

premoženja, težavah, s katerimi se lahko soočijo njihovi dediči, ter o njihovih pravnih možnostih. To je še toliko pomembneje zaradi dejstva, da pomemben delež imetnikov kriptovalut pripada mlajšim starostnim skupinam, ki pogosto ne razmišljajo o neizbežnosti svoje smrti in o nujnosti oporoke. Premišljeni in vestni ukrepi, kot so seznanitev bližnjih s svojim digitalnim premoženjem, varen, a po smrti dostopen zapis zasebnih ključev in gesel, ali navsezadnje oporočna določba z navodili glede dostopa in razpolaganja s kriptovalutami, lahko že v trenutnih zakonodajnih okvirih preprečijo številne nevšečnosti in navsezadnje nepovratno izgubo premoženja.

Na bolj sistemski ravni bodo za večjo pravno varnost na tem področju potrebni tudi zakonodajni ukrepi, kot sta zakonska opredelitev digitalne zapuščine in prilagoditev zapuščinskih postopkov posebnostim tovrstnega premoženja, ter vzpostavitev jasnejšega materialnopravnega okvira, ki bo upošteval tehnološke posebnosti kriptovalut in drugih digitalnih sredstev. Primerjalnopravni pregled je pokazal, da se s podobnimi izzivi srečujejo tudi druge države v naši pravni sosesčini, zato bi glede na globalno prenosljivost kriptovalut koristili tudi skupni mednarodni napor v smeri regulacije dostopa do podatkov o digitalnih sredstvih, zagotavljanja dostopa do sredstev po smrti imetnika (kolikor je to glede na njihovo decentralizirano naravo sploh mogoče) ter digitalnih oporok.

Literatura in viri

1. Abidin, M. I. (2025). Legal challenges and framework for cryptocurrency inheritance in Indonesia. *UAI Journal of Arts, Humanities and Social Sciences*, 2(1), 1–7. <https://doi.org/10.5281/zenodo.14697934>
2. Ackerman, A., & Kiernan, P. (2022). *Crypto could threaten financial system, Federal Risk Panel warns*. The Wall Street Journal. <https://www.wsj.com/articles/crypto-could-threaten-financial-system-federal-risk-panel-warns-11664826496>
3. Allen, G. J., Rauches, M., Blanding, A., & Bear, K. (2020). *Legal and regulatory considerations for digital assets*. Cambridge Center for Alternative Finance. <https://www.jbs.cam.ac.uk/wp-content/uploads/2020/10/2020-ccaf-legal-regulatory-considerations-report.pdf>
4. Beck, R., & Müller-Bloch, C. (2017). *Blockchain as radical innovation: A framework for engaging with distributed ledgers*. Hawaii International Conference on System Sciences (str. 5390). <https://scholarspace.manoa.hawaii.edu/server/api/core/bitstreams/86612670-480d-4e1d-8b39-b00e3cfe4234/content>
5. Berlee, A. (2017). Digital inheritance in the Netherlands. *Journal of European Consumer and Market Law*(6), 256–260. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3082802
6. Carata, C., & Chelaru, A. (2024). *The evolution of the digital inheritance: Legal, technical, and practical dimensions of cryptocurrency transfer through succession in French-inspired legal systems*. Cornell University. <https://doi.org/10.48550/arXiv.2410.22907>

7. Ciaian, P., Rajcaniova, M., & Kancs, d. (2016). The economics of BitCoin price formation. *Applied Economics*, 48(19), 1799–1813. <https://doi.org/10.1080/00036846.2015.1109038>
8. CoinDesk. (2024). *The story behind QuadrigaCX and Gerald Cotten, Netflix's 'Crypto King'*. CoinDesk. <https://www.coindesk.com/learn/the-story-behind-quadrigacx-and-gerald-cotten-netflixs-crypto-king>
9. CoinDesk (2025). *What is cryptocurrency?* CoinDesk. <https://www.coindesk.com/learn/what-is-cryptocurrency>
10. Grlica, I. (2023). Kriptovalute v slovenski zakonodaji in sodni praksi. *Revija Odvetnik*, 110(2). <https://www.tax-finlex.si/Dokument/Podrobnosti?rootEntityId=4bbb44a1-cb28-4e1e-b937-598c87cd6728>
11. Justiz, B. d. (brez datuma). *Bürgerliches Gesetzbuch (BGB)*. Bundesministerium der Justiz und für Verbraucherschutz. <https://www.gesetze-im-internet.de/bgb/>
12. Kaur, G. (2024). *Who is Hal Finney: Behind the scenes of the first Bitcoin transaction*. Cointelegraph. <https://cointelegraph.com/learn/hal-finney>
13. Kriptomat. (2024). *Davek na kriptovalute v Sloveniji 2024*. Kriptomat. <https://kriptomat.io/sl/kriptovalute/davek-na-kriptovalute-v-sloveniji/>
14. Lacity, M. (2020). Crypto and blockchain fundamentals. *Arkansas Law Review*, 73(2), 364. https://heinonline-org.ezproxy.lib.ukm.si/HOL/Page?collection=journals&handle=hein.journals/arklr73&id=1&men_tab=srchresults
15. Lamovec Hren, P. (2024). *Oporoka: institut, raba, prihodnost*. Ljubljana: Uradni list Republike Slovenije in Inštitut za primerjalno pravo pri Pravni fakulteti.
16. McClure, Z. (2024). *What happens to your crypto when you die*. TokenTax. <https://tokentax.co/blog/what-happens-to-your-crypto-when-you-die>
17. Morris, A. (2018). Next generation: With the rise of cryptocurrency, estate lawyers caution that it shouldn't be treated like any other asset. *ABA Journal*, 104(11), 33–34. <https://law-journals-books.vlex.com/vid/next-generation-842451869>
18. Nemeth, K., & Carvalho, J. M. (2017). Digital inheritance in the European Union. *Journal of European Consumer and Market Law*, 6(6), 253. <https://jorgemoraiscarvalho.com/wp-content/uploads/2018/02/Digital-Inheritance-in-the-European-Union.pdf>
19. Pantin, L. P. (2023). Financial inclusion, cryptocurrency, and Afrofuturism. *Northwestern University Law Review*, 118(3), 647–648. https://heinonline-org.ezproxy.lib.ukm.si/HOL/Page?collection=journals&handle=hein.journals/illlr118&id=670&men_tab=srchresults
20. Ruan, K. (2019). *Digital asset valuation and cyber risk measurement: Principles of cybernomics*. London: Academic Press.
21. Simasko, P. M. (2025). *Heirs inheriting crypto? Don't make it a headache for them*. Kiplinger. <https://www.kiplinger.com/retirement/inheriting-crypto-dont-make-it-a-headache-for-your-heirs>
22. Skubic, Z. (2019). Dedovanje digitalne zapuščine. *Pravna praksa*, 38(32), 28–29.
23. Storrow, R. F. (2022). Legacies of pandemic: remote attestation and electronic wills. *Mitchell Hamline Law Review*, 48(4), 826–862. <https://ssrn.com/abstract=4160852>
24. The Investopedia Team. (2024). *Private key: What it is, How it works, and best ways to store*. Investopedia. <https://www.investopedia.com/terms/p/private-key.asp>
25. The Law Office of Raymond E. Brown. (2023). *RUFADAA explained*. The Law Office of Raymond E. Brown: <https://raymondbrownlaw.com/rufadaa-explained/>

26. Uniform Law Commission. (2015). Revised Uniform Fiduciary Access to Digital Assets Act. Uniform Law Commission.
<https://www.uniformlaws.org/HigherLogic/System/DownloadDocumentFile.ashx?DocumentFileKey=47cdcf85-e35a-995f-09ee-8030d01148a9&forceDialog=1>
27. Uršič, J. (2025). *Obdavčitev kriptovalut (davek na kriptovalute)*. Odvetniška družba Pirc, o.p., d.o.o. <https://odp.eu/obdavcitev-kriptovalut/>
28. Vučković, R. M., & Kanceljak, I. (2019). Does the right to use digital content affect our digital inheritance? *EU and Comparative Law Issues and Challenges Series (ECLIC)*, 3, 724-746. <https://doi.org/10.25234/eclic/9029>
29. ZD. (1976). *Zakon o dedovanju*. Uradni list SRS, št. 15/76, 23/78, Uradni list RS, št. 13/94 – ZN, 40/94 – odl. US, 117/00 – odl. US, 67/01, 83/01 – OZ, 73/04 – ZN-C, 31/13 – odl. US, 63/16 in 102/24.
30. ZDDD. (2006). *Zakon o davku na dediščine in darila*. Uradni list RS, št. 117/06 in 36/16 – odl. US.
31. ZEPEP. (2000). *Zakon o elektronskem poslovanju in elektronskem podpisu*. Uradni list RS, št. 98/04 – uradno prečiščeno besedilo, 61/06 – ZEPT, 46/14, 121/21 – ZEISZ in 130/22 – ZN-H.
32. ZN. (1994). *Zakon o notariatu*. Uradni list RS, št. 2/07 – uradno prečiščeno besedilo, 33/07 – ZSReg-B, 45/08, 91/13, 189/20 – ZFRO, 130/22, 49/23 – ZUS-1C in 102/23 – ZFPPIPP-H.
33. ZPPDFT-2. (2022). *Zakon o preprečevanju pranja denarja in financiranja terorizma*. Uradni list RS, št. 98/04 – uradno prečiščeno besedilo, 61/06 – ZEPT, 46/14, 121/21 – ZEISZ in 130/22 – ZN-H.
34. ZST-1. (2008). *Zakon o sodnih taksah*. Uradni list RS, št. 37/08, 97/10, 63/13, 58/14 – odl. US, 19/15 – odl. US, 30/16, 10/17 – ZPP-E, 11/18 – ZIZ-L, 35/18 – odl. US in 204/21.
35. Zupančič, K. (2005). *Dedovanje*. Ljubljana: Uradni list Republike Slovenije.
36. Zupančič, K., & Žnidaršič Skubic, V. (2009). *Dedno pravo*. Ljubljana: Uradni list Republike Slovenije.

UPORABNOST TEHNOLOGIJE BLOCKCHAIN V ZEMLJIŠKI KNJIGI

Jovana Pajkowska, študentka, Univerza v Mariboru, Pravna fakulteta 

Asist. dr. Kristjan Zahrastnik, Univerza v Mariboru, Pravna fakulteta 

Povzetek: Blockchain bi lahko revolucionarno spremenil vodenje zemljiškoknjižnega sistema v Sloveniji, saj bi imel zmožnost povečati preglednost, varnost in učinkovitost. Glede na to, da lahko trajno beležimo transakcije in decentraliziramo dostop, se lahko izognemo napakam in zmanjšamo birokracijo v tem, kar je pogosto zapleten proces. Po drugi strani pa, čeprav blockchain veliko obeta, prinaša tudi pomembne pravne izzive, ki zahtevajo pravne spremembe, zlasti na področju varstva podatkov. Poleg tega so se pojavile dileme glede pravne veljavnosti tovrstnih digitalnih zapisov in tega, ali je treba spremeniti zakonodajo, da bi omogočili nemoteno implementacijo blockchaina v pravni sistem. Večina držav je izbrala pristop »počakaj in poglej«, kar je postala običajna praksa pri oblikovanju stališč do novih tehnoloških rešitev. Prispevek obravnava obstoječe pravne ukrepe, ocenjuje morebitne koristi in slabosti ter analizira prakse v državah, ki so že uvedle blockchain v zemljiške knjige.

Ključne besede: blockchain, zemljiška knjiga, implementacija tehnologije blockchain, pravni izzivi, primerjalni vidik.

Cobiss: 1.08

1 Uvod

Razvoj tehnologije je močno vplival na pisanje, komunikacijo, poslovanje in upravljanje podatkov ter jim dodal nove dimenzije. Informatizacija in digitalizacija sta še dodatno pospešili globalne spremembe ter omogočili razvoj novih inovativnih rešitev na različnih področjih. Pojavnost in vsakdanjost interneta in omrežja sta prinesli številne nove priložnosti, hkrati pa tudi izzive na področju varnosti, zaupanja in transparentnosti v digitalnem poslovnem okolju. Prav iskanje rešitev za te izzive je spodbudilo razvoj blockchain tehnologije, ki temelji na decentraliziranem in varnem shranjevanju podatkov neodvisno od posrednikov. Čeprav se je blockchain najprej razvil kot platforma za kriptovalute, se je pozneje razširil in postal prelomna inovacija z vplivom na številna druga področja (Nakamoto, 2008).

Blockchain je matematični algoritem, ki zagotavlja visoko varnost transakcij z uporabo kriptografskih metod. Temelji na porazdeljeni zbirki podatkov, ki vsebuje šifrirane podatke, odporne na spreminjanje ali posege vanje. Že iz izraza »blockchain« je razvidno, da je termin sestavljen iz dveh besed: blok in veriga. Gre torej za vrsto blokov, ki vsebujejo ključne informacije in so med seboj povezani v verigo. Pri tem se uporablja kriptografija oz. t. i. razpršilni algoritmi, ki identificirajo posamezne bloke, jih povezujejo ter hkrati preprečujejo spreminjanje vsebine enega bloka, ne da bi se pri tem spremenila vsebina vseh blokov, ki mu sledijo (Cvetković, 2020, str. 127–144). Ravno to je ena izmed njegovih najpomembnejših značilnosti – nespremenljivost podatkov, ki so enkrat vpisani v blok. Posamezno potrjevanje izvaja neomejen krog enakopravnih uporabnikov. Blockchain se uporablja kot porazdeljena baza podatkov, v nasprotju s tradicionalnimi sistemi, ki jih upravlja en sam (centraliziran) subjekt. Pri tem ni posrednikov, saj izmenjava poteka od uporabnika do uporabnika (angl. *peer to peer* ali *P2P*) (Rodrigo, Perera, Senaratne, & Jin, 2018).

Tako ima vsakdo dostop do teh podatkov, vendar jih zaradi decentralizacije ne more spreminjati. Večinoma gre za podatke o izvedenih transakcijah, ki so zabeleženi v kronološkem vrstnem redu. Vsaka transakcija vsebuje informacije o tem, kdo je komu, kdaj in v kolikšnem znesku poslal sredstva. Pomembno je, da pošiljatelj in prejemnik nista identificirana z imenom in priimkom, temveč z naslovom svojih denarnic. Denarnica predstavlja računalniški program, kjer posameznik hrani svoje kriptovalute. Transakcije se beležijo v posameznih blokih, ki se po zapolnitvi zapečatijo in povežejo v verigo blokov, medtem ko se nove transakcije vpisujejo v novoustvarjenem bloku (Nakamoto, 2008).

Prispevek najprej opisuje osnovne lastnosti tehnologije blockchaina, nato pa se osredotoča na njeno morebitno uporabo v povezavi z zemljiško knjigo, pri čemer prikaže tudi spremembe, ki jih prinaša novela ZZK-1C. V nadaljevanju so obravnavane prednosti in slabosti takšne uporabe, na koncu pa še primerjalni vidik, ki razkriva, kako je implementacija blockchain tehnologije urejena v nekaterih drugih državah.

2 Temeljne značilnosti blockchain tehnologije

Za učinkovito regulacijo te tehnologije in pojavov, ki jo obkrožajo, je ključno predvsem razumevanje njenih temeljnih značilnosti. Med osrednje lastnosti blockchain tehnologije sodijo transparentnost, decentralizacija podatkov, nespremenljivost vnesenih podatkov, anonimnost subjekta in avtonomnost sistema (Cvetković, 2020).

Kot smo že poudarili, je ena ključnih značilnosti blockchain tehnologije decentralizacija podatkov. V običajnih centraliziranih sistemih (npr. centralna banka) osrednji organ preverja vsako transakcijo in v celoti nadzoruje podatke. Nasprotno pri blockchainu ni centralnega nadzornega organa – vsi povezani uporabniki v omrežju so enakovredni, pri čemer vsaka oseba deluje kot vozlišče. Ta vozlišča zagotavljajo brezhibno delovanje sistema in shranjujejo celotne kopije verige blokov. Ker informacije niso shranjene na enem mestu oz. so razpršene po omrežju, mora vse spremembe v sistemu odobriti celotno omrežje. Pri centraliziranih sistemih lahko okvara glavnega strežnika povzroči popolno zrušitev sistema. Na ta način se precej izboljša varnost, saj ni niti ene točke okvare, ki bi lahko ogrozila celoten sistem. (Zheng, Xie, Dai, Chen, & Wang, 2017)

Nespremenljivost pomeni, da vsaka transakcija, ki jo potrdi omrežje, ostane trajno zabeležena in je ni mogoče spreminjati ali izbrisati. To se doseže z uporabo kriptografskih povezav med bloki in razpršenim shranjevanjem podatkov (Kosba, Miller, Shi, Wen, & Papamanthou, 2016). Kljub temu obstajajo določena tveganja, kot je npr. »napad 51«, pri katerem posameznik ali skupina prevzame nadzor nad več kot polovico računalnikov (računske moči) omrežja, kar jim omogoča spreminjanje podatkov v verigi.

Transparentnost pomeni, da so vse potrjene transakcije trajno shranjene in povezane v neprekinjeno verigo, kar omogoča sledenje vse do prve transakcije. Ta lastnost zagotavlja popolno sledljivost in vpogled v zgodovino vseh transakcij (Kosba, Miller, Shi, Wen, & Papamanthou, 2016).

Anonimnost uporabnikov se kaže v tem, da transakcije niso neposredno povezane z identitetami oseb, temveč z njihovimi psevdonimi oz. IP-naslovi. Kljub temu ne moremo govoriti o popolni anonimnosti, saj so vse transakcije javno dostopne, zaradi česar je mogoče določene subjekte identificirati. To predstavlja problem pri širši uporabi pametnih pogodb, ker veliko posameznikov in organizacij obravnava finančne transakcije kot zaupne (Kosba, Miller, Shi, Wen, & Papamanthou, 2016). Pri regulaciji blockchaina je treba upoštevati vse omenjene značilnosti. Ker lahko nezadostna regulacija povzroči pravno dvoumnost in zmanjša zaupanje uporabnikov, je treba ustvariti pravni okvir z upoštevanjem edinstvenih značilnosti različnih področij uporabe.

3 Zemljiška knjiga z osrednjim poudarkom na noveli ZZK-1C

Zakon o zemljiški knjigi (ZZK, 1995) je določil, da se zemljiška knjiga lahko vodi z uporabo računalniške tehnologije. Na podlagi tega zakona je bila uvedena elektronsko vodena zemljiška knjiga, vendar ne takoj leta 1995, temveč nekoliko pozneje. Od takrat je slovenska zemljiška knjiga preživela več bistvenih sprememb in je postopoma prehajala iz klasičnih papirnatih registrov v digitalno obliko. (Vrenčur, 2010, str. 66).

Če povzamemo ključne spremembe digitalizacije zemljiške knjige, so te naslednje:

1. ZZK-1:

Zakon o zemljiški knjigi (ZZK-1) je uvedel elektronsko zemljiško knjigo in informatizacijo procesov. Zemljiškoknjižni predlogi so se začeli vpisovati elektronsko z overjenim digitalnim podpisom. Izboljšala se je dostopnost oz. možnost elektronskega dostopa do zemljiškoknjižnih podatkov.

2. ZZK-1A:

Novela je uvedla obvezno vlaganje elektronskih predlogov pri notarjih ter vzpostavila splošne oz. enotne krajevne pristojnosti sodišč. Določila je pravno podlago za prevzemanje podatkov iz matičnih evidenc ter skrajšanje postopka vzpostavitve zemljiškoknjižnih listin. Novela ni bila dovolj premišljena, saj ni bila v celoti izvedljiva brez dodatne informatizacije sistema (Vrenčur, 2010, str. 66).

3. ZZK-1B:

Zadevna novela odlaga rok za uveljavitev prejšnje novele.

4. ZZK-1C:

Z novelo ZZK-1C, ki je začela veljati 5. aprila 2011, je slovenski zemljiškoknjižni sistem doživel popolno digitalizacijo, saj je novela odpravila papirne postopke. Vsi predlogi so se začeli vlagati izključno v elektronski obliki. Postopek preverjanja podatkov je postal hitrejši in bolj avtomatiziran, pravna varnost pa je bila okrepljena z dodatnimi zaščitnimi določbami pri overjanju listin in digitalni identiteti strank. Novosti so tudi vključevanje ukinitvev zemljiškoknjižnih vložkov, uvedb novih materialnopravnih pojmov v zemljiškoknjižnem sistemu ter obvezno elektronsko vlaganje zemljiškoknjižnih predlogov prek kvalificiranih vlagateljev (notarji, odvetniki, državno pravobranilstvo, občinska pravobranilstva). Da bi se razbremenila sodišča, je bila uvedena splošna krajevno pristojnost, kar pomeni, da zemljiškoknjižni predlogi niso več vezani na lego nepremičnine. Informacijski sistem e-ZK avtomatsko dodeljuje zadeve glede na zasedenost sodišč. Uporabniki lahko brezplačno dostopajo do zemljiške knjige preko sistema e-ZK, ki ponuja tudi možnost računalniškega izpisa oblikovane glavne knjige. Prav tako so na voljo brezplačni izpisi zemljiškoknjižnih rednih in zgodovinskih podatkov, vključno s podatki o izvedenih pravicah, pravnih dejstvih in morebitnih vpisanih plombah. Poleg tega izpisi vsebujejo katastrske podatke o nepremičninah, kar je povečalo preglednost nepremičninskih evidenc (Vrenčur, 2010, str. 66–68).

Torej, če pogledamo zgodovinski razvoj slovenske zemljiške knjige, lahko ugotovimo, da se je od leta 1995 do danes postopoma digitalizirala, se prilagodila sodobnim pravnim in tehnološkim zahtevam ter bistveno izboljšala dostopnost in pravno varnost podatkov.

4 Prednosti in slabosti blockchaina v zvezi z zemljiško knjigo in nepremičnine

V nadaljevanju sledi analiza SWOT za uporabo blockchaina, ki je prikazana v tabeli 1.

Tabela 1: Analiza SWOT uporabe blockchain tehnologije.

Prednosti	Slabosti
– Decentralizacija – Preglednost – Varnost in zaščita podatkov – Nespremenljivost podatkov – Hitrejše in cenejše transakcije	– Pomanjkanje predpisov in pravne regulacije – 51-odstotni napad – Tehnična zahtevnost – Nova tehnologija
Priložnosti	Nevarnosti
– Preprečevanje goljufij – Hitrejši mednarodni prenosi – Odpornost na kibernetne napade (razen 51-odstotni napad) – Povečana zaupnost – Oblikovanje digitalne identitete lastnikov (večja varnost in nadzor nad osebnimi podatki)	– Sprememba zakonodaje in zakonska usklajenost – Velike naložbe v implementacijo – Dovzetnost za določene tehnološke zlorabe (51-odstotni napad) in človeške napake (napačen vnos podatkov)

Vir: Lastni.

Tradicionalni nepremičninski sektor je pogosto časovno zamuden, saj večina postopkov v fazi nakupov in prodaj zahteva pravne formalnosti, kot so overjanje dokumentov in podpisovanja pogodbenih listin. Z uporabo blockchaina bi se lahko večina teh postopkov poenostavila in avtomatizirala.

Pametne pogodbe omogočajo avtomatizacijo prodaje in nakupa nepremičnin, kar odpravlja potrebo po posrednikih ter zmanjšuje stroške in obseg birokratskih ovir. Poleg tega bi lahko dokumente overjali digitalno in jih shranjevali na verigi blokov, kjer bi bili transparentno in varno shranjeni (Mohanta, Panda, & Jena, 2018). Blockchain ponuja številne rešitve na nepremičninskem področju, velika večina pa je zaenkrat zgolj teoretično zasnovana.

Konceptualne zasnove omenjajo predvsem štiri glavne kategorije, in sicer: zemljiško administracijo, nepremičninske transakcije, tokenizacijo in upravljanje nepremičnin (Saari, Jussi, & Seppo, 2022). Kot navaja odvetnik Jadek, prenos lastninske pravice na nepremičninah z zavarovanjem zahteva več (zapletenih in časovno zamudnih) korakov: odobritev kredita s strani banke, sklenitev kupoprodajne pogodbe, plačilo davka na promet nepremičnin, pridobitev potrdila o plačilu, notarska overitev, vložitev zemljiškoknjižnega predloga, odločitev sodišča, pravnomočnost, vpis pravice v zemljiško knjigo, vpis hipoteke in sprostitev kredita. Celoten

postopek lahko traja več kot mesec dni. Če pa bi bila zemljiška knjiga vodena na blockchainu, bi bil prenos lastninske pravice bistveno enostavnejši in učinkovitejši. Vse funkcije, ki jih opravljajo FURS, notar, sodišče, banka in sedanji sistem digitalne zemljiške knjige, bi lahko blockchain združil v en sam korak. Računalniška koda bi izvedla prenos lastninske pravice, sprostitev kredita, plačilo nakupne cene in davka ter vpis hipoteke v isti juridični sekundi, potem ko bi se kupec, prodajalec in banka dogovorili o vseh komponentah pametne pogodbe. Takšen sistem bi pospešil razpolaganje z nepremičninami, zaustavil zlorabe in odpravil potrebo po plombah na nepremičninah, saj bi se vse takoj vknjižilo (Jadek, 2017). Za izvedbo takšnega postopka bi morale stranke kupoprodajne, kreditne in zavarovalne pogodbe integrirati izvršitev teh procesov v blockchain tehnologijo. Šele s tem bi se omogočilo popolno integracijo pametnih pogodb v promet z nepremičninami.

Zelo pomemben mejnik za Slovenijo na področju nepremičninske tehnologije je bilo leto 2018, ko je slovensko podjetje Blocksquare kot prvo na svetu uspešno tokeniziralo nepremičnine na blockchainu (Tomšič & Prevc, 2023). Tokenizacijo definiramo kot razdelitev premoženja na digitalne žetone, pri čemer vsak žeton predstavlja delež vrednosti nepremičnine oz. postopek, kjer se pravice do fizičnega premoženja digitalizirajo v obliki žetonov (Joshi & Choudhury, 2024). S tem so se v Sloveniji ustvarili zametki digitalizacije prometa z nepremičninami, vendar bodo tovrstni poskusi digitalizacije imeli omejen uspeh, dokler tehnologija blockchain ne bo v celoti implementirana v zemljiško knjigo.

5 Primerjalni vidik

V tem poglavju sta predstavljeni dve evropski državi, ki sta začeli implementirati blockchain v svoje zemljiškoknjižne sisteme – Estonija in Švedska. Prikazani so raven digitalizacije, način delovanja ter izzivi in različni pristopi k uporabi te tehnologije.

5.1 Estonija

Estonija je znana kot ena najnaprednejših in najbolj digitaliziranih držav na svetu z liberalno zakonodajo, ki spodbuja tehnološke raziskave. Tamkajšnja zemljiška knjiga je popolnoma digitalizirani informacijski sistem. Deluje na način, da sodni registratorji (sodniški pomočniki) izdajo digitalne odločbe, potem ko so vse vloge za registracijo oddane prek spleta. Za zagotavljanje varnosti podatkov se pri registraciji uporablja blockchain. Poleg tega so sodni pomočniki odgovorni tudi za vodenje poslovnega registra, ki je register podjetij in drugih pravnih

oseb. Zemljiška knjiga in poslovni register sta medsebojno povezana preko posebne pravne osebe – stanovanjske skupnosti. Sistem samodejno oblikuje novo stanovanjsko skupnost v poslovnem registru takoj, ko je stanovanjska stavba razdeljena na ločena lastniška stanovanja in vpisana v zemljiško knjigo. V praksi to pomeni, da gre za posebno IT-agencijo, ki je pod okriljem ministrstva za pravosodje in skrbi za upravljanje, razvoj programske opreme ter zagotavljanje spletnih informacijskih storitev za zemljiško knjigo. Podatki iz zemljiške knjige so javno dostopni in so tudi na voljo v strojno in človeško berljivih formatih. Čeprav registratorji delujejo v estonščini, je celoten informacijski sistem dvojezičen in dostopen tudi v angleščini (Peep, 2024).

Dostop do podatkov iz zemljiške knjige je plačljiv, vendar strošek ni pretirano velik, pri čemer so javne ustanove oproščene plačila, kadar gre za obvezne poizvedbe. Vsak posameznik pa ima možnost brezplačnega vpogleda v lastne podatke. Dostop do podatkov je možen le, če ima uporabnik preverjeno e-identiteto. Obstaja tudi posebna platforma Data Tracker, ki omogoča vpogled v podatke o tem, kdo, kdaj in zakaj je dostopal do osebnih podatkov v javnih registrih (vključno z zemljiško knjigo). Vsi vpisi v zemljiško knjigo so javno dostopni, izvorni dokumenti pa so zaščiteni. To pomeni, da so vsi zemljiškoknjižni vpisi in zaznambe prosto dostopne, medtem ko podatki o pogodbah (npr. pogodba o prodaji nepremičnin, pogodba o hipotekarnem kreditu) niso javni. Če želi oseba pridobiti vpogled v takšne dokumente, mora izkazati upravičen interes, ki ga preveri notar. Zahteve za dostop do podatkov obravnavajo IT-agencije (spletno) ali notarji (spletno oz. osebno) (Peep, 2024).

5.2 Švedska

Švedska je že leta 2016 začela raziskovati možnost uporabe blockchain tehnologije v zemljiški knjigi. Začela je s preučevanjem možnosti uporabe te tehnologije za nepremičninske transakcije in predstavila tehnično demonstracijo, ki prikazuje njene potencialne koristi za družbo. Projekt je bil razdeljen na tri faze. V prvi fazi so na Švedsekm razvili temeljito teoretično razumevanje o tehnologiji blockchain, njenem delovanju in njeni relevantnosti za zemljiško knjigo. Druga faza pa je bila osredotočena na razvoj tehnologije, ki bi najbolje ustrezala potrebam in zahtevam lastnikov nepremičnin in vlade. Obe fazi sta bili uspešno zaključeni. V zadnji fazi je bilo predvideno testiranje sistema z namenom zagotoviti njegovo učinkovito delovanje (Zeilhofer & Eror, 2019).

Pri uvajanju blockchain tehnologije v zemljiške knjige države po navadi sledijo dvema različnima pristopoma implementacije: 1) popolni prenovi obstoječega sistema ali ustvarjanju novega

sistema ali 2) ohranitvi obstoječega sistema z izboljšanjem (Proskurovska & Dörry, 2022). Švedska se je odločila za drugi pristop, pri čemer je navkljub uspešnemu konceptu projekt obstal, kar je preprečilo učinkovito integracijo blockchain tehnologije v tamkajšnjo zemljiško knjigo. Švedska torej predstavlja eno izmed držav, kjer so poskusili z digitalizacijo zemljiške knjige z blockchain tehnologijo, vendar se za to spremembo – vsaj za zdaj – niso odločili.

6 Sklep

Prispevek je okvirno predstavil blockchain in njegov možni vpliv na slovensko zemljiško knjigo, pri čemer je izpostavil tako pozitivne kot tudi negativne vidike njene uporabe. Čeprav v slovenskem pravnem redu ni zaznati premikov pri implementaciji blockchaina v zemljiško knjigo, pa so v zasebnem sektorju vidni drugi premiki in prizadevanja za digitalizacijo prometa z nepremičninami, kar kaže, da bi lahko Slovenija v prihodnosti znova stopila na pot digitalne preobrazbe.

Pri tem je ključno razumevanje, da bo implementacija blockchain tehnologije takšna, kot jo bomo sami oblikovali. Njene temeljne lastnosti, kot so nespremenljivost, transparentnost in decentralizacija, predstavljajo tako prednosti kot izzive. Po eni strani lahko izboljšajo pravno varnost, zmanjšajo goljufije in omogočijo večjo dostopnost podatkov, po drugi strani pa odpirajo vprašanja glede varstva zasebnosti, regulativnih zahtev in pravnih omejitev.

Tako bo treba temeljito premisliti, ali bi bila zamenjava tehnologije zemljiške knjige sploh smiselna. Glavna prednost blockchain tehnologije v primerjavi s trenutnim sistemom je pohitritev in poenostavitev postopkov s pametnimi pogodbami, vendar je treba upoštevati, da bo ta tehnologija ekonomično učinkovitejša le, če bo v medsebojni povezavi z drugimi deležniki, kot so banke in zavarovalnice. Brez te povezave je njen potencial precej omejen.

Druga prednost blockchain tehnologije se kaže v decentraliziranosti sistema, ki preprečuje posege, značilne za centralizirane sisteme. Trenutno ni poročil o kibernetičnih napadih ali zlorabah elektronske zemljiške knjige, zato ni močnega vzgiba za sistemsko spremembo zemljiške knjige. To sicer velja danes, prihodnjih potreb trga pa ni mogoče z gotovostjo napovedati. Nedvoumno pa blockchain predstavlja tehnologijo, ki lahko pospeši in poenostavi postopke na varen in zanesljiv način. Kljub tem izzivom je slovensko podjetje Blocksquare pokazalo, da lahko blockchain ponudi inovativne rešitve za nepremičninski sektor, kar potrjuje njen obetaven potencial za nadaljnji razvoj. Ključno vlogo pri tem bodo imeli tudi zakonodajalec in drugi regulatorji, na katerih bo

odgovornost za vzpostavitev ustreznih pravnih okvirov za učinkovito in varno implementacijo blockchain tehnologije v zemljiško knjigo.

Literatura in viri

1. Cvetković, P. (2020). Blockchain kao pravni fenomen: uvodna razmatranja. *Zbornik radova Pravnog fakulteta u Nišu*, 59(87), 127–144. <https://doi.org/10.5937/zrpfno-24414>
2. Jadek, A. (2017). *Povzetek mojega prispevka na okrogli mizi – Priložnosti in izzivi, ki jih »Blockchain« tehnologije prinašajo v Sloveniji*. LinkedIn. https://www.linkedin.com/pulse/povzetek-mojega-prispevka-na-okrogli-mizi-izzivi-ki-alja%C5%BE-jadek?fbclid=IwY2xjawl9ci5leHRuA2FlbQlxMAABHY6OaIQ7f1_S5yobZ06HdhqlqERXqvQzh-mqc4Jlo-OdjCw1392WK1kCuw_aem_5zsOphowxb5U6Vvb6W6S9A
3. Joshi, S., & Choudhury, A. (2024). Tokenization of real estate assets using blockchain. *International Journal of Intelligent Information Technologies*, 18(3), 171–384. <https://doi.org/10.4018/IJIT.309588>
4. Kosba, A., Miller, A., Shi, E., Wen, Z., & Papamanthou, C. (2016). Hawk: The blockchain model of cryptography and privacy-preserving smart contracts. *IEEE Symposium on Security and Privacy: proceedings*, 839–858. <https://doi.org/10.1109/SP.2016.55>
5. Mohanta, K. B., Panda, S. S., & Jena, D. (2018). An overview of smart contract and use cases in blockchain technology. *9th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*, 1–4. <https://doi.org/10.1109/ICCCNT.2018.8494045>
6. Nakamoto, S. (2008). *Bitcoin: A peer-to-peer electronic cash system*. Bitcoin. <https://bitcoin.org/bitcoin.pdf>
7. Peep, V. (2024). *Land administration in estonia: A synthesis of old institutions and modern technology*. <https://www.bk-agarwal.com/post/land-administration-in-estonia-a-synthesis-of-old-institutions-and-modern-technology>
8. Proskurovska, A., & Dörry, S. (2022). The blockchain challenge for Sweden's housing and mortgage markets. *Environment and Planning A*, 54(8), 1569–1585. <https://doi.org/10.1177/0308518X221116896>
9. Rodrigo, M., Perera, S., Senaratne, S., & Jin, X. (2018). *Blockchain for construction supply chains: A literature synthesis*. ResearchGate. https://www.researchgate.net/publication/329607336_BLOCKCHAIN_FOR_CONSTRUCTION_SUPPLY_CHAINS_A_LITERATURE_SYNTHESIS
10. Saari, A., Jussi, V., & Seppo, J. (2022). Blockchain in real estate: Recent developments and empirical applications. *Land Use Policy*, 121. <https://doi.org/10.1016/j.landusepol.2022.106334>
11. Tomšič, M., & Prevc, M. (2023). Prvi na svetu: prelomen nepremičninski projekt slovenskega podjetja. Siol. <https://siol.net/novice/digisvet/prvi-na-svetu-prelomen-nepremicninski-projekt-slovenskega-podjetja-616678>
12. Vrenčur, R. (2010). *Uvedba polne informatizacije v zemljiškoknjižnem poslovanju po noveli ZZZK-1C*. Zbornik referatov, 66–76.
13. Zakon o spremembah in dopolnitvah Zakona o zemljiški knjigi (ZZK-1A). *Uradni list RS*, št. 45/08.
14. Zakon o spremembah in dopolnitvah Zakona o zemljiški knjigi (ZZK-1C). *Uradni list RS*, št. 25/11.
15. Zakon o spremembah Zakona o zemljiški knjigi (ZZK-1B). *Uradni list RS*, št. 28/09.
16. Zakon o zemljiški knjigi (ZZK). *Uradni list RS*, št. 33/95, 50/02 – odl. US in 58/03 – ZZK-1.

17. Zakon o zemljiški knjigi (ZZK-1). *Uradni list RS*, št. 58/03, 37/08 – ZST-1, 45/08, 28/09, 25/11, 14/15 – ZUUJFO, 69/17, 11/18 – ZIZ-L, 16/19 – ZNP-1 in 121/21.
18. Zeilhofer, N., & Eror, A. (2019). Blockchain tehnologija – primerjalni pregled. https://fotogalerija.dz-rs.si/datoteke/Publikacije/Zborniki_RN/2019/Blockchain_tehnologija.pdf
19. Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017). An overview of blockchain technology: Architecture, consensus, and future trends. *IEEE International Congress on Big Data*, 557–564. <https://doi.org/10.1109/BigDataCongress.2017.85>

PRAVNI VIDIKI ZAŠČITE ZDRAVSTVENIH SISTEMOV IN PODATKOV: SLOVENSKI IN EVROPSKI PRISTOP

Žiga Rodošek, Univerza v Mariboru, Pravna fakulteta, Slovenija ✉ 

Red. prof. dr. Andreja Primec, Univerza v Mariboru, Ekonomsko-poslovna fakulteta, Slovenija 

Povzetek: V dobi hitre digitalizacije in naraščajoče uporabe umetne inteligence v zdravstvenem sektorju postajata varnost občutljivih podatkov in zanesljivost informacijskih sistemov ključnega pomena. Osrednja tema prispevka je pravni okvir kibernetске varnosti zdravstvenega sistema Republike Slovenije s poudarkom na posameznih aktih EU in RS: direktivi NIS-2, ZVOP-2 ter Uredbi GDPR, ZInfV, Aktu o kibernetски varnosti in Aktu o kibernetски odpornosti. Poleg poznavanja konceptov kibernetске varnosti in umetne inteligence vse večjo pozornost zbuja etične dileme kot posledica hitrega razvoja digitalizacije v zdravstvu. Z vse večjo stopnjo integracije digitalnih sistemov v vsakdanje življenje je treba ugotoviti prednosti in ranljivosti trenutnega pravnega okvira, opozoriti na posledice morebitnega vdora ter ponuditi priporočila za nadaljnje izboljšave zakonodaje. Kot ključno je mogoče izpostaviti, da lahko le celovit in dinamičen pravni okvir zadostno zaščiti podatke in zagotovi varnost v hitro spreminjajočem se digitalnem okolju.

Ključne besede: Kibernetска varnost, zdravstvo, pravni okvir (EU in RS), umetna inteligenca, etični izzivi

Cobiss: 1.08

1 Uvod

V zadnjih letih digitalizacija in uvajanje naprednih tehnologij spreminjata skoraj vse vidike sodobne družbe. Zdravstveni sistem, ki je eden izmed ključnih na področju javnih služb, ni izjema. Digitalizacija zdravstvenih procesov, vpeljava elektronskih kartotek, uporaba telemedicine in vse večja integracija umetne inteligence (UI) predstavljajo korak naprej k učinkovitejši in bolj prilagodljivi oskrbi pacientov, vendar ta tehnološki napredek prinaša tudi številne varnostne izzive. Kibernetški napadi, kraje podatkov, manipulacije in druge grožnje postavljajo pod vprašaj zanesljivost celotnega sistema, kar lahko ogrozi tako posamezne paciente kot širšo družbo (Uršič, 2022).

V tem prispevku bo podrobneje obravnavan pravni okvir kibernetске varnosti zdravstvenega sistema v Republiki Sloveniji. Posebno pozornost je namenjena šestim ključnim pravnim aktom: Direktivi o ukrepih za visoko skupno raven kibernetске varnosti (NIS-2), Zakonu o varstvu osebnih podatkov (ZVOP-2) ter Splošni uredbi o varstvu podatkov (GDPR), Zakonu o informacijski varnosti (ZInfV), Aktu EU o kibernetški varnosti in Aktu EU o kibernetški odpornosti. Prispevek obravnava pregledno analizo pravnih aktov, ki urejajo zdravstveni sistem, in se osredotoča na primerjavo slovenskega zdravstvenega sistema z mednarodnimi praksami. Poleg tega se v obravnavo vključujejo etični in varnostni vidiki, ki so ključni za zagotavljanje zanesljive in učinkovite zdravstvene oskrbe. Namen raziskave je dokazati nujnost vzpostavitve trdnega in prilagodljivega pravnega okvira ter opozoriti na morebitne posledice varnostnih napadov, ki ogrožajo stabilnost in varnost zdravstvenega sistema.

Kakšne posledice lahko povzroči kibernetški napad v zdravstvenem sistemu posamezne države, ilustrativno prikazujemo v naslednjem primeru, ki se je zgodil maja 2021.

14. maja 2021 je irska nacionalna zdravstvena služba Health Service Executive (HSE) doživela obsežen izsiljevalski napad z zlonamerno programsko opremo Conti, ki je prisilil izklop vseh informacijskih sistemov po državi in onemogočil dostop do elektronskih zdravstvenih kartonov, s čimer so bile blokirane ključne diagnostične storitve, vključno z radioterapijo, CT (računalniško tomografijo), kardiološkimi pregledi in testiranjem na covid-19 (Corera, 2021). Napadalci, pripisani mednarodni kriminalni skupini Wizard Spider (Conti), so v omrežje vdrli več tednov pred sprožitvijo napada, kar bi brez pravočasnega zaznavanja lahko vodilo do obsežne odtujitve občutljivih medicinskih in osebnih podatkov pacientov ter celo neposrednega ogrožanja njihovega zdravja. Kljub hitremu sodelovanju z Nacionalnim centrom za kibernetško varnost in mednarodnimi partnerji je ocenjena finančna škoda presegla desetine milijonov evrov, operativna

motnja pa je povzročila masovno odpovedovanje neurgentnih ambulantnih posegov in zamude pri cepljenju proti covidu-19, kar je dodatno izpostavilo tveganje za življenja ranljivih skupin bolnikov (Corera, 2021). Incident velja za najresnejši kibernetški napad na irsko državno agencijo doslej in največji znani napad na zdravstveni sistem, saj so napadalci pridobili dostop do osebnih in kliničnih podatkov več sto pacientov, ki so bili pozneje objavljeni na temni spletni strani, kar je ogrozilo zasebnost in varnost prizadetih.

Za preprečevanje podobnih vdorov v digitalne sisteme je nujen pregled razvoja digitalizacije zdravstvenega sistema v Sloveniji, ki vključuje analizo implementacije sodobnih tehnologij in primerjavo s praksami v izbranih tujih državah. To omogoča identifikacijo prednosti, slabosti in morebitnih priložnosti za izboljšave, kar je ključno za oblikovanje strategij za prihodnost (Dokl, 2012).

Za zagotavljanje ustrezne stopnje varnosti informacijskih sistemov je potrebna tudi ustrezna zakonodaja.

Prispevek tako obravnava obstoječi slovenski pravni okvir. Poseben poudarek je namenjen preučevanju potenciala, ki ga ta zakonodaja ponuja, ter odkrivanju njenih pomanjkljivosti in ranljivosti. Analizirane so možnosti za izboljšanje pravnega okvira in predstavljene smernice za prihodnje zakonodajne spremembe, katerih cilj je krepiti varnost in učinkovitost zdravstvenega sistema ter zagotoviti ustrezno zaščito pred kibernetškimi grožnjami. Prispevek s tem prispeva k boljšemu razumevanju in krepitvi pravnega in varnostnega okvira, kar je bistveno za trajnosten razvoj in delovanje zdravstvenega sistema v digitalni dobi.

2 Metode

Pri nastajanju prispevka so bile uporabljene uveljavljene metode za pravno raziskovanje, ki jih ponuja pravna epistemologija (Novak, 2010). V največji meri je bila uporabljena avtonomnopravna oz. normativno-dogmatična metoda za preučitev trenutne pravne ureditve kibernetške varnosti v zdravstvenem sistemu v Republiki Sloveniji. Primerjalnopravna metoda je bila uporabljena za pojasnitev pravne ureditve in različnih praks pri ravnanju v digitalnem svetu med različnimi državami, s poudarkom na državah Evropske unije.

3 Osnovni pojmi kibernetike varnosti in umetne inteligence

3.1 Opredelitev kibernetike varnosti

Kibernetika varnost se nanaša na zaščito informacijskih sistemov, omrežij in podatkov pred nepooblaščenim dostopom, krajo, uničenjem ali zlorabo (Dokl, 2012). V kontekstu zdravstvenega sistema, kjer se obdelujejo zelo občutljivi in osebni podatki pacientov, je pomen kibernetike varnosti še posebej velik. Zaradi velike količine zaupnih informacij, kot so zdravstveni zapisi, rezultati preiskav in drugi osebni podatki, predstavlja vsaka varnostna luknja resno grožnjo tako pacientom kot tudi institucijam, ki te podatke obdelujejo (Fernández-Alemán idr., 2013).

Napadi, kot so izsiljevalska programska oprema (angl. *ransomware*), lažno predstavljane (angl. *phishing*), napadi DDoS (napad s porazdeljeno ohromitvijo storitve, angl. *Distributed Denial of Service*) in druge vrste vdora, lahko povzročijo hude motnje v delovanju zdravstvenih ustanov. Takšni napadi pogosto vodijo do začasne nedosegljivosti ključnih informacijskih sistemov, kar lahko privede do resnih zamud pri nudenju nujne zdravstvene oskrbe. Poleg tega lahko kršitve varnosti ogrozijo zasebnost pacientov in povzročijo finančne ter znatne izgube, kar ima dolgoročne posledice za delovanje in zaupanje v zdravstveni sistem (Perakslis, 2014).

Za učinkovito zaščito zdravstvenih sistemov je treba implementirati večplastne varnostne ukrepe. Ti vključujejo tehnične rešitve, kot so šifriranje podatkov, požarni zidovi, sistemi za zaznavanje vdora ter redne in hitre varnostne posodobitve programske opreme. Poleg tehničnih ukrepov je pomembno tudi izvajanje organizacijskih in pravnih ukrepov, ki zagotavljajo, da se varnostni protokoli dosledno izvajajo in nadzorujejo. Usposabljanje osebja ter razvoj kriznih načrtov za primer kibernetike vdora sta nadaljnja ključna elementa, ki pomagata zmanjšati tveganja in zagotoviti učinkovito odzivanje na morebitne vdore ali podobne incidente. S celovitim pristopom, ki združuje tehnološke, organizacijske in pravne rešitve, se lahko zagotovi visoka raven varnosti v zdravstvenem sistemu in s tem zaščiti podatke pacientov (Uršič, 2022).

3.2 Umetna inteligenca v zdravstvu

Umetna inteligenca (UI) zajema tehnologije, ki računalnikom in sistemom omogočajo izvajanje nalog, ki zahtevajo človeško inteligenco, kot so učenje, prepoznavanje vzorcev, analiza podatkov in odločanje (Gordon idr., 2019). V zadnjih letih se razvoj UI močno povečuje, kar odpira nove možnosti na različnih področjih, med katerimi je zdravstvo eno najbolj perspektivnih. V zdravstvu se UI uporablja za diagnosticiranje bolezni, analizo medicinskih slik, optimizacijo administrativnih procesov ter personalizacijo zdravljenja. Algoritmi za prepoznavanje vzorcev lahko npr.

pripomorejo k hitrejšemu odkrivanju anomalij na slikah, kar vodi k zgodnejši diagnostiki in učinkovitejšemu zdravljenju. Poleg tega se UI uporablja pri analizi ogromnih količin podatkov, ki jih generirajo sodobne medicinske naprave, kar zdravnikom omogoča, da na podlagi natančne analize sprejemajo bolj informirane odločitve pri izbiri terapij in prilagajanju zdravljenja posameznim pacientom (Gričnik idr., 2024).

V praksi to pomeni, da lahko sistemi z umetno inteligenco analizirajo medicinske slike, kot so rentgenski posnetki, magnetnoresonančne slike (MRI) in računalniška tomografija (CT), z visoko stopnjo natančnosti. Tako lahko algoritmi prepoznajo vzorce, ki bi jih človeško oko lahko spregledalo, kar pripomore k zgodnjemu odkrivanju bolezni, kot so rak, nevrodegenerativne bolezni in druge resne zdravstvene težave. Poleg diagnostike se UI uspešno uporablja tudi pri spremljanju poteka zdravljenja, kjer sistemi analizirajo odziv telesa na določene terapije in s tem pomagajo pri prilagajanju zdravljenja, kar prinaša prednosti personalizirane medicine (Gričnik idr., 2024).

Vendar pa uporaba UI prinaša tudi številne varnostne in etične izzive. Eden izmed glavnih izzivov je možnost, da sistem, ki temelji na UI, vsebuje napake ali pristranskosti, ki lahko vodijo do napačnih diagnoz in posledično neustreznega zdravljenja. Napačne diagnoze lahko vodijo do nepotrebnega zdravljenja ali zamujenih priložnosti za pravočasno intervencijo, kar ima lahko resne posledice za paciente. Poleg tega obstaja nevarnost, da bi ljudje manipulirali z algoritmi, s čimer bi ogrozili integriteto celotnega sistema. Zaradi tega je nujno, da se razvoj in uporaba umetne inteligence spremljata z ustreznimi varnostnimi protokoli in etičnimi smernicami, ki so zapisane v pravnem okviru (Gordon idr., 2019).

Pomembno je, da se etični vidiki integracije UI v zdravstveni sektor obravnavajo kot prihodnji temeljni dejavnik pri sprejemanju teh tehnologij. Transparentnost algoritmov, odgovornost razvijalcev in zagotavljanje pravice pacientov do varstva osebnih podatkov so temeljne vrednote, ki jih je treba uveljaviti. Razvoj UI mora biti usklajen z vrednotami, kot so pravičnost, varnost in spoštovanje človekovih pravic, kar zahteva sodelovanje med tehnološkimi podjetji, zdravstvenimi institucijami in zakonodajalci (Evropska Komisija, 2025c).

4 Pomen pravnega okvira za kibernetско varnost in etični vidiki

4.1 Zakaj je pravni okvir pomemben?

Vzpostavitev trdnega pravnega okvira predstavlja ključen temelj za zagotavljanje varnosti informacijskih sistemov, zlasti v javnem sektorju (kot je zdravstvo), kjer se obdelujejo občutljivi

podatki. Pravni akti določajo minimalne varnostne standarde, ki jih morajo izpolnjevati institucije, s čimer zagotavljajo ustrezno zaščito pacientovih osebnih in zdravstvenih podatkov. Takšna zakonodaja opredeljuje odgovornosti vseh vpletenih deležnikov – od zdravstvenih ustanov do ponudnikov programske opreme – in natančno določa postopke, ki jih je treba upoštevati v primeru varnostnih incidentov. Na ta način se preprečuje zloraba podatkov, kar je še posebej pomembno v času, ko digitalizacija zdravstvenih storitev hitro napreduje (Uršič, 2022).

Pravni okvir ne deluje zgolj kot preventivni mehanizem, ampak tudi kot orodje, ki mora biti učinkovito za odzivanje, ko pride do varnostnega problema. V primeru vdora v zdravstveni sistem so predpisani ukrepi in postopki, ki morajo biti izvedeni, da se zmanjšajo posledice morebitnega napada ali pa da se vdori kaznujejo, če napada ni več mogoče preprečiti (Zhang, 2024). Takšna zakonodaja prispeva k hitremu odzivu, saj jasno določa, kdo je odgovoren za izvedbo varnostnih ukrepov ter kako naj se incidenti prijavljajo in obravnavajo. S tem se ne varuje le integritete in varnosti podatkov, ampak se tudi vzpostavlja sistem, ki spodbuja naložbe v varnostne tehnologije in izobraževanje strokovnjakov s področja kibernetske varnosti. Sodobni pravni akti pogosto vključujejo tudi direktive o rednih pregledih in posodobitvah varnostnih standardov, kar zagotavlja, da so varnostni ukrepi prilagojeni hitro spreminjajočim se tehnološkim izzivom (ZInfV, NIS 2).

Vključitev pravnih določb v digitalno infrastrukturo zdravstvenih sistemov ima pozitivne učinke, saj spodbuja izboljševanje varnostnih sistemov in razvijanje novih rešitev, ki nastajajo hkrati z razvojem tehnologije. To ne pomeni zgolj formalnosti, temveč dejansko prispeva k večji odpornosti celotnega sistema pred morebitnimi napadi, hkrati pa daje zaupanje med vsemi deležniki. Jasno opredeljene obveznosti in postopki v primeru kršitev varnosti npr. povečujejo pripravljenost zdravstvenih ustanov na nepredvidene situacije in zmanjšujejo negativne posledice, kot so finančne izgube ali škoda ugledu (Gordon idr., 2019).

4.2 Etični vidiki digitalizacije in uporabe UI

Etični vidiki so neločljivo povezani s kibernetsko varnostjo in uporabo UI. V sodobnem času, ko se podatki zbirajo, obdelujejo in analizirajo v večjih količinah, postajajo etična vprašanja vse bolj pomembna. Temeljna etična vprašanja vključujejo varstvo zasebnosti, transparentnost delovanja algoritmov, preprečevanje diskriminacije ter zagotavljanje odgovornosti v primeru napak. Pri uporabi UI v zdravstvenem sektorju lahko nepravilna uporaba privede do napačnih diagnoz, nepravičnih odločitev ali celo do škodovanja pacientom, kar vzbuja pomembne etične dileme (Gričnik idr., 2024). Na eni strani je tehnologija lahko orodje za izboljšanje zdravstvenih storitev, na drugi pa lahko, če se ne uporablja pravilno, povzroči resne posledice.

Etični standardi zahtevajo, da so vsi postopki pri obdelavi podatkov jasni, pregledni in odgovorni. To pomeni, da morajo organizacije zagotoviti pacientom vpogled v to, kako in zakaj se njihovi podatki obdelujejo, ter omogočiti, da lahko izrazijo nestrinjanja s posegom v njihove osebne podatke. V ta namen se vzpostavljajo mehanizmi za pritožbe in nadzor nad delovanjem teh sistemov, kar omogoča pravočasno odkrivanje in odpravljanje napak.

4.3 Vpliv pravnega okvira na zaupanje javnosti

Zaupanje javnosti je pomemben dejavnik uspešne implementacije digitalnih sistemov, zlasti v javnih sektorjih, kjer gre za shranjevanje podatkov velikega števila oseb. Ko pacienti vedo, da so njihovi osebni in zdravstveni podatki zaščiteni z jasnimi in strogimi pravili, se povečuje njihova pripravljenost na sodelovanje v digitalnih procesih (Gričnik idr., 2024). Zanesljiv pravni okvir zagotavlja občutek varnosti in zaupanja, kar je nujno za uspešno sprejemanje in uporabo novih tehnologij v zdravstvenem sektorju.

V primeru, da primanjkuje ustrezne zakonodaje in varnostnih protokolov, lahko pride do širšega občutka negotovosti in nezaupanja. To pa lahko privede do zmanjšane uporabe digitalnih zdravstvenih storitev, saj se posamezniki bojijo zlorab in neustrezne obdelave svojih podatkov (Gordon idr., 2019). Pravnega okvira se zato ne sme le implementirati, temveč ga je treba tudi redno posodablјati in prilagajati novim tehnološkim izzivom. Ko so postopki jasno določeni in hitro izvedeni, se potrjuje zavezanost državnih institucij k zaščiti občutljivih podatkov.

Poleg zaščite podatkov ima pravni okvir pomembno vlogo tudi pri spodbujanju inovacij in naložb v nove tehnologije. Organizacije, ki so prepričane o varnosti in stabilnosti sistema, so bolj pripravljene vlagati v napredne tehnologije, kar vodi v stalno izboljševanje storitev (Zhang, 2024). Prav tako se s tem povečuje tudi medsebojno zaupanje med različnimi deležniki v sistemu, saj vsi delujejo v okviru jasnih in preglednih pravil, kar zmanjšuje možnost sporov in nesporazumov.

Vzpostavitev in vzdrževanje pravnega okvira je ključnega pomena za uspešno digitalizacijo in uporabo naprednih tehnologij, kot je umetna inteligenca, v zdravstvenem sektorju. Le s takšnim pristopom je mogoče zagotoviti varnost, etično uporabo in vzajemno zaupanje med pacienti, zdravstvenimi delavci in državnimi organi. Integracija pravnih, tehničnih in etičnih vidikov ustvarja celovit sistem, ki se lahko uspešno odzove na izzive sodobne digitalne dobe, obenem pa prispeva k izboljšanju kakovosti zdravstvene oskrbe in varovanju temeljnih človekovih pravic.

5 Primerjava slovenskega zdravstvenega sistema z mednarodnimi praksami

Evropska unija je z Direktivo NIS 2 zastavila nov, enoten okvir za kibernetško varnost v ključnih sektorjih, med katerimi je zdravstvo, z namenom zagotavljanja večje odpornosti na kibernetške grožnje, jasnejših zahtev glede upravljanja tveganj ter strožjih sankcijskih mehanizmov (Evropski parlament in Svet Evropske unije, 2022). Direktiva NIS 2, sprejeta decembra 2022, je državam članicam naložila, da v nacionalne zakonodaje prenesejo enotne standarde za zaščito omrežij in sistemov, ki služijo oskrbi občutljivih zdravstvenih podatkov.

V Estoniji so temelji digitalizacije zdravstvenega sistema bili postavljeni že z vzpostavitvijo Estonskega nacionalnega zdravstvenega informacijskega sistema (ENHIS) konec leta 2008. Vsi zdravstveni ponudniki so zavezani k nočnemu sinhroniziranju elektronskih zdravstvenih kartotek, bolniki pa lahko na portalu »My E-Health« spremljajo in po potrebi prekličejo dostop do svojih podatkov, ob tem pa se beležijo vsi vpogledi in spremembe (Metsallik idr., 2019). Da bi zagotovila nepreklicno integriteto teh zapisov, Estonija uporablja blockchain Keyless Signature Infrastructure (KSI), ki znotraj distribuirane mreže potrjuje vsako dejanje — od vpogleda do spremembe — in s tem praktično onemogoča retroaktivno manipulacijo zgodovine podatkov (Metsallik idr., 2019). Estonija namerava sprejeti Zakon o kibernetški varnosti, ki prenaša Direktivo NIS 2 in upravljavcem kritičnih omrežij, kamor sodijo tudi zdravstveni sistemi, nalaga redne ocene tveganj, tehnične in organizacijske ukrepe ter obveznost poročanja o incidentih v »razumnem roku« po odkritju (Evropska Komisija 2025 b; Metsallik idr., 2019).

Nemčija je svoje zdravstvene subjekte identificirala kot operaterje kritične infrastrukture že v IT-Sicherheitsgesetz 1.0 iz leta 2015, pozneje nadgrajenem v IT-Sicherheitsgesetz 2.0. Ta zakon znižuje prag za včlanitev bolnišnic v KRITIS-register in zahteva uvedbo minimalnih varnostnih ukrepov, kot so sistemi za odkrivanje vdorov, upravljanje ranljivosti ter neprekinjenost poslovanja, ob tem pa nalaga poročanje o varnostnih incidentih znotraj 24 ur Federalnemu uradu za informacijsko varnost (BSI) (Kavyn idr., 2021). Hkrati je Zakon o varstvu pacientovih podatkov (PDSG) in § 75 Knjige socialne varnosti V (SGB V) od oktobra 2020 uveljavil zahtevo po »stanju tehnike« IT-varnostnih ukrepov v skladu z za sektor specifičnim standardom B3S, ki opredeljuje več konkretnih zahtev na področju šifriranja, nadzora dostopa in upravljanja incidentov (Kavyn idr., 2021). Z novim § 393 SGB V, ki je začel veljati 1. julija 2024, so bile uvedene stroge omejitve za uporabo oblačnih storitev pri obdelavi zdravstvenih podatkov: obvladovanje podatkov je dovoljeno le znotraj Nemčije, EU/EEA ali v državi z odločbo o primernosti, izvajalci morajo pridobiti certifikat C5 Basic ter zagotoviti tehnične in organizacijske ukrepe ter ustrezne pogodbe z dobavitelji oblačnih storitev (Kavyn idr., 2021).

Na Švedskem Zakon o pacientovih podatkih (Patientdatalag 2008:355) z uredbo SOSFS 2008:14 določa stroge pogoje za zaupnost, omejen dostop le pooblaščenim osebam ter obvezno beleženje vseh aktivnosti v elektronskih zdravstvenih kartotekah. Leta 2023 je začel veljati Zakon 2022:913 o skupni zdravstveni dokumentaciji, ki poskuša poenotiti postopke izmenjave in zaščite pacientovih podatkov po vsej državi (Papakonstantinou, 2022). Prva Direktiva NIS je Švedska prenesla prek Zakona o informacijski varnosti za kritične in digitalne storitve (2018:1174), ki zdravstvenim subjektom nalaga tehnične in organizacijske ukrepe ter poročanje o resnih incidentih Agenciji za civilne pripravljenosti (MSB) (Evropska Komisija, 2025). V skladu z Direktivo NIS 2 namerava Švedska leta 2025 sprejeti nov samostojen zakon o kibernetiski varnosti, ki bo uvedel konkretne zahteve glede upravljanja tveganj (avtentikacija, kontinuitetna oskrba), strategij šifriranja in varnosti dobavne verige ter strožje nadzorne in sankcijske določbe (Papakonstantinou, 2022).

Estonija, Nemčija in Švedska torej presegajo minimalne zahteve Direktive NIS 2 s celovitimi, specifičnimi in strogo nadzorovanimi pravnimi okviri, ki vključujejo napredne tehnološke rešitve (npr. blockchain v Estoniji), za sektor specifične standarde (B3S v Nemčiji) in integracijo nacionalnih sistemov poročanja o incidentih (Švedska). Ti modeli lahko služijo kot vzor za Slovenijo pri oblikovanju lastnega, robustnega pravnega in tehnološkega okolja za kibernetisko varnost v zdravstvenem sektorju.

6 Pravni okvir kibernetске varnosti v slovenskem zdravstvenem sistemu

6.1 Ključni pravni akti in njihova vloga

6.1.1 Evropski akti

Uredba (EU) 2019/881 – Uredba o kibernetiski varnosti

Uredba (EU) 2019/881 (Uradni list Evropske unije L 151/15), znana kot Uredba o kibernetiski varnosti, je temeljni pravni okvir za certificiranje varnosti informacijskih in komunikacijskih tehnologij (IKT) na ravni Evropske unije. S tem aktom je bila Evropska agencija za kibernetisko varnost (ENISA) opremljena s stalnim mandatom za podporo državam članicam, pripravo tehničnih smernic ter izdajo in upravljanje shem certificiranja (Uredba (EU) 2019/881, 2019). Glavni cilj Uredbe je vzpostavitev enotnega evropskega okvira za ocenjevanje varnosti izdelkov in storitev, ki vključuje postopke ocene skladnosti informacijskih sistemov, omrežij in aplikacij. Posebna vrednost certifikacije je zagotovitev zaupnosti, integritete in razpoložljivosti storitev, kar

je pri digitalizaciji zdravstvenih sistemov ključno za varno izmenjavo pacientovih podatkov in interoperabilnost različnih platform (Evropska Komisija, n. d. b).

Leta 2025 je bil okvir Uredbe o kibernetiski varnosti razširjen z novimi določbami, ki uvajajo obvezne sheme certificiranja za storitve upravljanja kibernetiske varnosti, vključno z odzivom na incidente (CSIRT-storitve), varnostnim testiranjem in varnostnimi revizijami (Evropska komisija, n. d. b). Te spremembe so nastale kot odgovor na naraščajoče število napadov na zdravstvene organizacije v času pandemije covida-19, ko je bila odvisnost od digitalnih rešitev izjemno velika (Smith & Abbasi, 2024). S tem se je krepilo zaupanje javnosti in zdravstvenih ponudnikov v certificirane rešitve, saj certifikat pomeni, da je izdelek ali storitev preстал neodvisno oceno in izpolnjuje najvišje varnostne standarde.

Regulacija (EU) 2024/2847 – Uredba o kibernetiski odpornosti

Regulacija (EU) 2024/2847 (Uradni list Evropske unije, 2024/2847), prevedena v slovenski kontekst kot Uredba o kibernetiski odpornosti, prinaša horizontalne zahteve za kibernetisko varnost vseh izdelkov z digitalnimi elementi, vključno z medicinskimi napravami, IT-opremo in medicinsko programsko opremo (Regulacija (EU) 2024/2847, 2024). Glavni poudarek je na načelih »security-by-design« in »security-by-default«, kar pomeni, da morajo proizvajalci že v fazi načrtovanja in razvoja vključiti mehanizme za zaščito pred znanimi in neznanimi grožnjami. Poleg tega morajo zagotoviti postopek rednih varnostnih posodobitev, sistem za prijavljanje ranljivosti in navodila za odzivanje na incidente, kar bistveno pripomore k proaktivni obrambi zdravstvenih naprav pred zlorabami (Evropska Komisija, n. d. b).

Uredba o kibernetiski odpornosti bo v veljavo stopila decembra 2027, ko bodo morali proizvajalci zdravstvenih pripomočkov v tehničnih datotekah predložiti podrobno oceno tveganj, protokole za izdajo posodobitev, navodila za namestitve in redne revizije (Regulacija (EU) 2024/2847, 2024). Zdravstveni sektor bo dobil jasne standarde, ki določajo, kako upravljati ranljivosti medicinskih naprav, kar bo zmanjšalo možnost, da bi napadalci izkoristili odkrite šibke točke in motili delovanje kritičnih življenjskih sistemov (Gričnik idr., 2024).

Direktiva (EU) 2022/2555 – NIS 2

Direktiva (EU) 2022/2555 (Uradni list Evropske unije L 333/80), poznana kot NIS 2, predstavlja nadgradnjo prvotne direktive NIS iz leta 2016. Z novimi določbami je razširjen krog zavezancev, strožji so minimalni varnostni standardi in višje kazni za neskladnost (Urad Vlade RS za informacijsko varnost, 2024). Direktiva uvaja zahteve po pripravi nacionalnih strategij za

kibernetsko varnost, vzpostavitvi struktur internih CSIRT-jev ter rednem poročanju o incidentih v 24 urah od odkritja. Poleg tega se krepi nadzor dobavne verige, da bi preprečili vnos ranljivih komponent v kritične sisteme, kar je posebej pomembno za medicinsko opremo (Evropska Komisija, 2025 b).

Rok za prenos NIS 2 v nacionalno zakonodajo je bil 17. oktober 2024, vendar Slovenija implementacije še ni zaključila, zato je Evropska Komisija proti njej sprožila postopek za ugotavljanje kršitev (Urad Vlade RS za informacijsko varnost, 2024). Zaradi zamude slovenski zdravstveni zavodi trenutno nimajo zakonsko določenih minimalnih standardov za poročanje o incidentih, ocenjevanje tveganj in izvedbo varnostnih vaj, kar povečuje njihovo ranljivost za sofisticirane kibernetske napade (Evropska Komisija, 2024).

6.1.2 Nacionalni akti

Zakon o informacijski varnosti (ZInfV, 2018)

Zakon o informacijski varnosti (ZInfV) (Uradni list RS, št. 30/18, 95/21, 130/22 – ZEKom-2, 18/23 – ZDU-1O in 49/23) je bil sprejet kot prenos osnovnih določb prve direktive NIS iz leta 2016. Ustanovil je Urad Vlade Republike Slovenije za informacijsko varnost (URSIV), ki nadzoruje in usklajuje izvajanje varnostnih ukrepov pri upravljavcih kritične infrastrukture, vključno z zdravstvenim sektorjem (Vlada RS, 2016). ZInfV določa obvezne tehnične, organizacijske in administrativne ukrepe, kot so redni varnostni pregledi, enkripcija občutljivih podatkov, stroga politika dostopa do sistemov ter priprava celovitih načrtov uvajanja varnostnih incidentov (Vlada RS, 2016). V praksi to pomeni, da morajo bolnišnice in druge zdravstvene ustanove vzpostaviti varnostne operativne centre, izvajati redne revizije in dokumentirati vse postopke upravljanja incidentov.

Zakon o informacijski varnosti – (ZInfV-1, 2025)

Zakon ZInfV-1, predstavljen aprila 2025, prinaša korenite spremembe, saj razširja krog zavezancev z dobrih 80 na več kot 1000 subjektov, med drugim vse javne bolnišnice, specializirane zdravstvene domove, izbrane zasebne izvajalce in ponudnike digitalnih rešitev (Vlada RS, 2025). ZInfV-1 je bil v Uradnem listu Republike Slovenije št. 40/25 dne 4. junija 2025 tudi objavljen. Predstavlja nov zakon in pravni okvir na področju kibernetske varnosti v Republiki Sloveniji. Zakon v slovenski pravni red končno prenaša evropsko direktivo NIS 2 in določa pravila za izboljšanje varnosti omrežij ter informacijskih sistemov (Urad Vlade Republike Slovenije za informacijsko varnost, 2025). Zakon začne veljati 19. junija 2025, uvaja pa strožje zahteve za oceno tveganj,

obveznost vzdrževanja neprekinjenega poslovanja ključnih storitev ter natančno opredelitev odgovornosti upravljalcev in njihovih dobaviteljev. Zahteva prav tako redno poročanje o varnostnih incidentih v dvanajstih urah od odkritja in vzpostavitev sistema za upravljanje ranljivosti, ki vključuje centralizirano evidenco in sledljivost popravkov (Vlada RS, 2025). S tem se krepi preglednost dobavne verige in zmanjšuje tveganje, da bi nepreverjene komponente kompromitirale kritične sisteme v zdravstvu.

Zakon o varstvu osebnih podatkov (ZVOP-2, 2022)

ZVOP-2 (Uradni list RS, št. 163/22) je nacionalni prenos Splošne uredbe o varstvu podatkov (GDPR, 2016/679) (Uradni list Evropske unije L 119/1) s poudarkom na specifičnih varnostnih ukrepih za zdravstvene, biometrične in genetske podatke (Ministrstvo za zdravje RS, 2022). ZVOP-2 uvaja izvršilne postopke za izrek glob, določa pravila za pridobivanje soglasij pacientov ter ureja izredne razmere pri raziskovalni uporabi zdravstvenih podatkov. Ključni elementi vključujejo obvezno anonimno hrambo primarnih zdravstvenih evidenc, dvostopenjski dostop do občutljivih zapisov in stroge zahteve glede tehničnih varnostnih ukrepov, kot so sistemi za zaznavanje vdorov (IDS) in upravljanje ključev (Ministrstvo za zdravje RS, 2022). Združevanje zahtev ZInfV in ZVOP-2 pomeni, da morajo zdravstvene organizacije vzpostaviti integrirane informacijske sisteme, ki hkrati zagotavljajo kibernetsko varnost in varstvo osebnih podatkov – kar postavlja visoke zahteve za manjše enote z omejenimi viri (Fernández-Alemán idr., 2013; Uršič, 2022).

6.2 Analiza implementacije pravnega okvira

6.2.1 Operativni vidiki

Učinkovita implementacija evropskih in nacionalnih aktov zahteva vzpostavitev kompleksnih notranjih procesov in organizacijskih struktur v zdravstvenih zavodih. Poleg vzpostavitve notranjih CSIRT-jev in varnostnih operativnih centrov (SOC) ter povezave z nacionalnim URSIV-om morajo organizacije razviti standardizirane politike poročanja o incidentih, ki omogočajo takojšnjo mobilizacijo odgovornih ekip (Smith & Abbasi, 2024). Implementacija NIS 2 bo dodatno zahtevala redne simulacije in varnostne vaje (angl. *tabletop exercises*), saj direktiva predpisuje, da morajo vse kritične institucije izvajati redne scenarije odzivanja na incidente (Urad Vlade RS za informacijsko varnost, 2024).

ZInfV in ZInfV-1 določata vrsto tehničnih ukrepov, kot so segmentacija omrežij, strogo uveljavljanje načela najmanjših privilegijev, napredno šifriranje in redne varnostne revizije (Vlada RS, 2016; 2025). Izvedba teh zahtev pa je močno odvisna od heterogenosti zdravstvenih institucij – klinični

centri imajo pogosto interno ekipo strokovnjakov, medtem ko manjši zdravstveni domovi pogosto najemajo zunanje ponudnike, kar lahko privede do neenotnosti in težav pri koordinaciji (Dokl, 2012).

ZVOP-2 uvaja stroge časovne roke za obveščanje Informacijskega pooblaščenca RS in prizadetih oseb v roku 72 ur od odkritja kršitve, sicer so predvidene visoke globe (Ministrstvo za zdravje RS, 2022). Integracija teh postopkov zahteva vzpostavitev notranjega nadzora ter dokumentiranje vseh korakov in elektronskih evidenc, kar je za manjše enote pogosto administrativno in tehnološko breme (Dunn, 2005).

6.2.2 E-zdravje

Pravna podlaga za čezmejno interoperabilnost je Direktiva o čezmejnem zdravstvenem varstvu (2011/24/EU), ki omogoča varno in učinkovito izmenjavo zdravstvenih podatkov med državami članicami. Na podlagi člena 14 te direktive je bila vzpostavljena mreža e-zdravje, ki povezuje nacionalne organe za e-zdravje ter razvija smernice in standarde za enotno čezmejno izmenjavo podatkov. Trenutno sta v praksi na voljo dve glavni čezmejni storitvi – e-recepti in povzetki zdravstvenih podatkov, dostopni prek platforme MyHealth@EU. Za uravnotežen razvoj e-zdravja je bil sprejet tudi evropski zdravstveni podatkovni prostor (European Health Data Space, EHDS), ki določa jasna pravila in tehnične standarde za primarno uporabo (klinična oskrba) in sekundarno uporabo (raziskave, inovacije, politika) zdravstvenih podatkov. EHDS uvaja zanesljivo digitalno infrastrukturo in upravljalne prakse, ki zagotavljajo skladnost z visokimi zahtevami EU glede varstva osebnih podatkov, pri čemer namenja posebno pozornost varnosti prenosa, hrambe in dostopa do zdravstvenih informacij (Evropska Komisija, n. d. a).

Varnostni izzivi e-zdravja so tesno povezani z razdrobljenostjo obstoječih sistemov: zdravstvene ustanove pogosto hranijo podatke v različnih formatih in ločenih bazah, kar otežuje robustno zaščito celotnega življenjskega cikla informacij. Neenotna tehnična in organizacijska struktura notranjih CSIRT-jev, neustrezna segmentacija omrežij ter neenotno uveljavljanje načela najmanjših privilegijev lahko povečajo tveganje nepooblaščenih dostopov in kopičenja ranljivosti, zato pravni okvir e-zdravja zahteva usklajen pristop h kibernetiski varnosti, ki vključuje redne revizije, varnostne simulacije in jasne mehanizme obveščanja v primeru incidentov, skladno z Direktivama NIS 2 in GDPR (Evropska Komisija, n. d. a).

6.2.3 Izzivi in priložnosti

1. Kadri in usposabljanje: Pomanjkanje kvalificiranih strokovnjakov za kibernetško varnost je ena največjih ovir. Raziskave kažejo, da redna izobraževanja in simulacije bistveno zmanjšajo verjetnost človeške napake, ki je pogosto glavni vzrok incidentov (Kavyn idr., 2021). Priložnost predstavlja uvedba kontinuiranih e-plattform za učenje in certificiranih treningov na ravni sistema e-zdravja (Ministrstvo za zdravje RS, 2022).
2. Finančni viri: Vlaganja v varnostno infrastrukturo, kot so sistemi za upravljanje varnostnih informacij in dogodkov (SIEM), enkripcija podatkov v mirovanju in v prenosu ter orodja za odkrivanje zlonamerne dejavnosti, za zdravstvene organizacije predstavljajo velik strošek (Mantelero idr., 2020). V okviru financiranja iz evropskih kohezijskih skladov je sicer možno sofinanciranje projektov za krepitev kibernetške odpornosti, kar odpira priložnost za modernizacijo varnostne opreme.
3. Medinstitucionalno sodelovanje: Učinkovita izmenjava informacij o novih grožnjah med bolnišnicami, zdravstvenimi domovi in nacionalnimi CSIRT-ji je ključno orodje za preprečevanje incidentov. Kot vzor lahko služi estonski model, kjer sta e-zdravje in kibernetška varnost že več kot desetletje tesno integrirana (Metsallik, 2019; Papakonstantinou, 2022). Slovenija lahko okrepi sodelovanje prek vzpostavitve skupnih platform za deljenje indikatorjev kompromitiranja (IoC) in rednih delavnic strokovnjakov.

6.3 Etični vidiki pravnega okvira

Pravni okvir je treba podpreti z jasnimi etičnimi smernicami, ki zagotavljajo, da so pri vzpostavljanju odpornosti in odzivanju na incidente vedno v ospredju pacientove pravice, dostojanstvo in dobrobit. Etične smernice strokovnih združenj poudarjajo načela:

1. Pravica do obveščenosti
2. Pacienti morajo biti pravočasno in jasno obveščeni o vsaki grožnji, incidentu ali zlorabi njihovih zdravstvenih podatkov, vključno z opisom narave incidenta, potencialnega vpliva ter ukrepov, ki jih organizacija izvaja za omilitev škode (Gordon idr., 2019). Transparentnost prispeva k zaupanju in pacientom omogoča, da sprejmejo informirane odločitve glede svojega zdravja in zaščite podatkov.
3. Odgovornost in povračilo škode
4. Institucije morajo vzpostaviti mehanizme za oceno škode in nudenje podpore prizadetim pacientom, kar vključuje svetovanje o ukrepih za zaščito pred nadaljnjo zlorabo podatkov,

psihološko podporo in pravno svetovanje (Mantelero idr., 2020). To načelo sledi načelu pravičnosti in spoštuje pacientovo dostojanstvo.

5. Preprečevanje diskriminacije
6. Pri razvoju in uporabi varnostnih algoritmov in analitičnih orodij mora biti zagotovljeno, da ne vodi do diskriminacije ali neenakega obravnavanja pacientov zaradi starosti, spola, etnične pripadnosti ali drugih občutljivih kategorij (Perakslis, 2014). Razvijalci morajo izvajati redne preglede algoritmov (*bias audits*) in zagotavljati, da so podatkovni nabori uravnoteženi.
7. Neprestano učenje in prilagajanje
8. Organizacije naj sistematično zbirajo lekcije iz izvedenih incidentov, posodabljaajo notranje politike, postopke in usposabljanja ter vzpostavijo kulturo neprestanega izboljševanja (Gordon idr., 2019; Mantelero idr., 2020). To vključuje redne simulacije, varnostne vaje in izmenjavo dobrih praks med zdravstvenimi institucijami.

Vključitev etičnih načel v pravni in operativni okvir krepí zaupanje pacientov in širše javnosti. S tem se ne krepí le varnosti zdravstvenih podatkov, ampak se dviguje tudi kakovost zdravstvene obravnave in dolgoročno vzdržnost digitalnega zdravja v Sloveniji.

6.4 Priporočila za nadaljnje izboljšave

Slovenski zdravstveni sistem, ki je v zadnjih letih napredoval na področju digitalizacije, potrebuje celovit pristop k nadaljnjemu razvoju, ki bo temeljil na izboljšanju interoperabilnosti, krepitvi kibernetске varnosti, izpolnjevanju določb Akta o kibernetски varnosti in Akta o kibernetски odpornosti, nadgradnji izobraževanja kadrov ter povečanju digitalne vključenosti pacientov (Ministrstvo za zdravje Republike Slovenije, 2022).

Interoperabilnost ostaja osrednji izziv – brez jasno opredeljenih standardov in odprtih vmesnikov ni mogoče zagotoviti nemotenega pretoka podatkov med bolnišničnimi sistemi, primarno oskrbo in zasebnimi ponudniki, zato je nujno sprejeti mednarodno priznane standarde za strukturiranje in prenos zdravstvenih zapisov, kot je HL7 FHIR, ter vzpostaviti varno nacionalno platformo API-jev. Takšna rešitev bo pospešila razvoj aplikacij, telemedicinskih storitev in mobilnih orodij ter omogočila tekoče vključevanje raziskovalnih inovacij v klinično prakso (Zhang, 2024).

Kibernetска varnost zahteva redne neodvisne preglede in simulacije napadov (angl. *penetration testing*) s strokovnjaki. Anonimno poročanje o rezultatih in priprava akcijskih načrtov bosta odpravila odkrita tveganja ter okrepila zaupanje deležnikov (Smith & Abbasi, 2024). Ključno je vzpostaviti nacionalni center CSIRT HZ za usklajeno odzivanje na incidente ter uvesti obvezno

šifriranje podatkov z naprednimi, celo kvantno odpornimi algoritmi, da se zaščitijo občutljive informacije (Zhang, 2024).

V skladu z Aktom o kibernetski varnosti in Aktom o kibernetski odpornosti morajo zdravstvene ustanove oblikovati celovite načrte za obvladovanje tveganj, izvajati redne revizije in simulacije incidentov ter deliti preverjene varnostne rešitve v centraliziranem repozitoriju (Evropski parlament in Svet Evropske unije, 2022; Vlada Republike Slovenije, 2025). Stalno usposabljanje zdravstvenih delavcev in IT-osebja prek certificiranih tečajev, univerzitetnih modulov ter delavnic v sodelovanju z raziskovalnimi inštituti bo zagotovilo dolgoročno odpornost sistema (Dokl, 2012; Uršič, 2022).

Digitalna vključenost pacientov naj bo izboljšana z uporabniku prijaznimi portali za dostop do lastnih podatkov, naročanje pregledov, plačilo storitev in dvosmerno komunikacijo z zdravniki. Nacionalne kampanje, lokalne delavnice ter soustvarjanje storitev (angl. *co-design*) bodo spodbudili sprejetost rešitev in upoštevanje potreb končnih uporabnikov (Fernández-Alemán idr., 2013; Gordon idr., 2019).

Pravni okvir, vključno z ZVOP 2, ZInfV in predlogom ZInfV 1, mora vsebovati mehanizme za hitro posodabljanje, da se odzove na tehnološki napredek in nove grožnje (Vlada RS, 2016; Vlada RS, 2021; Vlada Republike Slovenije, 2025). Spodbujanje javno-zasebnih partnerstev z davčnimi spodbudami in sofinanciranjem raziskovalnih projektov bo pospešilo inovacije ter dolgoročno okrepilo odpornost slovenskega zdravstvenega sistema (Mantelero idr., 2020; Kavyn idr., 2021).

7 Sklep

V času, ko digitalizacija in uporaba umetne inteligence preoblikujeta klinične in administrativne prakse, kibernetska varnost predstavlja temeljno odgovornost vseh deležnikov v zdravstvenem sistemu (Ministrstvo za zdravje Republike Slovenije, 2022). Slovenski sistem mora uravnotežiti hiter tehnološki napredek z vedno obsežnejšimi grožnjami v digitalnem prostoru, kjer neustrezno zaščiteni sistemi izpostavljajo občutljive podatke tveganju zlorabe, manipulacije ali popolne nedostopnosti (Uršič, 2022). Analiza pravnega okvira – direktive NIS-2, ZVOP-2 ter GDPR, ZInfV, Akta o kibernetski varnosti in Akta o kibernetski odpornosti – poudarja, da so trdni varnostni standardi in jasni postopki ključni za preprečevanje varnostnih incidentov, hkrati pa morajo temeljiti na mednarodno usklajeni zakonodaji (Evropska komisija, 2025a; Vlada Republike Slovenije, 2025).

Celovit pristop, ki združuje tehnološke rešitve, etične smernice in pravno regulacijo, je edina pot,

da se zagotovi zanesljivo in varno delovanje zdravstvenega sistema (Perakslis, 2014). Tehnološke rešitve, kot so kvantno odporni algoritmi za šifriranje in redne simulacije napadov (angl. *penetration testing*), morajo biti podprte z neodvisnim tretjim nadzorom in objavo anonimnih poročil o ranljivostih, kar povečuje transparentnost in zaupanje javnosti (Smith & Abbasi, 2024 in Dunn, 2005). Prav tako je nujno vzpostaviti specializirani nacionalni center za odzivanje na incidente v zdravstvu (CSIRT-HZ), ki bo združeval pravne, tehnične in komunikacijske strokovnjake za hitro obveščanje, analizo ter odzivanje na kibernetične napade (Gordon idr., 2019).

Izobraževanje in usposabljanje kadrov igra ključno vlogo pri dolgoročni varnosti in učinkovitosti – tako kliničnega osebja kot IT-strokovnjakov – saj pomanjkanje digitalne pismenosti povečuje tveganje človeške napake in neustreznega upravljanja z varnostnimi sistemi (Fernández-Alemán idr., 2013). Nacionalni program digitalne pismenosti, ki zajema teme e-zdravja, kibernetične varnosti in telemedicine, ter obvezni moduli na medicinskih in tehničnih fakultetah bodo gradili kompetence prihodnjih strokovnjakov (Metsallik, 2019). Pomembno je tudi spodbujanje izmenjave izkušenj z evropskimi pionirji, kot sta Estonija in Nemčija, kjer so sistemi e-zdravja že globoko integrirani v vsakodnevno prakso (Kavyn idr., 2021).

Digitalna vključenost pacientov je še en temelj prihodnjega razvoja. Uporabniku prijazni portali in mobilne aplikacije, ki omogočajo pregled rezultatov, naročanje na preglede in varno komunikacijo z zdravstvenim osebjem, bodo izboljšali dostopnost in učinkovitost (Ministrstvo za zdravje Republike Slovenije, 2022). Da bi preprečili digitalno izključenost ranljivih skupin, kot so starejši, je treba organizirati nacionalne delavnice in kampanje na lokalni ravni, ki krepijo zaupanje in veščine pri uporabi novih tehnologij (Fernández-Alemán idr., 2013).

Prihodnost zdravstvenega varstva v Sloveniji bo odvisna od sposobnosti prilagajanja nenehnim tehnološkim spremembam in naraščajočim grožnjam (Zhang, 2024). Ključni elementi te prilagodljivosti so vlaganje v napredne varnostne tehnologije, redno posodabljanje varnostnih protokolov in simulacije kibernetičnih napadov ter krepitev medsektorskega sodelovanja med zdravstvenimi zavodi, podjetji in vladnimi organi (Papakonstantinou, 2022 in Evropska Komisija, 2020). Transparentnost, odgovornost in etični vidiki morajo ostati temelj, na katerem gradimo nov digitalni zdravstveni sistem (Mantelero idr., 2020).

Sklepamo, da je robusten pravni okvir, ki se stalno posodablja glede na najnoveše evropske in mednarodne standarde, nujen za preprečevanje katastrofalnih posledic morebitnih kibernetičnih napadov (Urad Vlade Republike Slovenije za informacijsko varnost, 2024; Evropska komisija, 2025b). Le s kombinacijo tehnoloških, izobraževalnih in pravnih ukrepov bomo zagotovili, da bo

digitalizacija zdravstvenega sistema prinesla več koristi kot tveganj, seveda ob krepitvi zaupanja pacientov in trajnostni rasti kakovosti zdravstvenih storitev. Ta zaključek naj služi kot spodbuda za nadaljnje raziskave, praktične izboljšave in oblikovanje politike, ki bo združevala tehnološki napredek s pravno in etično odgovornostjo.

Literatura in viri

1. Corera, G. (2021). *Irish health cyber-attack could have been even worse, report says*. BBC News. <https://www.bbc.com/news/technology-59612917>
2. Dokl, J. (2012). *Kibernetska varnost omrežij, magistrsko delo, Univerza v Ljubljani, Fakulteta za družbene vede*. Ljubljana: UL FDV.
3. Dunn, M. (2005). *Comparative analysis of cybersecurity initiatives worldwide*. ITU, WSIS Thematic Meeting on Cybersecurity. Ženeva: ITU. https://www.itu.int/osg/spu/cybersecurity/docs/Background_Paper_Comparative_Analysis_Cybersecurity_Initiatives_Worldwide.pdf
4. Evropska komisija. (2024). *Dva postopka zaradi kršitev zakonodaje EU*. Evropska komisija. https://slovenia.representation.ec.europa.eu/novice-dogodki/novice-0/dva-postopka-zaradi-kršitev-zakonodaje-eu-2024-11-28_sl
5. Evropska komisija. (2025a). *Evropski akcijski načrt za kibernetsko varnost bolnišnic in izvajalcev zdravstvenih storitev*. Evropska komisija. https://slovenia.representation.ec.europa.eu/novice-dogodki/novice-0/kibernetska-varnost-bolnisnic-zdravstvenih-ustanov-v-eu-2025-01-15_sl
6. Evropska komisija. (2025b). *Komisija poziva k prispevkom za izboljšanje kibernetske varnosti za bolnišnice in izvajalce zdravstvenih storitev*. Digital Strategy. <https://digital-strategy.ec.europa.eu/sl/news/commission-seeks-contributions-enhance-cybersecurity-hospitals-and-healthcare-providers>
7. Evropska komisija. (2025c). *Evropski pristop k umetni inteligenci*. Evropska komisija. <https://digital-strategy.ec.europa.eu/sl/policies/european-approach-artificial-intelligence>
8. Evropska komisija. (n.d. a). *Digitalno zdravje in oskrba*. Evropska komisija. https://health.ec.europa.eu/ehealth-digital-health-and-care/digital-health-and-care_sl
9. Evropska komisija. (n.d. b). *Politike kibernetske varnosti*. Evropska komisija. <https://digital-strategy.ec.europa.eu/sl/policies/cybersecurity-policies>
10. Evropska Komisija (2025). *Revidirana direktiva o varnosti omrežij in informacij: nova pravila o kibernetski varnosti omrežij in informacijskih sistemov*. Evropska komisija. <https://digital-strategy.ec.europa.eu/sl/policies/nis2-directive>
11. Evropski parlament in Svet Evropske unije. (2022). *Direktiva (EU) 2022/2555 Evropskega parlamenta in Sveta z dne 14. decembra 2022 o ukrepih za visoko skupno raven kibernetske varnosti v Uniji, o spremembi Uredbe (EU) št. 910/2014 in Direktive (EU) 2018/1972 ter o razveljavitvi Direktive (EU) 2016/1148 (Direktiva NIS 2)*. *Uradni list Evropske unije*, L 333, 80–152. <https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng>
12. Fernández-Alemán, J. L., Señor, I. C., Lozoya, P. Á. O., & Toval, A. (2013). Security and privacy in electronic health records: A systematic literature review. *Journal of Biomedical Informatics*, 46(3), 541–562.
13. GDPR GURU. (2025). *EK: Kibernetska varnost bolnišnic*. GDPR GURU. <https://www.gdpr-guru.eu/blog/blog-5/post/ek-kibernetska-varnost-bolnisnic-9454>

14. Gordon, W. J., Fairhall, A., & Landman, A. (2019). Threats to information security—Public health implications. *The New England Journal of Medicine*, 380(1), 23–26.
15. Gričnik, A. M., & Zore, S. (2024). Umetna inteligenca v zdravstvu. *Izzivi managementu*, 16(1-2), 66–77.
16. Kavyn, Sviatoslav & Bratsuk, Ivan & Lytvynenko, Anatoliy. (2021). Regulatory and legal enforcement of cyber security in countries of the European Union: The experience of Germany and France. *Teisė*. 121, 135–147. <https://doi.org/10.15388/Teise.2021.121.8>
17. Mantelero, A., Vaciago, G., Samantha Esposito, M., & Monte, N. (2020). The common EU approach to personal data and cybersecurity regulation. *International Journal of Law and Information Technology*, 28(4), 297–328.
18. Metsallik, J. (2019). Ten years of the e-Health system in Estonia. https://ceur-ws.org/Vol-2336/MMHS2018_invited.pdf
19. Ministrstvo za digitalno preobrazbo. (2024). *Mednarodna konferenca: Voditeljstvo v zdravstvu v dobi novih tehnologij*. MDPRS. <https://www.gov.si/novice/2024-06-14-mednarodna-konferenca-voditeljstvo-v-zdravstvu-v-dobi-novih-tehnologij>
20. Ministrstvo za digitalno preobrazbo. (2024). *Potrjen prvi zakonodajni okvir na svetu, ki bo reguliral področje umetne inteligence*. MDPRS. <https://www.gov.si/novice/2024-02-02-potrjen-prvi-zakonodajni-okvir-na-svetu-ki-bo-reguliral-podrocje-umetne-inteligence>
21. Ministrstvo za zdravje Republike Slovenije. (2022, November). *Slovenija – e-zdravje za bolj zdravo družbo (REFORM/SC2021/061)* [Strategija]. MZRS. <https://www.gov.si/assets/ministrstva/MZ/DOKUMENTI/staro/Slovenija-E-zdravje-za-bolj-zdravo-druzbo-v2.pdf>
22. Papakonstantinou, V. (2022). Cybersecurity as praxis and as a state: The EU law path towards acknowledgement of a new right to cybersecurity? *Computer Law & Security Review*, 44, 1–15.
23. Perakslis, E. D. (2014). Cybersecurity in health care. *New England Journal of Medicine*, 371(5), 395–397.
24. Smith, D. A., & Abbasi, N. (2024). Cybersecurity in healthcare: Securing patient health information (PHI), HIPAA compliance framework and the responsibilities of healthcare providers. *Journal of Knowledge Learning and Science Technology*, 3(3), 278–287.
25. Urad Vlade Republike Slovenije za informacijsko varnost (2024). *Direktiva o ukrepih za visoko skupno raven kibernetске varnosti (NIS 2): vprašanja in odgovori*. <https://www.gov.si/novice/2024-10-24-direktiva-o-ukrepih-za-visoko-skupno-raven-kibernetске-varnosti-nis-2-vprasanja-in-odgovori/>
26. Urad Vlade Republike Slovenije za informacijsko varnost. (2025). Zakon o informacijski varnosti (ZInfV-1) objavljen v Uradnem listu Republike Slovenije. <https://www.gov.si/novice/2025-06-04-zakon-o-informacijski-varnosti-zinfv-1-objavljen-v-uradnem-listu-republike-slovenije/>
27. Uršič, J. (2022). *Kibernetška varnost v zdravstvu* (Doktorska disertacija), Univerza v Ljubljani, Fakulteta za elektrotehniko).
28. Vlada Republike Slovenije. (2025). *Vlada določila besedilo predloga novega Zakona o informacijski varnosti (ZInfV-1)*. GOV.SI. <https://www.gov.si/novice/2025-04-10-vlada-dolocila-besedilo-predloga-novega-zakona-o-informacijski-varnosti-zinfv-1/>
29. Vlada RS. (2016). *Predlog zakona o informacijski varnosti*. GOV.SI. <https://euprava.gov.si/drzava-in-druzba/e-demokracija/predlogi-predpisov/predlogpredpisa.html?id=8587>
30. Vlada RS. (2021). *Predlog sprememb in dopolnitev Zakona o informacijski varnosti (ZInfV-A)*. GOV.SI. <https://imss.dz-rs.si/IMiS/ImisAdmin.nsf/ImisnetAgent?OpenAgent&2&DZ>
31. Zhang, W. (2024). Constructing the legal framework for cybersecurity: A review of comparative legal approaches to cyberspace security governance and their insights. *Journal of Networking and Telecommunications*, 6(1), 3551.

PROBLEMATIKA DISKRIMINACIJE V ZVEZI Z UPORABO UMETNE INTELIGENCE PRI ZAPOSLOVANJU

Lisa Elizabeth Strouken, študentka, Univerza v Mariboru, Pravna fakulteta, Slovenija 

Doc. dr. Aljoša Polajžar, Univerza v Mariboru, Pravna fakulteta, Slovenija 

Povzetek: Prispevek obravnava problematiko diskriminacije v zvezi z uporabo umetne inteligence (UI) pri zaposlovanju. Pri tem se pri pregledu problematike osredotoča tako na predstavitev stališč in konkretnih primerov, ki so dokumentirani v literaturi, kakor tudi na oris osnovnega relevantnega pravnega okvira po pravu EU. Pregled literature pokaže, da s pomočjo UI delodajalci, med drugim, iščejo ustrezne kandidate, izvajajo celoten postopek izbire kandidata itd. Pri tem v praksi prihaja do nevarnosti (tveganja) diskriminatorne obravnave kandidatov. Tudi uporaba UI namreč ne pomeni (popolne) izključitve (diskriminatornih) subjektivnih vplivov pri izbiri kandidatov. Uporaba UI lahko slednje zgolj še dodatno (sistemsko) utrdi. Problematiko otežuje dejstvo, da se lahko delodajalci zanašajo na te sisteme, ne da bi spremljali vzorce odločanja svojih algoritmov, zaradi česar je težje prepoznati ali preprečiti diskriminacijo. Na podlagi napravljenega pregleda so v zaključku članka strnjene nekatere obstoječe konkretne prakse ter pravne rešitve za naslovitev predmetne problematike.

Ključne besede: zaposlovanje, umetna inteligenca, algoritmi, diskriminacija, delovna razmerja

Cobiss: 1.08

1 Uvod

V članku se obravnava problematika diskriminacije v zvezi z uporabo umetne inteligence (v nadaljevanju: UI) v procesih zaposlovanja. Slednje je postalo pomemben trend, saj delodajalci s pomočjo UI iščejo ustrezne kandidate ali pa celoten postopek izbire kandidata prepustijo algoritmu. Sistemi UI v delovnem okolju prevzemajo vloge, ki so bile tradicionalno v domeni človeka, kar vsaj v enem delu odstranjuje človeško prisotnost in dehumanizira postopek zaposlovanja in delovnega okolja nasploh. V procesih zaposlovanja, kjer se uporabljajo sistemi UI, se pojavlja izziv pri uravnoteženju človeških in umetnih vrednot, ki jih je UI podelil ustvarjalec sistema (Rigotti & Fosch-Villaronga, 2024). V luči navedenega tudi številna podjetja ponujajo storitve uporabe UI za pomoč delodajalcu pri procesu zaposlovanja. Slogan podjetja Canditech (ki ponuja tovrstne storitve) se denimo glasi: *»Unlike humans, AI is blind to gender, ethnicity, age, and background. It can automatically grade an unlimited number of candidate assessments and analyze an endless amount of information in order to help hiring teams make the best recruiting decisions in no time«* (Canditech, n. d.).

Članek je v nadaljevanju razdeljen na dva glavna dela. V prvem delu se obravnava relevanten dejanski okvir problematike, in sicer v 2. poglavju navaja izsledke študij, ki obravnavajo problematiko diskriminacije v zvezi z uporabo UI pri zaposlovanju. Pri tem je poudarek na obravnavi konkretnih dejanskih primerov uporabe sistemov UI pri zaposlovanju ter praktičnih izzivov algoritemske diskriminacije pri zaposlovanju v vsaki posamezni fazi zaposlovanja. Tako so obravnavani ključni dejavniki, ki k njej prispevajo, in vrste diskriminacije v algoritmičnih sistemih zaposlovanja ter v 3. poglavju so razkriti ukrepi za njeno preprečevanje. Poudarek je na prepoznavanju dobrih praks in učinkovitih pravnih rešitev za pravičnejši pristop. V drugem delu članka, in sicer v 4. poglavju, se obravnavajo relevantni pravni viri oz. regulativni okvir v zvezi z obravnavano problematiko na ravni EU. Nazadnje pa so v 5. poglavju članka na podlagi napravljene raziskave strnjene nekatere obstoječe konkretne prakse in pravne rešitve za naslovitev problematike diskriminacije v zvezi z uporabo UI pri zaposlovanju.

2 UI kot potencialno sredstvo (za zmanjšanje) diskriminacije v postopku e-zaposlovanja

Na navedeno problematiko so bile napravljene številne strokovne študije in analize. Po podatkih Komisije za enake zaposlitvene možnosti (EEOC) iz ZDA več kot 80 % delodajalcev že uporablja avtomatizirane pripomočke pri zaposlovanju (Garrison, 2024). Posledično se je pojavilo vprašanje

algoritmične diskriminacije pri zaposlovanju, ki je preusmerilo poudarek teorije diskriminacije z običajnega zaposlovanja na t. i. pametno e-zaposlovanje (Chen, 2023). EEOC je avgusta 2023 dobila svojo prvo tožbo zaradi diskriminacije pri zaposlovanju z UI. V primeru EEOC proti iTutorGroup je EEOC tožila tri podjetja, ki so uporabljala program UI, ki je »samodejno zavrnil prijaviteljice, stare 55 let ali več, in prijavitelje, stare 60 let ali več«, kar je izločilo več kot 200 kandidatov zaradi starosti (Kempe, 2024). Tožba se je končala s poravnavo, na podlagi katere se je toženo podjetje (iTutorGroup) zavezalo, da bo posameznikom, ki so bili zaradi svoje starosti avtomatično zavrtni, skupaj izplačalo odškodnino v znesku 365.000 USD (EEOC, 2023).

Nadalje mnogi strokovnjaki menijo, da UI lahko pomaga zmanjšati človeške pristranskosti in izboljšati odločanje. Seppälä in Matecka v svoji študiji denimo navajata Greenwalda, ki UI vidi kot sredstvo za zmanjšanje diskriminacije, ki jo povzročajo implicitne pristranskosti. Izbor kandidata z UI se pogosto smatra za pravičnejšega in bolj objektivnega v primerjavi z odločitvami, ki temeljijo na človeški presoji, vendar je treba opozoriti, da k pristranskosti nismo nagnjeni le ljudje, saj so sistemi UI prav tako izpostavljeni algoritemski pristranskosti, ki izhaja iz pristranskih podatkov ali algoritmov, kar lahko vodi do diskriminacije določenih družbenih skupin. Ključni dejavniki so nameni in cilji, zaradi katerih so te tehnologije uvedene, ter način, kako so zasnovane programske rešitve (Seppälä & Matecka, 2024).

Študija Evropskega parlamenta ugotavlja, da je uporaba teh tehnologij pogosto površna in osredotočena na zmanjšanje stroškov namesto na dejansko izboljšanje zaposlovanja, saj podjetja raje iščejo nove kadre na trgu, namesto da bi vlagala v razvoj obstoječih zaposlenih. Pri tem se pogosto zanašajo na preproste in cenovno ugodne algoritme ter slepo zaupajo razvijalcem sistemov UI, ne da bi sami preverili njihovo učinkovitost (European Parliamentary Research Service, 2022, str. 23).

Garrison trdi, da problematiko diskriminacije z UI otežuje dejstvo, da večina uporabnikov sistemov za zaposlovanje z UI ne razkrije delovanja svojih algoritmov. Brez vpogleda v notranje delovanje teh sistemov je težko preprečiti ali prepoznati diskriminacijo, saj se delodajalci lahko zanašajo na te sisteme, ne da bi spremljali vzorce odločanja (Garrison, 2024). UI se nenehno uči iz obstoječih podatkov, zato lahko prepozna in nadalje utrdi obstoječe pristranskosti (Acuna Ocana, 2023). Obenem je raziskovalna ekipa na Univerzi Princeton odkrila, da algoritmi nimajo dostopa do absolutne resnice ter da strojni korpus vsebuje pristranskosti, ki tesno spominjajo na implicitne pristranskosti, kot tudi da ima UI potencial, da ohranja obstoječe vzorce pristranskosti in

diskriminacije, saj so ti sistemi običajno usposobljeni za ponavljanje izidov. Vendar percepcija objektivnosti, ki obkroža visokotehnološke sisteme, zakriva to dejstvo (Raso, Hilligoss, Krishnamurthy, Bavitz & Kim, 2018, str. 45; Chen, 2023).

Iz tega sledi, da lahko pristranskost v sisteme UI pride bodisi (ne)namerno že pri modeliranju bodisi skozi učenje na podlagi pristranskih preteklih odločitev ali zaradi nepravilne uporabe oz. napačne razlage podatkov. Torej kandidat kot tak ne vpliva neposredno na zaposlitveni algoritem, temveč je presojen na podlagi vnaprej vnesenih podatkov in meril, ki so lahko predhodno določeni (Fisher Phillips, 2023). Pri tem je treba upoštevati, da UI, ki analizira življenjepise, video intervjuje ali naloge, pogosto išče kandidate, ki so podobni trenutnim zaposlenim. Goodman meni, da ta orodja ne odpravljajo človeške pristranskosti, ampak jo le prenašajo v programsko opremo (Goodman, 2018).

Izbira kandidata je namreč vsaj v enem delu subjektivna odločitev delodajalca. »Izhodni« logiki teh sistemov je težko slediti, zato se sisteme UI pogosto označuje kot »sistem črne skrinjice«, skozi katero imajo delodajalci malo ali nobenega vpogleda v razloge za določeno odločitev in niso sposobni povedati, kateri uporabljeni kriterij je pripeljal do diskriminatornega učinka (Rigotti & Fosch-Villaronga, 2024; Osborne Clarke, 2023). Posledično je treba dokazati, kateri izmed kriterijev, ki se na prvi pogled zdijo nevtralni, so bili vzročno povezani z UI za diferenciran »output«. Rigotti in Fosch-Villaronga sta mnenja, da ta nepreglednost sistemov UI predstavlja izziv v dokazovanju diskriminacije v postopkih zaposlovanja, zaradi česar je dokazovanje za posameznika izjemno težko (*probatio diabolica*), saj so takšni sistemi pogosto zaščiteni s pravicami intelektualne lastnine in otežujejo sledljivost odločitev, kar predstavlja izziv tako za neizbrane kandidate kot delodajalce, ki morajo zagotoviti jasnost postopkov, da se razbremenijo dokaznega bremena in morebitne odgovornosti (Rigotti & Fosch-Villaronga, 2024).

Pri tem je pomembno, da pravično in predvsem nediskriminatorno zaposlovanje temelji na dejanskem postopku odločanja, ne pa na njegovem rezultatu. Z drugimi besedami, poudarek ni samo na odločitvi o zaposlitvi, temveč na obravnavi kandidata za zaposlitev v postopku zaposlovanja in izbire, s čimer se implicitno favorizira procesno razumevanje pravičnosti (Rigotti & Fosch-Villaronga, 2024).

Postopek zaposlovanja je niz dogodkov, ki jih je moč razvrstiti v štiri faze: iskanje oz. oglaševanje delovnega mesta, prijava na delovno mesto in pregledovanje le-teh, intervjuji in izbira kandidata.

Chen trdi, da vsaka faza vključuje različne dejavnosti, pri katerih lahko tehnologija UI vpliva na izvedbo vsakega koraka (Chen, 2023).

2.1 Faza iskanja oz. oglaševanja delovnega mesta

V prvi fazi bi morali, po mnenju Oxley, delodajalci biti previdni pri objavljanju oglasov za zaposlitev na spletu, saj lahko tretje strani uporabljajo diskriminatorne algoritme (Oxley, 2023). Sistem iskanja spletnih vsebin išče pasivne kandidate za zaposlitev na družbenih medijih in platformah za zaposlovanje ter analizira njihove profile v skladu z vnaprej določenimi opisi delovnih mest (Chen, 2023). Leta 2021 je bilo ugotovljeno, da so algoritmi Facebooka ciljali oglase na podlagi zbranih podatkov, pri čemer je bilo 96 % uporabnikov, ki so videli oglas za delovna mesta mehanikov, moških, in 95 % uporabnikov, ki so videli oglas za delovna mesta vzgojiteljev, žensk (Oxley, 2023). Samodejno so prikazovali »ustrezna« delovna mesta, kot so blagajničar/-ka v supermarketih, predvsem ženskam, in delovna mesta pri podjetjih za prevoze s taksiji temnopoltim uporabnikom (Garrison, 2024).

Posledično takšne platforme omogočajo delodajalcem, da svoje oglase usmerijo na določene vrste kandidatov, kar pa pomeni, da nekateri iskalci zaposlitve sploh nimajo možnosti videti določenih oglasov. Kdo vidi določen oglas, pa je odvisno tako od ciljanja delodajalca kot od algoritmičnih mehanizmov platforme. Že začetni korak – oglaševanje delovnih mest specifičnim skupinam – lahko vodi v neupravičeno izključitev iskalcev zaposlitve. To ni nujno le posledica izbire delodajalcev, temveč tudi delovanja oglaševalskih platform, ki lahko same ustvarjajo pristranske in potencialno diskriminatorne rezultate (European Parliamentary Research Service, 2022, str. 22).

V skladu z navedenim je treba zagotoviti razumne prilagoditve, kjer je to potrebno, saj morajo delodajalci omogočiti človeški nadzor pri zaposlovalnih postopkih, ki jih poganja UI, kot je bilo odločeno v primeru AECOM proti Mallonu iz Združenega kraljestva, kjer je UI v postopku prijave posameznika z invalidnostjo postavila v slabši položaj (Oxley, 2023). Delodajalci morajo razkriti obstoj avtomatiziranih procesov odločanja, vključno s profiliranjem, in zagotoviti celovite podrobnosti o osnovni logiki, pomenu in morebitnih posledicah teh sistemov.¹ Pomembno vlogo

¹ F) točka 2. odst. 13. člena in g) točka 2. odst. 14. člena GDPR.

ima 1. odst. 22. člena GDPR², ki posameznikom zagotavlja pravico, da niso podvrženi odločitvam, temelječim izključno na avtomatizirani obdelavi, če te odločitve pomembno vplivajo nanje. Teološka interpretacija nalaga, da je prepovedano sprejemanje popolnoma avtomatiziranih odločitev brez pomembnega človeškega posredovanja (Katsioti & Maratou, 2024).

2.2 Faza prijave na delovno mesto in pregledovanje le-teh

Faza pregledovanja vključuje ocenjevanje kvalifikacij kandidatov, kjer UI pomaga kadrovikom pri analizi življenjepisov in vrednotenju kompetenc. Sistemi lahko razvrstijo kandidate glede na relevantnost kvalifikacij (Chen, 2023). Upošteva prispevek Fisherja Phillipsa, lahko programi za pregledovanje, podprti z UI, prevzamejo breme človeških kadrovikov, saj pregledujejo velike količine prijav in življenjepisov ter iščejo ključne besede, izkušnje, veščine in druge kriterije, da bi prepoznali kvalificirane kandidate, ki bi jih bilo treba podrobneje preučiti.³ Ta orodja lahko avtomatsko komunicirajo s kandidati o njihovem statusu v postopku prijave in jih celo usmerijo k drugim delovnim priložnostim (Fisher Phillips, 2023). Leta 2014 je Amazon razvil algoritem za avtomatizacijo zaposlovanja, ki je hitro pokazal pristranskost proti ženskam, zlasti pri tehničnih delovnih mestih. Vzpostavljen je bil na podatkih iz pretežno moške ekipe, zato je privilegiral moške kandidate in zavračal tiste z ženskimi fakultetami ali omembo besede »ženska« v življenjepisih (Goodman, 2018).

Oxley kot pogost problem za delodajalce izpostavlja dolžnost, da opravijo razumne prilagoditve za kandidate z invalidnostjo. Ta dolžnost nastane, ko invalidna oseba bodisi vloži svojo prijavo za zaposlitev bodisi obvesti delodajalca, da se namerava prijaviti. Čeprav spletni postopki prijave vedno bolj postajajo norma, bi morali biti delodajalci pozorni, da ti postopki niso vedno dostopni kandidatom z invalidnostjo (Oxley, 2023). Nadalje raziskave kažejo, da ženske pogosteje omilijo svoje sposobnosti in dosežke, zaradi česar v svojih življenjepisih uporabljajo bolj umirjen in nevtralen jezik, medtem ko moški pogosto uporabljajo bolj odločen in samozavesten jezik, ki bolje sovпада z zahtevami delovnih mest. Algoritmi pogosto dajejo boljše ocene moškim, četudi imajo ženske enake kvalifikacije (Acuna Ocana, 2023). Lytton je v svoji študiji predstavila, da je v enem

² 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 ali GDPR). 2016. Uradni list Evropske unije L 119/1, str. 1–88.

³ Podjetja, kot so Under Armour, Red Bull in Mercedes Benz, uporabljajo platformo HireVue, ki temelji na UI, za obvladovanje na tisoče življenjepisov (Fisher Phillips, 2023).

primeru kandidat, ki je bil izločen, s spreminjanjem datuma rojstva pridobil intervju. Drugje je algoritem pri pregledovanju življenjepisov dajal prednost moškim, ki so omenjali »bejzbol« ali »košarko«, medtem ko so ženske, ki so omenjale »softball«, prejele slabše ocene (Lytton, 2024).

Nadalje delodajalci pogosto dodajajo vedno več pogojev, ki jih morajo kandidati izpolnjevati, da prestanejo avtomatsko selekcijo. Tako se seznam zahtev širi, kar vodi do stalnega zmanjševanja števila ustreznih kandidatov. Rezultat je, da so milijoni potencialnih delavcev izključeni s trga dela. Poleg tega se nekateri kandidati zavrnejo avtomatsko, pogosto brez človeškega posredovanja (European Parliamentary Research Service, 2022, str. 22).

2.3 Faza razgovora

Naslednja faza je intervju, ki naj bi se s pomočjo UI opravil petkrat hitreje od običajnega razgovora. To je verjetno najbolj individualna faza postopka izbire in zato naj ne bi bila v celoti avtomatizirana z UI (Chen, 2023). Delodajalci, ki uporabljajo UI pri intervjujih, od kandidatov zahtevajo odgovore na vprašanja v določenem časovnem okviru preko videoposnetka. UI oceni kandidate na podlagi vizualnih, verbalnih in vokalnih kriterijev, kot so obrazni izrazi, besednjak in ton govora. Oxley je v svoji raziskavi izpostavila primer Uberja iz Nizozemske, ki je pokazal, da ima tehnologija prepoznavanja obrazov težave pri prepoznavanju temnopoltih in manjšinskih etničnih kandidatov, kar vodi v slabše ocene (Oxley, 2023). Prav tako so kandidati z močnimi naglasi ali govornimi ovirami pogosto izločeni zaradi tehničnih omejitev tehnologije. Raziskovalci z Univerze v Cambridgeu so ugotovili, da lahko dejavniki, kot so svetloba, ozadje, oblačila in obrazni izrazi, vplivajo na oceno kandidata (University of Cambridge, 2022). To pomeni, da podjetja, ki prepuščajo predizbor UI, tvegajo izločitev kvalificiranih kandidatov, ki ne ustrezajo tehnološkim predpostavkam (Acuna Ocana, 2023).

Pri tem Stockhem in Fourcans poudarjata, da so sistemi UI, ki se uporabljajo za preverjanje osebnosti, sposobnosti in kognitivnih sposobnosti ali za ugotavljanje, ali so kandidati »kulturno primerni«, lahko še posebej diskriminatorni do invalidov, saj lahko od prosilcev zahtevajo uporabo orodij, ki jim niso dostopna. Test, ki zahteva govorne odgovore, npr. ni dostopen osebam, ki ne morejo (začasno ali trajno) govoriti. Uporabljajo se lahko tudi za testiranje osebnostnih lastnosti, ki niso potrebne za opravljanje vseh del, kot je optimizem (Stockhem & Fourcans, 2023). Takšni algoritmi lahko izločijo kandidate, katerih govorni vzorec ali očesni stik odstopa od tistega, ki ga običajno uporabljajo kandidati določene etnične skupine (Goodman, 2018).

2.4 Faza izbire kandidata

Zadnja faza je izbira kandidata, kjer delodajalec sprejme končno odločitev o zaposlitvi. V tej fazi sistemi UI izračunajo plače in ugodnosti ter napovedujejo tveganja za posamezne kandidate (Chen, 2023). Poleg tega ponudniki programske opreme za zaposlovanje pogosto oglašujejo sisteme z »ekstravagantnimi« orodji UI, katerih dejanska uporabnost je vprašljiva (European Parliamentary Research Service, 2022, str. 11). Katsioti in Maratou sta izpostavila Pymetrics, platformo za oceno mehkih veščin, ki uporablja igre na osnovi UI za oceno kognitivnih, socialnih in vedenjskih lastnosti kandidatov. »Digits Memory Game« npr. ocenjuje spominske sposobnosti kandidatov z izzivom, da si zapomnijo hitro utripajoče zaporedje števil. Po končanem izzivu platforma analizira njihove sposobnosti in ustvari podatkovne profile, da poišče najprimernejše kandidate za delovno mesto (Katsioti & Maratou, 2024).

To pomeni, da so igre in testi, ki jih UI uporablja za ocenjevanje nagnjenosti k tveganju ali osebnostnih lastnosti, lahko zavajajoči. Digitalni test s simulacijo napihovanja balona za merjenje tveganj, ki se uporablja pri zaposlovanju, npr. morebiti ne odraža resničnega vedenja kandidatov. Tudi videoigre, ki se uporabljajo za izbor kandidatov, so lahko učinkovite pri merjenju določenih specifičnih vidikov, vendar je njihova splošna veljavnost vprašljiva. Poleg tega nekateri raziskovalci opozarjajo, da lahko digitalni razkorak med posamezniki – pri čemer imajo nekateri boljše internetno povezavo, naprednejše naprave ali so bolj digitalno pismeni – vodi v neenakost in posledično diskriminatoren izbor kandidatov. Drugi delodajalci uporabljajo programsko opremo UI za preverjanje kandidatov skozi pregled njihovih objav na družbenih omrežjih (t. i. *cybervetting*). V zvezi s tem so raziskovalci opozorili na pomanjkanje doslednih raziskav, ki bi potrjevale veljavnost in zanesljivost takšnega pristopa, ne da bi sploh upoštevali pomisleke glede zasebnosti (European Parliamentary Research Service, 2022, str. 22–23).

3 Ukrepi za preprečevanje algoritmične diskriminacije v praksi

Nadalje iz študij izhajajo številni možni ukrepi (za delodajalce) za preprečitev pojava algoritmične diskriminacije v praksi. Arrowsmith, Intezari, Pauleen in Soleimani poudarjajo, da je za kadrovske strokovnjake ključnega pomena izvedba strukturiranega programa usposabljanja, osredotočenega na razvoj informacijskih sistemov in UI. To usposabljanje bi moralo zajemati osnove razumevanja UI, prepoznavanje pristranskosti v sistemih UI in strategije za ublažitev le-teh (Arrowsmith, Intezari, Pauleen & Soleimani, 2024). Čeprav je neizpodbitno dejstvo, da sodobni

načini pridobivanja in opravljanja dela zahtevajo ustrezna znanja in kompetence, se na trgu dela srečujemo z nizko motivacijo za usposabljanje, zlasti pri starejših delavcih in tistih z nižjo izobrazbo, zato bi bilo smiselno razmisliti o uvedbi finančno-davčnih spodbud in drugih mehanizmov, ki bi omogočili lažje in učinkovitejše pridobivanje znanj ter kompetenc za delo v digitalni dobi (Franca, 2023, str. 10–11).

Peče izpostavlja, da je vselej treba upoštevati, da sistemi UI sami po sebi ne nastanejo in sami po sebi nimajo negativnega vpliva na človekove pravice, temveč imata takšen vpliv njihova implementacija in uporaba za človeško interakcijo. Za vsako odločitvijo avtonomnega sistema stoji fizična ali pravna oseba, ki ta sistem uporablja v določen namen (Peče, 2023, str. 136). V tej luči je pomembno spodbujanje boljšega sodelovanja med kadrovskimi strokovnjaki in razvijalci UI, saj bi s tem zagotovili, da so podatki, uporabljeni v postopkih zaposlovanja, ki jih vodi UI, kulturno raznoliki in reprezentativni za različne demografske skupine (Arrowsmith, Intezari, Pauleen & Soleimani, 2024). V nasprotnem primeru Chen meni, da zbiranje podatkov algoritma nima količine in kakovosti ter bo neuspešno predstavljalo realnost objektivno. Brez skrbnega načrtovanja večina podatkovnih nizov vsebuje nestrukturirane podatke, pridobljene z opazovalnimi metodami, ki nimajo strogih metod v nadzorovanih okoljih (Chen, 2023).

Poleg tega bi si delodajalci morali prizadevati za ustvarjanje ekip, ki vključujejo strokovnjake za kadrovske zadeve in UI. Ti lahko pomagajo premostiti komunikacijsko vrzel in bolje uskladiti njihova prizadevanja.⁴ Pri tem pa se mora upoštevati širjenje priložnosti za premalo zastopane skupine pri razvoju UI, kar bi doprineslo k zagotovitvi, da različne perspektive oblikujejo sisteme, ki vplivajo na odločitve o zaposlovanju (Women of Influence, 2025).

Predvsem pa se je kot učinkovita praksa izkazalo izvajanje certifikacije in redne algoritmične revizije pristranskosti UI, kot jih že uvajajo v New Yorku (Women of Influence, 2025). Ena ključnih prednosti avtomatiziranega odločanja je možnost predhodnega testiranja sistema, kar omogoča oceno njegove pravičnosti in odpravo morebitnih diskriminatornih pristranskosti še pred njegovo dejansko uporabo (Peče, 2023, str. 160). Stockhem in Fourcans zavzemata stališče, da je redno pregledovanje in posodabljanje algoritmov UI obvezno za preprečevanje pristranskosti in

⁴ Zasledovanje potrebe po pismenosti pa omenja tudi 20. uvodna točka Akta o UI, Komisija in države članice pa bi morale skupaj z deležniki olajšati pripravo prostovoljnih kodeksov ravnanja za izboljšanje pismenosti med razvijalci, operaterji in uporabniki UI (4. člen Akta o UI).

ohranjanje pravičnosti v procesu zaposlovanja. Ta proaktivni pristop pomaga prepoznati in odpraviti vse pristranskosti, ki so nenamerno vgrajene v sistem. Revizije bi preverjale delodajalčeve prakse, npr. kot odziv na prijave žvižgačev, ali služile kot obvezni ukrep za sisteme UI, ki dosežejo določeno stopnjo uporabe (Stockhem & Fourcans, 2023). Microsoft je ustanovil odbor za UI in etične standarde, ki uveljavlja ta načela in vse prihodnje izdelke UI podvrže etični preiskavi, medtem ko je Google uvedel funkcijo Model Card, ki je podobna priročniku za algoritme, in pojasnjuje uporabljeni algoritem, izpostavi njegove prednosti in slabosti ter deli operative rezultate iz različnih podatkovnih nizov (Chen, 2023).

Pri tem pa ElMorsy izpostavlja, da človeška presoja ostane del procesa.⁵ Ta hibridni model uporablja UI za podporo zaposlovalcem, namesto da bi jih nadomestili. Kandidati bi morali dobiti jasne informacije o tem, kako se UI uporablja v procesu zaposlovanja, in povratne informacije o tem, zakaj niso bili izbrani (ElMorsy, 2024). To opisuje t. i. »human in the loop«, kjer so inteligentni sistemi zasnovani tako, da povečajo ali izboljšajo vlogo človeka, in UI služi kot orodje, ki ga je mogoče uporabljati prek človeške interakcije. V bistvu gre za združevanje UI in človeškega znanja. McCabe trdi, da lahko ljudje UI zagotovijo kontekst pri analizi, prispevajo vpoglede, ki temeljijo na izkušnjah, ki jih UI morda ne bi upoštevala, ter sprejemajo končne odločitve, ki vključujejo širši spekter dejavnikov. Prav tako lahko ocenijo pravilnost njenih ugotovitev, prepoznajo napake ter pomagajo pri izboljšanju in prilagajanju algoritmov (McCabe, 2024).

Dodatno sta Stockhem in Fourcans opozorili, da poleg splošnih strukturnih vprašanj obstajajo tudi specifični izzivi. Osebe z invalidnostjo npr. pričakujejo prilagoditve pri zaposlitvenih razgovorih, a ni jasno, kako bodo orodja UI zagotovila enako obravnavo. Prav tako je odprto vprašanje varstva poslovnih skrivnosti – Direktiva (EU) 2016/943⁶ ščiti algoritmične sisteme in UI v upravljanju kadrov kot poslovno skrivnost, kar lahko omeji dostop do informacij, potrebnih za dokazovanje diskriminacije. Praktične težave vključujejo tudi spremenljivost sistemov UI, saj se lahko diskriminatorni učinki pojavijo le v določenih obdobjih, zato je ključno voditi podrobno

⁵ 14. člen Akta o UI določa, da morajo visokotvegani sistemi UI biti zasnovani in razviti tako, da jih lahko fizične osebe v obdobju njihove uporabe učinkovito nadzorujejo, tudi z ustreznimi vmesniškimi orodji človek – stroj.

⁶ Direktiva (EU) 2016/943 Evropskega parlamenta in Sveta z dne 8. junija 2016 o varstvu nerazkritih strokovnih znanj in izkušenj (poslovnih skrivnosti) pred njihovim nezakonitim pridobivanjem, uporabo in razkritjem. 2016. Uradni list Evropske unije L 157, str. 1–18.

dokumentacijo o razvoju algoritmov skozi čas, da bi zagotovili preglednost in možnost preverjanja (Stockhem & Fourcans, 2023).

Z neposredno obravnavo teh izzivov lahko delodajalci utrejo pot v prihodnost, v kateri tehnologija podpira resnično pravičnost pri zaposlovanju (Women of Influence, 2025), vendar samoregulacija nima zavezujoče moči, zato sta potrebna zunanje nadzorovanje preko testiranja s strani tretjih oseb ter razvoj načel, zakonov in predpisov UI s strani zunanjih regulatorjev (Chen, 2023).

4 Regulativni okvir na ravni EU

Prepoved diskriminacije in načelo enake obravnave sta trdno zasidrana v temeljih EU (Peče, 2023, str. 128). Na evropski ravni že veljajo številni pravno zavezujoči predpisi, ki urejajo razvoj, uvajanje in uporabo umetnointeligenčnih sistemov ali so zanje pomembni. Med ključne pravne vire sodijo primarna zakonodaja EU, kot sta Pogodbi Evropske unije⁷ in Listina EU o temeljnih pravicah (v nadaljevanju: Listina EU)⁸, ter sekundarna zakonodaja EU⁹ (European Parliamentary Research Service, 2022, str. 9–10).

V 2. členu PEU je določeno, da EU »temelji na vrednotah spoštovanja človekovega dostojanstva, svobode, demokracije, enakosti, pravne države in spoštovanja človekovih pravic, vključno s pravicami pripadnikov manjšin« ter da to skupno družbo držav članic označujejo pluralizem, nediskriminacija, strpnost, pravičnost, solidarnost ter enakost moških in žensk. Tovrsten princip

⁷ Glede na velik vpliv, ki ga lahko ima UI na družbo, in potrebo po vzpostavitvi zaupanja je bistveno, da se UI in njen regulativni okvir razvijata v skladu z vrednotami Unije iz člena 2 PEU, temeljnimi pravicami in svoboščinami, ki so zapisane v Pogodbah, in, na podlagi člena 6 PEU, v Listini EU (6. uvodna točka Akta o UI).

⁸ Listina Evropske unije o temeljnih pravicah. 2016. Uradni list Evropske unije C 326, str. 389–405.

⁹ Za okvir predmetnega prispevka velja navesti, da področje diskriminacije med drugim naslavlja: Direktiva (EU) 2024/1499 o standardih za organe za enakost na področju enakega obravnavanja oseb, Direktiva (EU) 2024/1500 o standardih za organe za enakost na področju enakega obravnavanja in enakih možnosti za ženske in moške v zadevah zaposlovanja in poklica, Direktiva 2000/43/ES – izvajanje načela enakega obravnavanja ne glede na raso ali narodnost, Direktiva 2006/54/ES o uresničevanju načela enakih možnosti ter enakega obravnavanja moških in žensk pri zaposlovanju in poklicnem delu, Direktiva 2010/41/EU Evropskega parlamenta in Sveta z dne 7. julija 2010 o uporabi načela enakega obravnavanja moških in žensk, ki opravljajo samostojno dejavnost, Direktiva Sveta 2000/78/ES z dne 27. novembra 2000 o splošnih okvirih enakega obravnavanja pri zaposlovanju in delu, ki zagotavlja enako obravnavo oseb glede na vero ali prepričanje, invalidnost, starost ali spolno usmerjenost na delovnem mestu ter preprečuje diskriminacijo na teh podlagah.

je nadalje poudarjen v 2. odstavku 3. člena PEU, kjer je določeno, da se EU bori proti izključenosti in diskriminaciji (Peče, 2023, str. 128).

Nadalje je pomembna Listina EU, ki ima enako pravno veljavo kot Pogodbi EU. To pomeni, da je treba vso sekundarno zakonodajo EU in nacionalno zakonodajo, ki izvaja pravo EU, razlagati v skladu z določbami Listine EU. Na podlagi teh določb je treba pri ocenjevanju obstoječe zakonodaje EU v povezavi z uporabo UI na delovnem mestu nujno upoštevati tudi pravice iz Listine EU. EU ima torej obsežen nabor zakonodajnih instrumentov za preprečevanje diskriminacije. Pri tem je ključnega pomena 21. člen Listine EU, ki prepoveduje diskriminacijo na podlagi spola, rase, barve kože, etničnega ali socialnega izvora, genetike, jezika, vere, političnega prepričanja, lastnine, invalidnosti, starosti ali spolne usmerjenosti. Ta člen služi kot »krovna določba«, ki omogoča usklajevanje navedenih direktiv, hkrati pa ni pomemben zgolj zaradi neposredne prepovedi diskriminacije, temveč zaradi jasne opredelitve lastnosti, na katerih temeljijo skupine, ki jih je v boju zoper diskriminacijo treba zaščititi (European Parliamentary Research Service, 2022, str. 47–59; Peče, 2023, str. 129).

Zakonodaja EU o preprečevanju diskriminacije temelji na načelu, da namen diskriminacije ni relevanten. To pomeni, da tudi če razvijalci UI niso nameravali diskriminirati, je uporaba zaščitnih osebnih lastnosti (npr. spola, starosti) kot spremenljivk lahko diskriminatorna.¹⁰ Izvajanje zakonodaje pa je v praksi zahtevno. Ključni izziv predstavlja razlika med neposredno in posredno diskriminacijo. Neposredna diskriminacija pomeni, da je ena skupina delavcev obravnavana slabše od druge v primerljivi situaciji na podlagi zaščitnih značilnosti (kot je starost, rasa ali invalidnost). Posredna diskriminacija pa zajema na videz nevtralne prakse, ki določene skupine

¹⁰ V zvezi z navedenim poročilo Evropskega parlamenta navaja zadevo »Frank« pri podjetju Deliveroo, kjer je algoritem samodejno znižal oceno kurirjev, ki so odpovedali izmeno manj kot 24 ur pred njenim začetkom. Ne glede na razlog odpovedi (bolezen, stavka) so vsi delavci utrpeli enake negativne posledice. Sodišče v Bologni je zato razsodilo, da gre za posredno diskriminacijo (European Parliamentary Research Service, 2022, str. 60).

neporocionalno postavljajo v slabši položaj¹¹ (European Parliamentary Research Service, 2022, str. 60).¹²

Večinoma se diskriminacija uveljavlja prek individualnih tožb, vendar je avtomatizirana diskriminacija pogosto abstraktna, subtilna in težko zaznavna. To zmanjšuje verjetnost, da bodo iskalci zaposlitve in delavci sploh prepoznali krivico in ukrepali. Tudi če posamezniki sumijo na diskriminacijo, morajo pred sodiščem dokazati vsaj *prima facie* diskriminacijo – statistične razlike, iz katerih bi se dalo sklepati na diskriminacijo, kar dodatno oteži dostop do sodnega varstva pravic.¹³ Uspešnost individualnih sodnih primerov na tem področju bo torej v veliki meri odvisna od tega, kako enostavno je obrniti dokazno breme – opaziti, da vodja diskriminira nosečnice, je npr. eno, ugotoviti, ali tehnologija UI napoveduje verjetnost nosečnosti in to vpliva na zaposlitvene odločitve, pa je drugo in veliko težje (European Parliamentary Research Service, 2022, str. 60). V tem kontekstu Bagari izpostavlja, da mora delodajalec, ne glede na način izbire kandidata, tudi če pri tem uporablja algoritme, spoštovati določbe, ki omejujejo njegovo pogodbeno svobodo pri izbiri kandidata (Bagari, 2022, str. 44).¹⁴

¹¹ Sodišče Evropske unije je prvič prepoznalo posredno diskriminacijo v zadevi Sotgiu (C-152/73) v povezavi z osebno okoliščino državljanstva. Sodba se je nanašala na pravilo, po katerem so delavci, zaposleni v kraju, oddaljenem od njihovega prebivališča, prejeli višje nadomestilo za ločeno življenje, če so imeli ob začetku zaposlitve prebivališče v Nemčiji, medtem ko so delavci iz drugih držav prejeli nižje nadomestilo. Čeprav je bil predpis na prvi pogled nevtralen glede na državljanstvo, je Sodišče ugotovilo, da so v praksi zaposleni iz drugih držav članic zaradi tega prejeli manj ugodno obravnavo (Kogovšek Šalamon, 2016, str. 533).

¹² Pojem tako neposredne kot tudi posredne diskriminacije je podan v drugem odstavku 2. člena Direktive 2000/78/ES o splošnih okvirih enakega obravnavanja pri zaposlovanju in delu (za podrobnejšo opredelitev glej 2. odst. 2. člena predmetne Direktive). Po določilu prvega odstavka tega člena obe predstavljata kršitev načela enakega obravnavanja, v smislu te direktive (European Parliamentary Research Service, 2022, str. 60).

¹³ Ko tožnik predloži dovolj dokazov, se dokazno breme prenese na toženo stran, ki mora dokazati, da njihovi algoritmi delujejo na podlagi objektivnih, nediskriminatornih dejavnikov. Čeprav GDPR daje pravico do dostopa do informacij in pojasnil v primeru avtomatiziranega odločanja, je lahko kljub temu izjemno težko zbrati zadostne dokaze o diskriminaciji. Kljub temu je prag *prima facie* dokazov ključen, saj prisili lastnike sistemov UI, da predložijo podrobnejše dokaze. Sodišča bi lahko, kot v primeru sodbe CJEU v zadevi Danfoss, obravnavala nepripravljenost uporabnikov UI za razkritje informacij kot razlog za prenos dokaznega bremena nanje (European Parliamentary Research Service, 2022, str. 60).

¹⁴ Na nacionalni ravni (po slovenskem pravu) to vključuje določbe, kot je 9. člen Zakona o delovnih razmerjih (ZDR-1), ki omejujejo svobodo pri izbiri pogodbenih strank, in druge zakonske prepovedi. Med najpomembnejšimi sta prepoved diskriminacije po 6. členu ZDR-1 in obveznost predhodne javne objave prostega delovnega mesta po 25. členu ZDR-1.

V nadaljevanju (poglavje 4.1) bomo izmed zavezujočih pravnih virov na ravni EU podrobnejšo pozornost namenili Aktu o umetni inteligenci (v nadaljevanju: Akt o UI),¹⁵ ki določa pravila za uporabo sistemov UI v EU ter posledično vsebuje relevantna specialna pravna pravila, ki naslavljajo problematiko diskriminacije v zvezi z uporabo UI pri zaposlovanju. Zaradi omejenega obsega prispevka zgoraj omenjenega primarnega in sekundarnega (relevantne direktive EU s področja diskriminacije itd.) prava EU (vključno z relevantno sodno prakso Sodišča EU), ki se nanaša na področje diskriminacije v zvezi z delom, v nadaljevanju ne bomo podrobneje obravnavali¹⁶. V drugem delu (poglavje 4.2) pa bomo obravnavali še nekatere vire mehkega prava EU in politične strateške dokumente na področju UI (na ravni EU), ki naslavljajo problematiko diskriminacije v zvezi z uporabo UI pri zaposlovanju.

4.1 Akt o umetni inteligenci

Po mnenju Weingerl so nekatere države že začele sprejemati zakonodajo v zvezi z uporabo UI pri iskanju, preverjanju, intervjujih in zaposlovanju kandidatov zaradi težav z algoritemsko diskriminacijo, predvsem na podlagi rase in spola, ki je že vgrajena v programsko opremo. V to smer gre tudi EU s t. i. Aktom o UI, ki določa pravila za uporabo sistemov UI v EU. Sistemi UI so razvrščeni glede na potencialna tveganja (angl. *risk-based approach*).¹⁷ Akt o UI tako razlikuje med uporabami UI, ki ustvarjajo (i) nesprejemljivo tveganje, (ii) veliko tveganje in (iii) majhno tveganje

Delodajalci morajo zagotoviti, da pri uporabi algoritmov ne kršijo pravic kandidatov, zlasti v zvezi z diskriminacijo, in da so postopki zaposlovanja transparentni in pošteni (Bagari, 2022, str. 44).

¹⁵ Uredba (EU) 2024/1689 Evropskega parlamenta in Sveta z dne 13. junija 2024 o določitvi harmoniziranih pravil o umetni inteligenci in spremembi uredb (ES) št. 300/2008, (EU) št. 167/2013, (EU) št. 168/2013, (EU) 2018/858, (EU) 2018/1139 in (EU) 2019/2144 ter direktiv 2014/90/EU, (EU) 2016/797 in (EU) 2020/1828 (Akt o umetni inteligenci). 2024. Uradni list Evropske unije L 2024/1689.

¹⁶ Za podrobnejšo obravnavo relevantnega primarnega in sekundarnega prava (vključno z relevantno sodno prakso Sodišča EU) v zvezi s problematiko diskriminacije pri zaposlovanju glej, med drugim: European Union Agency for fundamental rights, 2014; Evropska komisija, 2012; Dolenc, 2011; Evropska komisija, 2015; Trstenjak, 2010; Kogovšek Šalamon, 2016; Zagovornik načela enakosti, 2023; Evropska komisija, 2020. Ključne zadeve iz sodne prakse Sodišča EU s tega področja so, med drugim: Sodišče EU, 2005; Sodišče EU, 2008a; Sodišče EU, 2008b; Sodišče EU, 2011; Sodišče EU, 2013a; Sodišče EU, 2013b; Sodišče EU, 2014; Sodišče EU, 2017a; Sodišče EU, 2017b; Sodišče EU, 2018.

¹⁷ Znotraj Akta o UI je zajeta Okvirna konvencija Sveta Evrope o UI in človekovih pravicah, demokraciji in pravni državi, ki zagotavlja mednarodni okvir za obvladovanje tveganj UI ter usklajevanje z demokratičnimi vrednotami. Njena načela veljajo za vse faze življenjskega cikla UI, pri čemer lahko zasebni akterji izbirajo med neposredno uporabo obveznosti ali drugimi ustreznimi ukrepi. Predvideva izjeme za raziskave, razvoj in nacionalno varnost (Evropska komisija, 2025c).

(Weingerl, 2023, str. 368), pri čemer so nekateri, kot so orodja (z nesprejemljivim tveganjem) za prepoznavanje čustev na delovnem mestu in družbeno točkovanje, prepovedani. Nekateri sistemi UI, ki se uporabljajo v zaposlovanju, so zaradi njihovega pomembnega škodljivega vpliva temeljne pravice obravnavani kot visoko tveganje. V 57. uvodni točki je izpostavljeno, da bi bilo treba šteti sisteme UI, uporabljene pri zaposlovanju in izboru oseb ter za sprejemanje odločitev, kot visoko tvegane, saj lahko občutno vplivajo na poklicne možnosti, preživetje in pravice delavcev.¹⁸

Nadalje iz Akta UI izhaja, da je za sisteme UI ključno, da so osredotočeni na človeka. Morala bi biti orodja za ljudi, končni cilj pa bi moral biti povečanje njihove blaginje.¹⁹ Delodajalci, ki uvajajo visokotvegane sisteme UI, morajo sprejeti ustrezne tehnične in organizacijske ukrepe ter zagotoviti človeški nadzor usposobljenih oseb – omogočeno mora biti, da rezultat preverita vsaj dve fizični osebi²⁰ – ter vodenje evidence.²¹ Pred uvedbo sistema morajo obvestiti delavce in njihove predstavnike.²² Prav tako lahko od ponudnika zahtevajo EU izjavo EU o skladnosti za vsak visokotvegani sistem UI, ki jo morajo hraniti in omogočiti dostop nacionalnim organom še deset let po uvedbi sistema.²³

Predvsem pa je treba izpostaviti točko b) 1. odstavka 5. člena (»Prepovedane prakse UI«)²⁴, ki določa, da je prepovedano dajati na trg, v uporabo ali uporabljati sistem UI, ki izkorišča katere koli

¹⁸ To vključuje UI za izbiro kandidatov, odločanje o delovnih pogojih, napredovanju, odpovedi pogodb, dodeljevanje nalog ter spremljanje in ocenjevanje zaposlenih. Taki sistemi lahko ohranjajo diskriminatorne vzorce iz preteklosti glede spola, starosti, invalidnosti, rasnega ali etničnega porekla ter spolne usmerjenosti. Prav tako lahko UI za spremljanje učinkovitosti in vedenja delavcev ogroža njihove pravice do zasebnosti in varstva podatkov (44. uvodna točka Akta o UI).

¹⁹ Glej 6. uvodno točko Akta o UI.

²⁰ Visokotvegani sistemi UI morajo omogočati človeški nadzor v celotnem življenjskem ciklu. Ponudniki morajo pred uvedbo določiti ustrezne ukrepe, kot so operativne omejitve, odzivnost na človeškega operaterja ter usposobljenost nadzornikov. Sistem mora vključevati mehanizme za obveščanje nadzornikov o potrebi po posredovanju ali zaustavitvi delovanja ob nepravilnostih. Pri biometrični identifikaciji morata rezultat preveriti vsaj dve fizični osebi, razen če bi to povzročilo nesorazmerne ovire v kazenskih preiskavah, nadzoru meje ali azilu (73. uvodna točka Akta o UI).

²¹ 12. člen Akta o UI določa vodenje evidence visokotveganih sistemov, in sicer samodejno beleženje dogodkov oz. dnevnikov.

²² Glej 26. člen Akta o UI.

²³ Glej 47. člen Akta o UI.

²⁴ Na podlagi Smernic o prepovedanih praksah UI. Te zagotavljajo pregled praks UI, ki veljajo za nesprejemljive zaradi morebitnih tveganj za evropske vrednote in temeljne pravice. Smernice so oblikovane z namenom zagotavljanja dosledne, učinkovite in enotne uporabe Akta o UI po celotni EU. Čeprav nudijo dragocen vpogled v interpretacijo prepovedi s strani Komisije, niso pravno zavezujoče, saj je verodostojna razlaga pridržana Sodišču Evropske unije.

šibke točke fizične osebe ali določene skupine oseb zaradi njihove starosti, invalidnosti ali posebnega socialnega ali ekonomskega položaja s ciljem ali učinkom bistvenega izkrivljanja vedenja te osebe ali osebe iz te skupine na način, ki tej ali drugi osebi povzroči znatno škodo ali za katerega obstaja razumna verjetnost, da bo povzročil znatno škodo (Evropska komisija, 2025b).²⁵

Obenem pa Akt o UI nalaga obveznosti za sisteme z visokim tveganjem, ki zahtevajo pripravo, izvajanje in stalni nadzor. Ti vključujejo sisteme UI za zaposlovanje, vključno s ciljno usmerjenimi oglasi, analizo prijav in ocenjevanjem kandidatov, kot tudi sisteme UI za odločanje o delovnih pogojih, napredovanju, prekinitvi zaposlitve, dodeljevanju nalog ter za spremljanje uspešnosti in vedenja zaposlenih.²⁶ Akt o UI uvaja jasen, na tveganju temelječ regulativni okvir za razvijalce in uvajalce UI, ki določa pravila za njeno specifično uporabo (Evropska komisija, 2024a), zato morajo delodajalci, ki uporabljajo sisteme UI za preverjanje kandidatov, ocenjevanje zaposlenih in drugo odločanje v zvezi z zaposlovanjem v EU, sprejeti ustrezne ukrepe za izpolnjevanje zahtev Akta o UI v zvezi z uporabo sistemov UI z visokim tveganjem (Hunton, 2024).

Nadalje velja omeniti, da se postavlja vprašanje odškodninske odgovornosti delodajalca – v kolikor se kljub varovalkam, ki jih predvideva zakonodaja, tveganja vseeno uresničijo in se preko uporabe sistemov UI kandidatom in delavcem povzroči škoda (Weingerl, 2023, str. 370).²⁷ Glede tematike odgovornosti je bila 28. septembra 2022 predlagana tudi Direktiva o odgovornosti za umetno inteligenco,²⁸ ki je bila mišljena kot dopolnitev k Aktu o UI, ki določa, da so uvajalci in uporabniki lahko odgovorni, če zaradi njihove napake nastane škoda. Ta napaka je lahko dejanje ali opustitev, tudi kadar uvajalci ali uporabniki niso spoštovali svoje dolžnosti skrbnega ravnanja in niso sprejeli ravnanja, da bi se izognili škodi »pravnim interesom«, kot so temeljne pravice.

Vsebujejo pravna pojasnila in praktične primere, ki deležnikom pomagajo pri razumevanju in izpolnjevanju zahtev akta (Evropska komisija, 2025a).

²⁵ 29. uvodna točka Akta o UI določa, da sistemi UI lahko tudi sicer izkoriščajo šibke točke določene osebe ali skupine oseb zaradi njihove starosti, invalidnosti (v smislu Direktive (EU) 2019/882 Evropskega parlamenta in Sveta) ali posebnih socialnih ali gospodarskih razmer, zaradi katerih so te osebe verjetno bolj izpostavljene izkoriščanju – denimo osebe, ki živijo v skrajni revščini, ter etnične ali verske manjšine.

²⁶ Skladno z 2. odst. 6. člena in Prilogo III Akta o UI.

²⁷ Podrobneje o tem problemu glej: Weingerl, 2023, ter Lešnik in Weingerl, 2024. Za več o izzivih odškodninske odgovornosti v zvezi z uporabo sistemov UI glej tudi Weingerl, 2020.

²⁸ Evropska komisija je 11. februarja 2025 v »delovnem programu 2025« razkrila, da bo umaknila omenjeni predlog direktive in napovedala, da bo preučila potrebo po novem predlogu ali alternativnem pristopu k urejanju odgovornosti za UI (Evropska komisija, 2025a).

Predlagana Direktiva je vključevala tudi posebne določbe za sisteme UI z visokim tveganjem, in sicer bi nacionalna sodišča lahko odredila razkritje dokazov in v primeru nerazkritja s strani tožene stranke odločila na podlagi domneve o neizpolnjevanju dolžnosti skrbnega ravnanja tožene stranke. Nacionalna sodišča bi lahko sklepala tudi na domneve vzročne zveze med krivdo in škodo, če bi bili izpolnjeni nekateri pogoji. Predlagana direktiva o odgovornosti za UI pa se ne bi nanašala na obstoječo zaščito pred zakoni EU o enakosti, ki dokazno breme v primeru diskriminacije pri zaposlovanju prelaga na delodajalca (Stockhem & Fourcans, 2023). Iz preambule predloga direktive sicer izhaja, da bi se njena uporaba lahko omejila le na škodo, ki nastane v primeru popolnoma avtomatiziranega sprejemanja odločitev, kar spominja na 22. člen GDPR (Weingerl, 2023, str. 375).

4.2 Nezavezujoči viri, sprejeti na ravni EU na področju UI

Za naslovitev obravnavane problematike so relevantni tudi nekateri drugi viri mehkega prava EU oz. drugi dokumenti, sprejeti na ravni EU. Pomembno je denimo upoštevati Smernice politike zaposlovanja, ki so bile sprejete na podlagi 148. člena PDEU in ki so usklajene z evropskim stebrom socialnih pravic. Med njimi izstopa tudi spodbujanje enakih možnosti z obravnavanjem neenakosti v sistemih spodbujanja vključujočih trgov dela z ukrepi za boj proti diskriminaciji in spodbujanje enakih možnosti ter zagotavljanje enake obravnave za skupine, ki so premalo zastopane pri zaposlovanju (Evropska komisija, 2022).

Nadalje je Evropska komisija leta 2018 imenovala skupino strokovnjakov za svetovanje o njeni strategiji UI (AI HLEG) (Evropska komisija, 2024b). Kot izstopajoč končni izdelek omenjene skupine so leta 2019 bile sprejete Etične smernice za zaupanja vredno UI (Evropska komisija, 2019). Slednje temeljijo na sedmih načelih, ki vključujejo človeško delovanje in nadzor,²⁹ tehnično robustnost in varnost, zasebnost in upravljanje podatkov, preglednost³⁰, raznolikost,

²⁹ V skladu s smernicami AI HLEG človeško delovanje in nadzor pomeni, da se sistemi UI razvijajo in uporabljajo kot orodje, ki služi ljudem, spoštuje človeško dostojanstvo in osebno avtonomijo ter deluje tako, da ga ljudje lahko ustrezno upravljajo in nadzorujejo (27. uvodna točka Akta o UI).

³⁰ Preglednost pomeni, da se sistemi UI razvijajo in uporabljajo na način, ki omogoča ustrezno sledljivost in razločljivost, obenem pa so ljudje seznanjeni s tem, da komunicirajo ali da so v stiku s sistemom UI, uvajalci so ustrezno obveščeni o zmogljivostih in omejitvah zadevnega sistema UI, osebe, na katere vpliva sistem UI, pa o svojih pravicah (27. uvodna točka Akta o UI).

nediskriminacijo in pravičnost³¹ ter družbeno in okoljsko blaginjo in odgovornost. Cilj smernic je zagotavljanje UI, osredotočene na človeka, v izboljšanju blaginje in skupnega dobrega. Pilotni seznam za ocenjevanje zaupanja vredne UI vključuje test diskriminacije, ki zahteva strategijo za preprečevanje pristranskosti v podatkih in algoritmihi, spremljanje pristranskosti skozi celoten življenjski cikel sistema ter mehanizme za prijavo diskriminacije. Prav tako poudarja raznolikost in reprezentativnost uporabnikov, testiranje na posebnih populacijah, zagotavljanje dostopnosti za invalide ter vključevanje ranljivih skupin v razvoj sistema. Poleg tega spodbuja sodelovanje deležnikov in delavcev pri uvedbi UI ter oceno njenega vpliva na temeljne pravice uporabnikov (Strokovna skupina na visoki ravni za umetno inteligenco, 2018).

Natančneje je eden izmed temeljev zaupanja vredne UI tudi enakost, nediskriminacija in solidarnost. Kot izhaja iz 44. točke Etičnih smernic za zaupanja vredno umetno inteligenco, je treba zagotoviti *»enako spoštovanje moralne vrednosti in dostojanstva vseh ljudi. To presega nediskriminacijo, ki dopušča razlikovanje med različnimi situacijami na podlagi objektivnih razlogov. Pri UI enakost pomeni, da delovanje sistema ne more dati nepošteno pristranskih rezultatov (npr. podatki, ki se uporabljajo za učenje sistemov UI, bi morali biti čim bolj vključujoči in predstavljati različne skupine prebivalstva). Za to je potrebno tudi ustrezno spoštovanje potencialno ranljivih oseb in skupin, kot so delavci, ženske, invalidi, etnične manjšine, otroci, potrošniki ali druge osebe, ki jim grozi izključenost«* (Strokovna skupina na visoki ravni za umetno inteligenco, 2018, str. 13).

Na področju uporabe UI v delovnih razmerjih pa so bili na ravni EU aktivni tudi socialni partnerji. Evropski socialni partnerji so v Okvirnem sporazumu o digitalizaciji iz leta 2020 določili, da mora uvajanje sistemov UI slediti načelu *»človek nadzoruje UI«* ter biti pregledno, razumljivo in imeti učinkovit nadzor. Kolektivno dogovarjanje in sindikalne pobude so lahko učinkovit način za uresničevanje obstoječih pravnih varovalk pred tveganji algoritmičnega upravljanja ter za prilagajanje hitremu razvoju UI. Posamezni delavci lahko imajo težave pri uveljavljanju svojih pravic, npr. pri dostopu do svojih podatkov in preverjanju njihove obdelave, medtem ko lahko kolektivne pravice delavcev okrepijo zaščito ter jim pomagajo uveljavljati njihove interese. Če

³¹ Raznolikost, nediskriminacija in pravičnost pomenijo, da se sistemi UI razvijajo in uporabljajo na način, ki vključuje različne akterje in spodbuja enakopraven dostop, enakost spolov in kulturno raznolikost, hkrati pa se preprečujejo diskriminatorni učinki in nepravilni predsodki, ki jih pravo Unije ali držav članic prepoveduje (27. uvodna točka Akta o UI).

socialni partnerji dosežejo skupno razumevanje težav in rešitev ter imajo potrebna znanja in sredstva za njihovo uveljavitev, lahko kolektivne pogodbe določijo omejitve nadzora UI in izboljšajo preglednost odločanja, ki ga podpira UI, ob upoštevanju interesov tako delavcev kot delodajalcev. Sindikati so že začeli »pogajanja o algoritmih« v različnih evropskih državah z različnimi industrijskimi modeli. Evropska sindikalna konfederacija (UNI Europa) vodi podatkovno bazo kolektivnih pogodb, ki vključujejo določbe o UI in algoritmičnem upravljanju, trenutno s 23 dogovori. Poročilo navaja, da bi se predstavniki delavcev morali osredotočiti na implementacijo UI na ravni podjetij, kjer se lahko interesi delavcev upoštevajo že v fazi načrtovanja, razvoja in uporabe algoritmičnih sistemov (Evropski parlament, 2024, str. 6).

Pri zaposlovanju, ocenjevanju in odpuščanju sta tako ključni transparentnost in možnost človeškega posredovanja. Delavci morajo imeti pravico izpodbijati odločitve, ki jih sprejme UI, ter zahtevati neodvisno preverjanje rezultatov (ZSSS, 2022).

5 Sklep

Na podlagi vsega obravnavanega se glede uporabe UI pri zaposlovanju pojavlja ključna dilema med učinkovitostjo avtomatiziranega odločanja in (sistemskim) tveganjem diskriminacije – za katerega je treba zagotoviti ustrezne pravne varovalke. Uporaba UI v postopkih zaposlovanja bo postala čedalje bolj razširjena, saj si bodo podjetja prizadevala za optimizacijo svojega poslovanja.

Iz obravnavane literature tako izhajajo primeri uporabe v različnih fazah zaposlovanja – fazi iskanja oz. oglaševanja delovnega mesta, fazi prijave na delovno mesto ter pregledovanja prijav, fazi razgovora in fazi izbire kandidata. V vseh navedenih položajih pa prihaja do sistemskih tveganj za manj ugodno (diskriminatorno) obravnavo kandidatov na podlagi njihovih osebnih okoliščin (npr. spola, starosti, rase, etnične pripadnosti itd.). Sistemi UI lahko npr. avtomatsko prikazujejo oglase določenim demografskim skupinam, s čimer posredno izključujejo druge kandidate. Prav tako lahko ti sistemi zavrnejo kandidate na podlagi nerelevantnih podatkov, ki so povezani z njihovim spolom, starostjo ali drugimi zaščitnimi lastnostmi. Konkretni obravnavani primer tovrstne slabe prakse je denimo postopek Komisije za enake zaposlitvene možnosti (EEOC) iz ZDA proti iTutorGroup zaradi uporabe sistema UI, ki je iz prijav samodejno zavrnil prijaviteljice, stare 55 let ali več, in prijavitelje, stare 60 let ali več.

Nadalje se ugotavlja, da iz obravnavane literature izhajajo številni konkretni predlogi za naslovitev problematike diskriminacije v zvezi z uporabo UI pri zaposlovanju. Veliko lahko podjetja naredijo že sama – ključno je namreč upoštevati, da sisteme UI (ne glede na njihovo avtonomnost) v končni fazi še zmeraj uporablja človek. Eden izmed ukrepov je ustrezno usposabljanje zaposlenih, ki bi morale zajemati osnove razumevanja UI, prepoznavanje pristranskosti v sistemih UI ter strategije za ublažitev le-teh. Prav tako je pomembno sodelovanje različnih deležnikov (IT-strokovnjakov, kadrovskih strokovnjakov itd.) že pri razvoju sistemov UI. Primer dobre prakse je tudi izvajanje certifikacije in redne revizije morebitne pristranskosti uporabljenih sistemov UI. Prav proaktivni pristop z rednim pregledovanjem in posodabljanjem algoritmov UI lahko pripomore k prepoznavi in odpravi vseh pristranskosti, ki so nenamerno vgrajene v sistem.

Ključne varovalke za naslovitev problematike diskriminacije pri zaposlovanju pa izhajajo iz zavezujočega pravnega okvira. Iz prispevka izhaja, da je na ravni EU dobro razvit pravni okvir varstva pred diskriminacijo. Večji problem se lahko pojavi pri njegovem uveljavljanju v praksi, saj morajo kandidati izkazati vsaj dejstva, ki nakazujejo na obstoj diskriminacije (na delodajalcu pa je potem obrnjeno dokazno breme, da dokaže, da do diskriminacije ni prišlo). Glede uveljavljanja pravnega varstva s strani kandidatov se lahko zgodi, da slednji zanj pogosto niti ne bodo zainteresirani, saj sploh ne bodo vedeli, da so bili v postopkih zaposlovanja uporabljeni sistemi UI, katerih delovanje je bilo (vsaj potencialno) manj ugodno za kandidate določene osebne okoliščine (starosti, spola itd.). Posledično je ključna varovalka transparentnost glede morebitne uporabe sistemov UI pri zaposlovanju. Že na ta način se lahko v ključni meri pripomore k preprečevanju diskriminacije v praksi. Delodajalci bodo namreč vedeli, da se ne morejo preprosto zanašati na avtomatizirano sprejete odločitve, saj bo treba v konkretnem primeru izbire kandidata tudi potencialno dobro utemeljiti (ne)izbiro kandidatov. V nasprotnem primeru jih namreč lahko doleti odškodnina zaradi kršitve prepovedi diskriminacije. Pri odločitvi bi tako zagotovo moral v končni fazi ključno vlogo odigrati človek. Prav tako zahteva po transparentnosti pomeni tudi možnost revizijskega vpogleda v delovanje sistemov UI v okviru sodnega postopka. Posledično se delodajalcem jasno sporoča, da bo morebitna uporaba UI z njegove strani spremljana ter v primeru prepovedanega načina uporabe (npr. kršitev prepovedi diskriminacije ipd.) tudi sankcionirana.

Predvsem pa je na ravni EU ključnega pomena tudi pravni okvir, ki se specifično nanaša na uporabo sistemov UI, predvsem Akt o UI. Področje UI sicer naslavljajo tudi nekateri pravni

instrumenti mehkega prava, od katerih je z vidika delovnega prava in delovanja socialnih partnerjev na evropski ravni najrelevantnejši Okvirni sporazum o digitalizaciji iz leta 2020. Iz slednjega izhaja, da mora uvajanje sistemov UI slediti načelu »človek nadzoruje UI« ter biti pregledno, razumljivo in imeti učinkovit nadzor. Pri vsem navedenem lahko v okviru podjetja pomembno vlogo odigrajo tudi socialni partnerji.

Nazadnje tako velja izpostaviti ključne pravne rešitve po Aktu o UI, ki bodo posegle tudi na področje problematike diskriminacije pri zaposlovanju. Pomembno je, da obveznosti uvajalcev sistemov UI (mednje sodijo tudi delodajalci) rastejo glede na stopnjo tveganja, v katero je umeščen posamezni sistem. Delodajalci, ki uvajajo visokotvegane sisteme UI, morajo sprejeti ustrezne tehnične in organizacijske ukrepe ter zagotoviti človeški nadzor usposobljenih oseb. Prav tako mora biti vodena evidenca uporabe tovrstnega sistema UI. Pred uvedbo sistema morajo obvestiti delavce in njihove predstavnike. Ključno je, da skladno s Prilogo III Akta o UI med visokotvegane sisteme UI sodijo sistemi UI za zaposlovanje, vključno s ciljno usmerjenimi oglasi, analizo prijav in ocenjevanjem kandidatov. Navedene določbe Akta o UI tako vsebujejo ključne varovalke, ki so tudi sicer izhajale iz obravnavane teorije – omogočanje revizijske sledi, transparentnost, človeški nadzor, vključitev delavcev in njihovih predstavnikov itd.

Čas bo pokazal, kako se bodo različni akterji soočili s problematiko diskriminacije v zvezi z uporabo UI pri zaposlovanju. Ključno bo, da se bo pravni okvir uveljavljal tudi v praksi. Raba UI bo na tem in na nešteto drugih področjih družbenega življenja korenito spremenila dosedanje prakse, vendar pa to ne sme pomeniti, da bodo posledice predstavljale množično kršenje človekovih pravic šibkejših posameznikov oz. tudi sicer izvotlitev temeljnih etičnih civilizacijskih standardov. Prav zato mora biti uporaba novih tehnologij ustrezno pravno regulirana – ter nadzorovana v praksi.

Literatura in viri

1. Acuna Ocana, N. (2023). *Will using AI lead to more discrimination in recruitment?* LinkedIn. <https://www.linkedin.com/pulse/using-ai-lead-more-discrimination-recruitment-nicky-acuna-ocana>
2. Arrowsmith, J., Intezari, A., Pauleen, D. J. & Soleimani, M. (2024). *What will a robot make of your résumé? The bias problem with using AI in job recruitment.* <https://theconversation.com/what-will-a-robot-make-of-your-resume-the-bias-problem-with-using-ai-in-job-recruitment-231174>
3. Bagari, S. (2022). Uporaba algoritmov na področju delovnih razmerij in socialne varnosti. *Delavci in delodajalci* 22, št.1. Inštitut za delo pri Pravni fakulteti Univerze v Ljubljani.
4. Canditech. (n.d.). *We understand both people and technology.* <https://www.canditech.io/technology/>

5. Chen, Z. (2023). Ethics and discrimination in artificial intelligence-enabled recruitment practices. *Humanities & Social Sciences Communications*, 10, 567. <https://www.nature.com/articles/s41599-023-02079-x>
6. Dolenc, P. (2011). *Diskriminacija na trgu dela v Sloveniji*. Fakulteta za management, Univerza na Primorskem. <https://www.dlib.si/stream/URN:NBN:SI:doc-06CXJJRN/b2b6ec26-35e6-4167-819b-ca9e57a98162/PDF>
7. ElMorsy, M. (2024). *8 pitfalls of AI-driven recruitment and how to overcome them*. CareerEdge. <https://www.careeredge.ca/8-pitfalls-of-ai-driven-recruitment-and-how-to-overcome-them/>
8. European Parliamentary Research Service. (2022). *AI and digital tools in workplace management and evaluation, An assessment of the EU's legal framework*. Scientific Foresight Unit (STOA). [https://www.europarl.europa.eu/RegData/etudes/STUD/2022/729516/EPRS_STU\(2022\)729516_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2022/729516/EPRS_STU(2022)729516_EN.pdf)
9. European Union Agency for Fundamental Rights, European Court of Human Rights – Council of Europe. (2014). *Handbook on European non-discrimination law*. https://fra.europa.eu/sites/default/files/fra_uploads/1510-FRA-CASE-LAW-HANDBOOK_EN.pdf
10. Evropska komisija. (2012). *Priročnik za usposabljanje o diskriminaciji*. https://www.migpolgroup.com/_old/public/docs/Slovenia.pdf
11. Evropska komisija. (2015). *Zavedajte se svojih pravic – zaščita pred diskriminacijo*. https://eur-lex.europa.eu/resource.html?uri=cellar:5a511c88-b218-47b5-9f3e-4709d650e28b.0023.03/DOC_1&format=PDF
12. Evropska komisija (2019). *Etične smernice za zaupanja vredno umetno inteligenco*. <https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai>
13. Evropska komisija. (2020). *Sporočilo Komisije Evropskemu parlamentu, Svetu, Evropskemu ekonomsko-socialnemu odboru in odboru regij, Unija enakosti: akcijski načrt EU za boj proti rasizmu 2020–2025*. <https://eur-lex.europa.eu/legal-content/SL/ALL/?uri=CELEX:52020DC0565>
14. Evropska komisija. (2022). *Smernice politike zaposlovanja za leto 2022–2023*. <https://eur-lex.europa.eu/SL/legal-content/summary/2022-2023-guidelines-on-employment-policies.html?fromSummary=17>
15. Evropska komisija. (2024a). *Akt o umetni inteligenci*. <https://digital-strategy.ec.europa.eu/sl/policies/regulatory-framework-ai>
16. Evropska komisija. (2024b). *Strokovna skupina na visoki ravni za umetno inteligenco*. <https://digital-strategy.ec.europa.eu/en/policies/expert-group-ai>
17. Evropska komisija (2025a). *Annexes to the Communication from the Commission to the European parliament, the Council, the European Economic and Social Committee and the Committee of the Regions*. https://commission.europa.eu/document/download/7617998c-86e6-4a74-b33c-249e8a7938cd_en?filename=COM_2025_45_1_annexes_EN.pdf
18. Evropska komisija (2025b). *Komisija je objavila smernice o prepovedanih praksah umetne inteligence, kot so opredeljene v aktu o umetni inteligenci*. <https://digital-strategy.ec.europa.eu/sl/library/commission-publishes-guidelines-prohibited-artificial-intelligence-ai-practices-defined-ai-act>
19. Evropska komisija (2025c). *Komisija je podpisala Okvirno konvencijo Sveta Evrope o umetni inteligenci in človekovih pravicah, demokraciji in pravni državi*. <https://digital-strategy.ec.europa.eu/sl/news/commission-signed-council-europe-framework-convention-artificial-intelligence-and-human-rights>
20. Evropski parlament. (2024). *Addressing AI risks in the workplace: Workers and algorithms*. [https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/762323/EPRS_BRI\(2024\)762323_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/762323/EPRS_BRI(2024)762323_EN.pdf)

21. Direktiva 2000/43/ES Sveta z dne 29. junija 2000 o izvajanju načela enakega obravnavanja ne glede na raso ali narodnost. (2000). *Uradni list Evropske unije L 180*, str. 22–26.
22. Direktiva 2000/78/ES Sveta z dne 27. novembra 2000 o splošnih okvirih enakega obravnavanja pri zaposlovanju in delu. (2000). *Uradni list Evropske unije L 303*, str. 16–22.
23. 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. (2006). *Uradni list Evropske unije L 204*, str. 23–36.
24. Direktiva 2010/41/EU Evropskega parlamenta in Sveta z dne 7. julija 2010 o uporabi načela enakega obravnavanja moških in žensk, ki opravljajo samostojno dejavnost. (2010). *Uradni list Evropske unije L 180*, str. 1–6.
25. Direktiva (EU) 2024/1499 Evropskega parlamenta in Sveta z dne 7. maja 2024 o standardih za organe za enakost na področju enakega obravnavanja oseb. (2024). *Uradni list Evropske unije L 2024/1499*.
26. Direktiva (EU) 2024/1500 Evropskega parlamenta in Sveta z dne 14. maja 2024 o standardih za organe za enakost na področju enakega obravnavanja in enakih možnosti za ženske in moške v zadevah zaposlovanja in poklica. (2024). *Uradni list Evropske unije L 2024/1500*.
27. Direktiva (EU) 2016/943 Evropskega parlamenta in Sveta z dne 8. junija 2016 o varstvu nerazkritih strokovnih znanj in izkušenj (poslovnih skrivnosti) pred njihovim nezakonitim pridobivanjem, uporabo in razkritjem. (2016). *Uradni list Evropske unije L 157*, str. 1–18.
28. Fisher Phillips. (2023). How is HR using AI? An employer's list of tools and potential pitfalls. <https://www.fisherphillips.com/en/news-insights/hr-using-ai-employers-list-tools-potential-pitfalls.html>
29. Franca, V. (2023). Ranotežje moči v dobi umetne inteligence: bodo kolektivne dogovore sklepali algoritmi? *Delavci in delodajalci* 23, št. 4. Inštitut za delo pri Pravni fakulteti Univerze v Ljubljani.
30. Goodman, R. (2018). Why Amazon's automated hiring tool discriminated against women. ACLU. <https://www.aclu.org/news/womens-rights/why-amazons-automated-hiring-tool-discriminated-against-women>
31. Hunton. (2024). The impact of the EU AI Act on human resources activities. <https://www.hunton.com/insights/legal/the-impact-of-the-eu-ai-act-on-human-resources-activities>
32. Katsioti, M., & Maratou, E. (2024). AI in talent acquisition: Legal considerations for modern recruitment in EU. Rokas. https://www.lexology.com/library/document/?tk=eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzUxMiJ9.eyJleHAiOiE3MzcycyMDA3MTgslmRhdGEiOnsiRG9jdW1lbnRHdWlkIjoiaNzViOWQwNTItZWmxOS00ZTgwLTkwOWltMWI2NDRI2Mzg0ODY5Iiwic3Nmb2dpbil6dHJ1ZX19.FL6xNq2q9d3uv4xzBCLCum3JJedIJGjBYl0fLWBWy_feaD-Wn2UOOPX2nlutFR6iTie5zp0ggygeD7QzZR0GPZw
33. Kempe, L. (2024). Navigating the AI employment bias maze: Legal compliance guidelines and strategies. American Bar Association. https://www.americanbar.org/groups/business_law/resources/business-law-today/2024-april/navigating-ai-employment-bias-maze/
34. Kogovšek Šalamon N. (2016). Disparitetni učinek posredne diskriminacije v pravu Evropske unije in Sveta Evrope ter v slovenski sodni praksi. *Pravnik* 133, št. 7–8. Zveza društev pravnikov Slovenije.
35. Lešnik, A., & Weingerl, P. (2024). Pravna ureditev odgovornosti za škodo, povzročeno z umetno inteligenco v Sloveniji. DIGITALNA EKONOMIJA IN PRAVO 2024 Študentsko posvetovanje o ekonomskih in pravnih izzivih digitalne preobrazbe, str. 120–132. Društvo ekonomistov Maribor.

36. Listina Evropske unije o temeljnih pravicah. (2016). *Uradni list Evropske unije* C 326, str. 389–405.
37. Lytton, C. (2024). *AI hiring tools may be filtering out the best job applicants*. BBC. <https://www.bbc.com/worklife/article/20240214-ai-recruiting-hiring-software-bias-discrimination>
38. McCabe, L. (2024). *Why keeping humans in the loop is key for AI in HR*. Medium. <https://medium.com/@lauriemccabe/why-keeping-humans-in-the-loop-is-key-for-ai-in-hr-8c559c89106d>
39. Garrison, M. (2024). *What is AI discrimination in recruitment and hiring?* NOLO. <https://www.nolo.com/legal-encyclopedia/what-is-ai-discrimination-in-recruitment-and-hiring.html>
40. Osborne Clarke. (2023). *Employers using AI to recruit skilled workers need to stay up-to-date in Germany*. <https://www.osborneclarke.com/insights/employers-using-ai-recruit-skilled-workers-need-stay-date-germany>
41. Oxley, L. (2023). *AI and recruitment: An invaluable tool, or source of discrimination?* Walker Morris. <https://www.walkermorris.co.uk/comment-opinion/ai-and-recruitment-an-invaluable-tool-or-source-of-discrimination/>
42. Peče, O. (2023). *ALGORITEMSKA DISKRIMINACIJA. Temeljne pravice in izzivi digitalizacije: Od pravne ureditve do prakse*. Univerza v Mariboru.
43. Raso, F. A., Hilligoss, H., Krishnamurthy, V. Bavitz, C., & Kim, L. (2018). *Artificial intelligence & human rights: Opportunities & risks*. *The Berkman Klein Center for Internet & Society at Harvard University*, 2018-6. <https://ssrn.com/abstract=3259344>
44. Rigotti, C. & Fosch-Villaronga, E. (2024). *Fairness, AI & recruitment*. *Computer Law & Security Review*, 53, 105966. <https://www.sciencedirect.com/science/article/pii/S0267364924000335>
45. Seppälä, P., & Matecka, M. (2024). *AI and discriminative decisions in recruitment: Challenging the core assumptions*. *Big Data & Society*, 11(1). <https://journals.sagepub.com/doi/10.1177/20539517241235872>
46. Sodišča Evropske unije. (2013a). *Sodba v zadevi Asociația Accept*, C-81/12 z dne 25. 4. 2013.
47. Sodišče Evropske unije. (2017a). *Sodba v zadevi Bougnaoui*, C-188/15 z dne 4. 3. 2017.
48. Sodišče Evropske unije. (2008a). *Sodba v zadevi Coleman*, C-303/06 z dne 17. 7. 2008.
49. Sodišče Evropske unije. (2008b). *Sodba v zadevi Feryn*, C-54/07 z dne 10. 7. 2008.
50. Sodišče Evropske unije. (2014). *Sodba v zadevi FOA*, C-354/13 z dne 18. 12. 2014.
51. Sodišče Evropske unije. (2017b). *Sodba v zadevi G4S Secure Solutions*, C-157/15 z dne 14. 3. 2017.
52. Sodišče Evropske unije. (2018). *Sodba v zadevi IR proti JQ*, C-68/17 z dne 11. 9. 2018.
53. Sodišče Evropske unije. (2013b). *Sodba v zadevi Kuso*, C-614/11 z dne 12. 9. 2013.
54. Sodišče Evropske unije. (2005). *Sodba v zadevi Mangold*, C-144/04 z dne 22. 11. 2005.
55. Sodišče Evropske unije. (2011). *Sodba v zadevi Prigge in drugi*, C-447/09 z dne 13. 9. 2011.
56. Stockhem, O., & Fourcans, C. (2023). *Discrimination in hiring: The case for alignment of the EU AI Act with EU equality laws*. Center for Democracy & Technology (CDT). <https://cdt.org/insights/discrimination-in-hiring-the-case-for-alignment-of-the-eu-ai-act-with-eu-equality-laws/>
57. Strokovna skupina na visoki ravni za umetno inteligenco. (2018). *Etične smernice za zaupanja vredno umetno inteligenco*. https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/JURI/DV/2019/11-06/Ethics-guidelines-AI_SL.pdf
58. Trstenjak, V. (2010). *Novejša sodna praksa sodišča EU na področju prepovedi diskriminacije pri zaposlovanju. Delavci in delodajalci 10*, št. 2/3. Inštitut za delo pri Pravni fakulteti Univerze v Ljubljani.

59. University of Cambridge. (2022). *Claims AI can boost workplace diversity are 'spurious and dangerous'; researchers argue*. <https://www.cam.ac.uk/research/news/claims-ai-can-boost-workplace-diversity-are-spurious-and-dangerous-researchers-argue>
60. U.S. Equal Employment Opportunity Commission (EEOC). (2023). *iTutorGroup to pay \$365,000 to settle EEOC discriminatory hiring suit*. <https://www.eeoc.gov/newsroom/itutorgroup-pay-365000-settle-eeoc-discriminatory-hiring-suit>
61. 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). (2016). *Uradni list Evropske unije* L 119/1, str. 1–88.
62. Uredba (EU) 2024/1689 Evropskega parlamenta in Sveta z dne 13. junija 2024 o določitvi harmoniziranih pravil o umetni inteligenci in spremembi uredb (ES) št. 300/2008, (EU) št. 167/2013, (EU) št. 168/2013, (EU) 2018/858, (EU) 2018/1139 in (EU) 2019/2144 ter direktiv 2014/90/EU, (EU) 2016/797 in (EU) 2020/1828 (Akt o umetni inteligenci). (2024). *Uradni list Evropske unije* L 2024/1689.
63. Weingerl, P. (2023). *Odškodninska odgovornost za uporabo umetne inteligence v delovnem razmerju. Delavci in delodajalci* 23, št. 4. Inštitut za delo pri Pravni fakulteti Univerze v Ljubljani.
64. Weingerl, P. (2020). *Novosti glede odškodninske odgovornosti za umetno inteligenco. Podjetje in delo*, št. 6–7. Lexpera d. o. o.
65. Women of Influence. (2025). *Digital glass ceilings: The challenges of AI in recruitment — and how to overcome them*. <https://www.womenofinfluence.ca/2025/01/16/digital-glass-ceilings-the-challenges-of-ai-in-recruitment-and-how-to-overcome-them/>
66. Zagovornik načela enakosti. (2023). *Zagotavljanje enakih možnosti in preprečevanje diskriminacije pri zaposlovanju in delu: Priročnik za delodajalce*. Zagovornik načela enakosti.
67. ZSSS. (2022). *Okvirni sporazum evropskih socialnih partnerjev o digitalizaciji*. <https://www.zsss.si/wp-content/uploads/2022/06/Prevod-evropski-sporazum-o-digitalizaciji.pdf>

PRAVNA VPRAŠANJA TOKENIZACIJE NEPREMIČNIN

Matej Velichkovski, študent, Univerza v Mariboru, Pravna fakulteta 

Izr. prof. mag. dr. Nataša Samec Berghaus, Univerza v Mariboru, Pravna fakulteta 

Povzetek: Prispevek analizira blockchain kot tehnologijo za decentralizirano shranjevanje podatkov in transakcije brez posrednikov, s posebnim poudarkom na tokenizaciji premoženja. V prispevku so uvodoma predstavljene osnovne vrste digitalnih žetonov oz. tokenov (plačilni, premoženjski, finančni, nezamenljivi) ter ključni pravni izzivi, povezani z njihovo pravno razvrstitvijo in izdajo. Zakonodaja EU določa različne načine izdaje, odvisno od značilnosti tokenov. Članek se dotika analize pravne narave tokenov v smislu slovenske zakonodaje. Osrednji del članka se posveti tokenizaciji realnega premoženja (premičnin in nepremičnin). Predstavljene so prednosti in problemi, s katerimi se sooča tokenizacija. Pri nepremičninah se izpostavlja tudi razlike med neposredno in posredno tokenizacijo. Neposredno tokenizacijo zavirajo stroge obličnostne zahteve (npr. vpis v zemljiško knjigo), medtem ko posredna tokenizacija (prek nepremičninskih družb ali skladov) omogoča lažje razdeljevanje lastniških deležev z uporabo tokenov. V zvezi s tem se opozarja na zakonske podlage v državah, kot sta Lihtenštajn in Nemčija, ki že omogočajo pravno varno uporabo blockchaina pri prenosu lastninskih pravic, medtem ko se bo Slovenija pri urejanju tega področja še morala prilagoditi.

Ključne besede: blockchain, tokenizacija, premoženje, MiCA, prenos lastninske pravice, pravna razvrstitev tokenov oz. digitalnih žetonov, neposredna vs. posredna tokenizacija, vrednostni papirji

Cobiss: 1.08

1 Uvod

Blockchain je tehnologija decentralizirane baze podatkov, ki omogoča varno shranjevanje in beleženje transakcij. S pomočjo te tehnologije je mogoče preverjati in slediti transakcijam med udeleženci na varen in pregleden način, brez potrebe po posrednikih, kot so banke ali vladne institucije (Akda, Karkas Geik & Hakan, 2024, str. 9). Podatki v bloku se ne morejo spreminjati, ne da bi spremenili tudi vse prejšnje bloke. Za to bi bilo potrebno soglasje celotnega omrežja (oz. odvisno od mehanizma soglasja $> 50\%$), kar zagotavlja zelo visoko veljavnost shranjenih podatkov (Völkle, 2025, str. 1.). Ključne značilnosti blockchaina vključujejo decentralizacijo (Samec Berghaus & Dnovšek, 2019, str 19), trajnost, anonimnost in revizijsko sledljivost. Te lastnosti omogočajo znatno zmanjšanje stroškov in izboljšanje učinkovitosti (Zheng, Xie & Dai, 2017, str. 1). Prva znana uporaba te tehnologije se je pojavila leta 2008 z bitcoinom, ki je bil sprva zasnovan kot eksperimentalni »peer-to-peer« sistem elektronskega denarja, ki omogoča neposredna plačila med dvema uporabnikoma preko interneta, brez potrebe po posredovanju tretje strani (Bečić, 2023, str. 2).

Kmalu pa se je izkazalo, da lahko blockchain služi še mnogim drugim namenom. Namesto zgolj za kriptovalute (kot sta bitcoin ali ethereum, ki imata lastno verigo blokov) se je tehnologija začela uporabljati tudi za kriptotokene, ki so zgrajeni na že obstoječih verigah (npr. na Ethereumovem blockchainu). Kripto token je digitalna enota, ki je shranjena na blockchainu in lahko predstavlja različne vrste sredstev – od digitalnih kovancev, slik in zvokov, do tokenov z glasovalno pravico (Peres, A. Schreier, Schwweidel & Sorescu, 2023, str. 2). Za razliko od samostojnih kriptovalut (npr. Bitcoin, Ethereum) tokeni nimajo svoje lastne verige blokov, ampak jih upravljajo pametne pogodbe na gostujočem blockchainu. Te določajo pravila in funkcionalnosti tokena (npr. glasovanje, izdajanje nagrad, ustvarjanje novih tokenov ipd.), ki se izvajajo samodejno, ko so izpolnjeni vnaprej določeni pogoji. Takšni tokeni se pogosto uporabljajo v različnih projektih ali decentraliziranih aplikacijah (v nadaljevanju dApps)¹. Povedano preprosto, dApp je aplikacija, ki za svoje delovanje izkorišča lastnosti blockchaina in pametnih pogodb, s čimer uporabnikom zagotavlja varno in decentralizirano okolje brez posrednikov. V takšnih aplikacijah tokeni služijo kot sredstvo za interakcijo, glasovanje ali plačevanje storitev znotraj ekosistema (di Angelo & Salzer, 2025, str. 3).

¹ Aplikacije v omrežju P2P, ki jih ne nadzira ena sama entiteta, so imenovane decentralizirane aplikacije (dApp).

Ena najpogostejše sprejetih razvrstitev tokenov je na (npr. Blandin, Cloots, & Hussain, 2019, str. 4; Grlica, 2023, str. 44; Johnpulle, 2024; Markheim & Berentsen, 2021, str. 66):

- plačilne (*payment tokens*),
- uporabniške (*utility tokens*),
- tokene vrednostnih papirjev oz. finančnih instrumentov (*security tokens*),
- premoženjske (*asset tokens*) (FINMA, 2018) in
- nezamenljive (*Non-Fungible*) tokene (v nadaljevanju NFT).

Plačilni tokeni (ali kriptovalute) služijo predvsem kot sredstvo za plačevanje, izmenjavo vrednosti, brez drugih pomembnih funkcij (podobno kot valute) (FINMA, 2018). To so tokeni, »namenjeni za uporabo, zdaj ali v prihodnosti, kot sredstva za plačilo za pridobivanje blaga ali storitev ali kot sredstva za prenos denarja ali vrednosti«, ki »ne podelijo nobenih pravic do svojega izdajatelja« (Blandin, Solfie Cloots & Hussein, 2019, str. 105–106).

Uporabniški token je vrsta kriptosredstva, namenjena predvsem zagotavljanju dostopa do določenega blaga ali storitve, ki jo ponuja izdajatelj tokena (člen 9(1), točka 9 Uredbe (EU) 2023/1114 Evropskega parlamenta in Sveta z dne 31. maja 2023 o trgih kriptosredstev (v nadaljevanju MiCA)). Takšni tokeni so pogosto povezani z določenim projektom, aplikacijo ali dApp, ki uporabnikom nudi konkretne koristi – npr. dostop do specifičnih funkcionalnosti ali vsebin. Z uporabo infrastrukture blockchain lahko uporabniški tokeni na pregleden in varen način omogočajo »digitalni dostop« do storitev. Poleg tega njihov namen pogosto vključuje tudi različne dodatne funkcije, kot so volilne pravice, sistem nagrajevanja ali upravljanje z vložki (angl. *staking*) (di Angelo & Salzer, 2025, str. 3).

Izrazi, kot so *tokenizacija*, *token*, *asset token*, *security token* ipd., še niso terminološko usklajeni v slovenskih pravnih ali jezikoslovnih standardih (npr. eSSJ ali ePravopis). Kljub temu jih uporablja domača in tuja strokovna literatura, zlasti v kontekstu finančnih in digitalnih tehnologij. V tem članku zato zaradi vsebinske natančnosti in primerljivosti z evropsko regulativo ohranjamo izvirne termine v angleščini ter jih, kjer je smiselno, dopolnimo s slovenskim opisom ali ustreznim prevodom².

² Slovenski uradni prevod Uredbe (EU) 2023/1114 o trgih kripto-sredstev (MiCA) dosledno prevaja angleški termin *token* kot »žeton«. Očitno je sledil francoskemu prevodu, ki uporablja enak izraz *jeton*. Nemška različica MiCA pa – kljub temu

Osrednje raziskovalno vprašanje prispevka je, kako obstoječa evropska in slovenska pravna ureditev naslavljata tokenizacijo premoženja, zlasti nepremičnin, ter katere pravne ovire se pojavljajo pri neposredni in posredni tokenizaciji. Cilj je tudi z uporabo primerjalne analize v Švici, Nemčiji in Avstriji ter razmejitve med *security tokens* in *asset tokens* prepoznati ključne izzive in ponuditi ugotovitve za pravno varno vključitev blockchaina v postopke prenosa lastninske pravice. Teza prispevka je, da kljub tehnološki zrelosti blockchaina neposredna tokenizacija nepremičnin za zdaj ostaja pravno onemogočena predvsem zaradi obličnostnih in registrskih oz. zemljiškoknjižnih zahtev stvarnega prava; dokler te ne bodo prilagojene digitalnim registrom, bo pravno varna rešitev le posredna tokenizacija prek nepremičninskih družb ali skladov.

Prispevek je razdeljen na pet vsebinskih poglavij, poleg prvega, uvodnega, in zadnjega, sklepnega, poglavja. V uvodu so predstavljene osnovne vrste digitalnih žetonov (plačilni, premoženjski, finančni, nezamenljivi) ter ključni pravni izzivi, povezani z njihovo pravno razvrstitvijo in izdajo. V drugem poglavju smo predstavili razvrstitev posameznih vrst tokenov in izpostavili ključne razlike med njimi. Tretje poglavje je namenjeno pregledu zakonodaje Evropske unije, ki ureja področje tokenov in vrednostnih papirjev. V četrtem poglavju smo obravnavali tokenizacijo fizičnega premoženja, kjer smo pojasnili, kako se digitalni žetoni lahko navezujejo na realno premoženje ter kakšne so prednosti in izzivi takšnega pristopa. Peto poglavje se osredotoča na tokenizacijo nepremičnin, kjer smo prikazali konkretne primere, pravne izzive in razmerje do obstoječih zemljiškoknjižnih in lastninskopravnih ureditev. V šestem poglavju obravnavamo še posredno tokenizacijo, pri kateri pravni nosilec premoženja izdaja tokene, s čimer se izogne nekaterim pravnim in tehničnim oviram neposredne tokenizacije. V sedmem, sklepnem poglavju podamo ključne ugotovitve in zaključke, ki izhajajo iz analize, ter nakažemo možnosti nadaljnjega razvoja in raziskovanja na področju tokenizacije v pravnem okviru.

da nemščina za fizične igralniške ploščice pozna besede *Jeton*, *Chip*, *Münze* – v digitalnem kontekstu ohranja izvirnik *Token*, da se izogne pomenski zmedi. V slovenščini beseda žeton po Slovarju slovenskega knjižnega jezika pomeni predvsem okroglo ploščico, ki služi kot zamenjava za denar pri igrah na srečo ali v avtomatih; ta pomenski okvir ne zajame lastnosti digitalnega zapisa na verigi blokov. Da bi ohranila terminološko natančnost in primerljivost z evropsko ter mednarodno literaturo, v članku zavestno uporablja angleška izraza token in tokenizacija (nem. Token, Tokenisierung) ter jih ob prvem pojavu pojasniva z ustreznim slovenskim opisom (npr. digitalni žeton, postopek pretvorbe premoženja v digitalni žeton). S tem se izogneva neustrezni tvorjenki žetonizacija in morebitni pomenski zamegljenosti med fizičnimi žetoni in digitalnimi žetoni.

2 Security tokens, premoženjski (asset) tokeni in razlike med njimi

V tem poglavju se preučujejo tokeni (digitalni žetoni) in razlike med njimi. Predstavlja se *security tokens*, *asset tokens* in NFT-je. S pomočjo pravne ureditve v Švici se prikaže razlika med *security tokens* in *asset tokens*, saj je meja med njima v literaturi pogosto zabrisana, vendar obstajajo pomembne razlike.

2.1 Security token (token kot finančni instrument)

Security token (token kot finančni instrument) predstavlja kapitalske, premoženjske ali druge pravice (npr. prenos vrednosti ali obljubo donosov), ki so tokenizirane na blockchainu. Zaradi svoje ekonomske funkcije se pogosto obravnava kot finančni instrument, saj je po naravi podoben delnicam, obveznicam ali derivatom (Majaski, 2024). V praksi se pogosto pojavlja v obliki delniških tokenov, ki lahko imetniku zagotavljajo korporacijske ali premoženjske pravice v izdajateljski družbi, podobno kot delnice (di Angelo & Salzer, 2025, str. 3).

Security tokens se izdajajo preko ponudbe Security Token Offering (v nadaljevanju STO) (Kreppmeier, Laschinger, I. Sreiningner & Dorfleitner, 2022, str. 1). *Security tokens* spadajo pod zakonodajo o trgu finančnih instrumentov (securities law) (Lambert, Liebau & Roosenboom, 2022, str. 303). Po ponudbi je z njimi mogoče trgovati na sekundarnih trgih, kar omogoča prodajo in likvidnost. Koncept delnega lastništva z digitalnimi tokeni omogoča razdelitev določenega premoženja (npr. v družbi) na več tokenov (Kreppmeier, Laschinger, I. Sreiningner & Dorfleitner, 2022, str. 1).

2.2 Premoženjski (asset) tokeni

Premoženjski (*asset*) tokeni predstavljajo digitalizirano obliko pravic, ki so vezane na osnovno premoženje. To pomeni, da lahko takšni tokeni predstavljajo delež v realnem ali finančnem sredstvu, npr. nepremičnini, surovinah ali celo delnicah. Imetnik premoženjskega tokena običajno pridobi kapitalske in premoženjske pravice, kot so pravice do deleža dobička (npr. dividende), glasovalne pravice ali pravice, ki se uveljavljajo ob likvidaciji izdajateljske družbe.

V nasprotju z drugimi tokeni, katerih ceno oz. vrednost določata izdajatelj ter ponudba in povpraševanje na trgu (zaradi česar je vrednost tega kriptopremoženja izpostavljena veliki nestabilnosti/volatilnosti in jo je težje uporabiti kot denar, sredstvo izmenjave ali ohranjanja vrednosti), si izdajatelji premoženjskih tokenov prizadevajo, da bi vrednost teh tokenov ostala

stabilna. To dosežejo s tokenizacijo, tj. pretvorbo dejanskega premoženja v tokene na blockchainu, oz. z vezavo teh tokenov na dejansko premoženje, ki ga izdajatelj hrani v svojih rezervah in na podlagi katerega izda tokene (Bečić, 2023, str. 2).

2.2.1 Ureditev premoženjskih (asset) tokenov v Švici

Po smernicah švicarskega nadzornega organa Swiss Financial Market Supervisory Authority (FINMA, 2018), objavljenih kot ICO Guidelines, premoženjski tokeni predstavljajo tokenizirane terjatve do osnovnih sredstev ali prihodkovnih tokov in zato spadajo pod veljavno zakonodajo o vrednostnih papirjih.

S tem pristopom se jasno pokaže, da FINMA v svoji razvrstitvi ne loči posebej med *security tokens* in *asset tokens*, temveč premoženjske tokene obravnava kot tiste, ki zaradi tokeniziranih pravic spadajo v področje vrednostnih papirjev oz. finančnih instrumentov (tako lastniških kot dolžniških finančnih instrumentov, kot tudi izvedenih) (FINMA, 2018).

FINMA v svojih smernicah poudarja, da te kategorije niso nujno medsebojno izključujoče. V praksi lahko en token hkrati nosi lastnosti plačilnega in premoženjskega tokena (t. i. hibridni tokeni). V takšnem primeru morajo izdajatelji upoštevati vse ustrezne regulativne zahteve, ki veljajo za posamezne kategorije. FINMA v izvirniku navaja:

»The individual token classifications are not mutually exclusive. Asset and utility tokens can also be classified as payment tokens (referred to as hybrid tokens). In these cases, the requirements are cumulative...« [lastni prevod avtorjev: »Posamezne razvrstitve tokenov se med seboj ne izključujejo. Premoženjski in uporabniški tokeni so lahko razvrščeni tudi kot plačilni tokeni (t. i. hibridni tokeni). V takih primerih se zahteve kumulativno uporabljajo ...«] (FINMA, 2018, str. 3).

S tem FINMA pojasnjuje, da se lahko token v pravnem smislu hkrati obravnava kot sredstvo plačevanja in vrednostni papir, če izpolnjuje pogoje obeh kategorij. Ta delitev poudarja, da je za vsako vrsto tokena treba upoštevati specifične pravne in regulativne zahteve. Zlasti je pomembno, kako je urejena pravica, ki jo token prenaša, ter katere dodatne zahteve veljajo glede na osnovno sredstvo (valuta, surovina, nepremičnina ali vrednostni papir).

2.3 Security tokens vs. asset tokens

V teoriji se srečujemo z obema izrazoma. Američani v svoji literaturi uporabljajo izraz *security tokens* za vse kriptotokene, ki ustrezajo definiciji »vrednostnega papirja« (npr. po t. i. Howeyjevem testu). Pravo EU jih loči glede na ureditev, saj so *asset-referenced tokens* urejeni v uredbi MiCA, *security tokens* pa v Direktivi 2014/65/EU o trgih finančnih instrumentov (v nadaljevanju MiFID II) in so obravnavani kot finančni instrumenti. Vsebina obeh tokenov je podobna in tokenizacija nepremičnin se lahko izvede v obliki *security tokens* in *asset-referenced tokens*, pri čemer sta način izdaje in regulativa različna.

Če se tokeni lahko štejejo za finančni instrument, potem gre za ponudbo STO; v nasprotnem primeru pa gre za »Initial Coin Offering« (v nadaljevanju ICO) (AMF, 2020, str. 3). Po tem, ko so ICO-ji trpeli zaradi pomanjkanja zaščite vlagateljev in pogostih goljufij, so se *security tokens* pojavili kot inovativni in bolj zaupanja vredni naložbeni produkti (Miglo, 2021, str. 1).

V primeru STO bo tehnološka zasnova tokena podobna tisti, ki jo podjetja uporabljajo pri ICO, saj bo za izdajo tokenov uporabljena tehnologija porazdeljenih knjig (v nadaljevanju DLT) ali druga digitalna infrastruktura, ki omogoča tokenizacijo. Razlika je v tem, da se pri STO izdani tokeni nanašajo na točno določeno vrsto finančnih sredstev, ki se pravno štejejo za vrednostne papirje (npr. delnice, obveznice, nakupni boni ali opcije) ali pa zagotavljajo pravice, ki so enakovredne pravicam iz vrednostnih papirjev. Definicija, kaj predstavlja vrednostni papir, se bo razlikovala od jurisdikcije do jurisdikcije (Chance, 2020, str. 1).

Meja med tokeni, ki spadajo pod MiCA, in tokeni, ki jih je treba obravnavati kot vrednostne papirje, je lahko nejasna, zato je vsebina pomembnejša od oblike. Pravna kvalifikacija tokenov bo odvisna od vsakega posameznega primera (Paolo Patti, 2024, str.20), pri čemer lahko nastopijo tudi hibridne rešitve. Švica zavzema podobno stališče, zato tudi uporablja skupni pojem *asset tokens*.

Zaradi omenjenih nejasnosti in različnih možnosti lahko nepremičnino tokeniziramo bodisi v obliki *asset-referenced tokens* bodisi v obliki *security tokens* kot finančni instrument.

2.4 Nezamenljivi tokeni (NFT-ji)

NFT-ji so digitalna sredstva, ustvarjena s pomočjo blockchaine, ki predstavljajo edinstvene predmete ali vsebine, npr. umetniška dela, videoposnetke ali druge zbirateljske predmete (Sharma, 2024). Za razliko od zamenljivih tokenov (npr. plačilnih kriptovalut), kjer je vsaka enota

enaka, je NFT nezamenljiv (angl. *non-fungible*). To pomeni, da ima vsak token edinstveno identifikacijo, zaradi katere ga ni mogoče enakovredno zamenjati z drugim tokenom. Posamezen NFT je torej enkraten in je lahko izključno dodeljen enemu imetniku, kar omogoča sledljivost lastništva in potrjevanje pristnosti digitalnih sredstev (Richer, 2025, str. 1). NFT-je so npr. za predstavitev Slovenije na EXPO DUBAI 2020 leta 2021 v sodelovanju s strokovnjaki Fakultete za računalništvo in informatiko Univerze v Ljubljani ter podjetjem Hashnet zasnovali in izdali Ministrstvo za gospodarski razvoj in tehnologijo, Javna agencija SPIRIT Slovenija in Tehnološki park Ljubljana (Tehnološki park Ljubljana, 2021).

3 MiCA in MiFID II

V tem poglavju sta najprej predstavljena uredba MiCA in njen pristop k regulaciji različnih vrst kripto-sredstev, nato pa še temeljne določbe direktive MiFID II, ki ureja *security tokens* kot finančne instrumente.

3.1 MiCA

Uredba MiCA želi celostno urediti vsa kriptosredstva, ki niso hkrati finančni instrumenti (in torej ne sodijo pod MiFID II) (četrti odst. 2. člena MiCA). Med temi kriptosredstvi so tako tokeni, ki nimajo stabilne vrednosti (npr. klasični »utility tokens«), kot tudi tisti, ki so vezani na neko vrednost ali premoženje (t. i. *asset-referenced tokens*) (prvi odst. 1. člena MiCA). Nasprotno pa so kriptosredstva, ki izpolnjujejo pogoje za finančne instrumente — t. i. *security tokens* — podvržena pravilom MiFID II (Paolo Patti, 2024, str.18).

MiCA opredeljuje »kriptosredstvo« kot digitalno predstavitev vrednosti ali pravice, ki jo je mogoče elektronsko prenesti in shraniti z uporabo tehnologije razpršene evidence ali podobne tehnologije. Poleg njihove splošne definicije MiCA predvideva tri različne kategorije kriptosredstev: že omenjeni uporabniški tokeni, tokeni, povezani s premoženjem (*asset referenced tokens*), in tokeni elektronskega denarja (Paolo Patti, 2024, str.18).

Javna ponudba in uvrstitev za trgovanje s tokeni, vezanih na premoženje (*asset referenced tokens*) sta omejeni na pravne osebe s sedežem v Evropski uniji, ki so prejele odobritev za delovanje od pristojnega organa matične države članice, in na registrirane kreditne institucije (prvi odst. 16. člena MiCA). V obeh primerih obstaja obveznost izdelave bele knjige (prvi odst. 17. člena, 19. člen MiCA) s predpisano vsebino, ki jo mora pred objavo odobriti pristojno telo matične države članice

(takšnega odobrenja ni pri prvi kategoriji – »navadno kriptopremoženje«). Pristojno telo mora posebej oceniti, ali odobritev za delovanje izdajatelja teh tokenov in tokeni kot takšni lahko predstavljajo resno grožnjo integriteti trga, finančni stabilnosti, nemotenemu delovanju plačilnih sistemov in splošni monetarni suverenosti (Bečić, 2023 str. 22).

3.2 MiFID II

Namen MiFID II je zagotoviti trdnejše in preglednejše finančne trge v Evropski Uniji (v nadaljevanju EU) (EUR-Lex, 2025). Za potrebe tega članka je ključno vedeti, da MiFID II velja za *security tokens*, če se ti kvalificirajo kot finančni instrument po 44. točki prvega odstavka četrtega člena. Takšni *security tokens* se opredeljujejo kot prenosljivi vrednostni papirji (*transferable investment securities*) (Marjosola, 2022, str. 256). Osrednje vprašanje pri STO je, ali tokeni, ki se ponujajo, spadajo v eno izmed vrst vrednostnih papirjev, opisanih v točkah (a) do (c) 44. točke prvega odstavka 4. člena MiFID II. Pri STO-jih, kjer se ponujajo tokeni z značilnostmi, podobnimi lastniškim deležem, bi jih npr. lahko označili kot instrumente, ki podeljujejo pravice, primerljive s tistimi iz delnic, zato bi lahko spadali med »druge prenosljive vrednostne papirje« iz točke (44) prvega odstavka 4. člena MiFID II (Chance, 2020, str. 10).

Za izdajatelje vrednostnih papirjev pa je treba upoštevati tudi nacionalno zakonodajo, saj uredba MiFID II tega področja ne ureja izčrpno. V Sloveniji bodo tovrstni *security tokens*, kot prenosljivi vrednostni papirji (44. točka, prvega odstavka 4. člena MiFID II), spadali pod Zakon o trgu finančnih instrumentov (v nadaljevanju ZTFI-1). Ta v drugem odstavku 7. člena določa, da so med drugim tudi prenosljivi vrednostni papirji finančni instrumenti, kar pomeni, da se za *security tokens* uporablja ZTFI-1. Izdajatelji vrednostnih papirjev so določeni v 51. členu ZTFI-1, in sicer je izdajatelj oseba, ki izda ali namerava izdati vrednostne papirje, s katerimi se trguje na organiziranih trgih.

4 Pregled tokenizacije realnega (fizičnega) premoženja

Za namene tega članka je potrebno razumevanje pojma tokenizacije. Karkoli je lahko tokenizirano, tako premično kot nepremično premoženje: ustvarite lahko npr. token, ki pomeni lastništvo in registracijo avtomobila. Identifikacijska številka vozila (*Vehicle Identification Number* – v nadaljevanju VIN) oz. avtomobila bi lahko bila vnesena v blok na blockchainu skupaj z imenom lastnika, naslovom in drugimi informacijami, ki jih zahteva država za registracijo vozila. Ta token (shranjena različica informacij) bi se lahko prodajal in kupoval, s čimer bi se preneslo lastništvo avtomobila (Majaki, 2024), vendar je treba poudariti, da tokenizacija sama po sebi ne zagotavlja

pravnega prenosa lastninske pravice. Token lahko služi kot digitalna reprezentacija premoženja ali pravic, vendar mora biti za pravno učinkovit prenos lastništva avtomobila tak token pravno priznati pristojni organ – denimo kot uradni nosilec registracije pri državnem registru vozil. Poleg tega mora biti celotni proces prenosa izveden v skladu z veljavno zakonodajo, ki ureja prenos lastninske pravice nad premičninami. Brez ustrezne pravne in institucionalne podpore token predstavlja le tehnološko rešitev brez pravnega učinka.

Tokenizacija je torej postopek, pri katerem se premoženje razdeli na več tokenov, pri čemer vsak token predstavlja določeni del vrednosti (ne nastane pa pri tem nova stvar – oboje obstaja hkrati) (Pateter & Huber, 2022, str. 2). Ko tokeniziramo nepremičnino, razdelimo nepremično premoženje na posamezne tokene (dele), ki se lahko uporabljajo za različne namene – od lastniškega deleža in pravic do premoženja, do morebitnih dividend ali drugih oblik udeležbe v donosih (Joshi & Choudhury, 2022, str. 374).

4.1 Zakaj tokenizacija fizičnega premoženja?

Tokenizacija fizična premoženja lahko prinese številne prednosti. Glede na to, da so vse transakcije in njihova gospodarska vrednost javno dostopne, lahko rečemo, da tokenizacija premoženja na blockchainu omogoča preglednost. Enostavno lahko ugotovimo lastništvo nekega premoženja in s tem sledimo verigi lastništva, vendar je takšna preglednost pravno relevantna le v primeru, če pravni red priznava zapis na blockchainu kot dokaz o lastništvu ali ga integrira v uradni register (npr. zemljiško knjigo ali register vozil). V nasprotnem primeru tokeni predstavljajo zgolj informativno sledljivost brez neposrednega pravnega učinka. Pri trgovanju s tokeni, ki predstavljajo fizično premoženje, je prodaja med posamezniki neposredna. Posamezniki lahko digitalno shranijo tokene v svoje denarnice in jih neposredno prenesejo na drugega posameznika preko interneta. Ta neposrednost pa ne pomeni nujno, da se s tem pravno prenese lastninska pravica, saj mora biti vsak prenos skladen z veljavno zakonodajo in morebitnimi zahtevami po vpisu v uradne registre. Zlasti pri nepremičninah mora biti za pravno veljaven prenos izpolnjena tudi oblika, ki jo določa stvarno- in obligacijskoppravna zakonodaja.

Prav tako lahko tokenu pripišemo vrsto legitimacijske funkcije, saj se lahko lastnik tokena izkaže kot pravi lastnik tokeniziranega premoženja (Pateter & Huber, 2022, str. 3), vendar takšna legitimacija učinkuje zgolj v obsegu, v katerem pravni red priznava token kot sredstvo dokazovanja ali kot nosilca pravice. V Sloveniji trenutno takšno priznanje še ni sistemsko urejeno. S

tokenizacijo se poveča likvidnost, ki je največji potencial tokenizacije. Ta likvidnost se poveča preko t. i. delnega lastništva (angl. *fractional ownership*). Premoženje se lahko s pomočjo tokenov razdeli na manjše enote, kar omogoča tistim z nižjo kupno močjo, da pridobijo delež premoženja, ki bi sicer bil finančno nedostopen (Pateter & Huber, 2022, str. 3). To delno lastništvo je pomembno tudi z vidika tokenizacije nepremičnega premoženja, ki omogoča, da mladi vlagatelji postopoma vstopijo na lokalne trge nepremičnin z manjšimi mesečnimi naložbami, kar jim omogoča, da se zavarujejo pred tveganjem cen, dokler ne bodo sposobni kupiti svojih lastnih stanovanj oz. nepremičnin (Swinkels, 2023, str. 3). Pri tem je ključno, da je delno lastništvo pravilno strukturirano tudi pravno, saj se v nasprotnem primeru lahko uporabijo pravila o skupni lastnini oz. pravni skupnosti iz Obligacijskega zakonika (v nadaljevanju OZ). To odpira vprašanja glede upravljanja, razpolaganja in prenosa deležev, ki jih je treba ustrezno urediti bodisi s pogodbenimi dogovori bodisi z uporabo pravnih oblik, kot so družbe civilnega prava ali fiduciarne strukture.

Z uporabo blockchaina se zmanjšajo stroški (IBN, 2025), zaradi česar imajo podjetja, ki uporabljajo blockchain, večje možnosti za doseganje večjih dobičkov (Ko, Lee & Ryu, 2018, str. 4). Kljub temu je za uspešno in pravno varno uporabo te tehnologije nujno zagotoviti skladnost z zakonodajo o preprečevanju pranja denarja (angl. *Anti-Money Laundering*, AML), spoštovanje zahtev iz Uredbe (EU) 2016/679 o varstvu osebnih podatkov (General Data Protection Regulation, GDPR) ter spoštovanje kapitalskih in davčnih pravil.

Prav tako bodo pravni dokumenti, potrebni za tokenizacijo, sčasoma standardizirani in cenovno dostopni, kar bo zmanjšalo potrebo po posrednikih – bankah, odvetnikih, nepremičninskih posrednikih ipd. To bo dolgoročno zmanjšalo stroške kapitala pri tokenizaciji (Markhein & Berentsen, 2021, str. 72). Trenutno pa takšna standardizacija še ni vzpostavljena, zato je v praksi še vedno potreben angažma pravnih strokovnjakov, zlasti pri strukturiranju projektov skladno z regulacijo finančnih instrumentov, stvarnopravno zakonodajo in pogodbenim pravom. Pomembno je izpostaviti, da imajo pri transakcijah s tokeni ključno vlogo pametne pogodbe – računalniški programi, ki se znotraj blockchaina izvajajo avtomatizirano in vzpostavljajo posebno povezavo med strankama transakcije (Nägele & Bont, 2019, str. 663). Uporaba blockchaina prav tako prinese avtomatizacijo preko pametnih pogodb – vmesni koraki, kot so skladnost, preverjanje dokumentov, trgovanje, odprtje depozitivnega računa, potekajo avtomatsko preko blockchaina (Ganz, 2022). Pametne pogodbe pa morajo biti napisane na način, ki zagotavlja pravno izvršljivost

njihovih učinkov, kar trenutno v večini pravnih sistemov še ni povsem urejeno. Dodatno, obstoječe pravno okolje pogosto zahteva možnost pravnih sredstev, ki jih samodejna izvedba pogodbe (npr. brez človeškega nadzora) ne omogoča.

4.2 Pravna umestitev digitalnih tokenov in premoženja

S procesom tokenizacije ne nastane nova, enotna »stvar«, ki bi vključevala osnovno sredstvo (npr. lastninsko pravico na avtomobilu; finančne instrumente), kot tudi digitalni token. Kljub medsebojni povezanosti je treba obe entiteti še vedno obravnavati ločeno kot samostojni »stvari« (Pateter & Huber, 2022, str. 3). Stvarnopravni zakonik (v nadaljevanju SPZ), tako kot nemški civilni zakonik *Bürgerliches Gesetzbuch* (v nadaljevanju BGB), ne opredeljuje netelesnih stvari, temveč se prvenstveno nanaša na telesne stvari (15. člen SPZ, § 90 BGB). V prvem odstavku 16. člena SPZ je določeno, da je stvar samostojen telesni predmet, ki ga človek lahko obvladuje. Nasprotno pa avstrijski civilni zakonik, *Allgemeines bürgerliches Gesetzbuch* (v nadaljevanju ABGB) v § 285 določa, da je »vse, kar je od osebe ločeno in služi uporabi ljudi, v pravnem smislu stvar«, s čimer pod avstrijsko ureditev med »stvari« spadajo tudi netelesni objekti (npr. pravice) (Juhart, 2007, str. 62). vendar drugi odst. 15. člena SPZ pojem stvari širi tudi na »različne oblike energije in valovanja«, ki ne izpolnjujejo klasičnega kriterija telesnosti, vendar le pod pogojem, da jih je mogoče obvladovati.

Ker so kriptotokeni in kriptovalute v osnovi (zgolj) podatki, slovensko pravo za zdaj še ne predvideva lastninske pravice na podatkih (Sladič, 2019, str. 1372). Čeprav SPZ kot stvar priznava tudi različne oblike energije in valovanja, ki jih človek lahko obvladuje (drugi odst. 15. člena SPZ), se zaradi decentralizirane narave tokenov (ki jih ni mogoče enostransko obvladovati) ta razširitev pojma stvari nanje ne more neposredno uporabiti (Sladič, 2019, str. 1372). Ob tem velja izpostaviti tudi, da tokeni nimajo lastnih števil, zato jih ni mogoče identificirati v skladu z načelom specialnosti (Sladič, 2019, str. 1372). Nemška pravna teorija, ki prav tako ne pozna pojma netelesne stvari, dopušča možnost, da bi se načelo telesnosti stvari lahko apliciralo tudi na digitalne podatke, kot so tokeni, in sicer z določenim odstopanjem od načel stvarnega prava (Sladič, 2019, str. 1372). Za potrebe tokenizacije, uvrstitve tokenov in reševanja določenih problemov v prihodnosti je treba upoštevati nemško teorijo o razširitvi pojma »stvar«, saj je bil 15. člen SPZ oblikovan pod vplivom § 90 BGB (Sladič, 2019, str. 1372). Posledično lahko tokene – vsaj ob odstopanju od načel stvarnega prava – opredelimo kot stvar, kar bi omogočilo, da se jih v

pravnem prometu obravnava podobno kot klasične (telesne) predmete in da se zanje vzpostavijo ustrezni mehanizmi lastninskega varstva (UP RS, I U 75/2021-9, 14.2.2023).

V avstrijski pravni teoriji ni enotnega stališča, kako veljavno izvesti prenos tokena. Med predlogi se pojavlja uporaba pravil o cesiji, analogna uporaba pravil za fizični prenos (zlasti fizična izročitev) ali izročitev z izjavo v smislu § 428 AGBG (Pateter & Huber, 2022, str. 3).

Če to primerjamo s slovenskim pravnim redom, bi se prenos tokena lahko uredil na podoben način, pri čemer je ključno opredeliti pravno naravo tokena. V kolikor token (predvsem t. i. *security token*) pravno gledano ustreza vrednostnemu papirju, bi se zanj lahko uporabila pravila cesije iz 219. člena OZ, ki sicer ureja prenos imenskih vrednostnih papirjev (npr. prvi odst. 417. člena OZ). To bi bilo možno, ker so *security tokens* v osnovi definirani kot prenosljivi vrednostni papirji (prvi odst. 417. člen OZ), pri čemer se lahko dodelijo (ne)posredno določeni osebi, ne da bi bila njena identiteta nujno javno razkrita (Omlor, 2020, str. 6). V praksi bi to pomenilo, da bi tokene opredelili kot imenske vrednostne papirje in jih v skladu z določbami 219. člena OZ prenesli s cesijo. Kljub temu se na tej točki pojavi težava, saj je zaradi dvotirne narave (ločenost tokena in osnovne premičnine) treba »stvar« (tj. premičnino) tudi fizično prenesti na pridobitelja. To sledi iz tega, da je treba tako token kot premičnino obravnavati kot dve samostojni entiteti. Posledično zgolj cesija tokena še ne zadostuje za prenos lastninske pravice na pripadajoči premičnini.

Fizična izročitev je v SPZ urejena kot izročitev v smislu 60. člena. Za izročitev premičnine se šteje tudi izročitev listine, na podlagi katere lahko pridobitelj razpolaga s premičnino, pa tudi izročitev njenega dela oz. izločitev ali drugačna označitev stvari, ki pomeni njeno izročitev, vendar se v praksi pojavi težava pri nepovezanosti premoženja in digitalnega tokena, še posebej v naslednjem primeru: lastnik z digitalnim tokenom prenese lastninsko pravico na drugo osebo, a fizično stvar še vedno drži v svoji posesti. Nato jo v nasprotju z dogovorom proda tretji osebi, pri čemer prikrije prejšnji (tokenizirani) prenos (Kaisto, Juutilainen & Kauranen, 2024, str. 13). Če novi kupec izpolnjuje pogoje po 64. členu SPZ (t. i. dobroverna pridobitev *a non domino*), lahko kljub obstoju tokena veljavno pridobi lastninsko pravico na premičnini, zato bi bila kakršnakoli fizična izročitev prejšnjim pridobiteljem povsem brezpredmetna.

Poleg tega fizična izročitev ne reši nujno vprašanja v primerih, ko lastnik zaupa stvar tretji osebi (v posest), ta pa jo hrani v njegovem imenu. Zaradi močne povezanosti lastništva stvari z digitalnim tokenom bi v takih primerih potrebovali posebej prilagojena pravila (ni recimo dovolj, da token

prenesemo zgolj z izročitvijo listine, saj token še naprej obstaja v verigi blokov v denarnici odsvojitelja). Podobna problematika se pojavlja tudi v povezavi z avstrijsko izročitvijo »z izjavo« (ki bi jo lahko primerjali z izročitvijo na kratko ali dolgo roko v slovenskem pravu) (Kaisto, Juutilainen & Kauranen, 2024, str. 13).

Nepovezanost med prenosom tokena in fizičnim prenosom premične stvari je torej mogoče rešiti na več načinov. Ključno je, da sočasno izvedemo prenos drugega premoženja in pripadajočega tokena, da tokenizacija resnično zaživi. Ena od možnosti je denimo pogodbeno prepoved odtujitve in obremenitve na podlagi 38. člena SPZ (npr. § 364c AGBG), vendar to omejitev učinkuje le obligacijsko. Če bi se kljub temu stvar brez tokena prenesla, bi to morebiti vzpostavilo odškodninsko odgovornost, ne pa tudi ničnosti posla (Pateter & Huber, 2022, str. 4).

Za stvarnopravni učinek je zato primernejši dogovor pod odložnim pogojem, po katerem je prenos premičnine veljaven le, če je hkrati prenesen tudi token. Obratno bi se lahko dogovorilo, da pogodba preneha veljati (razvezni pogoj), če se stvar prenese brez pripadajočega tokena. Oboje je mogoče podpreti s 64. členom SPZ (npr. § 969 AGBG), ki omogoča, da se prenos lastninske pravice veže na razvezne ali odložne pogoje. V praksi bi morali tudi vse nadaljnje pogodbe obravnavati podobno, torej z obvezno zahtevo sočasnega prenosa tokena in premoženja pri vsakem naslednjem razpolaganju, saj le tako sistem v celoti deluje.

5 Tokenizacija nepremičnin

Pri tokenizaciji nepremičnin se pojavijo dodatne ovire, saj zaradi stroge obličnosti in načela zaupanja v zemljiško knjigo neposredna tokenizacija bodisi ni primerna ali je celo nemogoča (Pateter & Huber, 2022, str. 4). V slovenskem pravnem sistemu je za vpis v zemljiško knjigo potrebno zemljiškoknjižno dovolilo (intabulacijska klavzula) – nepogojna izjava tistega, čigar pravica se prenaša, spreminja ali preneha, da dovoljuje vpis v zemljiško knjigo. Poleg tega mora biti podpis na dovolilu notarsko overjen (23. člen SPZ), kar je v nasprotju z običajnimi cilji tokenizacije (zmanjšanje stroškov in povečanje likvidnosti) (Pateter & Huber, 2022, str. 6).

Nadalje je težavno tudi zagotavljanje dolgoletnega arhiviranja in preverjanje zgodovinskih prenosov lastništva, kar je za zemljiškoknjižni postopek ključno. Blockchain praviloma zahteva

soglasje večine omrežnih vozlišč za spremembe (t. i. *consensus mechanism*)³, zato bi odsotnost takšnega soglasja lahko preprečila nastanek lastninske pravice, ne glede na veljavnost posla po nacionalnem pravu (Völkle, 2025, str. 1). Slovensko pravo medtem določa, da se lastninska pravica na nepremičnini pridobi šele z vpisom v zemljiško knjigo, ne pa z zgolj »verižnim« potrditvijo transakcij v omrežju (Wilsch, 2017, str. 2.). Obenem pravnih sredstev za primer, ko bi omrežje zavrnilo potrditev vnosa, ni, kar dodatno otežuje uporabo te tehnologije (Wilsch, 2017, str. 7), tako da brez soglasja večine v blockchain omrežju nepremičnin ni mogoče prenesti, razdeliti, spremeniti ali obremeniti, kar pomeni omejitev razpolaganja.

Kljub navedenim izzivom pa se v praksi pojavljajo rešitve, kjer so v postopek tokenizacije nepremičnine vpeljeni notarski postopki in uradni vpis v zemljiško knjigo. Slovensko podjetje Blocksquare je, denimo, doseglo prvi notarsko overjeni in v zemljiško knjigo vpisani postopek tokenizacije nepremičnine (1. 10. 2023) (ABC novice, 2023), pri čemer je integriralo notarizacijo kot ključni element za premostitev pravnih ovir. S tem je nazorno pokazalo, da je – ob ustreznem sodelovanju notarjev, ustreznih pogodbenih klavzulah in zemljiškoknjižnih postopkih – možno do neke mere združiti prednosti blockchaina z zahtevanimi formalnostmi.

Ob odplačnem prenosu lastninske pravice na nepremičnini je treba plačati davek na promet nepremičnin, ki je urejen v Zakonu o davku na promet nepremičnin (v nadaljevanju ZDPN-2), ki določa, da davek na promet nepremičnin znaša 2 % kupnine. Poleg tega je v določenih primerih treba pridobiti dovoljenje pristojnih organov za promet z nepremičninami – npr. v skladu z Zakonom o kmetijskih zemljiščih (v nadaljevanju ZKZ), kadar je potrebno dovoljenje upravne enote (56.a člen ZKZ). Zankrat vse to ni mogoče avtomatizirati s pomočjo blockchaina (Pateter & Huber, 2022, str. 6).

Podobni problemi glede vpisa v zemljiško knjigo in prenosa lastninske pravice se pojavljajo tudi v Avstriji, Nemčiji in Švici, kjer se lastninska pravica na nepremičninah prav tako pridobi šele z vpisom v zemljiško knjigo (prim. § 838 BGB; § 431 ABGB; § 972 Schweizerisches Zivilgesetzbuch – švicarski civilni zakonik, v nadaljevanju ZGB). Lihtenštajn je prva država, ki je z *Gesetz über Token und VT-Dienstleister* (v nadaljevanju TVTG, 2019) celovito uredila tokenizirano gospodarstvo.

³ Vozlišča so ljudje, ki uporabljajo programsko opremo Bitcoina, in vsakdo lahko postane vozlišče, brez zahteve za dovoljenje.

Zakon omogoča tokenizacijo vseh vrst premoženja in pravic in je v veljavi od 1. januarja 2020 (Singh, 2024). Nemčija je leta 2021 z Zakonom o elektronskih vrednostnih papirjih (Gesetz über elektronische Wertpapiere, Electronic Securities Act, v nadaljevanju eWpG) omogočila izdajo in prenos elektronskih vrednostnih papirjev prek decentraliziranih registrov, s čimer se je odprla pot tudi k uporabi blockchaine pri upravljanju lastninskih pravic na nepremičninah, kar je bilo prej zakonsko omejeno (Henker, Atzberger, Scheibel & Döllner, 2023, str. 1). Švica je februarja 2021 z uveljavitvijo prvega dela Zveznega zakona o prilagoditvi zveznega prava razvoju tehnologije distribuiranih elektronskih registrov (Federal Act on the Adaptation of Federal Law to Developments in Distributed Ledger Technology, DLT Act) naredila korak naprej pri regulaciji blockchaine. Zvezni svet je nato 18. junija 2021 odločil, da zakon v celoti začne veljati 1. avgusta 2021, skupaj z okvirno uredbo (Federal Council Switzerland, 2021). S tem sta se dodatno okrepili pravna varnost in konkurenčnost švicarskega fintech ekosistema (State Secretariat for International Finance, n. d.).

Omenjeni problem z vidika prenosa lastništva nepremičnin in vpisa v zemljiško knjigo pri uporabi blockchaine pa ni ovira v konsenzualnih pravnih sistemih (npr. Franciji in Italiji), saj je prenos lastninske pravice načeloma odvisen le od pogodbe, ne pa od vpisa v javni register (Teruel & Morelo, 2021, str. 5–6).

Nekateri avstrijski avtorji predlagajo kot možno rešitev vpeljavo skrbnika (t. i. fiduciarja), ki bi navzven razpolagal z nepremičnino (in bil formalni lastnik), navznoter pa bi moral spoštovati interese dejanskih upravičencev v skrbniškem razmerju (Pateter & Huber, 2022, str. 6), vendar bi bila prekinitev takega razmerja pravno zapletena, saj ne pomeni avtomatične vrnitve skrbniškega premoženja dejanskemu upravičencu, temveč zahteva ponovno izpolnitev obličnostnih zahtev (ponoven prenos lastninske pravice in s tem povezane formalnosti), opisanih v tem poglavju (Pateter & Huber, 2022, str. 6).

6 Posredna tokenizacija nepremičnin

Pri tokenizaciji nepremičnin lahko razlikujemo med neposrednim in posrednim nakupom nepremičnin. Pri neposrednem nakupu je nepremičnina predmet tokenizacije (tj. pravice na nepremičnini se prenesejo na imetnike tokenov), medtem ko se pri posrednem nakupu družba (ali sklad), ki kupi nepremičnino, najprej vpiše kot lastnik v zemljiško knjigo, nato pa svoje deleže (delnice ali obveznice) tokenizira (Kiser & Meier, 2023). Na ta način pride do ekonomskega prenosa

pravic in koristi od nepremičnine (Luchsinger Gähwiler, 2022) (Kiser & Meier, 2023), ne pa do dejanskega prenosa lastništva v pravnem pomenu besede na več posameznikov. To se zgodi tako, da nepremičnino kupi nepremičninska družba, vlagatelji pa lahko sodelujejo kot upniki prek obveznic ali kot delničarji (lahko tudi prednostnih delnic) (Luchsinger Gähwiler, 2022). Nepremičninska družba je ta, ki se vpiše kot lastnik v zemljiško knjigo in nato tokenizira pravice v zvezi z nepremičnino. V zameno pa imetniki izdanih tokenov pridobijo soupravljalne pravice v zvezi z nepremičnino ter pravice do delitve dobička (npr. pravico do presežka iz najemnin ipd.) (Pateter & Huber, 2022, str. 7). Izdane obveznice, delnice ali prednostne delnice so vrednostni papirji, ki se lahko tokenizirajo (Luchsinger Gähwiler, 2022). Za izdajo teh vrednostnih papirjev velja obveznost prospekta v skladu z Uredbo o prospektu (EU) 2017/1129 (Pateter/ Huber, 2022, str. 7), enako kot pri tradicionalni izdaji vrednostnih papirjev (Kiser & Meier, 2023), razen če obstaja izjema od obveznosti prospekta (Pateter & Huber, 2022, str. 7).

Preko (posredne) tokenizacije lahko vlagatelji dobijo tiho udeležbo v zasebnih stanovanjskih nepremičninah v obliki tokenov, kar pomeni, da kupci tokenov sodelujejo v rasti vrednosti nepremičnine, vendar ne prejmejo prihodkov, kot so najemnine, in tudi na stroškovni strani nimajo obveznosti (npr. podjetje Brickbuy omogoča 49-odstotno tokenizacijo in prodaje nepremičnine) (de la Rubia, Sandner & Groß, 2021, str. 9).

Pri posredni tokenizaciji vlagatelji investirajo v sklade in/ali družbe (Wallace, 2019). Pri vlaganju v družbe (npr. v delniško družbo) bi vlagatelji z nakupom tokeniziranih delnic pridobili ne le premoženjske pravice, temveč tudi članske pravice in s tem možnost vplivanja na upravljanje nepremičnin. Druga možnost pa je tokenizacija deležev v pogodbenih investicijskih skladih, pri čemer bi vlagatelj z vplačilom sredstev pridobil pravico do deleža v vrednosti in dobičku sklada (Trandafir, 2020).

S posredno tokenizacijo se izognemo predhodno omenjenim problemom. Vpis v zemljiško knjigo bo urejen na način, da bo družba ali sklad vpisan kot lastnik, kar pomeni, da ni potrebe po večkratnem vpisu. S tem se nepremičnina lahko učinkoviteje razdeli na tokene in omogoči deljeno lastništvo (*fractional ownership*). Manjši vlagatelji lahko sčasoma pridobijo lastništvo nepremičnin v celoti.

V Nemčiji je marca 2019 berlinski finančni ponudnik Brickblock kot prvi v Evropi tokeniziral in prodal stanovanjsko nepremičnino v skupni vrednosti dveh milijonov evrov, pri čemer je nemški

zvezni nadzorni organ za finančne storitve (BaFin) odobril prodajo tokeniziranih obveznic tudi zasebnim vlagateljem (de la Rubia, Sandner & Groß, 2021, str. 9). S tem se je posredna tokenizacija nepremičnin v Nemčiji uveljavila že pred nekaj leti.

7 Sklep

Blockchain omogoča inovativno, decentralizirano shranjevanje podatkov in izvedbo transakcij brez posrednikov, hkrati pa odpira pot razvoju različnih vrst tokenov: plačilnih, uporabniških, premoženjskih (*asset tokens*), tistih, ki se obravnavajo kot finančni instrumenti (*security tokens*) ter NFT-jev. Ključna izziva pri regulaciji tokenov sta pravna razvrstitev in postopek njihove izdaje. Tokenizacija premoženja, tako nepremičnine kot premičnine, se lahko izvede v obliki *security tokens* (tokeni kot finančni instrument) ali *asset tokens* (premoženjski tokeni).

Security tokens so finančni instrumenti, ki se po MiFID II klasificirajo podobno kot prenosljivi vrednostni papirji. Nasprotno pa premoženjski tokeni (*asset tokens*), ki so vezani na določeno premoženje, spadajo pod uredbo MiCA, ki ureja kriptosredstva, ki niso finančni instrumenti. Večina držav uporablja *security tokens* pri tokenizaciji premoženja.

Tokenizacija premoženja predstavlja nov pristop, ki omogoča večjo preglednost, likvidnost in zmanjšanje stroškov pri transakcijah, hkrati pa odpira možnosti za širšo dostopnost investicij. Ugotovili smo, da je kljub številnim prednostim pravni okvir za obravnavo digitalnih tokenov in prenosa lastništva še vedno v razvoju. Zlasti na področju nepremičnin se pojavljajo izzivi zaradi obličnostnih zahtev, kot so vpis v zemljiško knjigo, ki jih je z blockchainom zaenkrat težko uskladiti. Zaradi tega neposredna tokenizacija nepremičnin zaenkrat ni izvedljiva. Po drugi strani pa posredna tokenizacija ponuja realne možnosti za tokenizacijo nepremičnin preko vlaganja v nepremičninske družbe ali sklade. Kljub vsem izzivom so države, kot so Lihtenštajn, Nemčija in Švica, že sprejele zakone, ki omogočajo pravno varno uporabo blockchaina za prenos lastninskih pravic, kar kaže na potencialno prihodnost tokenizacije premoženja. Posledično se potrjuje naša teza, da je ključna ovira za neposredno tokenizacijo nepremičnin prav obličnostna narava zemljiškoknjižnih pravil in ne zrelost tehnologije. Dokler Slovenija (oz. EU) ne uvede digitalneregistrskih rešitev, bodo investitorji in izdajatelji logično izkoriščali posredne modele ali preselili dejavnost v jurisdikcije, kjer zakonodaja (Lihtenštajn, Švica, Nemčija) blockchain že integrira v prenos lastninskih pravic. Ker se digitalni tokeni z vsakim dnem bolj uveljavljajo v vsakdanji rabi, lahko pričakujemo, da bodo vse zakonodaje nadaljevale z razvojem in širšo

integracijo tokenizacije v pravni red. Slovenija takšnega zakona zaenkrat še nima, a se bo prav tako morala pravočasno prilagoditi hitrim digitalizacijskim trendom.

Literatura in viri

1. ABC Novice. (2023, oktober 1). *Blocksquare prva na svetu: Notarsko overjena tokenizacija nepremičnine v zemljiški knjigi*. <https://www.abcnovice.si/24ur-novice/slovenija/blocksquare-prva-na-svetu-notarsko-overjena-tokenizacija-nepremicnine-v-zemljiski-knjigi/>
2. Akadal, E., Karkas Geyik, S., & Satman, M. H. (2024). *Blockchain: Concepts, issues, and applications*. IU Press. <https://iupress.istanbul.edu.tr/en/book/blockchain-concepts-issues-and-applications/home>
3. Autorité des Marchés Financiers [AMF]. (2020). *Legal analysis on the application of financial regulations to security tokens and precisions on bulletin board*. AFM. <https://www.amf-france.org/en/news-publications/news-releases/amf-news-releases/amf-publishes-depth-legal-analysis-application-financial-regulations-security-tokens>
4. ABGB. (1811, 1. junij). *Allgemeines bürgerliches Gesetzbuch (RGL. Nr. 946/1811; konsolidirana različica z dne 30. 3. 2025)*. Rechtsinformationssystem des Bundes. <https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10001622>
5. Bečić, M. (2023). Tokeni i digitalizacija imovine: Pitanje pravne regulative. *Royal Society Open Science*, 10, 180381. <https://doi.org/10.1098/RSOS.180381>
6. BGB. (1896, 18. avgust). *Bürgerliches Gesetzbuch (BGBL. I S. 42; konsolidirana različica z dne 23. 10. 2024)*. Gesetze-im-Internet. <https://www.gesetze-im-internet.de/bgb/>
7. Blandin, A., Cloots, A. S., Hussain, H., Rauchs, M., Saleuddin, R., Allen, J., Zhang, B., & Cloud, K. (2019). Global cryptoasset regulatory landscape study. *Cambridge Centre for Alternative Finance Working Paper No. 19/06*, University of Cambridge.
8. Chance, C. (2020, oktober 28). *Security token offerings – A European perspective on regulation*. Clifford Chance. <https://www.cliffordchance.com/content/dam/cliffordchance/briefings/2020/10/security-token-offerings-a-european-perspective-on-regulation.pdf>
9. Di Angelo, M., & Salzer, G. (2023). Identification of token contracts on Ethereum: Standard compliance and beyond. *International Journal of Data Science and Analytics*, 16, 333–352. <https://doi.org/10.1007/s41060-022-00358-3>
10. de la Rubia, C., Sandner, P., & Groß, J. (2021). *Studie zur Tokenisierung von Immobilien*. Frankfurt School Blockchain Center.
11. European Commission. (2025). Bolje regulirani in pregledni finančni trgi. *EUR-Lex*. https://eur-lex.europa.eu/legal-content/SL/TXT/?uri=LEGISSUM:240405_3
12. Federal Council Switzerland. (2021, 18 June). *Federal Council brings DLT Act fully into force and issues ordinance*. FCS. <https://www.news.admin.ch/en/nsb?id=84035>
13. FINMA. (2018, 16 februar). *ICO guidelines*. Swiss Financial Market Supervisory Authority. <https://www.finma.ch/en/news/2018/02/20180216-mm-ico-wegleitung/>
14. García-Teruel, R. M., & Simón-Moreno, H. (2025). The digital tokenization of property rights: A comparative perspective. *Computer Law & Security Review*, 41, 105543. <https://doi.org/10.1016/j.clsr.2021.105543>

15. Ganz, E. (2022). Tokenization – From illiquid to liquid real estate ownership. *EY Insights*. https://www.ey.com/en_ch/insights/real-estate-hospitality-construction/tokenization-from-illiquid-to-liquid-real-estate-ownership
16. Grlica, I. (2023). Kriptovalute v slovenski zakonodaji in sodni praksi. *Odvetnik*, 109–110, 44.
17. Henker, R., Atzberger, D., Scheibel, W., & Döllner, J. (2023, maj). Real estate tokenization in Germany: Market analysis and concept of a regulatory and technical solution. V *2023 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)* (str. 1–6). IEEE. <https://doi.org/10.1109/ICBC56567.2023.10174954>
18. IBM. (2025). *Benefits of blockchain*. IBM. <https://www.ibm.com/think/topics/benefits-of-blockchain>
19. Johnpulle, C. (2024, april 9). *What is a token? Understanding crypto tokens: Types and functionality*. Fiat Republic Blog. <https://fiatpublic.com/what-you-need-to-know-about-digital-tokens-today/>
20. Joshi, S., & Choudhury, A. (2022). Tokenization of real estate assets using blockchain. *International Journal of Information and Intelligent Technology*. <https://doi.org/10.4018/IJIT.309588>
21. Juhart, M. (2007). [Uvod]. V M. Juhart, M. Tratnik, & R. Vrenčur, *Stvarno pravo* (pp. 39–95). GV založba.
22. Kaisto, J., Juutilainen, T., & Kauranen, J. (2024). Non-fungible tokens, tokenization, and ownership. *Computer Law & Security Review*, 54, 105996. <https://doi.org/10.1016/j.clsr.2024.105996>
23. Kiser, L., & Meier, E. (2025, junij 5). Tokenisierung im Immobilienmarkt – Eine ernstzunehmende Entwicklung. *Hochschule Luzern – Immobilienblog*. <https://hub.hslu.ch/immobilienblog/2023/06/05/tokenisierung-im-immobilienmarkt-eine-ernstzunehmende-entwicklung/>
24. Ko, T., Lee, J., & Ryu, D. (2018). Blockchain technology and manufacturing industry: Real-time transparency and cost savings. *Sustainability*, 10(11), 4274. <https://doi.org/10.3390/su10114274>
25. Kreppmeier, J., Laschinger, R., Steininger, B. I., & Dorfleitner, G. (2023). Real-estate security token offerings and the secondary market: Driven by crypto hype or fundamentals? *Journal of Risk and Financial Management*, 16(2), 94. <https://doi.org/10.3390/jrfm16020094>
26. Lambert, T., Liebau, D., & Roosenboom, P. (2022). Security token offerings. *Small Business Economics*, 59, 299–325. <https://doi.org/10.1007/s11187-021-00507-7>
27. Luchsinger Gähwiler, C. (2025). Tokenisierung von Grundstücken in der Schweiz – eine Bestandesaufnahme. *MLL News*. <https://www.mll-news.com/tokenisierung-von-grundstuecken-in-der-schweiz-eine-bestandesaufnahme/>
28. Majaski, C. (2024). *Cryptocurrency security token: Definition, forms, investing in*. Investopedia. <https://www.investopedia.com/terms/s/security-token.asp>
29. Marjosola, H. (2021). Security tokens and the future of EU securities law: Rethinking the harmonisation project. *Helsinki Legal Studies Research Paper No. 70*. University of Helsinki. <https://ssrn.com/abstract=3897849>
30. Markheim, M., & Berentsen, A. (2021). Real-estate trifft auf blockchain: Chancen und Herausforderungen der Tokenisierung von illiquiden Vermögenswerten. *Zeitschrift für Immobilienökonomie*, 7, 51–66. <https://doi.org/10.1365/s41056-020-00051-3>
31. MiFID II. (2014, 15. maj). *Direktiva 2014/65/EU o trgih finančnih instrumentov*. Uradni list Evropske unije, L 173, 349–496. <https://eur-lex.europa.eu/eli/dir/2014/65/oj>
32. MiCA. (2023, 31. maj). *Uredba (EU) 2023/1114 o trgih kripto-sredstev*. Uradni list Evropske unije, L 150, 1–120. <https://eur-lex.europa.eu/eli/reg/2023/1114/oj>
33. Miglo, A. (2021). STO vs. ICO: A theory of token issues under moral hazard and demand uncertainty. *Journal of Risk and Financial Management*, 14(6), 232. <https://doi.org/10.3390/jrfm14060232>

34. Nagele, T., & Bont, P. (2019). Tokenized structures and assets in Liechtenstein law. *Trusts & Trustees*, 25(6), 633–663. <https://doi.org/10.1093/tandt/ttz073>
35. Nakamoto, S. (2008). *Bitcoin: A peer-to-peer electronic cash system*. <https://bitcoin.org/bitcoin.pdf>
36. OZ. (2001, 29. november). Obligacijski zakonik. Uradni list Republike Slovenije, 83/01 (z nadaljnjimi spremembami). <https://pisrs.si/pregledPredpisa?id=ZAKO2135>
37. Omlor, S. (2020). Digitales Eigentum an Blockchain-Token – rechtsvergleichende Entwicklungslinien. *Zeitschrift für Vergleichende Rechtswissenschaft*, 119, 41–58.
38. Pateter, K., & Huber, M. (2022). Zu den rechtlichen Rahmenbedingungen der Tokenisierung physischer Vermögenswerte. GRAU, 2022(24), 1–12. <https://rdb.manz.at/document/rdb.tso.LIgrau20220304>
39. Patti, F. P. (2024). The European MiCA regulation: A new era for initial coin offerings. *SSRN Electronic Journal*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4810910
40. Peres, R., Schreier, M., Schweidel, D. A., & Sorescu, A. (2023). Blockchain meets marketing: Opportunities, threats, and avenues for future research. *International Journal of Research in Marketing*, 40(1), 1–11. <https://doi.org/10.1016/j.ijresmar.2022.11.004>
41. Richter, J. (2022). Blockchain statt Besitz – Erwerb von Rechten auf Basis von Non-Fungible Token. *Neue Juristische Wochenschrift*, 75(48), 3469–3475.
42. Samec Berghaus, N., & Drnovšek, K. (2018). Iluzija pojma pametne pogodbe. In M. Repas (Ed.), *Konferenčni zbornik X. posveta Pravo in ekonomija: Digitalno gospodarstvo* (pp. 19– 30). UM Založba. <https://doi.org/10.18690/978-961-286-169-8.2>
43. Sharma, R. (2024, januar 18). Non-fungible token (NFT): What it means and how it works. *Investopedia*. <https://www.investopedia.com/non-fungible-token-nft-5115211>
44. Sladič, J. (2019). Kriptovalute (kriptotokeni, tokens) v zasebnem pravu in v izvršilnem postopku. *Podjetje in delo*, 45(8), 123–145.
45. SPZ. (2002, 4. oktober). Stvarnopravni zakonik. Uradni list Republike Slovenije, 87/02 (s kasnejšimi spremembami 91/13, 23/20). <https://pisrs.si/pregledPredpisa?id=ZAKO3242>
46. State Secretariat for International Finance. (n.d.). *Blockchain / DLT*. Swiss Federal Administration. <https://www.sif.admin.ch/en/blockchain-dlt-en>
47. Swinkels, L. (2022). Empirical evidence on the ownership and liquidity of real-estate tokens. *Financial Innovation*, 8(20). <https://doi.org/10.1186/s40854-022-00427-5>
48. Tehnološki park Ljubljana. (2021, 21. september). Slovenija prva država na svetu izdala NFT žetone (Non-fungible tokens). <https://www.tp-lj.si/sl/novice/slovenija-prva-drzava-na-svetu-izdala-nft-zetone-non-fungible-tokens-2021-09-21>
49. Trandafir, E. (2025, september 18). Blockchain: Vor dem entscheidenden Schub? *Real Estate Move*. <https://realestatemove.ch/2020/09/18/blockchain-vor-dem-entscheidenden-schub/>
50. TVTG. (2019, 3. oktober). Gesetz über Token und VT-Dienstleister (Token- und VT-Dienstleister-Gesetz; TVTG) [Zakon o žetonih in ponudnikih zaupanja vrednih tehnologij]. Liechtensteinisches Landesgesetzblatt, 2019(301). <https://www.gesetze.li/konso/2019301000>
51. Völkle, M. (2021). Grundbaustein der weiterentwickelten Digitalisierung des Rechts: Ethereum 2.0. *MMR – Zeitschrift für IT-Recht und Recht der Digitalisierung*, 24(7), 398–403.

52. Wilsch, P. (2017). Die Blockchain-Technologie aus der Sicht des deutschen Grundbuchrechts. *Zeitschrift für Digitalisierung des Rechts*, 1(2), 33–45.
53. ZGB. (1907, 10. december). Schweizerisches Zivilgesetzbuch vom 10. Dezember 1907 (SR 210). Systematische Sammlung des Bundesrechts. https://www.fedlex.admin.ch/eli/cc/24/233_245_233/de
54. Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017). An overview of blockchain technology: Architecture, consensus, and future trends. In *2017 IEEE International Congress on Big Data (BigData Congress)* (pp. 557–564). IEEE. <https://doi.org/10.1109/BigDataCongress.2017.85>
55. ZTFI-1. (2018, 30. november). Zakon o trgu finančnih instrumentov. Uradni list Republike Slovenije, 77/18 (z nadaljnjimi spremembami). <https://pisrs.si/pregledPredpisa?id=ZAKO7888>

0	1	0	1	0	0	1	1	1	0	0	1	0	1	1	0	0	1	1	0	1	1	0	1	1	1	0	0	1	0	1	0	1	0	0	
1	1	1	0	0	1	0	1	1	0	0	1	1	1	0	1	1	0	1	1	1	0	0	1	0	1	0	0	1	1	1	0	0	1	0	1
1	0	0	1	1	1	0	1	1	0	0	0	0	0	0	0	0	1	0	0	1	1	1	0	0	1	0	1	1	0	0	1	1	1	0	
1	1	1	0	0	1	0	1	0	0	1	1	1	0	0	1	0	1	1	0	0	1	1	1	0	1	1	0	1	1	1	0	0	0	1	
1	1	1	0	0	1	0	1	1	0	0	1	1	1	0	1	1	0	1	1	1	0	0	1	1	1	1	1	0	1	0	0	1	1	0	
0	1	1	0	0	1	1	1	0	1	0	0	0	0	0	0	0	1	0	1	0	1	1	1	0	0	1	1	1	0	0	0	1	0	1	
0	1	0	1	0	0	1	1	0	0	1	0	1	1	0	0	1	1	1	0	1	1	0	1	1	1	0	0	1	0	1	0	1	0	0	
1	1	1	0	0	1	0	1	1	0	0	1	1	1	0	1	1	0	1	1	0	1	1	1	0	1	1	1	0	0	1	1	0	0	1	
1	1	1	0	0	1	0	1	1	0	0	1	1	1	0	1	1	0	1	1	0	1	1	0	1	1	1	0	0	1	1	1	0	0	1	
1	0	0	0	0	1	0	1	1	0	0	1	1	1	0	1	1	0	1	1	0	1	1	0	0	1	0	1	0	0	1	1	1	0	0	
1	1	1	0	0	1	0	1	1	0	0	1	1	1	0	1	1	0	1	1	1	0	0	1	1	1	0	1	1	1	0	0	1	1	0	
0	1	1	0	0	1	0	1	1	0	1	1	1	0	0	0	1	0	1	0	1	1	1	0	0	1	1	1	1	0	0	0	1	0	1	
0	1	0	1	0	0	1	1	1	0	0	1	0	1	1	0	0	1	1	1	0	1	1	0	1	1	0	1	1	0	0	1	0	1	0	
1	1	1	0	0	1	0	1	1	0	0	1	1	1	0	1	1	0	1	1	1	0	1	1	0	1	1	1	0	0	1	1	1	0	0	
1	1	1	0	0	1	0	1	1	0	0	1	1	1	0	1	1	0	1	1	1	0	0	1	1	1	0	1	1	1	0	0	1	1	0	
0	1	1	0	0	1	0	1	1	0	0	1	1	1	0	1	1	0	1	1	1	0	0	1	1	1	1	0	1	0	0	1	1	1	0	
0	1	0	0	1	1	1	0	0	1	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1	1	0	0	1	1	0	
0	1	0	0	1	1	1	0	0	1	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1	1	0	0	1	0	1	1	0	0	1	
0	1	0	0	1	1	1	0	0	1	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1	1	0	0	1	0	1	1	0	0	1	
0	1	0																																	