

DIGITALNA EKONOMIJA IN PRAVO 2024

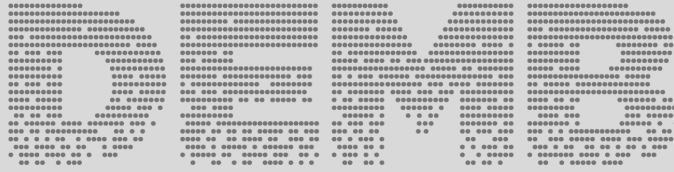
Študentsko posvetovanje o ekonomskih in pravnih izzivih
digitalne preobrazbe

ZBORNİK RECENZIRANIH ZNA NSTVENIH PRISPEVKOV

Dejan Romih (ur.)

Nejc Fir (ur.)





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

Maribor, avgust 2024

DIGITALNA EKONOMIJA IN PRAVO 2024

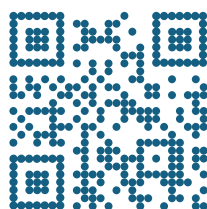
Študentsko posvetovanje o ekonomskih in pravnih izzivih digitalne preobrazbe

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

<https://demb.si/>

<https://demb.si/digitalna-ekonomija-in-pravo-2024/>

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 2024

Študentsko posvetovanje o ekonomskih in pravnih izzivih digitalne preobrazbe

Maribor

Društvo ekonomistov Maribor

2024

<https://demb.si/>

Zbornik recenziranih znanstvenih prispevkov

Uredila dr. Dejan Romih in Nejc Fir

Tehnično uredila dr. Dejan Romih in Nejc Fir

Recenzirali dr. Blaž Frešer, dr. Ivona Huđek, dr. Klavdij Logožar, dr. Domen Malc, dr. Gregor Polančič, dr. Andreja Primec, dr. Martina Repas, dr. Miha Šepec, dr. Bojan Tičar

Lektoriral Mitja Brünec

Založilo Društvo ekonomistov Maribor

2024

Licenčni pogoji



Vsebina zbornika je na voljo pod pogoji slovenske licence Creative Commons 4.0 CC BY NC-ND, ki ob navajanju in priznavanju avtorstva dopušča reproduciranje in distribuiranje, ne dovoljuje pa dajanja v najem, priobčevanja javnosti za komercialni namen in nobene predelave.

Kataložni zapis o publikaciji (CIP) pripravili v Narodni in univerzitetni knjižnici v Ljubljani

[COBISS.SI-ID 205549571](https://nbn-resolving.org/urn:nbn:si:Zve:205549571)

ISBN 978-961-6059-22-0 (PDF)

Organizacijski odbor

Dr. Dejan Romih, UM EPF, DEMB, predsednik

Dr. Blaž Frešer, UM EPF

Dr. Andreja Primec, UM EPF, UP FM

Nejc Fir, UM EPF, podpredsednik

Aljoša Polajžar, UM PF

Pina Slaček, Študentski svet UM EPF

Asja Lešnik, Študentski svet UM PF

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 2024, Posvetovanje o ekonomskih in pravnih izzivih digitalne preobrazbe, ki je potekalo 31. maja 2024 na daljavo s pomočjo aplikacije Microsoft Teams. Na študentskem posvetovanju je sodelovalo 13 študentov Univerze v Ljubljani in Univerze v Mariboru, ki so predstavili 13 znanstvenih prispevkov s področja digitalne ekonomije in prava. V tem zborniku je objavljenih 12 znanstvenih prispevkov, ki so jih študenti napisali skupaj z visokošolskim učiteljem ali sodelavcem.

Študentsko posvetovanje je potekalo od 10.00 do 13.59, pri čemer so njegove udeležence pozdravili red. prof. dr. Žan Jan Oplotnik, predsednik Društva ekonomistov Maribor, red. prof. dr. Jernej Belak, prodekan za mednarodno sodelovanje Ekonomsko-poslovne fakultete Univerze v Mariboru, izr. prof. dr. Miha Šepec, predsednik Akademskega zbora Pravne fakultete Univerze v Mariboru, študentska Pina Slaček, prodekanica za Študentska vprašanja Ekonomsko-poslovne fakultete Univerze v Mariboru, in študentska Asja Lešnik, prodekanica za študentska vprašanja Pravne fakultete Univerze v Mariboru, ki so študentom in njihovim mentorjem zaželeli uspešno predstavitev. Uvodno vabljeno predavanje je izvedel Damijan Pezdíček iz podjetja Visa Inc.

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

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

Zahvala

Društvo ekonomistov Maribor se iskreno zahvaljuje Ekonomsko-poslovni fakulteti Univerze v Mariboru (zlasti red. prof. dr. Poloni Tominc), Pravni fakulteti Univerze v Mariboru (zlasti red. prof. dr. Tomažu Kerestešu), Študentskemu svetu Ekonomsko-poslovne fakultete Univerze v Mariboru (zlasti študentki Pini Slaček) in Študentskemu svetu Pravne fakultete Univerze v Mariboru (zlasti Asji Lešnik) za soorganiziranje študentskega posvetovanja Digitalna ekonomija in pravo 2024, urednikoma doc. dr. Dejanu Romihu in asist. Nejcju Firu za urejanje zbornika znanstvenih prispevkov ter recenzentom za recenziranje znanstvenih prispevkov. Iskreno se zahvaljujemo tudi (drugim) udeležencem študentskega posvetovanja. Želimo si, da bi drugo leto sodelovalo še več visokošolskih ustanov in študentov.

Red. prof. dr. Žan Jan Oplotnik,
predsednik društva

Kazalo

Uporaba ChatGPT-ja v poslovanju

Jasmina Gergorec, Andreja Primec..... 13

Značilnosti spletnega nakupovanja mladih v Sloveniji

Lina Jenšac, Nejc Fir 30

Ozaveščenost o digitalnem evru med študenti ekonomije in tehnike

Katarina Leš, Nataša Gajšt, Nejc Fir 45

Analiza poročanja ameriških kabelskih televizijskih postaj o umetni inteligenci

Tinkara Primec, Alenka Kavkler, Dejan Romih..... 66

Uporaba YouTubea za izobraževanje med študenti medicine

Dominik Škrinjar, Domen Malc, Dejan Romih 76

Katere so vodilne sile na področju umetne inteligence po poročanju ameriških kabelskih televizijskih postaj

Timotej Peter Valcl, Dejan Romih 97

(Ne)dopustnost profiliranja za namene oglaševanja na spletu

Kaja Lenart, Jan Stajnko 108

Pravna ureditev odgovornosti za škodo, povzročeno z umetno inteligenco v Sloveniji

Asja Lešnik, Petra Weingerl..... 120

(Proti)pravna ravnanja v virtualni resničnosti

Matej Makoter Rožmarin, Kristjan Zahrastnik..... 133

Pravni položaj otrok vplivnežev

Andreja Mlinar, Katja Drnovšek 148

Pravna analiza e-športa s poudarkom na varstvu mladoletnikov

Žiga Rodošek, Andreja Primec..... 160

Problemi uporabe z umetno inteligenco obdelanih dokazov v kazenskem postopku

Oskar Peče..... 178

DIGITALNA EKONOMIJA

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

Uporaba ChatGPT-ja v poslovanju

Jasmina Gergorec ✉

BTC, d. d.

Ljubljana, Slovenija

Dr. Andreja Primec 

Univerza v Mariboru, Ekonomsko-poslovna fakulteta

Maribor, Slovenija

Povzetek: V zadnjem času je umetna inteligenca spremenila igro v poslovnem svetu, z orodji, kot je ChatGPT, pa prevzema pomembne vloge v različnih poslovnih operacijah. ChatGPT je napreden jezikovni model, ki ga je razvilo podjetje OpenAI, in je zasnovan za generiranje človeku podobnih odgovorov v naravnem jeziku. Sposobnost ChatGPT-ja omogoča podjetjem, da izboljšajo storitve za stranke, optimizirajo interne procese, avtomatizirajo marketinške kampanje, hitreje analizirajo velike količine podatkov, izboljšajo komunikacijske strategije z generiranjem privlačnih vsebin in pomagajo pri izobraževanju zaposlenih. Vendar pa se lahko podjetja pri implementaciji ChatGPT-ja soočajo z izzivi, ki vključujejo potrebo po kakovostnih podatkih, izzivi pri integraciji z obstoječimi sistemi ter pravnimi (varstvo zasebnosti in človekovih pravic) in etičnimi izzivi. V tem prispevku bomo raziskali ključne značilnosti in delovanje ChatGPT-ja ter na praktičnih primerih predstavili, kako lahko podjetja izkoristijo to tehnologijo za ustvarjanje konkurenčne prednosti. Ugotavljamo, da bo z nenehnim napredkom umetne inteligence vpliv teh tehnologij na poslovne modele in operacije še naprej naraščal. Podjetja, ki bodo sposobna uspešno integrirati in uporabljati ta orodja, pa bodo stala v ospredju inovacij in uspešno ohranjala svojo konkurenčno prednost.

Ključne besede: ChatGPT, intelektualna lastnina, obdelava naravnega jezika, umetna inteligenca, varstvo zasebnosti.

The use of ChatGPT in business

Jasmina Gergorec ✉

BTC, d. d.

Ljubljana, Slovenia

Andreja Primec, PhD 

University of Maribor, Faculty of Economics and Business

Maribor, Slovenia

Abstract: Recently, artificial intelligence has become a game-changer in the business world, with tools like ChatGPT taking on significant roles in various business operations. ChatGPT is an advanced language model developed by OpenAI, designed to generate human-like responses in natural language. The capabilities of ChatGPT allow companies to enhance customer service, optimize internal processes, automate marketing campaigns, analyze large amounts of data more quickly, improve communication strategies by generating engaging content, and assist in employee training. However, companies may face challenges when implementing ChatGPT, including the need for high-quality data, integration challenges with existing systems, legal issues (privacy protection and human rights), and ethical concerns. This paper explores the key features and functioning of ChatGPT and presents practical examples of how companies can leverage this technology to create a competitive advantage. We conclude that with the continuous advancement of artificial intelligence, the impact of these technologies on business models and operations will continue to grow. Companies that can successfully integrate and utilize these tools will be at the forefront of innovation and will maintain their competitive edge effectively.

Keywords: artificial intelligence, ChatGPT, intellectual property, natural language processing, privacy protection.

1 Uvod

Razvoj tehnologij, ki temeljijo na umetni inteligenci, je odprl vrata novim priložnostim, ki predstavljajo ključne dejavnike za pridobivanje konkurenčne prednosti za podjetja (Kuzior, Sira, & Brozek, 2023). Med raznolikimi tehnologijami umetne inteligence je ChatGPT, napredni jezikovni model, ki ga je razvil OpenAI. ChatGPT je v rekordnem času postal izjemno priljubljen, saj je samo dva meseca po svojem zagonu dosegel 100 milijonov aktivnih uporabnikov na mesec. Ta podvig ga uvršča na prvo mesto kot najhitreje rastočo potrošniško aplikacijo v zgodovini. To potrjuje študija investicijske banke UBS (UBS, 2023). Dnevno ChatGPT uporablja približno 13 milijonov obiskovalcev. Ta hiter vzpon presega rast drugih priljubljenih aplikacij, kot sta TikTok in Instagram, ki so za doseganje istega števila uporabnikov potrebovali devet mesecev oz. dve leti in pol (Hu, 2023).

Namen tega prispevka je analizirati vlogo ChatGPT-ja v podjetjih in raziskati pravne izzive, ki jih prinaša, s posebnim poudarkom na varstvu osebnih podatkov in pravicah intelektualne lastnine. V prvem delu prispevka bomo v poglavju Pregled literature predstavili ChatGPT, pomen varstva osebnih podatkov in to, s kakšnimi pravnimi izzivi se soočamo na področju pravic intelektualne lastnine. Drugi del je aplikativni del, kjer bomo na dveh praktičnih primerih predstavili delovanje ChatGPT-ja v poslovnem okolju: prvi se osredotoča na personalizacijo ponudbe, drugi pa na oblikovanje marketinške strategije. Sledi poglavje razprava, kjer bomo analizirali prednosti in slabosti uporabe ChatGPT-ja. Cilj je predstaviti funkcije ChatGPT-ja ter pravne izzive.

2 Pregled literature

V tem poglavju bomo obravnavali pravne izzive, povezane z uvajanjem jezikovnega modela ChatGPT v poslovne procese. Osredotočili se bomo na ključne vidike zagotavljanja zasebnosti in varstva podatkov ter na kompleksnost varovanja pravic intelektualne lastnine. Pregledali bomo regulativne okvire, kot je GDPR, in raziskali, kako ti vplivajo na uporabo umetne inteligence v poslovnem kontekstu.

2.1 Predstavitev jezikovnega modela ChatGPT

ChatGPT¹ predstavlja napreden jezikovni model, ki ga je ustvaril OpenAI. Uporablja obdelavo

¹ GPT – generative pre-trained transformer – je vrsta algoritma strojnega učenja, ki uporablja globoko učenje in veliko podatkovno bazo učnih besedil, da generira novo besedilo kot odgovor na uporabnikovo zahtevo.

naravnega jezika (NLP²) za generiranje besedila, podobnega človeškemu, kot odgovor na različne vnose (Lucchi, 2023). Ta sistem je bil razvit z uporabo obsežnih besedilnih zbirk in metod globokega učenja³, kar mu omogoča razumevanje jezikovnih vzorcev in zagotavljanje smiselnih ter relevantnih odgovorov (Arman & Laimya, 2023). Poleg osnovnega jezikovnega modeliranja ChatGPT vključuje tudi zmogljivosti za izvajanje specifičnih nalog, kot so programiranje, matematični izračuni, analiza podatkov in celo generiranje umetniških del (Sundar & Mok, 2023). ChatGPT je konec leta 2015 ustanovila skupina tehnoloških vizionarjev, med katerimi so Elon Musk, Sam Altman, Greg Brockman in Ilya Sutskever (Arman & Laimya, 2023). Prvi Generative Pre-Trained Transformer (GPT) je bil izdan junija 2018. Program, ki ga je razvil Open AI, je vseboval 117 milijonov parametrov (Olliver, in drugi, 2023). Z izdajo verzije GPT-4 je OpenAI znatno izboljšal zmogljivost na področju globokega učenja (Ray, 2023).

Vključitev ChatGPT-ja v družbo odpira številne priložnosti za izboljšanje življenja v različnih sektorjih, kot so izobraževanje, zabava, finance in zdravstvo (Sallam, 2023). V izobraževanju lahko študenti npr. hitreje dostopajo do informacij preko dialoga, medtem ko lahko zdravniki uporabljajo UI za hitrejše diagnoze. V finančnem sektorju omogoča hitrejše odločanje s pomočjo analize podatkov v realnem času, medtem ko v podjetjih aplikacije s podporo ChatGPT povečujejo učinkovitost zaposlenih. Vse te prednosti kažejo na pozitiven vpliv integracije GPT-ja v naše vsakdanje življenje, s čimer izboljšujemo kakovost življenja sedanjih in prihodnjih generacij (Shaji, Hovan, & Gabrio, 2023). Digitalni val je neizbežen in pomembno je, da ga sprejmemo kot priložnost. Bolj ko bomo opremljeni z digitalnim znanjem, uspešneje bomo sledili množici novih tehnologij in orodij, kar bo koristilo našemu napredku (Primec, 2022).

2.2 Zagotavljanje zasebnosti in varstvo podatkov

Pomen zasebnosti in varstva podatkov v sistemih umetne inteligence (UI) je ključen za etično, odgovorno in skladno uporabo teh tehnologij, pri čemer ima osrednjo vlogo Splošna uredba o varstvu podatkov (GDPR)⁴. Ta določa pravila o varstvu posameznikov pri obdelavi osebnih podatkov in pravila o prostem pretoku osebnih podatkov (Premzl, 2019). Brez regulacije se lahko podatki

² Angl. Natural Language Processing omogoča računalniškim sistemom, da interpretirajo in razumejo človeški jezik.

³ Napredna vrsta strojnega učenja, ki uporablja večplastne nevronske mreže za obdelavo in analizo podatkov.

⁴ Uredba (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES (Splošna uredba o varstvu podatkov).

uporabljajo na načine, ki ne služijo našim interesom (Ackermann, 2022). Etični vidiki zahtevajo spoštovanje in varovanje osebnih in občutljivih informacij uporabnikov, saj lahko vsaka zloraba vodi do resnih posledic, kot je kraja identitete ali finančna izguba. Te skrbi so bile obravnavane v različnih raziskovalnih člankih, ki razpravljajo o uporabi klepetalnih robotov na osnovi LLM⁵ (Hariri, 2023; Sebastian, 2023). Poleg tega je varovanje podatkov ključnega pomena za ohranjanje integritete podatkov in zaščito pred kibernetскими napadi, ki lahko manipulirajo z vedenjem modelov UI. Za podjetja, ki uporabljajo UI, kot je ChatGPT, je ključno, da ocenijo svoje postopke zbiranja, shranjevanja in obdelave uporabniških podatkov, da zagotovijo skladnost z GDPR in drugimi predpisi ter s tem krepijo zaupanje uporabnikov in spodbujajo širšo sprejetost tehnologij UI (Glorin, 2023).

OpenAI trdi, da je njegovo delovanje v skladu s predpisi, čeprav obstajajo pomisleki glede celovitosti zaščite zasebnosti. Možnost onemogočanja zgodovine klepeta je ena od funkcij za izboljšanje zasebnosti, vendar sama po sebi morda ne odpravlja vseh skrbi uporabnikov glede varovanja in obdelave njihovih osebnih podatkov (Xiaodong, Ran, & Jianbing, 2023). Gumb v nastavitvah omogoča izbris zgodovine klepetov in ustavi njihovo uporabo za treniranje UI, vendar ne pojasni, ali se pretekli pogovori lahko še vedno uporabljajo za »treniranje« (Colmenero-Fernandez, 2023). Vneseni podatki lahko postanejo del širše podatkovne baze, kar omogoča njihovo dostopnost tretjim osebam pri specifičnih povpraševanjih. To lahko vodi do neželenega razkritja podatkov, kar je v nasprotju z varnostnimi protokoli in politikami podjetja (IBM, 2023).

Prvo tveganje, ki ga povzroči uporaba ChatGPT-ja, izvira iz uporabe javno dostopnih podatkov za njegovo usposabljanje, vključno z osebnimi podatki, najdenimi na spletu, v blogih ali recenzijah prispevkov. Zaradi obsežnega zbiralnika podatkov, ki presega 570 GB, se pojavlja vprašanje, ali so bili ti podatki pridobljeni z ustrezno privolitvijo. Ker se tehnologija LLM razvija, postajajo ta vprašanja zasebnosti vse bolj pereča, saj se dotikajo vedno večjega kroga ljudi. Drugo tveganje je povezano z osebnimi vnosi uporabnikov, ki so izkoriščeni za izboljšanje odzivov ChatGPT-ja. To lahko vodi do zbiranja in shranjevanja občutljivih informacij, kar je spodbudilo nekatere države, da zastavijo vprašanja o skladnosti ChatGPT-ja z GDPR in sprožijo preiskave. Primeri, kjer ChatGPT razkrije osebne podatke na podlagi prejšnjih vnosov, dodatno poudarjajo potrebo po previdnosti pri ravnanju z občutljivimi podatki (Xiaodong, Ran, & Jianbing, 2023). Problem nastane, ker imajo modeli strojnega učenja kompleksne arhitekture črnih škatel, ki otežujejo razumevanje, kako je

⁵ Angl. large language model – veliki jezikovni model je vrsta algoritma strojnega učenja, ki je usposobljen na izjemno velikih podatkovnih zbirkah obstoječega jezika in je zasnovan za ustvarjanje novih, naravoslovnih odzivov na pozive.

določena točka podatkov ali skupina točk podatkov uporabljena. Ko je treba v modelu strojnega učenja izključiti specifične podatke, je to lahko problematično. Da se to stori, je običajno treba model ponovno usposobiti z novim naborom podatkov, ki te specifične podatke izključuje. Ponovno usposabljanje modela pa ni preprosto ali hitro opravilo. Potrebuje novo, očiščeno zbirko podatkov, kar lahko traja dolgo, poleg tega pa je proces lahko tudi drag (The Digital Watch observatory, 2023).

Samsung se je soočil s primerom, ko so njihovi inženirji pomotoma delili notranjo kodo z nalaganjem na ChatGPT, zaradi česar je podjetje začasno omejilo uporabo orodij generativne UI na službenih napravah. Podobne previdnostne ukrepe so sprejela tudi druga podjetja. Storitve za varovanje podatkov je npr. zabeležila in preprečila poskuse vnosa občutljivih podatkov v ChatGPT-ju pri 4,2 % od 1,6 milijona zaposlenih pri svojih klientih. Ti vnosi so vključevali podatke o strankah, izvorno kodo in druge zaupne informacije. V enem izmed primerov je vodja podjetja želel, da ChatGPT ustvari predstavitev na osnovi korporativne strategije. Drugi primer vključuje zdravnika, ki je modelu posredoval osebne podatke pacienta za pisanje pisma zavarovalnici. Obstaja skrb, da bi se takšni občutljivi podatki lahko nenamerno pojavili v odgovorih modela pri določenih pozvedbah (Swaney, 2023). Tako je ključno vzpostaviti pravni okvir, ki bo zagotavljal varno in učinkovito uporabo vseh vrst umetne inteligence (Primec, 2020).

2.3 Drugi pravni izzivi

V sodobni globalni ekonomiji je intelektualna lastnina postala osrednja komponenta tržnega sistema, saj igra ključno vlogo pri spodbujanju inovacij, konkurenčnosti in gospodarske rasti. Je bistveni del ekosistema, ki povezuje raziskovalce, podjetnike in potrošnike ter omogoča prenos znanja in tehnologije v gospodarsko korist (Pretnar, 2020). Vprašanja intelektualne lastnine, povezana z lastništvom kode ali besedil, ustvarjenih s pomočjo ChatGPT-ja, so lahko precej zapletena. Glede intelektualne lastnine je model ChatGPT treniran na zbirki že obstoječih del, a še vedno ni jasno, kako pravno ravnati z vsebino, pridobljeno iz intelektualne lastnine drugih, ugotavlja analitik Bern Elliot (McKendric, 2022). Pogoji storitve določajo, da outputi, ki jih ustvarijo uporabniki, pripadajo uporabnikom, ki so vnesli vhodne podatke (Cuomo, 2023). Lucchi (2023) poudarja pomen razumevanja kompleksnosti pravnih vidikov, ki obkrožajo uporabo avtorsko zaščitene materialov v kontekstu razvoja jezikovnih modelov UI, ob upoštevanju morebitnih izjem, kot je poštena uporaba.

Poleg tega se v kontekstu uporabe avtorsko zaščitene del pojavljajo vprašanja, ko UI ustvari dela, ki bi lahko bila avtorsko zaščitena. Razlikovanje med primeri, ko je UI le orodje v rokah avtorja, in situacijami, ko UI samostojno sprejema ustvarjalne odločitve, je ključnega pomena. Bogataj Jančič (2023) opozarja na legalne zaplete, ko dela, ustvarjena z UI, kršijo avtorske pravice drugih, in raziskuje vprašanja odgovornosti – kdo je odgovoren za kršitve, ki jih stori UI: njen ustvarjalec, trener ali uporabnik. Ta vprašanja bodo postajala še bolj zapletena, ko bo UI sposobna ustvarjati popolnoma samostojno, kar zahteva posebno pozornost in razumevanje pravnega okvira, ki ureja avtorske pravice na digitalnem enotnem trgu v EU, določbe o pošteni uporabi v Združenih državah Amerike in podobno, kar omogoča določeno uporabo brez dovoljenja avtorjev.

Nedavno je Evropski patentni urad (EPO) sprejel pomembno odločitev, s katero je zavrnil dve patentni vlogi, kjer je bila kot izumitelj navedena umetna inteligenca. Steven Thaler, ustvarjalec sistema DABUS, je predložil vlogi z namenom, da bi umetni inteligenci priznali pravico do izumov, ki jih je ta »ustvarila«. EPO je vlogi zavrnil, saj je mnenja, da mora biti izumitelj človek in ne stroj. Ta pogled delijo tudi pravni sistemi v Združenih državah Amerike in Združenem kraljestvu, medtem ko sta Južna Afrika in Avstralija sprejeli bolj progresivno stališče in priznavata, da je izumitelj tudi stroj (Gastaldi, Massimiliano, & Crisci, 2023). Ta razlika v interpretacijah odpira širše vprašanje o evoluciji pravnih okvirov, ki urejajo intelektualno lastnino, in sicer v luči tehnološkega napredka. Ta primer kaže na potrebo po mednarodni harmonizaciji prava intelektualne lastnine, ki bi upoštevala sodobne tehnološke dosežke in njihov vpliv na prakse podeljevanja patentov.

3 Metode

Prvi del prispevka predstavlja teoretični del, kjer smo s pomočjo pregleda literature raziskali ključne teoretične pojme, povezane z ChatGPT-jem, varstvo osebnih podatkov in pravice intelektualne lastnine. Naša deskriptivna analiza vključuje metode deskripcije in klasifikacije za določanje pojmov. Pregledali smo relevantno literaturo, da bi povzeli stališča drugih avtorjev s tega področja.

Drugi del je aplikativni del, kjer smo preučili, kako ChatGPT odpira nove možnosti za reševanje problemov v podjetjih in spodbuja napredek v različnih poslovnih segmentih. S poudarkom na praktičnih primerih smo prikazali, kako se lahko tehnologija ChatGPT uporablja za izboljšanje poslovnih procesov znotraj podjetja. Uporabili smo plačljivo različico ChatGPT-4 in ji zastavili dve vprašanji. Analiza vključuje pregled relevantnih zakonov, sodne prakse in strokovne literature. S

pomočjo komparativne metode smo primerjali varstvo osebnih podatkov ChatGPT-ja z GDPR. Naš raziskovalni pristop je interdisciplinaren in kombinira različne metode za celovito razumevanje vloge ChatGPT-ja v podjetjih. Ta pristop bo omogočil razvoj poglobljenih ugotovitev in konkretnih priporočil.

4 Raziskava

V tem poglavju je izvedena raziskava s klepetalnim robotom ChatGPT-4, ki se nanaša na personalizacijo ponudbe s ChatGPT-jem in oblikovanje marketinške strategije.

4.1 Primer 1: Personalizacija ponudbe s ChatGPT-jem

Na zastavljeno vprašanje »Kako lahko podjetje, ki na spletu prodaja pametne naprave, uporabi ChatGPT za izboljšanje in personalizacijo storitev za stranke?« je orodje OpenAI ChatGPT-4 generiralo sledeči odgovor:

Predstavljajmo si podjetje X, ki se ukvarja s prodajo pametnih naprav preko spleta. Svoje storitve za stranke želi izboljšati in personalizirati izkušnjo nakupovanja z uporabo ChatGPT. Tu je primer, kako bi to lahko storili:

1. Faza uvedbe ChatGPT kot virtualnega pomočnika: Podjetje X razvije virtualnega pomočnika, ki temelji na ChatGPT, in ga integrira na svojo spletno stran in v mobilno aplikacijo. Ta pomočnik je zasnovan tako, da ponuja takojšnje odgovore na pogosta vprašanja strank, kot so informacije o izdelkih, stanje naročil in podrobnosti o dostavi.

2. Analiza podatkov o vedenju in preferencah uporabnikov: Virtualni pomočnik zbira in analizira podatke o vedenju uporabnikov na spletni strani podjetja X – katere strani obiskujejo, kateri izdelki jih najbolj zanimajo in kakšna vprašanja zastavljajo. S pomočjo teh informacij ChatGPT nato personalizira priporočila izdelkov za vsakega posameznega uporabnika.

3. Individualizirana podpora in priporočila izdelkov: Ko stranka postavi vprašanje, ChatGPT ne samo da ponudi odgovor, ampak tudi predlaga izdelke, ki so prilagojeni njenim predhodnim interesom in vprašanjem. Če stranka na primer vpraša, kako lahko poveča življenjsko dobo baterije svoje naprave, ji ChatGPT lahko ponudi odgovor skupaj s priporočilom za nakup dodatne baterije ali napajalnika, ki je kompatibilen z njenim modelom naprave.

4. Zmanjšanje stroškov in izboljšanje zadovoljstva strank: Z zmanjšanjem potrebe po človeških agentih za rutinska vprašanja in zagotavljanjem hitrih in učinkovitih odgovorov 24/7, podjetje X zmanjša stroške in hkrati izboljša zadovoljstvo strank.

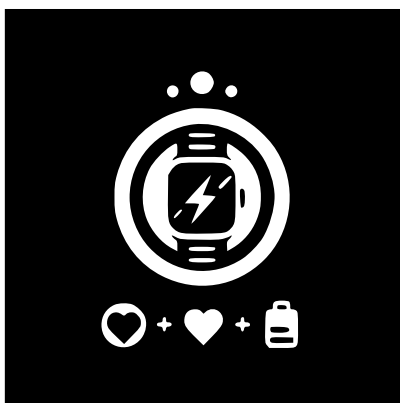
5. Zbiranje povratnih informacij in stalno izboljševanje: Podjetje X redno zbira povratne informacije od strank o njihovih izkušnjah z virtualnim pomočnikom in uporablja te informacije za nadaljnje izboljšave. To vključuje prilagajanje algoritmov za boljše razumevanje in predvidevanje potreb strank ter optimizacijo priporočil izdelkov.

S tem pristopom podjetje X ne samo da izboljša svoje storitve za stranke in jih naredi bolj personalizirane, ampak tudi povečuje prodajo s ciljno usmerjenimi priporočili izdelkov. Prav tako zmanjšuje operativne stroške in gradi močnejšo povezavo s svojimi strankami (OpenAI, 2024).

4.2 Primer 2: Oblikovanje marketinške strategije

Na zastavljeni ukaz »Razvijamo novo generacijo pametnih ur, ki vključuje senzorje za natančno merjenje krvnega tlaka in ravni kisika v krvi, poleg tega pa ima še funkcijo za spremljanje kakovosti spanca. Naša baterija omogoča dvakrat daljšo avtonomijo od konkurence. Prav tako razmišljamo o začetku prodaje v novembru, da bi izkoristili črni petek. Prosim, oblikuj slogan in preprost logotip črno-bele barve.« je orodje OpenAI ChatGPT-4 generiralo sledeči odgovor:

Slika 1: Logotip – ustvarjen s ChatGPT-4



Vir: OpenAI.

Za slogan, ob upoštevanju edinstvenih lastnosti vaše pametne ure, kot so natančno spremljanje zdravja (krvni tlak, nivo kisika), sledenje kakovosti spanja in izjemna življenjska doba baterije, ob hkratnem strateškem času lansiranja, da izkoristite prodajo za Črni petek, je tu predlog:

"Presežek časa: natančnost zdravja, neskončna moč."

Ta slogan ujame bistvo inovacij pametne ure, osredotočenih na zdravje, in njene superiorne življenjske dobe baterije in kot celovitega spremljevalca zdravja in življenjskega sloga. Prav tako namiguje na sposobnost pametne ure, da preseže običajno, kar je primerno sporočilo za njen prvenec okrog Črnega petka, časa, ko kupci iščejo izredne ponudbe in izdelke (OpenAI, 2024).

Na zastavljeni ukaz: »Prosim, da za ta primer sestaviš marketinški plan oglaševanja.« je orodje OpenAI ChatGPT-4 generiralo sledeči odgovor:

Faza 1: Ozaveščanje in gradnja pričakovanja

September - začetek oktobra

Začnite s predlansirno kampanjo, vključno z dražilnimi oglasi na socialnih omrežjih in YouTube-u.

Začnite sodelovanje z vplivneži in blogerji, da testirajo uro in delijo prve vtise.

Faza 2: Uvedba in vzpostavitev prisotnosti

Konec oktobra

Organizirajte uradno spletno lansiranje pametne ure, ki vključuje podrobno predstavitev in pričevanja uporabnikov.

Zaženite ciljane oglaševalske kampanje na iskalnikih in družbenih omrežjih.

Faza 3: Aktivacija in prodaja

Začetek novembra do črnega petka (konec novembra)

Dva tedna pred črnim petkom, obvestite potencialne kupce o ekskluzivnih ponudbah, ki bodo na voljo.

Na dan črnega petka, izvedite vse pripravljene promocijske aktivnosti in zagotovite, da so vse platforme optimizirane za visoko povpraševanje.

Faza 4: Vzdrževanje zanimanja in zvestobe

December - januar

Po črnem petku in med praznično sezono delite zgodbe zadovoljnih uporabnikov in pozitivne ocene.

Uvedite program zvestobe za spodbujanje nadaljnjih nakupov in priporočil.

Ta časovni načrt vam omogoča, da maksimalno izkoristite obdobje vodilno do črnega petka, zagotavljate neprekinjeno komunikacijo in angažiranost vaše ciljne skupine ter optimizirate prodajo v kritičnih trenutkih nakupovalne sezone. Pomembno je, da prilagodljivo upravljate s tem načrtom, saj lahko nepredvidene okoliščine zahtevajo prilagoditve strategije ali časovnega razporeda (OpenAI, 2024).

5 Rezultati in razprava

Iz prvega primera lahko povzamemo, da ChatGPT kot orodje za storitve za stranke predstavlja revolucionaren pristop v podjetjih. Od napovedne analitike do segmentacije strank, UI postaja integralni del številnih aspektov digitalnega marketinga, ki strokovnjakom za marketing omogoča, da dostavijo pravo sporočilo pravi osebi ob pravem času. (WireWheel, 2023). Na področju personalizacije ChatGPT omogoča e-trgovinam izboljšanje priporočil izdelkov in povečanje zadovoljstva strank, kar vodi do bolj personaliziranega marketinga. To odpira nove možnosti za zagonska podjetja, mala podjetja in druge organizacije pri oblikovanju ciljno usmerjenih kampanj in izboljšanju odnosov s strankami. To ne izboljša le zadovoljstva strank, temveč zmanjšuje tudi stroške, povezane s človeškim posredovanjem, in omogoča razvoj novih izdelkov s pridobivanjem podatkov o vzorcih vedenja uporabnikov (Tasci & Nil, 2023). Po drugi strani morebitne pasti vključujejo skrbi glede dobrega počutja potrošnikov, pristranskosti, napačnih informacij, pomanjkanja konteksta, skrbi glede zasebnosti, etičnih razmislekov in varnosti (Justin, Akiko, & Charles, 2023). Poleg tega je treba učinkovitost novih pristopov k razvoju marketinške vsebine strogo oceniti in preučiti v različnih kontekstih, da se zagotovi, da tehnologija resnično izpolnjuje pričakovanja strank in upošteva pravne zahteve, kot je GDPR (Tasci & Nil, 2023).

Na podlagi prvega primera morajo podjetja, ki se odločijo za uporabo ChatGPT-ja za personalizacijo, biti posebej pozorna na:

- Zbiranje in obdelavo osebnih podatkov: Zbiranje podatkov o vedenju uporabnikov in njihovih preferencah lahko vključuje obdelavo osebnih podatkov, kar zahteva skladnost z ustrežno zakonodajo o varstvu podatkov, kot je Splošna uredba o varstvu podatkov (GDPR)

v Evropski uniji. Pomembno je, da podjetje X pridobi jasno in nedvoumno soglasje uporabnikov za zbiranje in obdelavo njihovih podatkov za določene namene.⁶

- Transparentnost: Uporabniki morajo biti obveščeni o tem, kateri njihovi podatki se zbirajo, kako in za kakšne namene bodo ti podatki uporabljeni ter kako lahko dostopajo do svojih podatkov ali zahtevajo njihov izbris. To vključuje informacije o tem, kako ChatGPT uporablja njihove podatke za personalizacijo izkušnje.⁷
- Omejitev namena in minimalizacijo podatkov: Podjetje mora zagotoviti, da se osebni podatki uporabljajo izključno za izrecno določene namene (npr. izboljšanje storitev za stranke, personalizirana priporočila) in da se zbirajo samo tisti podatki, ki so nujno potrebni za doseg teh namenov.⁸
- Varnost podatkov: Podjetje mora uporabiti ustrezne tehnične in organizacijske ukrepe za zagotovitev varnosti osebnih podatkov, da se prepreči nepooblaščen dostop, izguba ali poškodba podatkov. To vključuje šifriranje podatkov, redne varnostne preglede in omejevanje dostopa do podatkov.⁹
- Pravica do pozabe in dostopa: Uporabniki imajo pravico do dostopa do svojih podatkov, njihovega popravka ali izbrisa. Podjetje mora zagotoviti enostavne mehanizme za uporabnike, da uveljavljajo te pravice.¹⁰

Strokovnjaki za marketing lahko uporabijo ChatGPT za ustvarjanje marketinške vsebine, kot so opisi izdelkov in e-poštna obvestila (Trampuž, Lampe, & Čebela, 2023). V drugem primeru ugotavljamo, da ChatGPT predstavlja dragoceno orodje za marketing, saj omogoča generiranje

⁶ Splošna uredba o varstvu podatkov (GDPR), Členi 6 in 7, ki obravnavajo pravno osnovo za obdelavo osebnih podatkov in pogoje za soglasje.

⁷ GDPR, Člen 12, ki obravnava transparentne informacije, komunikacijo in modalitete za uresničevanje pravic posameznika.

⁸ GDPR, Členi 5(1)(b) (omejitev namena) in 5(1)(c) (minimalizacija podatkov), ki določata, da morajo biti osebni podatki zbrani za določene, izrecne in zakonite namene ter morajo biti ustrezni, relevantni in omejeni na tisto, kar je potrebno za namene, za katere se obdelujejo.

⁹ GDPR, Člen 32, ki obravnava varnost obdelave, vključno s tehničnimi in organizacijskimi ukrepi za zagotavljanje varnosti osebnih podatkov.

¹⁰ GDPR, Členi 17 (pravica do izbrisa ali »pravica do pozabe«) in 15 (pravica dostopa posameznika do podatkov), ki uporabnikom omogočajo, da zahtevajo izbris svojih podatkov in dostop do podatkov, ki se nanašajo nanje.

kreativnih idej, konceptov in strategij, ki temeljijo na analizi ogromnih količin besedila. ChatGPT je še posebej koristen v začetnih fazah raziskovalnega procesa, saj pomaga pri kreiranju in sintezi informacij. Poleg tega je ChatGPT stroškovno učinkovit, saj zmanjšuje potrebo po obsežnih človeških analizah in omogoča obdelavo velikih podatkovnih zbirk (Varsha & Himanshu, 2023).

Iz obravnavanega drugega primera je razvidno, da je ChatGPT v izjemno kratkem časovnem okviru uspel zagotoviti slogan in ustvariti logotip. V primeru, kjer podjetje razvija novo generacijo pametnih ur z naprednimi zdravstvenimi funkcijami in izboljšano življenjsko dobo baterije, bi lahko deljenje določenih informacij predstavljalo tveganje za varnost in uhajanje podatkov. Informacije, ki smo jih delili, vključno s specifikacijami izdelka, ciljnim marketinškimi strategijami in načrtovanim časom lansiranja, so zelo občutljive narave. Razkritje marketinških strategij in ciljnih skupin lahko konkurentom omogoči, da razvijejo protiukrepe ali ciljajo na iste skupine z bolj prilagojenimi sporočili, kar bi lahko zmanjšalo učinkovitost vaših marketinških prizadevanj. Napoved načrta za začetek prodaje okrog črnega petka in popusti lahko konkurentom omogočijo, da časovno uskladijo svoje promocije in prodajne strategije, da neposredno tekmujejo z vašo ponudbo. Prav tako moramo preveriti oblikovani slogan in logotip na področju pravic intelektualne lastnine.

Prekomerna odvisnost od sistemov umetne inteligence lahko vodi v izgubo kreativnosti, kritičnega mišljenja in človeške intuicije. Najti je potrebno ravnovesje med odločanjem s pomočjo UI in človeškim vnosom, da se ohranijo kognitivne sposobnosti (Marr, 2023). Ugotavljamo tudi, da so delovna mesta vedno bolj izpostavljena tveganju avtomatizacije, kar povzroča zaskrbljenost glede tehnološke brezposelnosti. Na drugi strani pa se povečuje potreba po delovnih mestih, ki zahtevajo visoko stopnjo analitičnih, intuitivnih in empatičnih sposobnosti. Ta premik povzroča, da morajo delavci pridobiti nove veščine, da ostanejo relevantni na sodobnem trgu dela (Nurm, 2019).

Pri uporabi ChatGPT v poslovnem vodenju in strateškem odločanju morajo podjetja upoštevati več vidikov. Najprej morajo zagotoviti, da je ChatGPT pravilno integriran z obstoječimi poslovnimi sistemi, kar omogoča nemoten dostop do relevantnih podatkov in minimalne operativne motnje. Prav tako je potrebno ustrezno usposabljanje modela, da zagotavlja natančne in relevantne odgovore v poslovnem kontekstu. Varnost podatkov je ključna, saj uporaba UI vključuje izmenjavo občutljivih informacij, ki jih je treba zaščititi pred nepooblaščenim dostopom. Redno spremljanje in nadzor interakcij ChatGPT z zaposlenimi in strankami zagotavljata skladnost s podjetniškimi politikami. Medtem, ko lahko ChatGPT pomembno prispeva k procesu odločanja, pa morajo končne odločitve še vedno sprejemati ljudje, ki upoštevajo širši okvir in dolgoročne cilje podjetja.

Na koncu je ChatGPT lahko tudi dragoceno orodje za usposabljanje zaposlenih in izboljšanje njihovega znanja (Jusman & Ausat & Sumarna, 2023).

ChatGPT prinaša tudi izzive na področju trajnosti. Delovanje ChatGPT zahteva ogromno procesorske moči, kar vodi do velike porabe energije in posledično visokih emisij ogljikovega dioksida. Poleg tega so podatkovni centri, ki ga poganjajo, veliki porabniki vode za hlajenje, kar prispeva k povečanemu vodnemu odtisu. Nujno je, da se pri nadaljnjem razvoju in uporabi ChatGPT osredotočimo na zmanjšanje njegovega okoljskega vpliva, spodbujamo uporabo obnovljivih virov energije in raziskujemo trajnostne rešitve, ki bodo omogočile, da tehnologija umetne inteligence prispeva k bolj zeleni prihodnosti (Bhaskar & Seth, 2024).

Na koncu se podjetja soočajo s težko odločitvijo – kako izkoristiti prednosti ChatGPT, ne da bi pri tem tvegala pravne, finančne in etične posledice. Ključno je, da se podjetja zavedajo teh tveganj in se pripravijo na ustrezno upravljanje.

6 Sklep

V prispevku smo ugotovili, da ima prihodnost tehnologij umetne inteligence, vključno z jezikovnimi modeli, kot je ChatGPT, svetlo prihodnost z obetavnimi napredki, ki izhajajo iz izboljšanih učnih algoritmov in bogatejših zbirk podatkov. Takšne inovacije obetajo preobrazbo načina, kako se povezujemo s tehnologijo, in nudijo nove načine za obogatitev našega vsakdanjega življenja. Kljub temu pa smo poudarili, da je pri tem hitrem tehnološkem napredku pomembno upoštevati etične in družbene implikacije. Vprašanja, kot sta varstvo zasebnosti in vpliv na zaposlovanje, zahtevajo previden pristop in razmislek. Avtomatizacija storitev za stranke lahko npr. vpliva na delovna mesta, hkrati pa pri teh modelih zbiranje in obdelava podatkov prinašata izzive na področju zasebnosti. Poudarili smo, da morata razvoj in uporaba teh tehnologij potekati odgovorno in etično. V okviru analize vloge ChatGPT-ja v podjetjih smo raziskali pravne izzive, ki jih prinaša, s posebnim poudarkom na varstvu osebnih podatkov in pravicah intelektualne lastnine.

7 Viri

Ackermann, A. (2022). *GDPR for dummies: What is it? Why do we need it? Why does personal data have to be protected?* Tech&Rights. <https://www.liberties.eu/en/stories/gdpr-for-dummies/44076>

Arman, M., & Laimya, U. R. (2023). Exploring the implication of ChatGPT AI for business: Efficiency and challenges. *Journal of Innovation Information Technology and Application*, 5(1), 52. <http://dx.doi.org/10.31098/ijmadic.v1i2.1872>

Bhaskar, P., & Seth, N. (2024). Environment and sustainability development: A ChatGPT perspective. V *Applied Data Science and Smart Systems* (str. 54-62). CRC Press. <https://www.taylorfrancis.com/chapters/oa-edit/10.1201/9781003471059-8/environment-sustainability-development-chatgpt-perspective-priyanka-bhaskar-neha-seth>

Bogataj Jančič, M. (2021). *Ali je lahko umetna inteligenca avtor avtorskega dela?* V *Zbornik povzetkov: Umetna inteligenca, človekove pravice in družbena škoda* (str. 5). Inštitut za kriminologijo pri Pravni fakulteti v Ljubljani. <https://www.inst-krim.si/wp-content/uploads/2021/06/Zbornik-povzetkov-web.pdf>

Colmenero-Fernandez, A. (2023). *Navigating GDPR compliance in AI: A deep dive into OpenAI's ChatGPT — A perspective from multimedia design architecture*. ESS Open Archive. <https://doi.org/10.22541/essoar.169447413.36333907/v1>

Cuomo, J. (2023). *Exploring the risks and alternatives of ChatGPT: Paving a path to trustworthy AI*. IBM. <https://www.ibm.com/blog/exploring-the-risks-and-alternatives-of-chatgpt-paving-a-path-to-trustworthy-ai/>

European Innovation Council. (2023). *Intellectual property in ChatGPT*. European Commission. https://intellectual-property-helpdesk.ec.europa.eu/news-events/news/intellectual-property-chatgpt-2023-02-20_en

Hariri, W. (2023). *Unlocking the potential of ChatGPT: A comprehensive exploration of its applications, advantages, limitations, and future directions in natural language processing*. <https://doi.org/10.48550/arXiv.2304.02017>

Hu, K. (2023). *ChatGPT sets record for fastest-growing user base – analyst note*. Reuters. <https://www.reuters.com/technology/chatgpt-sets-record-fastest-growing-user-base-analyst-note-2023-02-01/>

IBM. (2023). *What is data privacy?* <https://www.ibm.com/topics/data-privacy>

Jusman, I., Ausat, A., & Sumarna, A. (2023). Application of ChatGPT in Business Management and Strategic Decision Making. *Jurnal Minfo Polgan*, 12(2), 1688–1697. <http://dx.doi.org/10.33395/jmp.v12i2.12956>

Justin, P., Akiko, U., & Charles, D. (2023). ChatGPT and consumers: Benefits, pitfalls and future research agenda. *International Journal of Consumer Studies*, 47(4), 1213–1225. <https://doi.org/10.1111/ijcs.12928>

Kuzior, A., Sira, M., & Brozek, P. (2023). Use of Artificial Intelligence in Terms of Open Innovation Process and Management. *Sustainability*, 15. <https://doi.org/10.3390/su15097205>

Lucchi, N. (2023). ChatGPT: A case study on copyright challenges for generative artificial intelligence systems. *European Journal of Risk Regulation*, 1–23. <https://doi.org/10.1017/err.2023.59>

Marr, B. (2023). The 15 Biggest Risks Of Artificial Intelligence. Forbes. <https://www.forbes.com/sites/bernardmarr/2023/06/02/the-15-biggest-risks-of-artificial-intelligence/>

- McKendric, J. (2022). *Who ultimately owns content generated by ChatGPT and other AI platforms?* Forbes. <https://www.forbes.com/sites/joemckendrick/2022/12/21/who-ultimately-owns-content-generated-by-chatgpt-and-other-ai-platforms/?sh=390a90385423>
- Mikuš, Š. (2023, December 6). *Kaj manjka Sloveniji, da bi vsaj ujela povprečje EU pri produktivnosti.* Finance. <https://www.finance.si/podjetnik/kaj-manjka-sloveniji-da-bi-vsaj-ujela-povprecje-eu-pri-produktivnosti/a/9019267>
- Nurm, K.-M. (2019). *The Possibilities and Potential Risks Of Using Artificial Intelligence In Marketing – A Literature Review.* Bachelor's thesis. https://www.researchgate.net/publication/336899450_The_Possibilities_and_Potential_Risks_Of_Using_Artificial_Intelligence_In_Marketing_-_A_Literature_Review
- Ollivier, M., Pareek, A., Dahmen, J., et al. (2023). A deeper dive into ChatGPT: History, use and future perspectives for orthopaedic research. *Knee Surgery, Sports Traumatology, Arthroscopy*, 31(6), 1190–1192. <http://dx.doi.org/10.1007/s00167-023-07372-5>
- OpenAI. (2024). *What is ChatGPT Enterprise?* <https://help.openai.com/en/articles/8265053-what-is-chatgpt-enterprise>
- Premzl, J. (2019). *Ureditev pogodbenih razmerij z zunanjimi sodelavci. Varstvo osebnih podatkov v podjetju priročnik za mala in srednja podjetja.* Univerzitetna založba Univerze v Mariboru. <https://doi.org/10.18690/978-961-286-293-0>
- Pretnar, B. (2020). *Zakaj potrebujemo intelektualno lastnino?* Kvarkadabra. <https://kvarkadabra.net/2020/01/intelektualna-lastnina/>
- Primec, A. (2020). Robot – sodelavec ali stroj? V *Pravo in ekonomija: Digitalno gospodarstvo*. Primec, A. (2022). *Digitalizacija kot izziv. V Izzivi digitalne preobrazbe* (str. 4–6). Univerzitetna založba Univerze v Mariboru. <https://doi.org/10.18690/978-961-286-366-1.3>
- Ray, P. P. (2023). ChatGPT: A comprehensive review on background, applications, key challenges, bias, ethics, limitations and future scope. *Internet of Things and Cyber-Physical Systems*, 3, 121-154. <http://dx.doi.org/10.1016/j.iot-cps.2023.04.003>
- Samoili, 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.* Luxembourg: Publications Office of the European Union. <https://ideas.repec.org/p/ipt/iptwpa/jrc118163.html>
- Sebastian, G. (2023). *Privacy and data protection in ChatGPT and other AI chatbots: Strategies for securing user information.* <http://dx.doi.org/10.2139/ssrn.4454761>
- Shaji, G., Hovan, G., & Gabrio, M. (2023). *A Review of ChatGPT AI's impact on several business sectors.* Partners Universal International Innovation Journal (PUIJ). <https://doi.org/10.5281/zenodo.7644359>

Sundar, S., & Mok, A. (2023, August 21). *What is ChatGPT? Here's everything you need to know about ChatGPT, the chatbot everyone's still talking about*. Business Insider. <https://www.businessinsider.com/everything-you-need-to-know-about-chat-gpt-2023-1>

Swaney, R. (2023). *ChatGPT and the race to secure your intellectual property*. SecurityIntelligence. <https://securityintelligence.com/articles/chatgpt-and-the-race-to-secure-your-intellectual-property/>

Tasci, M. F., & Nil, E. D. (2023). *ChatGPT applications in marketing. The Essentials of Today's Marketing-3*. https://www.researchgate.net/publication/373693078_ChatGPT_Applications_in_Marketing

The Digital Watch observatory. (2023). *ChatGPT and GDPR: Balancing AI innovation with data protection*. Retrieved from Geneva Internet Platform. <https://dig.watch/updates/chatgpt-and-gdpr-balancing-ai-innovation-with-data-protection>

Trampuž, M. (2023, March). *Vodič uvajanja umetne inteligence v mala in srednja podjetja v Sloveniji*. Ljubljana: Združenje za informatiko in telekomunikacije pri GZS. https://www.gzs.si/Portals/Panoga-ElektroIndustrija/Vodic_uvajanja_umetne_inteligence_v_mala_in_srednja_podjetja_vSloveniji_WEB2.pdf

Trampuž, M., Lampe, A., & Čebela, T. (2023). *ChatGPT je pretresel svet*. Glas gospodarstva. <https://www.gzs.si/Portals/Panoga-ZIT/Vsebine/26-27.pdf>

UBS. (2023). *Let's chat about ChatGPT*. UBS Chief Investment Office. https://www.ubs.com/global/en/wealth-management/marketnews/article/_jcr_content.0000023273.file/PS9jb250ZW50L2RhbmS9hc3NldHM-vMGM0L3VjLzEvNTAvMTkvNzQvMGMxNTkxNzctY2M3Mi00ZjhiLWI4ZDYtMGQzZmZkZmEzNGI1LnBkZg==/0c159177-cc72-4f8b-b8d6-0d3ffdf3a34b.pdf

Varsha, J., & Himanshu, R. (2023). *The prospects and challenges of ChatGPT on marketing research and practices*. SSRN. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4398033

WireWheel. (2023). *Personalization, ChatGPT, and privacy*. <https://wirewheel.io/blog/personalization-chatgpt-and-privacy/>

Xiaodong, W., Ran, D., & Jianbing, N. (2023). *Unveiling security, privacy, and ethical concerns of ChatGPT*. Department of Electrical & Computer Engineering, Queen's University, Kingston, Canada. <https://arxiv.org/pdf/2307.14192.pdf>

Značilnosti spletnega nakupovanja mladih v Sloveniji

Lina Jenšac  

Univerza v Mariboru, Ekonomsko-poslovna fakulteta

Maribor, Slovenija

Nejc Fir 

Univerza v Mariboru, Ekonomsko-poslovna fakulteta

Maribor, Slovenija

Povzetek: Spletno nakupovanje je dejanje nakupa blaga in storitev preko tehnološke infrastrukture. Obstaja že desetletja, število potrošnikov pa se po obdobju javnega življenja zaradi epidemije covid-19 povečuje. Spremembe nakupovalnih navad in prodajnih kanalov spreminjajo vedenje odjemalcev. V prispevku smo opredelili značilnosti spletne potrošnje mladih v Sloveniji in analizirali dejavnike, ki nanjo vplivajo. Podatke smo pridobili s spletnim anketnim vprašalnikom. Ugotovili smo, da večina mladih kupuje na spletu. Najpogosteje kupujejo oblačila in obutev ter izdelke in storitve za prosti čas.

Ključne besede: spletno nakupovanje, nakupovalne navade, spletna trgovina, mladi potrošniki, e-poslovanje

Characteristics of Young People's Online Shopping in Slovenia

Lina Jenšac  

University of Maribor, Faculty of Economics and Business
Maribor, Slovenia

Nejc Fir 

University of Maribor, Faculty of Economics and Business
Maribor, Slovenia

Abstract: Online shopping is the act of purchasing goods and services through a technological infrastructure. It has been around for decades; the number of consumers has been increasing after a period of public life due to the Covid-19 epidemic. Changes in shopping habits and sales channels are changing the consumer behaviour. In this paper, we defined the characteristics of online consumption by young people in Slovenia and analysed the factors that influence it. We obtained the data using an online questionnaire. We found that most young people buy online. Most often, they buy clothing and footwear, as well as leisure products and services.

Keywords: online shopping, shopping habits, online store, young consumers, e-business

1 Uvod

Spletno nakupovanje je v angleškem slovarju Oxford (Oxford English Dictionary) definirano kot dejanje nakupa blaga in storitev preko računalniškega omrežja (OED, 2023). Predstavlja skupek informacij in dejavnosti, ki kupcu omogoča izvedbo premišljenega nakupa ali poslovanja. Govorimo torej o izmenjavi podatkov in transakciji, izvedeni s pomočjo tehnološke infrastrukture (Ige, 2004). Čeprav spletno nakupovanje obstaja že desetletja, je razmah doživelo v novem tisočletju, še posebej po obdobju omejevanja javnega življenja zaradi pandemije covid-19.

Po podatkih Statističnega urada Republike Slovenije več kot polovica aktivnega prebivalstva nakupuje na spletu – leta 2022 so slovenska podjetja z vsaj desetimi zaposlenimi s spletno prodajo skupaj ustvarila približno 3.950 milijonov evrov prihodkov (brez DDV) (Mlakar, 2023). Nakupovalne navade se spreminjajo, prodajni kanali podjetij pa se širijo na splet. Število potrošnikov, ki nakupe opravlja tudi na spletu, se vsako leto povečuje. Prav tako se povečuje število spletnih trgovcev na drobno, ki se posledično soočajo z monopolistično konkurenco, le redki so dobičkonosni (Venkatesh idr., 2022). Namen prispevka je definirati nakupovalne navade mladih na področju spletnega nakupovanja in opredeliti dejavnike, ki nanje vplivajo. V ta namen je bil izveden anketni vprašalnik, rezultati analize pa so predstavljeni v prispevku.

Prispevek je razdeljen na šest poglavij. V drugem poglavju so predstavljene najpomembnejše ugotovitve pregleda literature raziskovalnega področja, v tretjem poglavju so opisane uporabljene metode raziskovanja, rezultati ankete so predstavljeni v četrtem poglavju, v petem je zapisana razprava o rezultatih raziskovanja, šesto poglavje pa je sklep, v katerem povzamemo najpomembnejše ugotovitve raziskave in podamo smernice oblikovalcem spletne prodaje v povezavi z vedenjem odjemalcev definirane ciljne skupine.

2 Pregled literature

V nadaljevanju je predstavljen pregled slovenske in tuje literature s področja spletnega nakupovanja s poudarkom na mladih potrošnikih. Predstavili smo vedenje odjemalcev, dejavnike spletne potrošnje in ugotovitve drugih avtorjev ter predhodno izvedenih raziskovalnih del, povezanih z obravnavano tematiko.

Vedenje odjemalcev je področje marketinga, pri katerem segmentiramo trg in ugotavljamo načine za učinkovito zadovoljevanje potreb odjemalcev. Razumevanje sprememb nakupnega vedenja

odjemalcev z uvedbo digitalnih tehnologij je v času dinamičnega povpraševanja ključno, saj nam omogoča prilagajanje marketinške strategije za doseganje večje prodaje in pridobivanja novih zvestih kupcev. Z utrjevanjem položaja na trgu kot posledico prepoznavanja potreb odjemalcev v podjetju vzpostavljamo in ohranjamo konkurenčno prednost in prispevamo k oblikovanju kakovostnih poslovnih strategij. Na vedenje odjemalcev vplivajo osebni, družbeni, kulturni in psihološki dejavniki (Nedoklan, 2021).

Zhou idr. (2007) so na podlagi sinteze strokovne in znanstvene literature identificirali devet vrst dejavnikov, ki vplivajo na nagnjenost k spletni potrošnji. Prvo skupino predstavljajo demografski dejavniki. Na spletne nakupovalne navade potrošnikov vplivajo še dejavniki, povezani z uporabo interneta, prepričanji, potrošnikovimi preferencami in nagnjenostjo k potrošnji, osebnostnimi značilnostmi, predhodnimi izkušnjami s spletom in spletnim nakupovanjem ter s psihološko percepcijo. Raziskovalci ugotavljajo, da moški na spletu kupujejo pogosteje kot ženske, prav tako je vrednost njihovega nakupa praviloma večja in so do spletnih trgovcev zaupljivejši, medtem ko v tradicionalnih oblikah trgovine med kupci prevladujejo ženske. Motivacijo žensk za nakup pogosto vzpodbudi osebni pristop, medtem ko moški pri nakupovanju cenijo udobje. Drugi razlog za razliko v pogostosti spletnih nakupov med spoloma je večje zaznano tveganje za potencialne grožnje na spletu pri ženskah – več žensk je namreč v raziskavi Citrina idr. (2003) trdilo, da na spletu ne najdejo izdelkov zase in da jih odvrne dejstvo, da izdelka pred nakupom ne morejo preizkusiti.

Prednost spletnega nakupovanja v primerjavi s tradicionalnimi oblikami nakupovanja v fizičnih prodajalnah ali z uporabo kataloga potrošniki vidijo v olajšani možnosti primerjave izdelkov. Za spletni nakup se odjemalci pogosto odločijo zaradi zavedanja vrednosti, prisotnosti impulzivnega nakupovalnega vedenja in užitka, ki jim ga spletno nakupovanje predstavlja. Glavna komponenta odločitve o spletnem nakupu je varnost oz. z njo povezane zaznane pasti izvedbe nakupa. Druga najpomembnejša komponenta vedenja odjemalcev na spletu je skladnost dobrin, ki so jih predhodno kupovali na druge načine, s tistimi na spletu. Potrošniki se torej prej odločijo za spletni nakup dobrin, ki jih poznajo in so jih že preizkusili, kot za nakup še nepreizkušenih dobrin. Skladajo se tudi namere spletnega nakupa in dejansko vedenje pri spletnem nakupovanju, kar lahko ponudniki dobrin izkoristijo za ciljno oglaševanje. Prav tako je tudi njihova raziskava z uporabo Chisnalovega modela pokazala, da so moški bolj naklonjeni spletnemu nakupovanju kot ženske (Venkatesh idr., 2022).

Prihodek, razvite veščine brskanja po internetu, zaznana uporabna vrednost izdelka in pozitivna izkušnja s predhodnim nakupom so spremenljivke, pri katerih je bila zaznana pozitivna korelacija z nagnjenostjo k spletni potrošnji. Večji povprečni prihodek spletnih potrošnikov v primerjavi s potrošniki fizičnih trgovin je bil zaznan v petih raziskavah, izvedenih med letoma 1999 in 2004, kjer kot razlog navajajo vrsto dobrin, ki so v času izvajanja raziskave bile najpogosteje v spletni košarici potrošnikov. Največkrat so ti kupovali normalne dobrine, povpraševanje po tej vrsti dobrin pa je dohodkovno elastično. To so bile predvsem elektronske naprave, počitnice in športni pripomočki. K spletnemu nakupovanju so bolj nagnjeni posamezniki kultur, ki so usmerjene k individualizmu. V takšnih kulturah posamezniki internet primarno uporabljajo za spletno nakupovanje in iskanje informacij, medtem ko v kolektivističnih kulturah posamezniki preko interneta najpogosteje komunicirajo, raziskujejo in ga uporabljajo za hobije. Pripravljenost za nakup se med različnimi skupinami blaga in storitev ne razlikuje. Tisti, ki so naklonjeni spletnemu nakupovanju, opravljajo nakupe za vse vrste dostopnega blaga v okviru lastnih nakupovalnih navad. Osebna inovativnost posredno in neposredno vpliva na nagnjenost k spletnemu nakupu. Potrošnika k spletnemu nakupovanju privabljajo večja izbira izdelkov in storitev, nizka cena, možnost personaliziranja izdelka in enostaven dostop do informacij (Zhou idr., 2007).

Fras (2022) je raziskoval nakupovalne navade v času covid-19 v Sloveniji in ugotovil, da med starejšimi in mlajšimi odjemalci ne obstajajo statistično značilne razlike v pogostosti spletnega nakupovanja, so pa starejši odjemalci v povprečju zadovoljnejši z zadnjim spletnim nakupom. Najpomembnejša dejavnika spletnega nakupa sta enostavnost nakupa (povprečna vrednost ocene pomembnosti je znašala 4,09 na lestvici od 1 do 5) in pestrost ponudbe (povprečna vrednost je znašala 3,78). Moški so v času covid-19 na spletu pogosteje kupovali nujna življenjska živila in računalniško ter elektronsko opremo, ženske pa tekstilne izdelke, kozmetiko, zdravila in izdelke za prosti čas. Hegler (2023) raziskave ni omejevala na obdobje covid-19, ampak na mlade in je prišla do enakih ugotovitev glede preferenc kategorij izdelkov po spolu. Ugotovila je tudi, da so moški bolj nagnjeni k spletnemu nakupovanju in to izvajajo pogosteje. Starejše generacije vidijo prednost v spletnem nakupovanju pred obiskom fizične trgovine v hitrosti nakupa, mlajše pa pritegnejo nižje cene in širša izbira artiklov. Na mlajše odjemalce imajo večji vpliv priporočila družine, prijateljev in t. i. influencerjev. Več kot polovica anketiranih nakupuje na spletu več v primerjavi z obdobjem pred covidom-19.

Po podatkih Statističnega urada Republike Slovenije je v prvem četrtletju leta 2023 na spletu nakupovalo 53 % oseb med 16. in 74. letom starosti – med mladimi, starimi med 16 in 24 let, je delež večji in znaša 84 %. 78 % potrošnikov je opravilo do pet spletnih nakupov, v spletni košarici so se najpogosteje znašla oblačila (66 %), športna oprema (25 %), kozmetika in izdelki za sprostitev (24 %), pohištvo in dodatki za dom (24 %) ter zdravila in prehranska dopolnila (24 %). Plačilo je dve tretjini e-kupcev poravnalo z debetno ali kreditno kartico, 43 % pa z gotovino ob prevzemu (Mlakar, 2023). Največje spletne prodajalne v Sloveniji glede na letni prihodek podjetja leta 2023 so Mimosvrste (125,7 milijona ameriških dolarjev), Merkur (34,5 milijona ameriških dolarjev), Big Bang (28,6 milijona ameriških dolarjev), About You (22,8 milijona ameriških dolarjev) in Spar (22,5 milijona ameriških dolarjev) (ECDB, 2024).

3 Metode

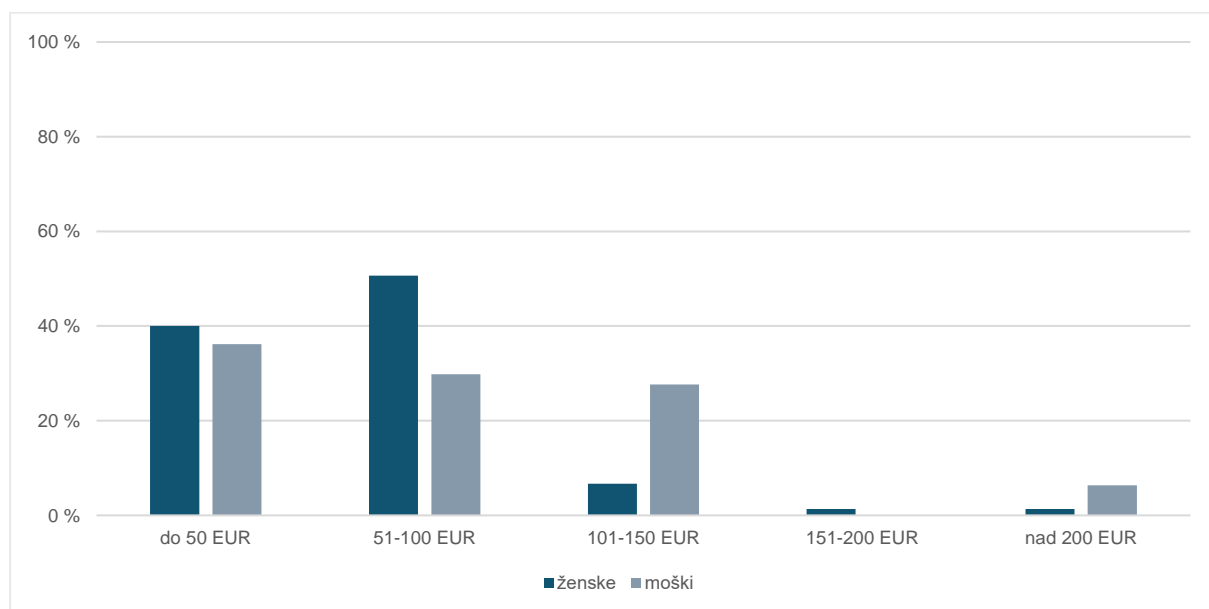
V teoretičnem delu smo z metodo deskripcije in metodo kompilacije opisali spletno nakupovanje in dejavnike, ki vplivajo na nagnjenost k spletni potrošnji. Pregledali smo relevantno literaturo raziskovalnega področja in jo povzeli. Pri pregledu literature smo se posluževali slovenskih in tujih znanstvenih ter strokovnih člankov z obravnavanega področja. Literaturo smo pridobili preko javno dostopnih baz podatkov. Zapisali smo spoznanja drugih avtorjev in njihovih raziskovalnih del, da bi bolje razumeli in pojasnili področje spletnega nakupovanja. V empiričnem delu smo uporabili metodo analize primarnega vira podatkov s pomočjo neeksperimentalne kvantitativne raziskave in metode spletnega anketiranja. Spletni anketni vprašalnik smo izvedli s pomočjo programa 1KA, ki je dostopen na povezavi <https://1ka.arnes.si/>. Za vzorec smo izbrali mlade med 15. in 26. letom starosti. Kvantitativne podatke predstavljajo nakupovalne navade in stališča anketirancev. Spremenljivke so številčne in kategorične. Za zbiranje podatkov o pomembnosti sestavin spletne prodaje smo uporabili Likertovo lestvico. Zbrane podatke spletnega vprašalnika smo analizirali s pomočjo programske opreme SPSS. Pri obdelavi podatkov smo izračunali frekvence, deleže in povprečne vrednosti. Rezultate raziskave smo analizirali, uporabili metodo komparacije z drugimi rezultati raziskav ter s pomočjo sinteze povzeli ugotovitve.

4 Rezultati

V tem razdelku so predstavljeni rezultati izvedene raziskave. Najprej smo obravnavali demografske podatke vzorca, nato pa analizirali in predstavili rezultate po posameznih vprašanjih oz. obravnavanih temah.

V vzorec je bilo vključenih 124 udeležencev raziskave. 122 udeležencev je že nakupovalo na spletu, kar predstavlja 98,39 %. Stališča in indikatorje spletnih nakupovalnih navad smo zbrali od 122 udeležencev, ki so že nakupovali na spletu. 61,5 % anketiranih je bilo žensk (75 udeleženk), 38,5 % pa moških (47 udeležencev). 18 % udeležencev je starih med 15 in 18 let, 63,9 % med 19 in 22 let ter 18 % med 23 in 26 let. 20,5 % anketiranih obiskuje srednjo šolo, 23 % visokošolski strokovni študijski program (VS), 38,5 % univerzitetni študijski program (UNI), 10,6 % magistrski študijski program (MAG), 2,5 % je brezposelnih in 4,9 % zaposlenih. Povprečni mesečni dohodek 24,6 % anketiranih znaša do 150 evrov, z zneskom od 151 do 300 evrov mesečno razpolaga 26,2 % anketiranih, kar predstavlja največji delež, 17,2 % z dohodkom od 301 do 450 evrov, 14,8 % od 451 do 600 evrov in 17,2 % z več kot 600 evri mesečno.

Slika 1: Povprečen znesek spletnega nakupa



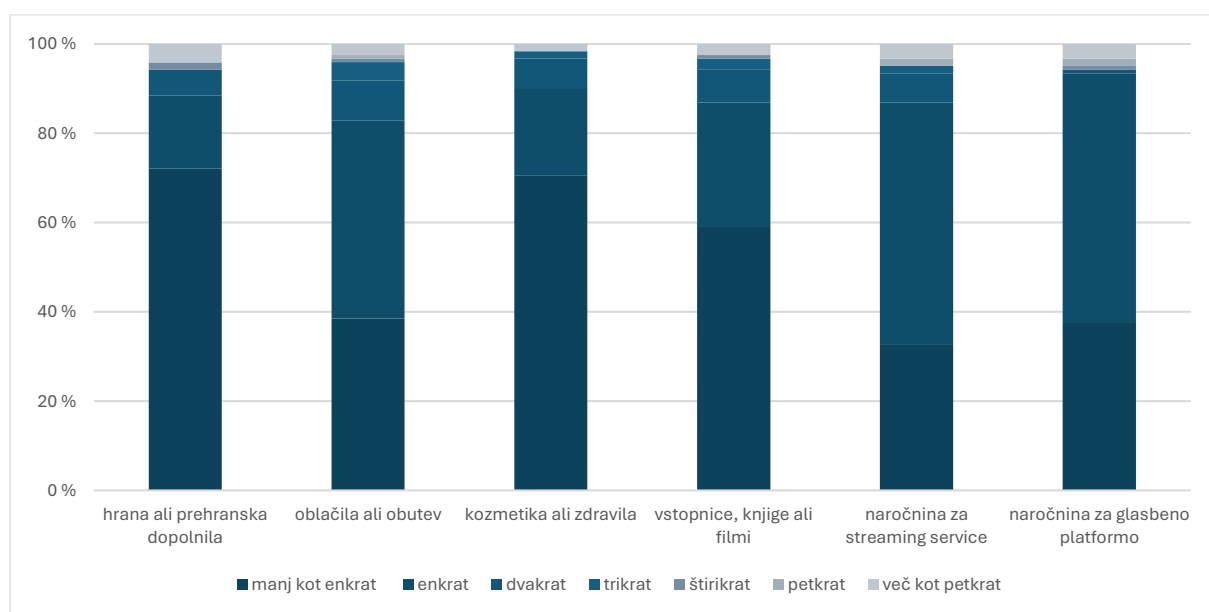
Vir: Lastni.

Rezultati ankete kažejo, da so bili anketiranci ob prvem spletnem nakupu stari med 10 in 25 let. Povprečna starost ob prvem spletnem nakupu je bila 15,32 leta. Mediana znaša 15 let, modus 16 let. Med spoloma pri starosti ob prvem spletnem nakupu ni statistično značilnih razlik. V nadaljevanju smo želeli ugotoviti, koliko znaša povprečen znesek spletnega nakupa pri mladih. Ugotovili smo, da povprečni znesek spletne košarice nakupa mladih najpogosteje znaša do 100 evrov. V to

kategorijo spadajo nakupi skupaj 81,1 % anketiranih. Povprečna vrednost košarice spletnega nakupa 38,5 % udeležencev raziskave je manjša od 50 evrov, 42,6 % najpogosteje opravi spletni nakup v vrednosti od 51 do 100 evrov, 14,8 % od 101 do 150 evrov, 0,8 % anketiranih od 151 do 200 evrov, 3,3 % pa za spletni nakup v povprečju odšteje več kot 200 evrov.

S pomočjo navzkrižne tabele (v izvirniku Crosstabulation) smo želeli preveriti, ali se povprečni znesek spletnega nakupa med moškimi in ženskami razlikuje. Rezultati so predstavljeni na Sliki 1. Ugotavljamo, da je v kategorijah z nižjimi povprečnimi zneski spletnega nakupa, torej v kategoriji do 50 evrov in od 51 do 100 evrov, delež žensk višji in skupaj znaša 90,67 %, medtem ko spletne nakupe v povprečni vrednosti do 100 evrov v povprečju kupuje 65,95 % moških. Spletni nakup v vrednosti od 101 do 150 evrov je povprečna vrednost transakcije 6,67 % žensk in 27,66 % moških. Sklepamo, da je povprečen znesek spletnega nakupa pri moških višji.

Slika 2: Pogostost spletnega nakupa kategorij izdelkov in storitev na mesec

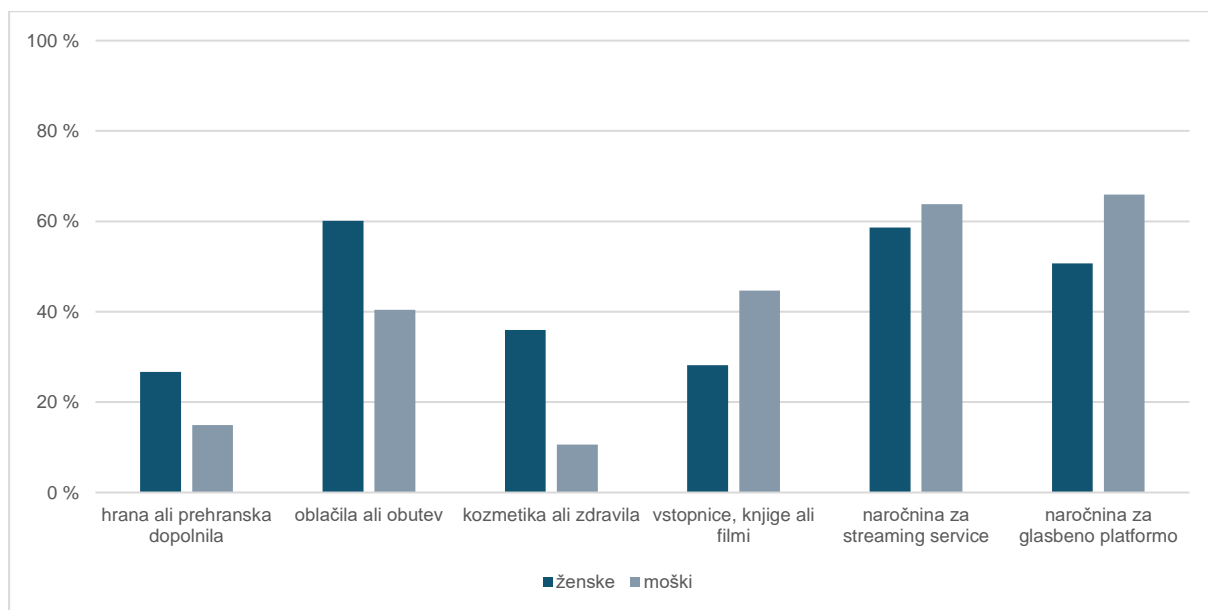


Vir: Lastni.

Slika 2 prikazuje pogostost nakupa kategorij izdelkov in spletnih storitev. Več kot 80 % anketirancev za vse naštetе kategorije opravi mesečno en spletni nakup ali manj. Več kot dva nakupa mesečno za vsako izmed navedenih kategorij opravi manj kot 7 % anketiranih. Največji delež opravljenega mesečnega spletnega nakupa opazimo pri naročninah. Mesečno naročnino na kanal vi-

deo vsebin (oz. v angleščini »streaming service«) kupuje 54,09 % udeležencev raziskave, naročnino na glasbeno platformo pa 55,73 % udeležencev raziskave. 53,27 % anketirancev oblačila in obutev na spletu kupi enkrat ali dvakrat mesečno, vstopnice, knjige ali filme pa 35,25 % anketirancev.

Slika 3: Pogostost spletnega nakupa kategorij izdelkov in storitev na mesec glede na spol



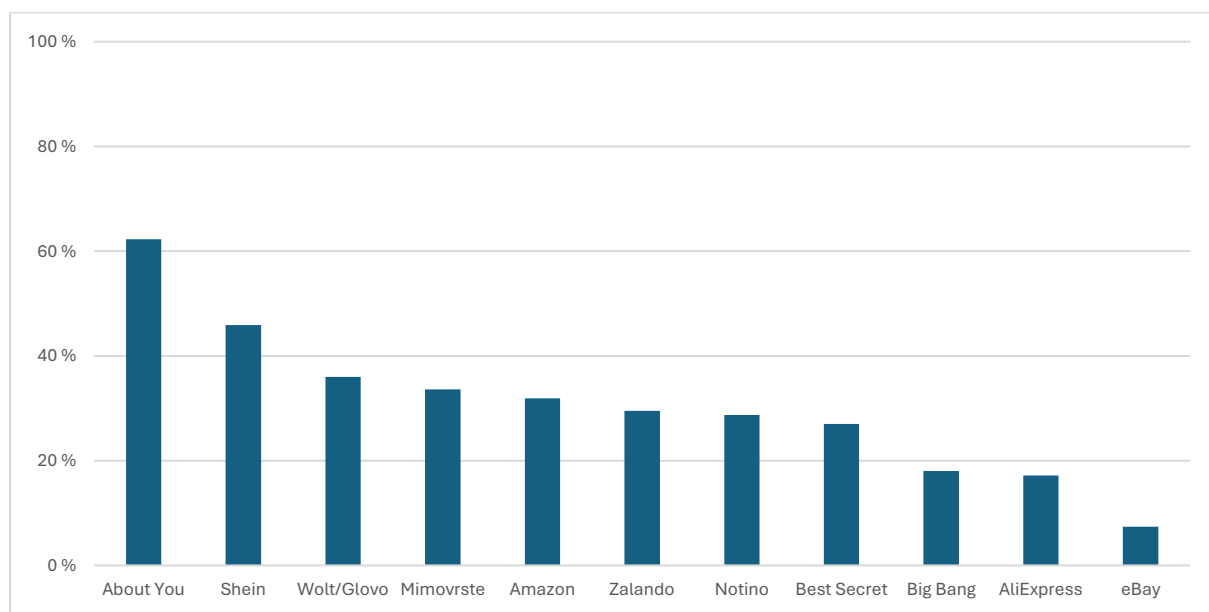
Vir: Lastni.

Na Sliki 3 je prikazana pogostost nakupa kategorij izdelkov in storitev glede na spol. Upoštevani so nakupi, opravljeni enkrat ali dvakrat mesečno. Ugotavljamo, da ženske pogosteje na spletu kupujejo hrano ali prehranska dopolnila, oblačila ali obutev ter kozmetiko ali zdravila v primerjavi z moškimi. 60,14 % žensk enkrat ali dvakrat mesečno na spletu opravi nakup oblačil ali obutve, teh nakupov pa je pri moških 19,74 odstotne točke manj. Moški najpogosteje opravijo nakup naročnine na glasbeno platformo, to mesečno stori 65,90 % anketiranih moških in 50,7 % žensk. Poleg naročnine za glasbeno platformo moški pogosteje kupujejo še naročnino na kanal z video vsebinami, vstopnice, knjige in filme.

Slika 4 prikazuje pogostost nakupa v spletnih prodajalnah. Anketiranci so označili tri spletne prodajalne, v katerih najpogosteje opravijo spletni nakup. Največ potrošnikov, vključenih v raziskavo (62,3 %), nakupuje izdelke spletne prodajalne About You, katere asortima izdelkov sestavljajo oblačila, obutev in modni dodatki. 45,9 % anketirancev nakupuje na spletni strani Shein. Gre za

tujo spletno stran, kjer lahko kupci poleg oblačil, obutve in modnih dodatkov nakupujejo tudi kozmetiko in dodatke za dom ter prosti čas. Na tretjem mestu po pogostosti nakupa sta spletna ponudnika logističnih storitev na področju hrane – Wolt in Glovo. Spletna ponudnika sta med tremi najpogosteje obiskanimi pri 36 % sodelujočih v raziskavi. Sledijo Mimovrste, Amazon, Zalando, Notino, Best Secret, Big Bang, AliExpress in najmanj obiskani med anketiranci, eBay. Med najpogosteje obiskanimi spletnimi prodajalnami obstajajo razlike glede na spol. Moški udeleženci najpogosteje nakupujejo v spletni trgovini About You. Druga najbolj priljubljena iz nabora je pri moških spletna trgovina Mimovrste, tam pogosto kupuje 47,8 % anketiranih moških, na tretjem mestu je Amazon, ki je ena izmed treh najbolj priljubljenih spletnih prodajaln 46,8 % anketiranih moških. Ženske, ki so sodelovale v raziskavi, najpogosteje nakupujejo na spletnih mestih Shein (67,4 %), About You (65,9 %) in Notino (36,7 %). Notino ponuja ličila in izdelke za nego.

Slika 4: Spletne prodajalne po pogostosti nakupa

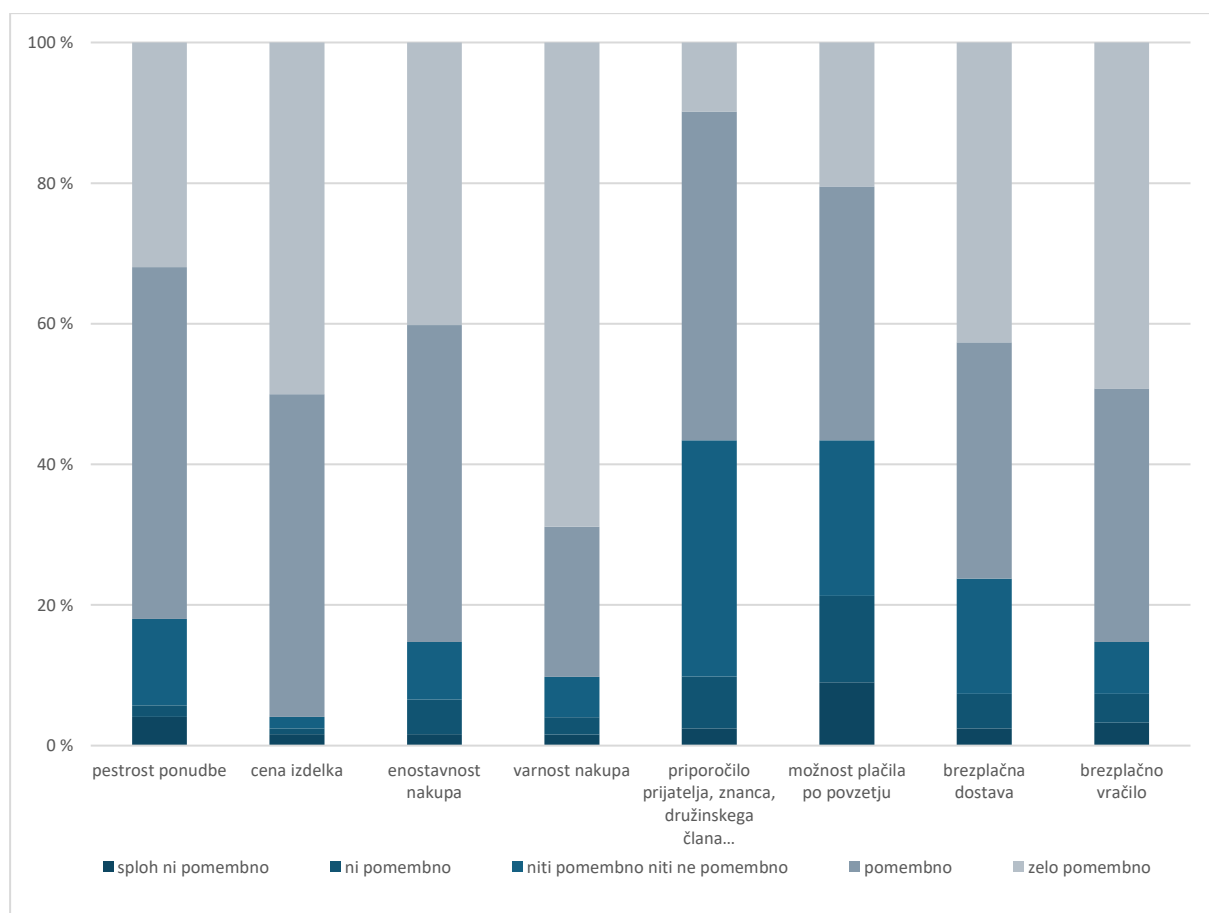


Vir: Lastni.

Pomembnost osmih dejavnikov, ki vplivajo na odločitev o spletnem nakupu, smo ocenjevali z uporabo petstopenjske Likertove lestvice, kjer so udeleženci svoje mnenje ocenjevali tako, da so označili pomembnost, ki je bila skladna z njihovim mnenjem. Izbirali so lahko med »sploh ni pomembno«, »ni pomembno«, »niti pomembno niti nepomembno«, »pomembno« in »zelo pomembno«. Rezultati so prikazani na Sliki 5. Ugotavljamo, da je potrošnikom, ki so delovali v razi-

skavi, pri odločitvi za spletni nakup najpomembnejša cena izdelka. Kot »zelo pomembno« ali »pomembno« jo dojema 95,9 % anketirancev. Drugi najpomembnejši dejavnik je varnost nakupa. Z »zelo pomembno« ali »pomembno« jo označuje 90,2 % anketiranih. Na tretjem mestu sta enostavnost nakupa in brezplačno vračilo, ki ju kot »pomembno« ali »zelo pomembno« ocenjuje 85,2 % sodelujočih v raziskavi. Sledijo pestrost ponudbe, brezplačna dostava in nato priporočilo prijatelja, znanca ali družinskega člana. Kot najmanj pomembnega izmed naštetih dejavnikov anketirani označujejo možnost plačila po povzetju. Tega je kot »sploh ni pomembno« označilo 9 % udeležencev, kot »ni pomembno« pa še 12,3 % udeležencev.

Slika 5: Dejavniki spletnega nakupa



Vir: Lastni.

V Tabeli 4 so povzeti deskriptivna statistika vseh osmih zajetih dejavnikov spletnega nakupa in rezultati Kolmogorov-Smirnovega testa. Iz rezultatov Kolmogorov-Smirnovega testa je razvidno,

da spremenljivke ne sledijo normalni porazdelitvi. S prikazom opisne statistike v raziskavo vključenih dejavnikov želimo omogočiti možnost podrobnejšega razumevanja rezultatov obravnavanih dejavnikov spletnega nakupovanja pri mladih.

Tabela 1: Deskriptivna statistika dejavnikov spletnega nakupa in rezultati Kolmogorov-Smirnovega testa

	Pestrost ponudbe	Cena izdelka	Enostavnost nakupa	Varnost nakupa	Priporočilo prijatelja, znanca, družinskega člana ...	Možnost plačila po povzetju	Brezplačna dostava	Brezplačno vračilo
N	122	122	122	122	122	122	122	122
VR	0,883	0,526	0,805	0,863	0,746	1,458	1,008	0,976
MIN	1	1	1	-1	1	1	1	1
MAX	5	5	5	5	5	5	5	5
AR	4,040	4,420	4,170	4,520	3,540	3,470	4,090	4,240
AR – sn	0,085	0,066	0,081	0,084	0,078	0,109	0,091	0,089
ST	0,939	0,725	0,897	0,929	0,864	1,207	1,004	0,988
KA	-1,420	-2,020	-1,326	-2,908	-0,598	-0,566	-1,080	-1,593
KA – sn	0,219	0,219	0,219	0,219	0,219	0,219	0,219	0,219
KS	2,642	7,082	1,992	11,402	0,608	-0,542	0,785	2,452
KS – sn	0,435	0,435	0,435	0,435	0,435	0,435	0,435	0,435
P20	4,000	4,000	4,000	4,000	3,000	3,000	4,000	4,000
P50	4,000	4,500	4,000	5,000	4,000	4,000	4,000	4,000
P75	5,000	5,000	5,000	5,000	4,000	4,000	5,000	5,000
K-S	0,302	0,289	0,276	0,387	0,268	0,236	0,244	0,272
K-S df	122	122	122	122	122	122	122	122
K-S Sig.	< 0,001	< 0,001	< 0,001	< 0,001	< 0,001	< 0,001	< 0,001	< 0,001

Vir: Lastni.

Opomba: VR = variacijski razmik, MIN = minimum, MAX = maksimum, AR = aritmetična sredina, AR – sn = standardna napaka ocene aritmetične sredine, ST = standardni odklon, KA = koeficient asimetrije, KA – sn = standardna napaka koeficienta asimetrije, KS = koeficient sploščenosti, KS – sn = standardna napaka koeficienta sploščenosti, P = percentili, K-S = statistika Kolmogorov-Smirnovega testa.

5 Razprava

Izmed 124 anketiranih, starih med 15 in 26 let, je 98,39 % vsaj enkrat opravilo spletni nakup. Odstotek je v primerjavi s podatkom Statističnega urada Republike Slovenije, kjer so ugotovili, da delež v starostni skupini med 16 in 24 let znaša 84 %, občutno višji. Razlog za to bi lahko bila velikost vzorca, saj so v raziskavi statističnega urada sodelovale 4.504 osebe, stare med 16 in 74 let.

Spletne nakupe v povprečni vrednosti košarice do 100 evrov izvaja 90,67 % žensk in 65,95 % moških, medtem ko se povprečna vrednost spletnega nakupa giblje od 101 do 150 evrov pri 6,67 % žensk in 27,66 % moških. Raziskava je pokazala, da je povprečen znesek spletnega nakupa višji pri odjemalcih moškega spola, kar je v skladu z ugotovitvami predhodno izvedenih raziskav drugih avtorjev. Do enakih rezultatov so prišli še Zhou idr. (2007) na podlagi sinteze strokovne in znanstvene literature s področja spletnega nakupovanja.

Na podlagi pregleda strokovne in znanstvene literature smo zasnovali vprašanje o pogostosti spletnega nakupa kategorij dobrin in storitev, ki so bile v predhodnih raziskavah ugotovljene za najpogostejše. Izdelke in storitve smo razdelili v šest kategorij. Prvo kategorijo predstavljajo hrana in prehranska dopolnila, drugo obutev in oblačila, tretjo kozmetika in zdravila. Izdelke in storitve za hobije smo razvrstili v tri kategorije. V prvo kategorijo smo zajeli vstopnice, knjige in filme, drugo kategorijo predstavlja naročnina na kanal za ogled video vsebin, kot so npr. Netflix, Voyo in HBO Max, tretja kategorija pa predstavlja spletni nakup naročnine za glasbeno platformo, npr. iMusic in Spotify. Ugotovili smo, da več kot 80 % mladih na spletu podane kategorije izdelkov in storitev kupi enkrat mesečno ali manj. Največ anketiranih mesečno na spletu opravi nakup naročnine za video in avdio platforme. Večina najbolj priljubljenih (vse izmed naštetih) platform uporablja model mesečne naročnine, zato je ta frekvenca nakupa pričakovana. Mesečno naročnino na kanal video vsebin kupuje 54,09 % udeležencev raziskave, mesečno naročnino na glasbeno platformo pa 55,73 % udeležencev raziskave. Poleg naročnin največ mladih, vključenih v raziskavo, na spletu nakupuje oblačila in obutev ter izdelke in storitve za prosti čas. Ženske v primerjavi z moškimi na spletu pogosteje kupujejo oblačila, obutev, kozmetiko in zdravila, kar se sklada z ugotovitvami predhodnih raziskav.

O priljubljenosti spletnega nakupovanja oblačil in izdelkov za prosti čas sta poročala že Fras (2022) in Henger (2023), prav tako je Mlakar (2023) v članku Statističnega urada Republike Slovenije zapisal, da 66 % potrošnikov na spletu nakupuje oblačila. Raziskovalci so za najpogostejše

izdelke in storitve v spletni košarici potrošnikov navajali še hrano, elektronske in računalniške naprave, pohištvo in izdelke za dom ter kozmetiko in prehranska dopolnila. Ker se raziskava, ki smo jo izvedli, osredotoča na ciljno skupino mladih, lahko s starostno razliko vzorcev pojasnimo odstopanja v kategorijah, ki predvidevajo nakup hrane, prehranskih dopolnil, kozmetike in zdravil. Velik delež mladih v Sloveniji namreč še živi pri starših, zato omenjene kategorije izdelkov in storitev pri več kot 80 % anketiranih ne spadajo med njihove mesečne nakupe. Alternativni razlog bi lahko bil, da je preferenca mladih nakup navedenih izdelkov in storitev v fizičnih prodajalnah.

Mladi, ki so sodelovali v raziskavi, najpogosteje nakupujejo v spletni trgovini About You, ki ponuja oblačila, obutev in modne dodatke širokega nabora znamk. Na spletu pogosto zasledimo njeno marketinško kampanjo. Na drugem mestu je Shein, ki poleg naštetih artiklov ponuja še kozmetiko in pripomočke za dom in prosti čas. Sledita ponudnika logističnih storitev na področju prehrane Wolt in Glovo. Prijubljenost spletnih strani About You in Shein se glede ponujenih artiklov sklada s kategorijo najpogosteje opravljenega spletnega nakupa blaga in storitev – oblačila ali obutev. About You je eden izmed največjih slovenskih trgovcev po prihodkih leta 2023. Mladim je pri odločitvi za spletni nakup najpomembnejša cena izdelka, pomembni se jim zdijo še varnost nakupa, enostavnost nakupa in možnost brezplačnega vračila. O pomenu nizke cene in enostavnosti ter varnosti nakupa kot odločilnih dejavnikov odločitve potrošnikov za spletni nakup so poročali tudi drugi avtorji.

6 Sklep

Večina mladih je že nakupovala na spletu, v naši raziskavi je bilo takšnih 98,39 % anketiranih. Po podatkih Statističnega urada Republike Slovenije delež tistih, ki so že opravili spletni nakup v starostni skupini med 16 in 24 let, znaša 84 %. Povprečna starost ob prvem spletnem nakupu pri mladih je 15,32 leta, povprečen znesek spletnega nakupa pa pri 81,1 % anketiranih znaša do 100 evrov. Povprečna vrednost košarice spletnega nakupa je praviloma večja pri moških.

Mladi najpogosteje kupujejo oblačila in obutev ter izdelke in storitve za prosti čas. Več kot polovica udeležencev raziskave mesečno na spletu plačuje naročnini za glasbeno platformo in kanal z video vsebinami. Hrana, prehranska dopolnila, kozmetika in zdravila za razliko od ugotovitev drugih avtorjev niso med mesečnimi nakupi 80 % mladih, vključenih v raziskavo. Razlog za to bi lahko bila nizka stopnja neodvisnosti mladih v Sloveniji od njihove primarne družine.

Ženske na spletu najpogosteje nakupujejo oblačila ali obutev, moški pa naročnino za glasbeno platformo. Med mladimi so najbolj priljubljene spletne prodajalne About You, Shein ter dostavljalca hrane Wolt in Glovo. Ženske najpogosteje nakupujejo na spletnih mestih Shein, About You in Notino, moški pa na spletnih mestih About You, Mimovrste in Amazon. Mladim sta pri odločitvi za spletni nakup najpomembnejši cena izdelka in varnost nakupa, najmanj pomembna je možnost plačila po povzetju.

Zahvala

Zahvaljujemo se red. prof. dr. Borutu Milfelnerju z Ekonomsko-poslovne fakultete Univerze v Mariboru za nasvete in pomoč pri pripravi ankete ter prodekanom in koordinatorjem tutorjev študentov fakultet Univerze v Mariboru za pomoč pri izvedbi ankete o spletnem nakupovanju med mladimi.

Viri

Citrin, A. V., Stem Jr., D. E., Spangenberg, E. R. & Clark, M. J. (2003). Consumer need for tactile input: An internet retailing challenge. *Journal of Business Research*, 56(11), 915–923. [https://doi.org/10.1016/S0148-2963\(01\)00278-8](https://doi.org/10.1016/S0148-2963(01)00278-8)

ECDB. (2024). *Top eCommerce stores in Slovenia*. ECDB. <https://ecommercedb.com/ranking/stores/si/all?page=1&pagesize=50&specialist=all¤cy=USD>

Fras, L. (2022). *Nakupovalne navade v času epidemije Covid-19 in zadovoljstvo odjemalcev s spletnim nakupovanjem v Sloveniji*. <https://dk.um.si/Dokument.php?id=163438&lang=slv>

Hegler, S. (2023). *Odnos mladih do spletnega nakupovanja*. <https://dk.um.si/Dokument.php?id=166612&lang=slv>

Ige, O. (2004). Electronic shopping: young people as consumers. *International Journal of Consumer Studies*, 28(4), 412–427. <http://dx.doi.org/10.1111/j.1470-6431.2004.00398.x>

Mlakar, T. (2023). *Prek spleta nakupovali okoli dve tretjini oseb*. STAT. <https://www.stat.si/StatWeb/News/Index/11446>

Nedoklan, V. Ž. (2021). *Utjecaj pandemije covid-19 na ponašanje potrošača*. Osijek: Ekonomski fakultet.

OED. (2024). *Online Shopping*. <https://www.oed.com/search/dictionary/?scope=Entries&q=online%20shopping&tl=true>

Venkatesh, V., Speier, P., C., Schuetz, S. W. (2022). Why do people shop online? A comprehensive framework of consumers' online shopping intentions and behaviors. *Information Technology & People*, 35(5). <http://dx.doi.org/10.1108/ITP-12-2020-0867>

Ozaveščenost o digitalnem evru med študenti ekonomije in tehnike

Katarina Leš  

Univerza v Mariboru, Ekonomsko-poslovna fakulteta
Ljubljana, Slovenija

Dr. Nataša Gajšt 

Univerza v Mariboru, Ekonomsko-poslovna fakulteta
Maribor, Slovenija

Nejc Fir 

Univerza v Mariboru, Ekonomsko-poslovna fakulteta
Maribor, Slovenija

Povzetek: Centralne banke, kot je Evropska centralna banka (ECB), aktivno raziskujejo novo obliko denarja, tj. centralnobančne digitalne valute. V primeru ECB je to digitalni evro, ki je digitalna oblika gotovine, ki jo izda centralna banka in je na voljo vsem v evrskem območju. Tema je trenutno aktualnejša kot kadar koli prej, ker se je oktobra 2023 končala prva faza projekta digitalnega evra, dvoletna faza preiskave o zasnovi in distribuciji. Ozaveščenost javnosti bo zato kmalu postala ključni dejavnik njenega uspeha. V tem prispevku analiziramo našo raziskavo, ki smo jo izvedli med 148 študenti o njihovi ozaveščenosti o digitalnem evru. Več kot polovica anketirancev je navedla, da poznajo izraz »digitalni evro« in da se zavedajo, da centralne banke raziskujejo centralnobančne digitalne valute. Kljub temu bi jih bilo le približno 40 % pripravljenih uporabljati digitalni evro, saj sta kibernetična varnost in varnost podatkov pogosta pomisleka. Po drugi strani se je 70 % študentov strinjalo, da bi bil digitalni evro v Evropi sprejet kot zakonito plačilno sredstvo. Mnenja o dejanski ali celo prednostni uporabi se med študenti zelo razlikujejo.

Ključne besede: centralnobančne digitalne valute, digitalni evro, ECB

The awareness of the digital euro among the students of economic sciences and of technical sciences

Katarina Leš  

University of Maribor, Faculty of Economics and Business
Maribor, Slovenia

Nataša Gajšt, PhD 

University of Maribor, Faculty of Economics and Business
Maribor, Slovenia

Nejc Fir 

University of Maribor, Faculty of Economics and Business
Maribor, Slovenia

Abstract: Central banks, such as the European Central Bank (ECB), are actively researching a new form of money, i.e. central bank digital currencies. In the case of the ECB, that is the digital euro, which is a digital form of cash issued by the central bank and available to everyone in the euro area. As the first phase of the digital euro project, a two-year investigation phase on design and distribution, ended in October of 2023, the topic is now more relevant than ever. Thus, public awareness will soon become a crucial factor in its success. In this paper, we analyse our survey of 148 students regarding their awareness of the digital euro. More than half of the respondents stated that they were familiar with the term “digital euro” and that they were aware that central banks are researching central bank digital currencies. However, only around 40% would be ready to use the digital euro as cyber and data safety are common concerns. On the other hand, 70% of students agreed that the digital euro would be accepted as legal tender in Europe. Opinions on actual usage or even priority usage vary a lot among students.

Keywords: central bank digital currencies, digital euro, ECB

1 Introduction

Central banks are actively researching a new form of money, i.e. central bank digital currencies. In the case of the European Central Bank (ECB), that is the digital euro. The digital euro would be a digital form of cash, as a form of public money it would be available free of charge to everyone in the euro area, for any type of digital payments. The digital euro would be issued by the European Central Bank (ECB, 2024).

The recent global shift towards digital payments is fuelling discussions and the development of new forms of money. Leucci (2023) writes that the need for a digital currency has only been exacerbated by recent events, such as the covid-19 crisis, which induced a shift towards digital payments and the rise in popularity of crypto-assets developed by private and/or informal organisations. Two distinct forms of digital currency – central bank digital currency (CBDC) and “stablecoins” have been in the forefront. Stablecoin is a broad term to describe digital currencies, they refer to typically DLT-based cryptocurrencies designed to maintain a stable value relative to another asset. The World Economic Forum’s Digital Currency Governance Consortium (DSGC) mentions two forms of CBDC, a retail form, which would enable households to utilize digital currencies and a wholesale form, which would be limited to licensed financial institutions (DCGC, 2021).

The ECB (2024) explains the difference between a crypto-asset and the digital euro. Crypto-assets are not backed or managed by a central bank or other governmental institution, which makes them risky and unreliable, there is no guarantee that one is able to exchange the crypto-assets for cash. On the other hand, digital euro would be backed by the ECB, which already manages the cash circulation of the euro area.

The ECB is not the only monetary authority that is researching and developing a CBDC. Some countries, such as the Bahamas, Jamaica and Nigeria, have already introduced such digital currencies. Many more countries are in the exploration stage, at the forefront are Brazil, China, India, the United Kingdom, and the euro area (Adrian, He, Mancini-Griffoli, & Sun, 2023).

The ECB (2024) states that a digital euro would offer another way to pay in stores, online shops or to send money to friends. Digital euro would be accepted in any shops and by merchants within the euro area that accept digital payments. It is intended to be used alongside physical cash and as mentioned above, the digital euro would be a public good, meaning that everyone in the euro

area would be able to pay with it free of charge. It is important to highlight that this new currency would be available offline, would be secure and private, as it would offer cash-like privacy. Lastly, the value of one digital euro would always be equivalent to the value of a EUR 1 coin.

Even though cash remains the most frequently used form of payment in Europe, electronic and mobile payments are becoming more and more popular, which creates the need to preserve central bank money as the key element of a well-functioning payments system, especially in an increasingly digital world. To illustrate, purchasing transactions with cash have declined from 79% in 2016 to 59% in 2022, whereas the use of payment cards has risen from 19% to 34% (General Secretariat of the Council, 2024). The ECB study on payment habits also reports that cash was the most frequently used payment method as it was used in 59% of transactions at the point of sale (POS) in 2022. Whilst contactless card payments increased significantly from 41% in 2019 to 62% in 2022, card payments still made up only 34% of POS transactions and the share of payments via a mobile app increased to only 3% in 2022 (ECB, 2022).

The digital euro project started in October 2020, when the ECB published a report which examined the possibility of a central bank digital currency denominated in euro. Next, during October 2020 and January 2021, the ECB ran a public consultation about the benefits and design of a digital euro. In July 2021, the investigation phase was launched. This phase focused on key design and distribution issues. Thus far, the ECB has published three progress reports and on the 28th of June 2023 the Commission presented legislative proposals. The investigation phase concluded in October 2023, and the Governing Council of the ECB has decided to move to the preparation and experimentation phase of this project. This phase could take around three years and will lay the foundation for a potential digital euro. The final decision on whether to introduce the digital euro will take place after the Council of the European Union and the European Parliament have adopted the necessary legislative framework (General Secretariat of the Council, 2024).

The proposed uses of the digital euro range from supporting the digitalisation of the European economy, responding to a significant decline of cash payments, alongside foreign CBDCs or private digital payments, as a new monetary policy transmission channel to mitigate the risks of payments services. The ECB discusses the potential negative effects, such as adverse effects on monetary policy and financial stability, the excessive use of the digital euro as a form of investments, risks of sudden large bank deposits shifts and cyber threats (ECB, 2020).

The World Economic Forum's DCGC (2021) warns of the many regulatory and policy gaps as both the private and public sectors are testing the potential of digital currencies. The main cause of these problems is the mismatch between the speed of innovation and the pace of regulation and policy making.

This paper continues as follows. First, we give review of the relevant literature. Next, we describe the method used in our study. The results and discussion are combined in the following chapter. Lastly, we conclude our paper with suggestions for future research, our limitations, and our key conclusions.

2 Literature review

The basis of our research and survey is a study on privacy concerns and trust in the digital euro done in Germany in 2022. The survey consisted of 1,034 respondents, who form a representative sample of the German adult population. The survey began with an introductory text, based on information provided by the ECB. The study focused on awareness, control, vulnerability, privacy, trust, the willingness to use the digital euro and perceived benefits (Tronnier, Harborth, & Hamm, 2022).

Tronnier, Harborth and Hamm (2022) state that past privacy concerns are not linked to the digital euro, the respondents do not link past financial privacy concerns regarding other financial institutions to privacy concerns regarding central banks. Respondents valued perceived control, meaning they would use the digital euro if they remained in control of sharing their own information. The researchers found that stronger privacy concerns are linked to a stronger fear of privacy threats, older respondents, and a decline in the willingness to use the digital euro. The study finds no significant differences between genders, education, or other personality traits. The results confirm the notion that Germans value privacy as their most important feature in a digital euro. Lastly the study highlights the importance of perceived benefits as they had the strongest effect of all variables. Convenience, proper communication, and education about the digital euro are all key factors for its success.

Desired features of the digital euro as outlined in the report on the public consultation of the ECB include privacy, security, usability throughout the euro area, no additional costs, and the option to use it offline. Respondents showed a preference for an offline solution compared to an online

one. Respondents value accessibility and ease of use as some of the important desired features. The ECB public consultation consisted of 18 questions and analysed the responses of 8,221 respondents from various European countries (ECB, 2021).

The ECB (2021) highlights the wish for the digital euro to be a part of the existing banking and payment solutions in its public consultation. Oversight of the intermediaries, appropriate user protection along with at least partial identification of users are all parts of the requirements to minimise data misuse and safety concerns. The ECB also found that regarding technical solutions the respondents prefer smart cards or secure elements in electronic devices, such as smartphones. Speed of cross-border payments, transparency regarding costs and exchange rates are also of importance to the respondents.

A Dutch survey of 2,552 respondents covered topics of currently available forms of payments, the opinion on current and savings accounts and CBDC. The study shows that half of the respondents had not heard about CBDC prior to the survey. The three most frequent reasons as to why CBDC can be useful are: (1) central banks do not have a profit target as they do not need to make a profit from customers, (2) the ability to use CBDC if other payment methods are not functional, and (3) the improved safety of CBDC compared to cash. Younger respondents also mentioned a lower environmental footprint, respondents over the age of 55 mentioned the improved safety, and middle-aged respondents mentioned the decreased dependency of citizens and business on commercial banks. Respondents would choose CBDC savings accounts due to better protection against theft or fraud and less money lost in case of bankruptcy. Almost half of the respondents would adopt a CBDC current and savings account. The study shows the potential for central banks to introduce digital currencies, as people see the potential resilience against disruptions. The results highlight the importance of clear communication and knowledge, as they are positively linked to the adoption and usage of CBDC (Biljsma, van der Cruijssen, Jonker, & Reijerink, 2021).

Another relevant survey for our study was conducted by Ipsos MORI across advanced and emerging 13 countries. The findings show that central banks are in a good position to issue digital currency. Most respondents showed confidence in digital money issued by the domestic monetary authority and expressed a lack of confidence in digital money issued by a tech or credit card company. The attitude towards accepting digital currencies varies widely depending on income, education, age, and nationality. Respondents valued safety from fraud and theft as the most

important feature, regardless of country. Interestingly, cash still has the highest average scores with special popularity in advanced economies. On the other hand, respondents in emerging economies show the greatest willingness to accept digital currency in the future (Patel & Ortlieb, 2020).

An example of a study on the willingness to adopt a digital currency at the national level is the study on the potential adoption of digital rupee. Gupta, Pandey, El Ammari, and Sahu (2023) focused on the perceived risk factors on one hand, such as financial, regulatory and security risks, as well as privacy and anonymity, and on the other hand, the study also mentioned perceived benefits factors, such as usefulness, ease of use, awareness, innovativeness, trust, and willingness to adopt digital rupee. Among the perceived risks, financial risk was found to have a significant negative impact on trust and the willingness to adopt the digital currency. Trust in the central bank acts as a bridge and can increase the consumers' trust in digital currency and reduce the perceived financial risk. Regulatory and security risks also have a negative impact, as transparency and privacy are a big concern.

Based on the above, we formulated the following research questions for our study:

1. What is the awareness about and attitude of the students of economics and of technical sciences towards the digital euro?
2. Are there any differences in the awareness about and the attitude towards the digital euro between the two groups of students?

3 Method

For this paper, we utilised a quantitative, questionnaire-based approach. The survey was carried out via the website 1KA (<https://www.1ka.si/d/sl>). This study used comparison, synthesis, description, and compilation methods to compare and analyse our results with the results from similar existing studies. Our study is static as it covers a set sample over a two-month period (November–December 2023). The process of online surveying consisted of preparing and testing the questionnaire, gathering the data, and analysing the results of the survey using Excel.

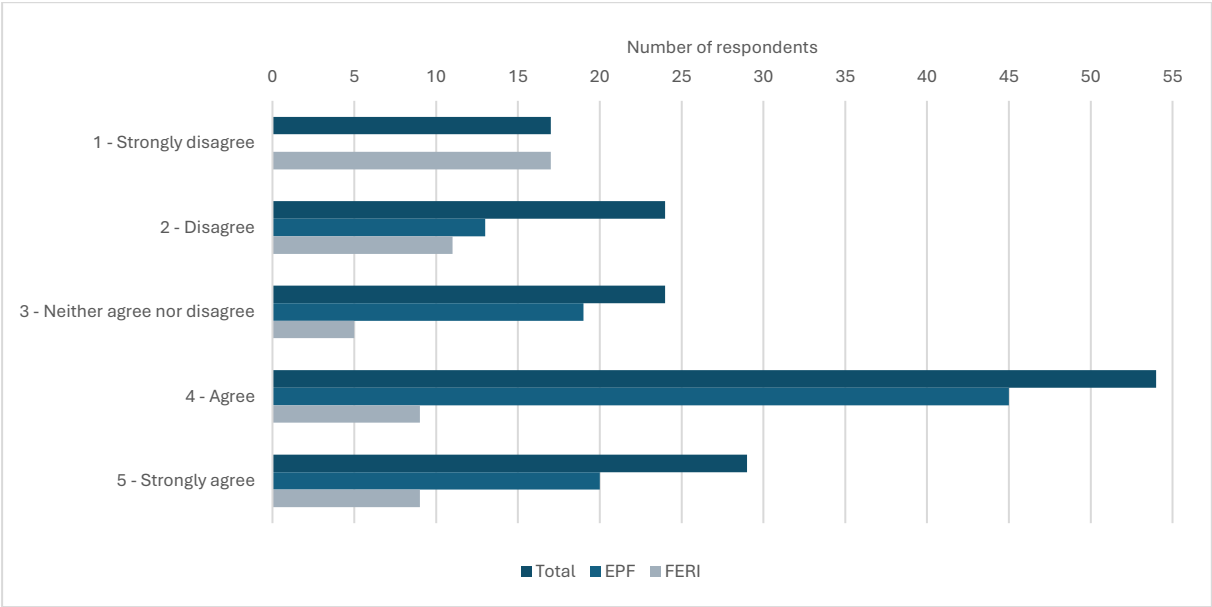
The sample consisted of 148 students from University of Maribor with just over half being female (55%) and the rest male (45%). 97 students were from the Faculty of Economics and Business

(EPF) and 51 from the Faculty of Electrical Engineering and Computer Science (FERI). The age range spanned from 19 to 25 years, with the majority being either 20 or 21 years old. The questionnaire consisted of 14 questions (see Appendix A). After the first two questions regarding familiarity with the topic, the respondents were given a short introductory text based on the text in the German study by Tronnier, Harborth and Hamm (2022) in order to receive some additional information on the topic.

4 Results and Discussion

In this section, we present and discuss our results in line with the two research questions. Regarding the familiarity with the term “digital euro”, we found the following. The results of the survey show that most of the respondents (56.1%) either strongly agree or agree with the statement “I am familiar with the term ‘digital euro’”, as shown in Figure 1. Our survey results show outcomes similar to the Dutch study by Biljsma, van der Crujisen, Jonker and Reijerink (2021), where 46% of the respondents had heard about CBDC prior to the study.

Figure 1: Students’ familiarity with the term “digital euro”



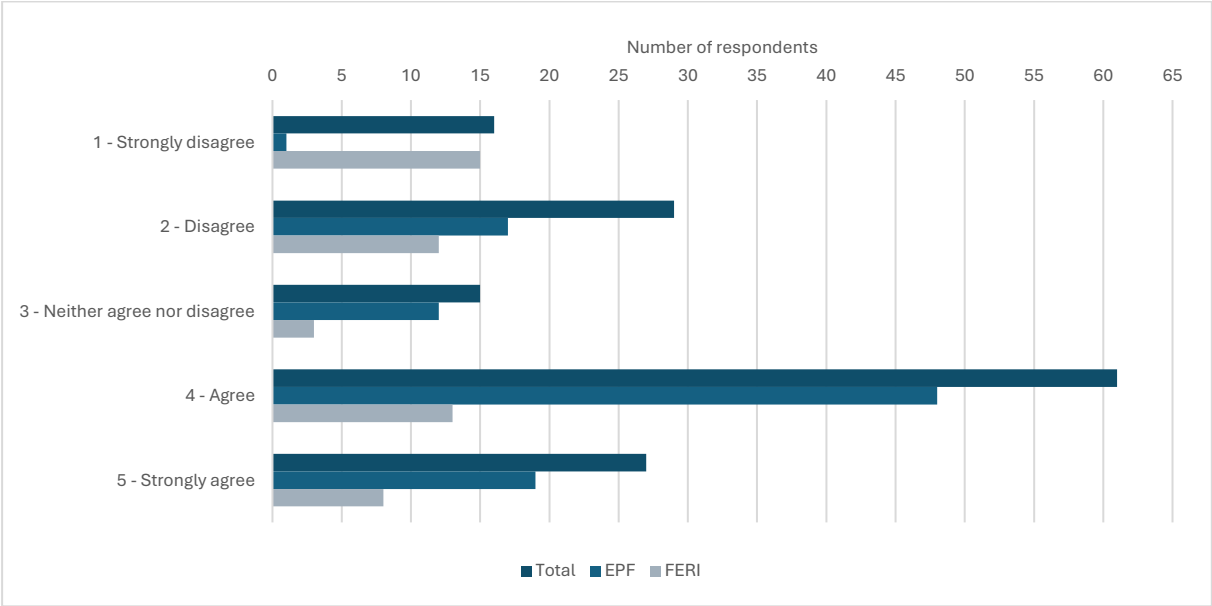
Source: Own data.

The comparison of the two different groups of students showed a notable difference. Namely, 67% of the economics students agreed or strongly agreed with the statement, whilst only 35.3% of the technical sciences students expressed the same opinion, meaning a difference of 31.7

percentage points. This difference could point to students of economics having a greater awareness of the digital euro.

Figure 2 below presents the results regarding the awareness of the respondents as a whole and divided by faculty about the research and development of CBDCs. Over half of the respondents agree or strongly agree with the statement “I am aware that the European Central Bank (ECB) and other central banks are researching and developing the digital euro or central bank digital currencies”, meaning that most respondents know about the current research into digital currencies. The chart is in line with the findings presented in Figure 1. That is, 58.8% of technical sciences students stated that they were not aware of these activities while almost three quarters of the economics students stated that they were. These differences in knowledge could be attributed to their different fields of study and the knowledge the students receive at their respective faculties.

Figure 2: Students’ awareness about the ECB’s and other central banks’ research and development of central bank digital currencies

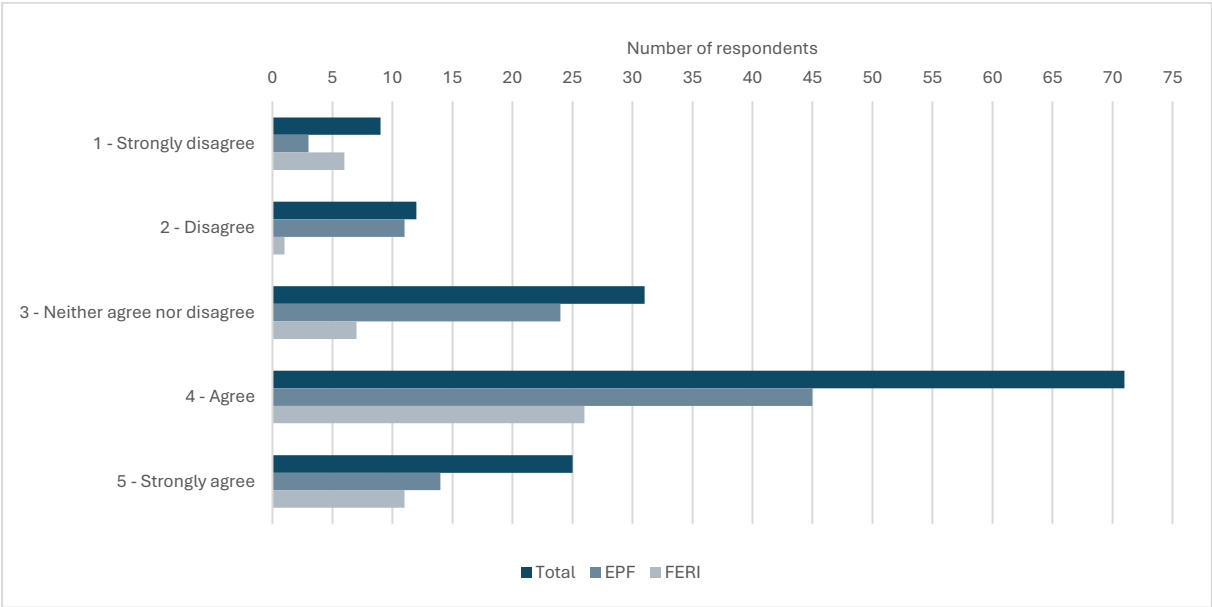


Source: Own data.

As stated in the ECB public consultation about the digital euro, i.e., “Privacy is considered the most important feature of a digital euro by both citizens and professionals” (ECB, 2021), privacy and data safety are the most pressing features. Our results highlight this opinion as two thirds of the respondents either agree or strongly agree with the statement “I would only use the digital

euro if I had control over my information, to which financial institutions have access to”, as shown in Figure 3.

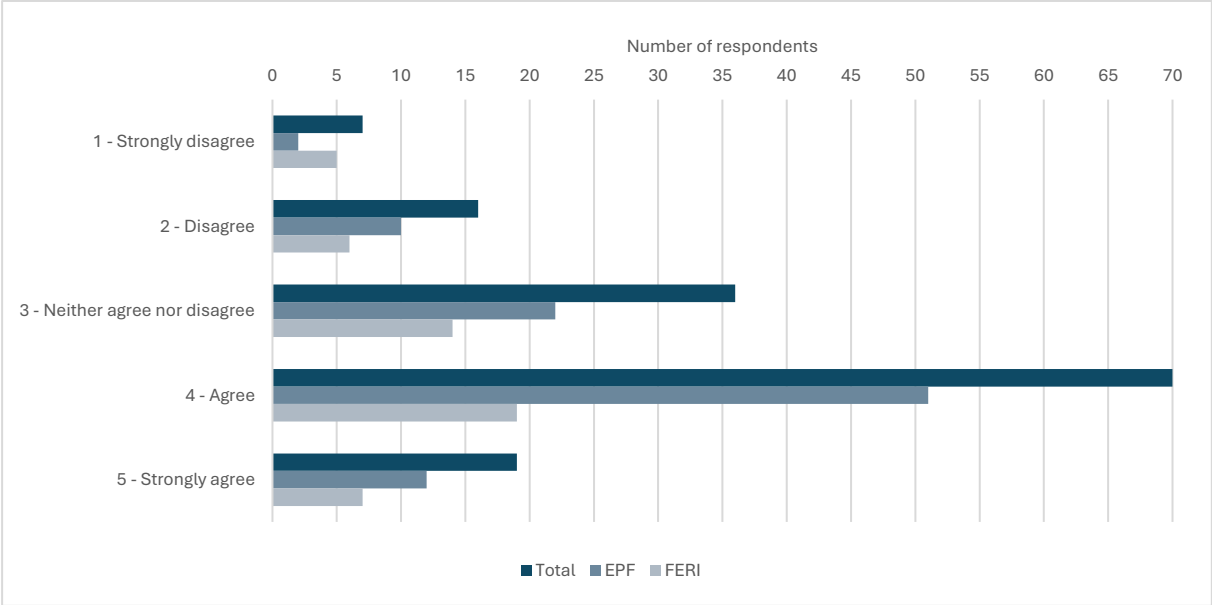
Figure 3: Students’ responses regarding the control over personal information



Source: Own data.

This concern is shared by both student groups, as both show a majority agreement, as illustrated in Figure 3. The World Economic Forum’s white paper on CBDCs echoes this concern, stating that consumers are becoming increasingly more aware of and concerned about whom to entrust their data and how it is used (DCGC, 2021).

Figure 4: Students’ responses regarding concerns about data misuse



Source: Own data.

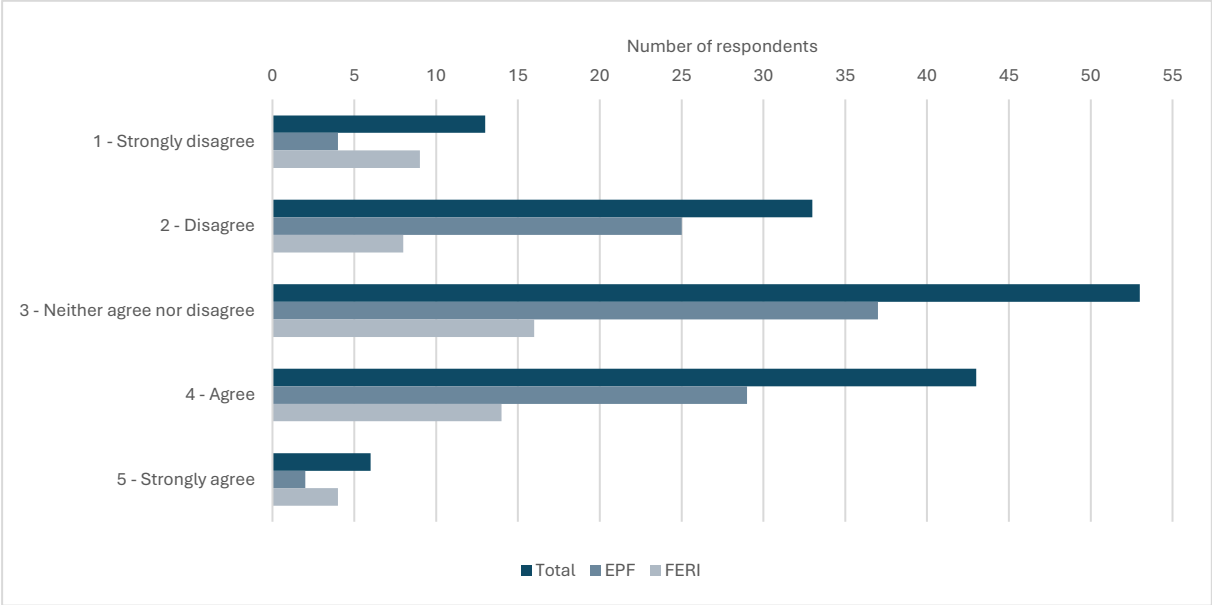
Students’ concerns over data protection and potential misuse can be seen in Figure 4, as 60% of the respondents agree or strongly agree with the statement “*I feel my personal data could be used inappropriately if I use the digital euro*”. Similar concerns, such as financial risks and security risk along privacy and anonymity are all factors that negatively impact the willingness to adopt a digital currency, as found in the study on the digital rupee. However, the study on the digital rupee also reports that trust can have a mediation effect to bridge the impact of perceived risks on the willingness to adopt (Gupta, Pandey, El Ammari, & Sahu, 2023).

The results illustrated in Figure 4 are somewhat counterintuitive when compared to the results of the OMFIF report done by Patel and Ortlieb (2020), whose results show that central banks have the highest trust rates globally. High rates of trust regarding the central banks are also noted in the World Economic Forum’s White Paper (DCGC, 2021). It is possible that the fear of inappropriate data use stems from the novelty of the digital euro, a lack of understanding and a fear of external cyber-attack, rather than a distrust in the central banks themselves.

As can be seen in Figure 5, the students’ opinions on personal data protection vary quite significantly, as one third of all students neither agree nor disagree with the statement “*I believe I could protect my personal information when using the digital euro*”. One fifth of all students disagree with the statements, whilst one third agree. Around 36% of both students of economics and of

technical sciences agree or strongly agree with the statement, which points to almost no difference between the students of the two study fields regarding this statement.

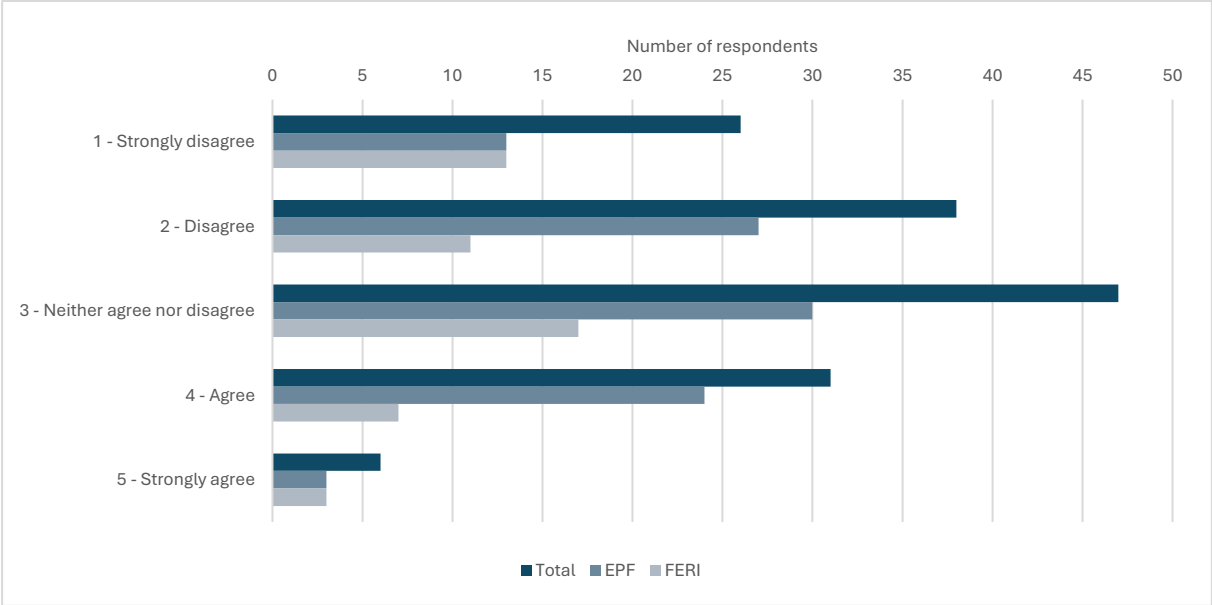
Figure 5: Students’ responses regarding the protection of personal data



Source: Own data.

The next section of the survey was concerned with the usability of digital euro. Figures 6, 7 and 8 present the students’ answers regarding their preferred online payment methods and the digital euro suitability. Figure 6 shows the distribution of students’ responses to the statement “*I would prefer to use the digital euro over other online payment methods*”.

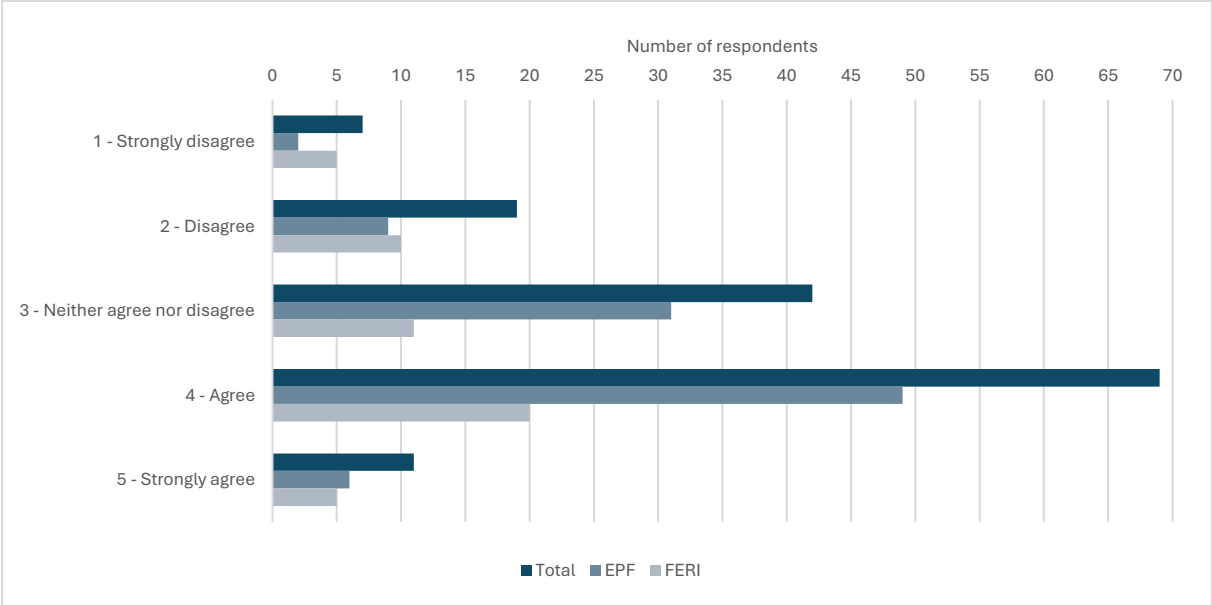
Figure 6: Student’s responses regarding digital euro preference as a payment method



Source: Own data.

What stands out in Figure 6 is that 41% of the economics students and 47% of the technical sciences students would strongly disagree or disagree with the statement, indicating a preference for other online payment methods rather than the digital euro. The economics students’ responses show a 65.9% disagreement rate, while the technical sciences students show a 50.9% disagreement rate. The OMFIF report by Patel and Ortlieb (2020) might explain this preference, as their study shows that cash remains a favourite, surprisingly even more so in some advanced economies. The ECB study on payment habits supports this preference, as it reports that cash was the most frequently used payment method in 2022 (ECB, 2022).

Figure 7: Students’ responses regarding the acceptance of the digital euro as a payment method



Source: Own data.

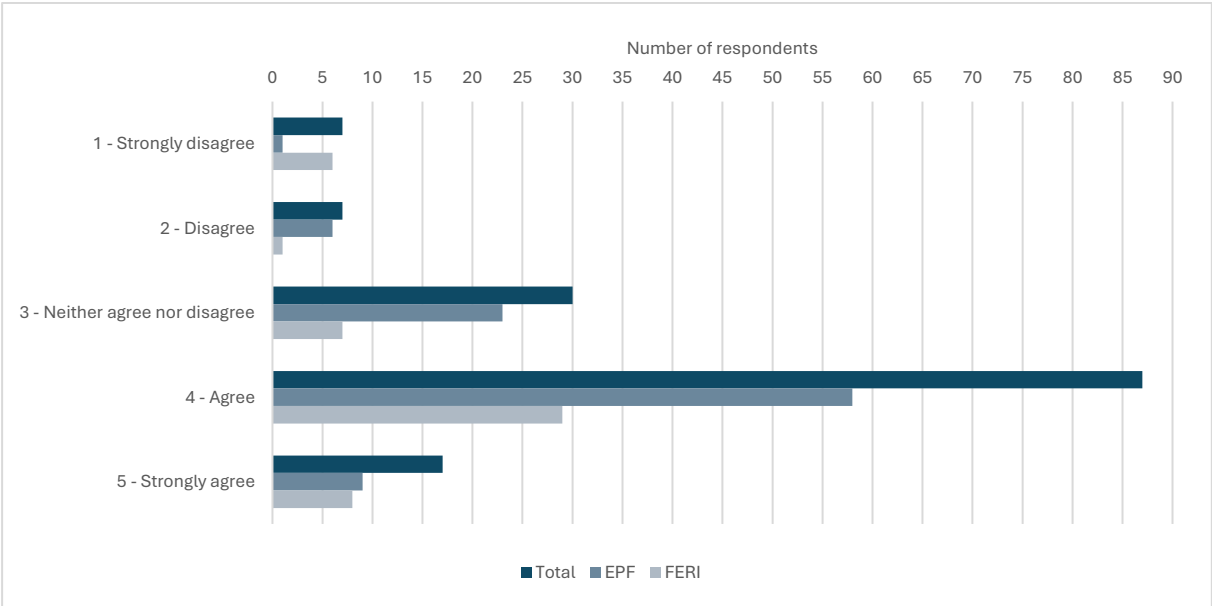
Contrastingly, Figure 7 shows a different sentiment regarding the availability and usability of the digital euro as a payment option. The ECB public consultation showed that respondents participating in the consultation opted for usability throughout the euro area as one of the most preferable options (ECB, 2021). Over half of the respondents in our study agree or strongly agree with the statement “*The digital euro would be accepted as a payment method all over Europe*”. It is worth noting that whilst only 10% of economics students disagree or strongly disagree with the statement, about 30% of technical sciences students do not think that the digital euro would be accepted as a payment method all over Europe.

The results shown in Figure 6 and Figure 7 might be explained by the lack of education regarding the benefits of the digital euro. Perhaps better public awareness about the potential features, uses and benefits of the digital euro could lead to a higher preference for it and help earn the public’s trust. Similarly, Tronnier, Harborth and Hamm (2022) emphasised the importance of proper communication and education about the digital euro.

Surprisingly, a great majority of the students (70%) agree or strongly agree with the statement “*The digital euro would be suitable for shopping and making purchases*”, as seen in Figure 8 below. 72.5% of economics students either agree or strongly agree with this statement, while technical sciences students’ agreement rate is only 3.4 percentage points lower. This high approval

rate might stem from the familiarity with online shopping, where the use of online payment methods is prevalent, thus making it easier to imagine making these transactions with a digital currency. During the pandemic, 32% of consumers included in the ECB survey regarding consumer payment behaviour used cash less often. Consumers stated convenience as the top reason for using less cash during the pandemic (ECB, 2022).

Figure 8: Students’ responses regarding the suitability of the digital euro for shopping



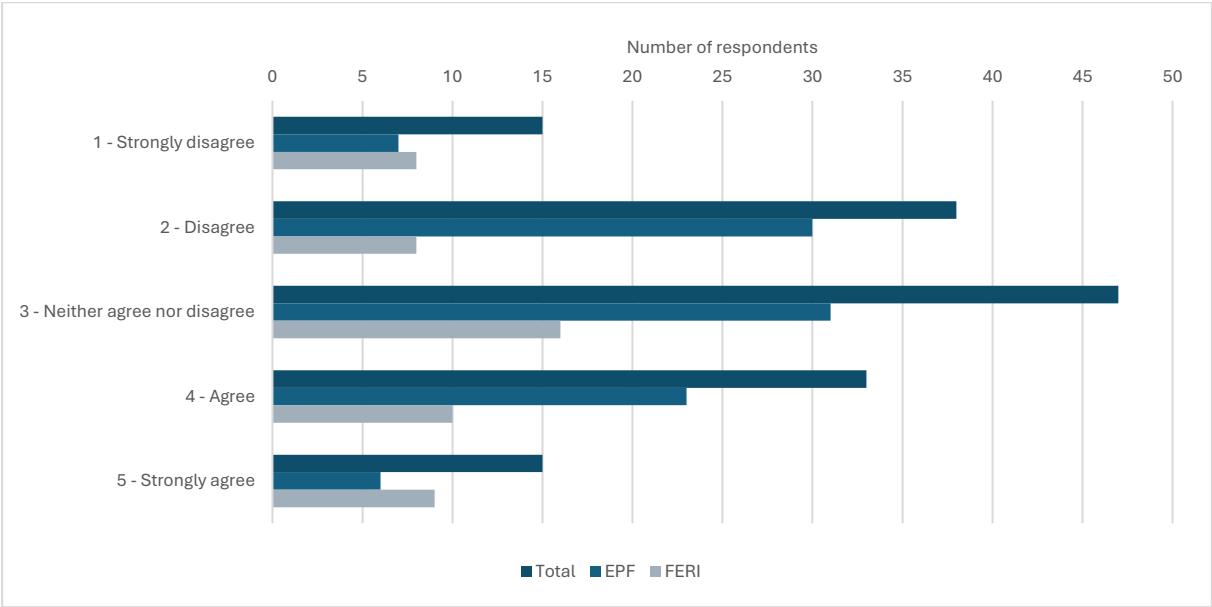
Source: Own data.

As mentioned previously, data safety and trust are some of the most important factors regarding the willingness to adopt a digital currency. Gupta, Pandey, El Ammari and Sahu (2023) found that while trust has a positive and significant effect on willingness to adopt a digital currency, it is also significantly affected by all perceived benefits and risks. These findings might explain our respondents’ varied answers regarding the safety and trustworthiness of the digital euro. Namely, 35.8% of all students disagree or strongly disagree with the statement “*The digital euro would be safe, trustworthy and could not be forged*”, which is only 3.4 percentage points higher than the share of all students who agree or strongly agree with the statement.

In contrast to other results of the survey, Figure 9 shows that 37.3% of technical sciences students agree or strongly agree with this statement, which is 7.4 percentage points higher than in the case of economics students. However, a third of all students neither agree nor disagree, which again might stem from their lack of knowledge of the digital euro. A similar scepticism

towards digital money is described by Patel and Ortlieb (2020). The authors state that emerging market respondents were much more open to digital money than those in advanced economies, i.e., 41% of German and 34% of French respondents stated concerns about privacy and protection as their main reason to score digital money poorly.

Figure 9: Students’ responses regarding digital euro safety and trustworthiness



Source: Own data.

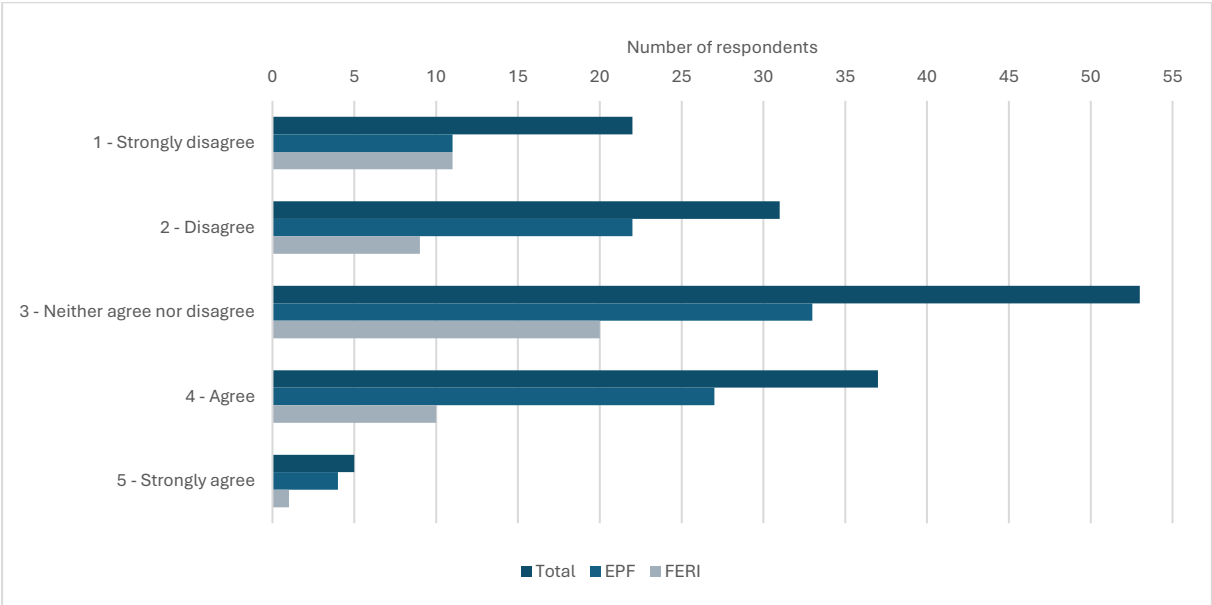
If we now turn to the last statement concerned with data safety, specifically trust in central banks, we can see a similar answer distribution to Figure 9. Figure 10 indicates that 35.8% of all respondents neither agree nor disagree with the statement “*Central banks would handle personal data correctly and safely*”. This could point to some uncertainty and perhaps their lack of knowledge. The share of students who agree or strongly agree is 7.4 percentage points lower than that of their uncertain counterparts. The disagreement rate between the students of economics is 5.2 percentage points lower than that of the technical sciences students.

The study by Tronnier, Harborth and Hamm (2022) might offer an explanation for these results (illustrated in Figures 9 and 10), as their findings suggest that soft trust factors, such as credibility and image, are directly related to privacy concerns. The authors state that individuals might take the hard trust factors of a digital euro for granted and expect them, given their experiences with cash and banknotes that have already proven to be trustworthy. However, the digital euro does

not exist yet, and the ECB cannot yet prove that it can successfully develop and implement a secure and reliable digital currency.

What emerges from our results is a varied opinion regarding data safety, trust and reliability. This is in contrast to Patel and Ortlieb (2020), who state that central banks are the most trusted institutions among all monetary service providers. In summary, our results show that a lot of uncertainty and novelty still exist regarding digital currencies and that the ECB, along with other central banks, might benefit greatly from better knowledge and even awareness of the digital euro. Knowledge and understanding of the digital euro’s useability might help raise people’s willingness to use such a CBDC in the future.

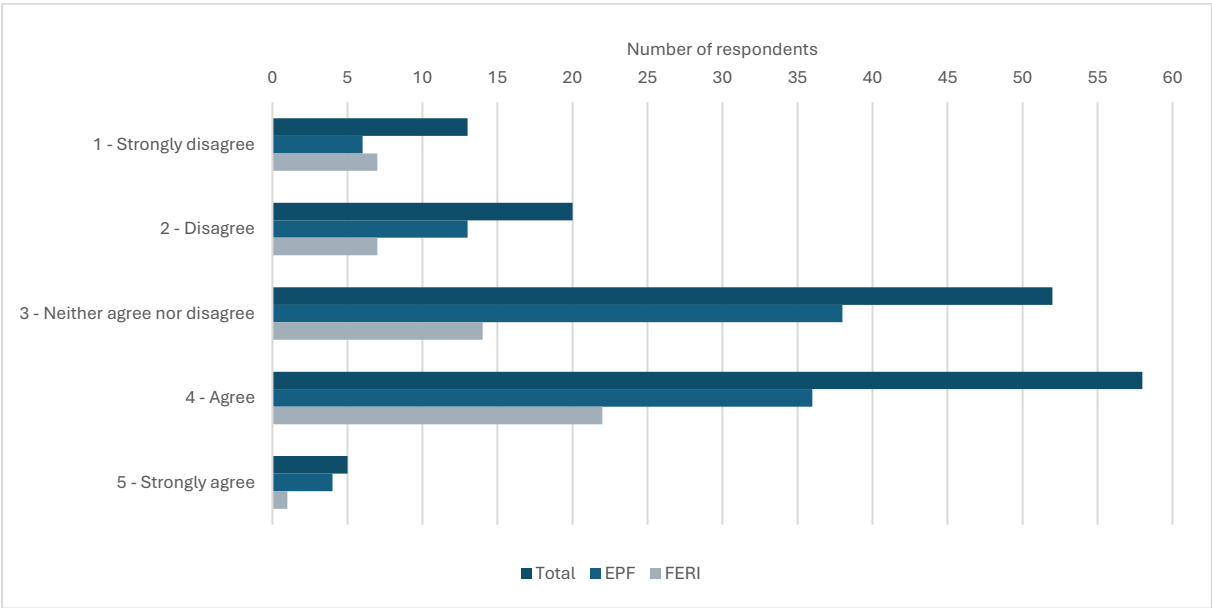
Figure 10: Students’ responses regarding correct central bank data handling



Source: Own data.

In the final part of the survey, respondents were asked about their willingness to use the digital euro. The most striking result to emerge from the data is that despite all of the perceived uncertainties (as presented above), 42.6% of all students in our survey would be willing to use the digital euro, as presented in Figure 11. On the other hand, 35.1% of students neither agree nor disagree with the statement “I would be willing to use the digital euro”. This points to a quite large share of students who are open to accepting this form of the euro.

Figure 11: Students’ responses regarding the willingness to use the digital euro



Source: Own data.

5 Conclusion

This paper set out to research the awareness of and attitudes towards the digital euro among the economics and technical sciences students at the University of Maribor. Additionally, we set to determine if there were any differences between the two groups of students.

The main findings of our study are that over half of the respondents are familiar with the term “digital euro” and are aware of the activities of the ECB regarding the digital euro. The second major finding was that data privacy and security were major concerns among students, with control over personal data being a priority. However, the digital euro has not been marked as a preferred payment method, but the respondents did find it suitable for making purchases. The study has also identified varied opinions regarding the perceived safety and trustworthiness of the digital euro and of the ECB. Despite the perceived risks, about two-fifths of the respondents would be willing to use the digital euro.

One of the more significant findings to emerge from this study is that there are differences between the two groups of students in their responses concerning the awareness about the digital euro and the ECB’s activities regarding the research and development of the digital euro. Apart

from that, there were notable differences when it came to the belief that the digital euro would be accepted as a Europe-wide payment method.

Taken together, these results suggest that clear communication and better education regarding the digital euro are key factors in its potential success. The respondents have shown a clear preference for privacy, data protection and safety, as echoed in much of the current literature.

The current study is limited by the fact that it only surveyed 148 students of the University of Maribor, namely from the Faculty of Economics and Business and the Faculty of Electrical Engineering and Computer Science. Our survey sample was disproportionate, as there were roughly twice as many economics students, which might have had an effect on the final results.

In spite of its limitations, this study contributes to our understanding of the awareness and attitudes towards the digital euro of economics and technical sciences students. This study presents an important contribution to the topic, as such a study has not yet taken place in Slovenia or has been conducted in the student population and the topic itself is relatively new and has not yet been extensively researched. Our sample of respondents consisted of a younger population, who is familiar with online shopping, other online transactions and online payment methods, meaning a share of the public who would be likely to use a CBDC. The insights gained from this study may be of assistance to educators and policymakers (BS, ECB...) to further the public awareness and understanding of the digital euro. This would likely lead to a higher adoption rate because the public would understand the system, the benefits and the risks.

A further study could research these topics in a sample of students from different faculties, from different regions and universities, as well as include more of the general population (diverse age range, incomes, education levels...).

References

Adrian, T., He, D., Mancini-Griffoli, T., & Sun, T. (2023, November 20). *Central bank digital currency development enters the next phase*. Retrieved March 13, 2024, from IMG Blog: <https://www.imf.org/en/Blogs/Articles/2023/11/20/central-bank-digital-currency-development-enters-the-next-phase>

Biljsma, M., van der Cruijssen, C., Jonker, N., & Reijerink, J. (2021). *What triggers consumer adoption of CBDC?* Amsterdam: De Nederlandsche Bank. https://www.dnb.nl/media/amwfjgey/working_paper_no-_709.pdf

DCGC. (2021, November). *Digital currency governance consortium white paper series*. Retrieved March 26, 2024, from World Economic Forum: <https://www.weforum.org/publications/digital-currency-governance-consortium-white-paper-series/>

ECB. (2020). *Report on a digital euro*. Frankfurt am Main: ECB. https://www.ecb.europa.eu/pub/pdf/other/Report_on_a_digital_euro~4d7268b458.en.pdf

ECB. (2021). *Eurosystem report on the public consultation on a digital euro*. Frankfurt am Main: ECB. https://www.ecb.europa.eu/pub/pdf/other/Eurosystem_report_on_the_public_consultation_on_a_digital_euro~539fa8cd8d.en.pdf

ECB. (2022). *Study on the payment attitudes of consumers in the euro area (SPACE)*. Retrieved March 28, 2024, from European Central Bank: https://www.ecb.europa.eu/stats/ecb_surveys/space/html/ecb.spacereport202212~783ffdf46e.en.html

ECB. (2024). *What would a digital euro be?* Retrieved March 3, 2024, from European Central Bank: https://www.ecb.europa.eu/paym/digital_euro/features/html/index.en.html

General Secretariat of the Council. (2024, March 7). *Towards a digital euro*. Retrieved March 13, 2024, from European Council, Council of the European Union: <https://www.consilium.europa.eu/en/policies/digital-euro/>

Gupta, S., Pandey, D., El Ammari, A., & Sahu, G. (2023). Do perceived risks and benefits impact trust and willingness to adopt CBDCs? *Research in International Business and Finance*, Volume 66. <http://dx.doi.org/10.1016/j.ribaf.2023.101993>

Leucci, S. (2023). *Central bank digital currency*. Retrieved March 13, 2024, from European Data Protections Supervisor: https://www.edps.europa.eu/press-publications/publications/techsonar/central-bank-digital-currency_en

Patel, B., & Ortlieb, P. (2020). *Digital currencies: A question of trust*. London: OMFIF. <https://www.omfif.org/wp-content/uploads/2020/02/Digital-currencies-A-question-of-trust-1.pdf>

Tronnier, F., Harborth, D., & Hamm, P. (2022, May-June). Investigating privacy concerns and trust in the digital Euro in Germany. *Electronic Commerce Research and Applications*, 53, 101158. <http://dx.doi.org/10.1016/j.ele-erap.2022.101158>

Appendix A: Questionnaire items (all items except 1. And 2. are measured on a 5-point Likert scale).

1. Age
2. Gender
3. I am familiar with the term “digital euro”.
4. I am aware that the European Central Bank (ECB) and other central banks are researching and developing the digital euro or central bank digital currencies.

Introductory text:

The European Central Bank (ECB) and national central banks of the euro area are working together on researching and developing the digital euro.

The digital euro would be a digital form of payment, issued by the central bank, which would be available to all citizens, similarly to cash, but in a digital, electronic form. It would enable payment in a fast, safe way, without additional costs. The digital euro would not replace cash, it would complement it.

The digital euro would be legal tender, which would work similarly to current online payment methods, additionally it would also work offline. The transaction would be done via an app, website, card or similar smart device (smart watches, mobile phones) in a similar way as other current payment methods (PayPal, Google Pay or Apple Pay).

5. I would only use the digital euro if I had control over my information, to which financial institutions have access to.
6. I feel my personal data could be used inappropriately if I use the digital euro.
7. I believe I could protect my personal information when using the digital euro.
8. I would prefer to use the digital euro over other online payment methods.
9. The digital euro would ensure a payment method all over Europe.
10. The digital euro would be suitable for shopping and making purchases.
11. The digital euro would be safe, trustworthy and could not be forged.
12. Central banks would handle personal data correctly and safely.
13. I would be willing to use the digital euro.

Analiza poročanja ameriških kabelskih televizijskih postaj o umetni inteligenci

Tinkara Primec ✉

Univerza v Ljubljani, Filozofska fakulteta
Ljubljana, Slovenija

Dr. Alenka Kavkler

Univerza v Mariboru, Ekonomsko-poslovna fakulteta
Maribor, Slovenija

Dr. Dejan Romih 

Univerza v Mariboru, Ekonomsko-poslovna fakulteta
Maribor, Slovenija

Povzetek: V tem prispevku analiziramo poročanje ameriških kabelskih televizijskih postaj o umetni inteligenci, pri čemer nas zanimajo razlike med CNN-om, tj. levičarsko kabelsko televizijsko postajo, in FOX-om, tj. desničarsko kabelsko televizijsko postajo. Na osnovi analize podatkov o času zaslona ugotavljamo, da je pred uvedbo ChatGPT-ja in po njej FOX o umetni inteligenci v povprečju poročal več kot CNN.

Ključne besede: mediji, umetna inteligenca, Združene države Amerike

An analysis of US cable television coverage of artificial intelligence

Tinkara Primec 

University of Ljubljana, Faculty of Arts
Ljubljana, Slovenia

Alenka Kavkler, PhD

University of Maribor, Faculty of Economics and Business
Maribor, Slovenia

Dejan Romih, PhD 

University of Maribor, Faculty of Economics and Business
Maribor, Slovenia

Abstract: In this paper, we analyse the coverage of artificial intelligence on US cable television, focusing on the differences between left-leaning CNN and right-leaning FOX. By analysing the screen time data, we find that FOX reported more on artificial intelligence on average than CNN before and after the introduction of ChatGPT.

Keywords: artificial intelligence, media, United States

1 Uvod

Namen tega prispevka je podati rezultate analize poročanja desničarske in levičarske ameriške kableske televizijske postaje o umetni inteligenci, ChatGPT-ju (<https://chat.openai.com/>) in OpenAI-ju (<https://openai.com/>), s čimer želimo zapolniti vrzel v literaturi. Izkazalo se je, da obstaja potreba po analiziranju poročanja ameriških kableskih televizijskih postaj o umetni inteligenci, ki je aktualna tema v ekonomiji, psihologiji, sociologiji in drugih vedah. Uvedba ChatGPT 30. novembra 2022 predstavlja veliko prelomnico, ki jo upoštevamo tudi v tem prispevku. Izkazalo se je, da od takrat naprej mediji veliko poročajo o umetni inteligenci, kar nas ne preseneča glede na njeno zmogljivost.

Raziskave (Beets idr., 2023; Choung, David & Ross, 2022; Chuan, Tsai & Cho, 2019; Yang idr., 2023) kažejo, da je poročanje medijev o umetni inteligenci pomembno, saj omogoča, da se ljudje znebijo strahu in predsodkov pred njeno uporabo, npr. v zdravstvu (Beets idr., 2023). V ta namen je Organizacija Združenih narodov za izobraževanje, znanost in kulturo izdala in založila priročnik o poročanju o umetni inteligenci (gl. Jaakkola, 2023), ki je lahko koristen pripomoček tudi za študente ekonomije, psihologije, sociologije in drugih ved.

Ta prispevek je strukturiran tako, da ima še štiri poglavja. V poglavju 2 podajamo metode raziskovanja, v poglavju 3 rezultate raziskovanja, v poglavju 4 razpravo o rezultatih raziskovanja, v poglavju 5 pa sklep, s čimer upoštevamo strukturo IMRaD (Introduction, Methods, Results, and Discussion).

2 Metode

V tem prispevku uporabljamo podatke o trajanju časa, v katerem je bila na zaslonu dveh ameriških kableskih televizijskih postaj (CNN-a, FOX-a) navedena besedna zveza artificial intelligence ali kratica AI ter besedi ChatGPT in OpenAI, pri čemer se omejujemo na obdobje od januarja 2010 do januarja 2024. Podatki, ki jih uporabljamo, so dostopni na <https://tvnews.stanford.edu/>. Dobil smo jih tako, da smo v iskalno polje vtipkali:

- text="artificial intelligence | AI" AND channel=CNN
- text="artificial intelligence | AI" AND channel=FOX
- name="Joe Biden" AND text="artificial intelligence | AI" AND channel=CNN
- name="Donald Trump" AND text="artificial intelligence | AI" AND channel=CNN

- text=ChatGPT AND channel=CNN
- text=ChatGPT AND channel=FOX
- text=OpenAI AND channel=CNN
- text=OpenAI AND channel=FOX

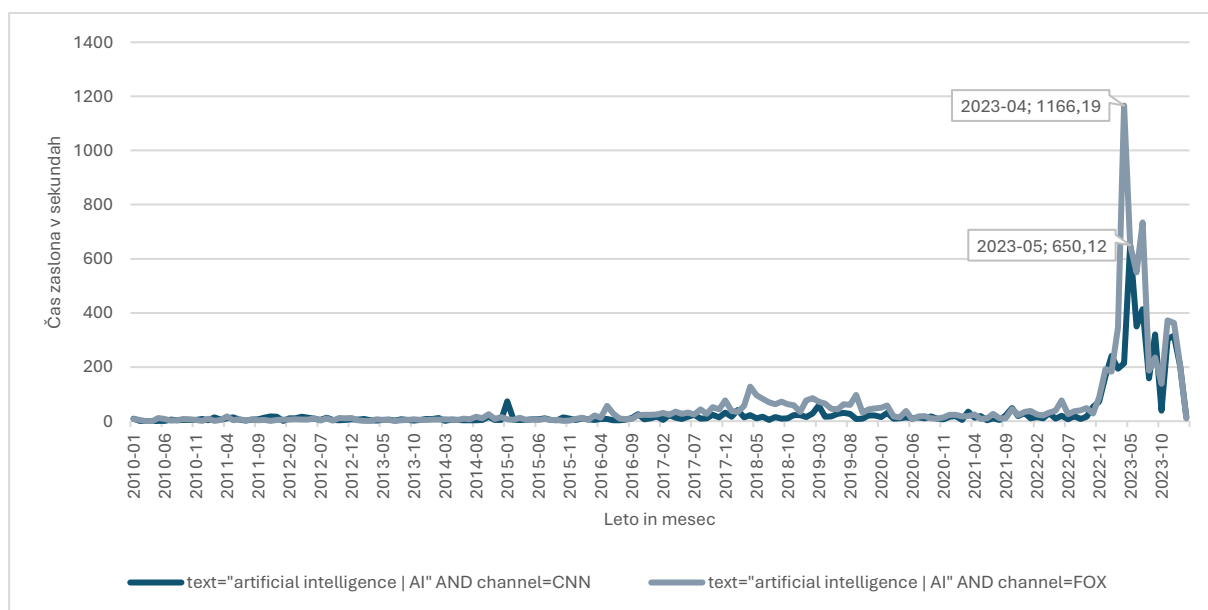
3 Rezultati

3.1 Rezultati analize poročanja ameriških kabelskih televizijskih postaj o umetni inteligenci

V tem poglavju podajamo rezultate analize poročanja CNN-a in FOX-a o umetni inteligenci. Podatki za CNN kažejo, da se je o umetni inteligenci največ poročalo maja 2023, ko je čas, v katerem je bila na zaslonu navedena besedna zveza artificial intelligence ali kratica AI, trajal 648 sekund ali 10,80 minute. Podatki za FOX pa kažejo, da se je o umetni inteligenci največ poročalo aprila 2023, ko je čas, v katerem je bila na zaslonu navedena besedna zveza artificial intelligence ali kratica AI, trajal 1164 sekund ali 19,40 minute. Podatki kažejo tudi, da je leta 2023 o umetni inteligenci največ poročal FOX (5100 sekund ali 85 minut), ki mu sledi CNN (3360 sekund ali 56 minut).

Zanimalo nas je tudi, kdaj se je na CNN-u in FOX-u največ poročalo o umetni inteligenci, medtem ko je bila na zaslonu prikazana slika Joeja Bidna ali Donalda Trumpa.

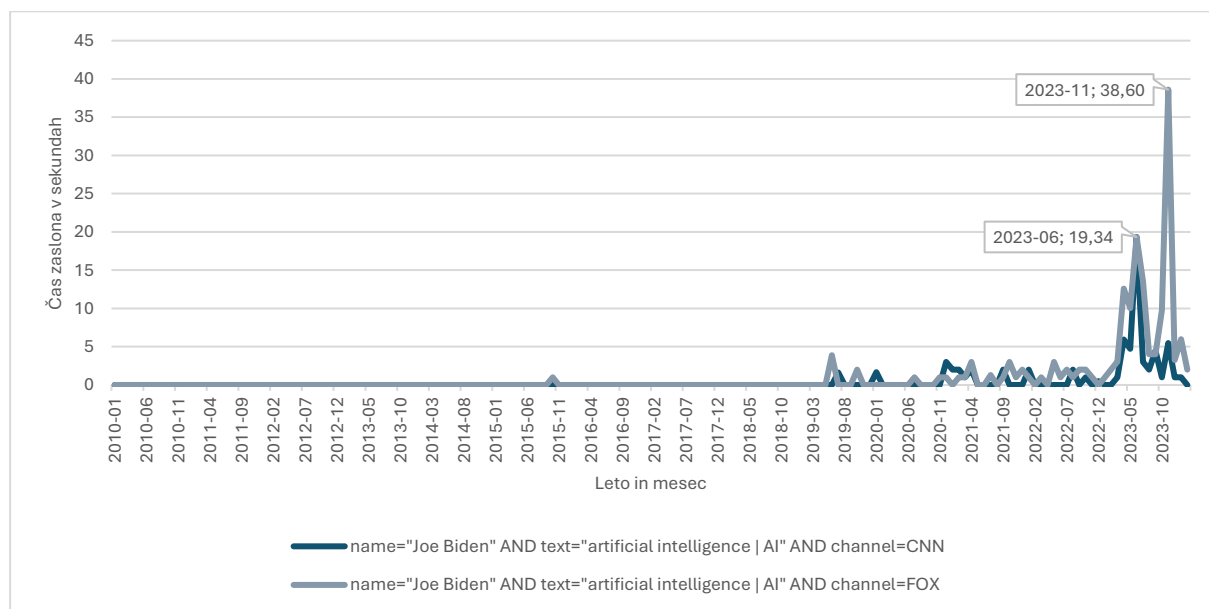
Slika 1: Poročanje ameriških kabelskih televizijskih postaj o umetni inteligenci



Vir podatkov: <https://tvnews.stanford.edu/>.

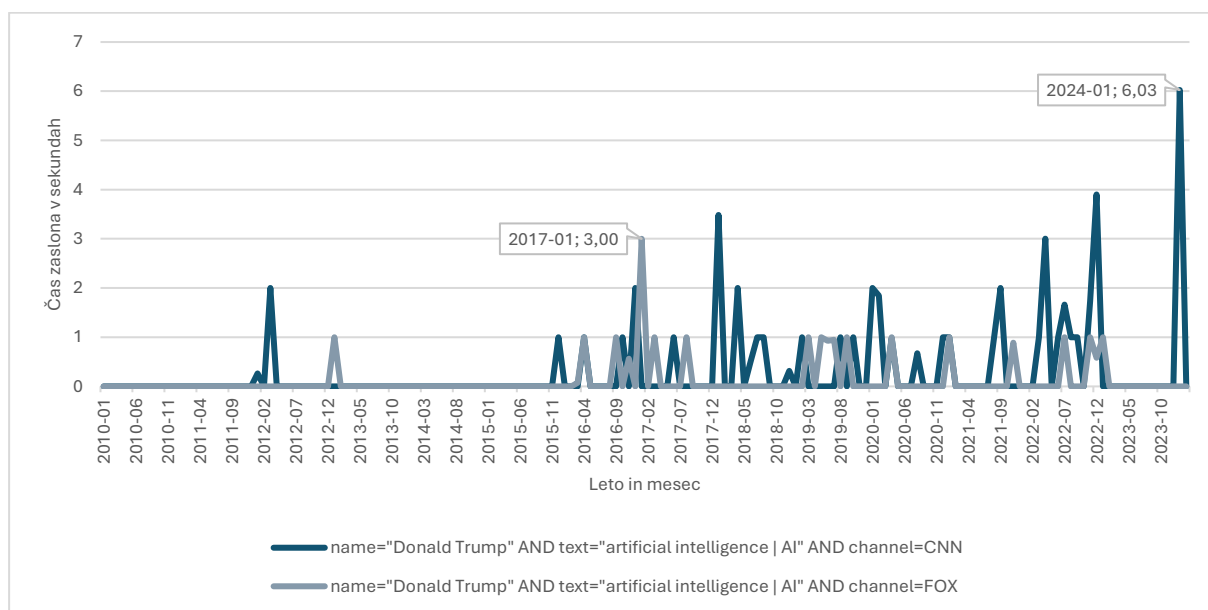
Podatki za CNN kažejo, da se je o umetni inteligenci, medtem ko je bila na zaslonu prikazana slika Joeja Bidna, največ poročalo januarja 2023, ko je čas, v katerem je bila na zaslonu prikazana slika 46. ameriškega predsednika in hkrati navedena besedna zveza artificial intelligence ali kratica AI, trajal 19,34 sekunde ali 0,32 minute, kar je za 16,34 sekunde ali 0,27 minute manj kot v primeru, v katerem je bila na zaslonu prikazana slika 45. ameriškega predsednika in hkrati navedena besedna zveza artificial intelligence ali kratica AI. Podatki za FOX pa kažejo, da se je o umetni inteligenci, medtem ko je bila na zaslonu prikazana slika Joeja Bidna, največ poročalo novembra 2023, ko je čas, v katerem je bila na zaslonu prikazana slika 46. ameriškega predsednika in hkrati navedena besedna zveza artificial intelligence ali kratica AI, trajal 38,60 sekunde ali 0,64 minute, kar je za 32,58 sekunde ali 0,54 minute več kot v primeru, v katerem je bila na zaslonu prikazana slika 45. ameriškega predsednika in hkrati navedena besedna zveza artificial intelligence ali kratica AI. Podatki kažejo tudi, da je leta 2023 o umetni inteligenci, medtem ko je bila na zaslonu prikazana slika Joeja Bidna, največ poročal FOX (38,60 sekunde ali 0,64 minute), ki mu sledi CNN (19,34 sekunde ali 0,32 minute).

Slika 2: Poročanje ameriških kabelskih televizijskih postaj o umetni inteligenci, medtem ko je na zaslonu prikazana slika sedanjega ameriškega predsednika



Vir podatkov: <https://tvnews.stanford.edu/>.

Slika 3: Poročanje ameriških kabelskih televizijskih postaj o umetni inteligenci, medtem ko je na zaslonu prikazana slika prejšnjega ameriškega predsednika

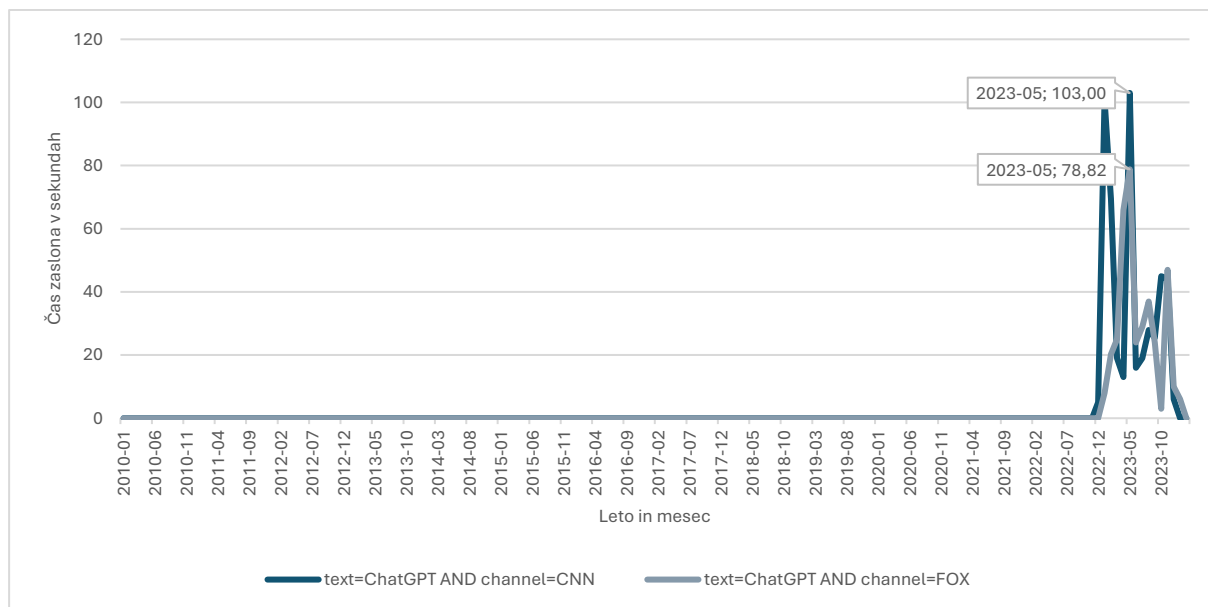


Vir podatkov: <https://tvnews.stanford.edu/>.

3.2 Rezultati analize poročanja ameriških kabelskih televizijskih postaj o ChatGPT-ju in OpenAI-ju

V tem poglavju podajamo rezultate analize poročanja CNN-a in FOX-a o ChatGPT-ju in OpenAI-ju. Podatki za CNN kažejo, da se je o ChatGPT-ju največ poročalo aprila 2023 (gl. sliko 2), ko je čas, v katerem je bila na zaslonu navedena beseda ChatGPT, trajal 103 sekunde ali 1,70 minute. Podatki za FOX pa kažejo, da se je o ChatGPT-ju največ poročalo marca 2023, ko je čas, v katerem je bila na zaslonu navedena beseda ChatGPT, trajal 78,82 sekunde ali 1,30 minute. Podatki kažejo tudi, da je leta 2023 o ChatGPT-ju največ poročal CNN (388,17 sekunde ali 6,47 minute), ki mu sledi FOX (349,74 sekunde ali 5,83 minute).

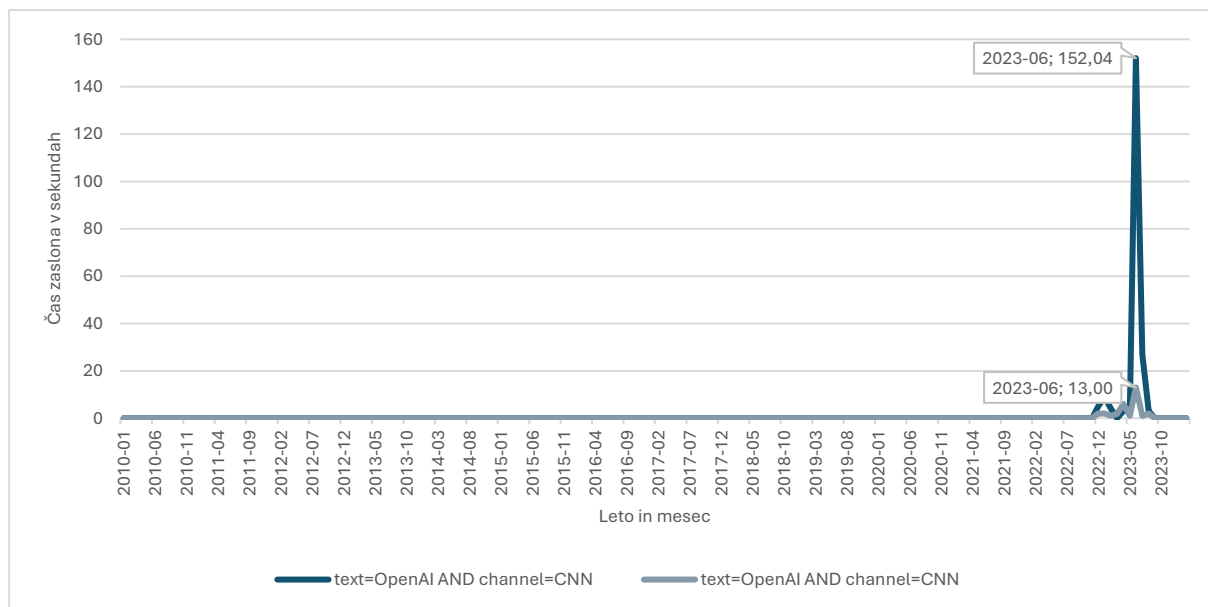
Slika 4: Poročanje ameriških kabelskih televizijskih postaj o ChatGPT-ju



Vir podatkov: <https://tvnews.stanford.edu/>.

Podatki za CNN kažejo, da se je o OpenAI-ju največ poročalo junija 2023 (gl. sliko 3), ko je čas, v katerem je bila na zaslonu navedena beseda OpenAI, trajal 152,04 sekunde ali 2,54 minute. Podatki za FOX pa kažejo, da se je o OpenAI-ju največ poročalo junija 2023, ko je čas, v katerem je bila na zaslonu navedena beseda OpenAI, trajal 13,00 sekunde ali 0,22 minute. Podatki kažejo tudi, da je leta 2023 o OpenAI-ju največ poročal CNN (201,04 sekunde ali 3,35 minute), ki mu sledi FOX (27,8 sekunde ali 0,46 minute).

Slika 5: Poročanje ameriških kabelskih televizijskih postaj o OpenAI-ju



Vir podatkov: <https://tvnews.stanford.edu/>.

3.3 Rezultati primerjave povprečnega časa, v katerem je bila na zaslonu navedena besedna zveza artificial intelligence

Tabela 1 kaže razlike v opisnih statistikah za čas, v katerem je bila na zaslonu navedena besedna zveza artificial intelligence, in sicer pred uvedbo ChatGPT-ja in po njej. Podatki kažejo, da je desničarska kabelska televizijska postaja pred uvedbo ChatGPT-ja o umetni inteligenci v povprečju poročala za 10,85 sekunde več kot levičarska, po uvedbi ChatGPT-ja pa za 117,81 sekunde več kot levičarska. Iz tabele 1 je razvidno tudi, da se je po uvedbi ChatGPT-ja čas poročanja o umetni inteligenci v primeru obeh kabelskih televizijskih postaj v povprečju povečal, kar smo pričakovali glede na aktualnost tematike.

Tabela 1: Opisne statistike

	Umetna inteligenca			
	Pred uvedbo ChatGPT-ja		Po uvedbi ChatGPT-ja	
	CNN	FOX	CNN	FOX
Povprečje	12,26	23,11	243,57	361,38
Minimum	0,00	0,00	14,00	10,00

Maksimum	73,57	127,53	650,01	1166,19
Standardni odklon	10,97	24,06	155,51	292,73
Koeficient variacije	89,48	104,13	63,84	81,00
Koeficient asimetrije	2,44	1,57	0,93	0,93
Koeficient sploščenosti	8,51	2,40	2,41	2,41

Vir podatkov: Lastni izračuni na osnovi podatkov Univerze Stanford.

4 Razprava

Ta prispevek omogoča vpogled v poročanje ameriških medijev o umetni inteligenci glede na njihovo politično usmeritev ter prikazovanje Bidna in Trumpa v ozadju. Rezultati raziskave kažejo, da je republikansko usmerjena medijska hiša v povprečju več poročala o umetni inteligenci kot demokratsko usmerjena, in sicer tudi če je bil v ozadju prikazan Biden, kar je verjetno posledica njene funkcije. Zanimivo bi bilo ugotoviti, ali prikazovanje demokratskega ali republikanskega politika (predsednika, ministra, kongresnika ...) v ozadju poročila vpliva na podton poročanja o umetni inteligenci, česar pa nam analizador, ki ga je razvila Univerza Stanford, ne omogoča.

Čeprav ima umetna inteligenca dolgo zgodovino, so začeli ameriški mediji o njej več poročati šele po uvedbi ChatGPT-ja, ki je prispeval k popularizaciji umetne inteligence med ljudmi. Izkazalo se je, da njeno uvajanje povzroča spremembe, ki v ljudeh vzbujajo strah in nezaupanje (Johnson & Verdicchio, 2017), zaradi česar je naloga medijev, da ju ne poglobljajo (Ouchchy, Coin & Dubljević, 2020). Pomembno je, da imajo mediji uravnotežen pristop k poročanju o umetni inteligenci, ki zajema tako pozitivne kot negativne vidike njenega razvoja.

5 Sklep

Namen tega prispevka ni bil samo analizirati poročanje ameriških kabelskih televizijskih postaj o umetni inteligenci, ampak tudi vzbuditi zanimanje študentov ekonomije, psihologije, sociologije in drugih ved za poročanje ameriških medijev o umetni inteligenci z namenom vzpostaviti kritičen odnos do nje. Izkazalo se je, da so potrebne dodatne raziskave, ki bi upoštevale tudi podton poročanja o umetni inteligenci.

Izkazalo se je, da se je po uvedbi ChatGPT-ja povečalo poročanje ameriških kabelskih televizijskih postaj o umetni inteligenci, pri čemer vodi FOX, ki velja za desničarsko kabelsko televizijsko hišo.

Slabost analizatorja, ki ga je razvila Univerza Stanford in ki ga uporabljamo v tem prispevku, je, da ne omogoča upoštevanja podtona poročanja, kar bi povečalo kakovost tega prispevka.

Viri

Beets, B., Newman, T. P., Howell, E. L., Bao, L., & Yang, S. (2023). Surveying public perceptions of artificial intelligence in health care in the United States: Systematic review. *Journal of Medical Internet Research*, 25, e40337. <https://doi.org/10.2196/40337>

Choung, H., David, P., & Ross, A. (2022). Trust in AI and its role in the acceptance of AI technologies. *International Journal of Human-Computer Interaction*, 39, 1727–1739. <https://doi.org/10.1080/10447318.2022.2050543>

Chuan, C. H., Tsai, W. H. S., & Cho, S. Y. (2019). Framing artificial intelligence in American newspapers. V Conitzer V., Hadfield G., Vallor S. (ur.), *The 2019 AAAI/ACM conference on AI, ethics, and society* (str. 339–344). ACM Digital Library. <https://doi.org/10.1145/3306618.3314285>

Jaakkola, M. (ur.) (2023). *Reporting on artificial intelligence: a handbook for journalism educators*. UNESCO. <https://doi.org/10.58338/HSMK8605>

Johnson, D. G. in Verdicchio, M. (2017). AI Anxiety. *Journal of the Association for Information Science and Technology*, 68(9), 2267–2270. <https://doi.org/10.1002/asi.23867>

Ouchchy, L., Coin, A. in Dubljević, V. (2020). AI in the headlines: the portrayal of the ethical issues of artificial intelligence in the media. *AI & Society*, 35, 927 – 936. <https://doi.org/10.1007/s00146-020-00965-5>

Yang, S., Krause, N. M., Bao, L., Calice, M. N., Newman, T. P., Scheufele, D. A., Xenos, M. A., & Brossard, D. (2023). In AI we trust: the interplay of media use, political ideology, and trust in shaping emerging AI attitudes. *Journalism & Mass Communication Quarterly*. <https://doi.org/10.1177/10776990231190868>

Uporaba YouTube za izobraževanje med študenti medicine

Dominik Škrinjar  

Univerza v Mariboru, Medicinska fakulteta
Maribor, Slovenija

Dr. Domen Malc 

Univerza v Mariboru, Ekonomsko-poslovna fakulteta
Maribor, Slovenija

Dr. Dejan Romih 

Univerza v Mariboru, Ekonomsko-poslovna fakulteta
Maribor, Slovenija

Povzetek: Znano je, da so na YouTube objavljeni videoposnetki, ki jih lahko študenti medicine uporabljajo za svoje izobraževanje. V tem prispevku nas zanima mnenje študentov medicine o uporabi YouTube za izobraževanje na področju svojega študija, pri čemer se omejujemo na študente Medicinske fakultete Univerze v Mariboru, ki smo jih v ta namen tudi anketirali. Izkazalo se je, da je lahko YouTube koristen učni pripomoček.

Ključne besede: anketa, izobraževanje, medicina, študent, YouTube

The use of YouTube for education among medical students

Dominik Škrinjar  

University of Maribor, Faculty of Medicine
Maribor, Slovenia

Domen Malc, PhD 

University of Maribor, Faculty of Economics and Business
Maribor, Slovenia

Dejan Romih, PhD 

University of Maribor, Faculty of Economics and Business
Maribor, Slovenia

Abstract: It is well known that videos published on YouTube can be used by medical students for their education. In this paper, we are interested in the opinions of medical students regarding the use of YouTube for educational purposes in their field of study, focusing specifically on students from the Faculty of Medicine at the University of Maribor, who were surveyed for this purpose. It has been found that YouTube can be a useful learning tool.

Keywords: survey, education, medicine, student, YouTube

1 Uvod

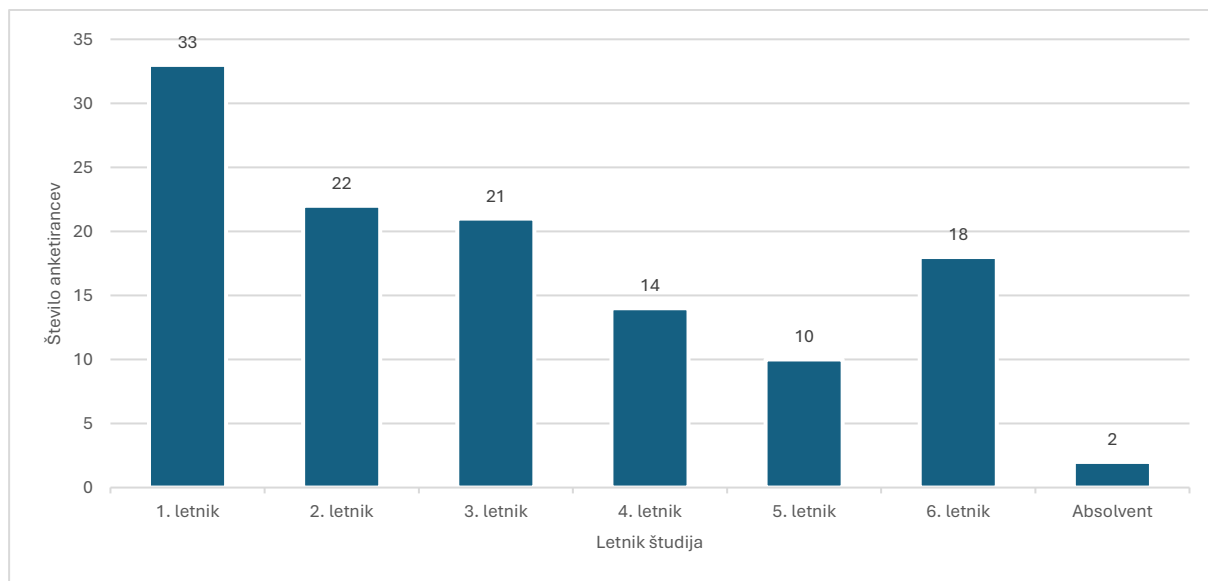
YouTube je podjetje, ki so ga februarja 2005 ustanovili Steven Chen, Chad Hurley in Jawed Karim ter ga oktobra 2006 prodali Googlu za 1,65 milijarde ameriških dolarjev. Je tudi platforma, ki je dostopna na <https://youtube.com/>. Na njej so objavljeni videoposnetki, ki jih lahko njeni uporabniki (npr. študenti) uporabljajo za (samo)izobraževanje. To velja tudi za študente medicine, ki se lahko s pomočjo YouTube (samo)izobražujejo na področju študija (Azer idr., 2022; Chai idr., 2024; Cousins idr., 2020; Curran idr., 2020; Drozd idr., 2018; Gorgy idr., 2022; Green idr., 2022; Gupta idr., 2016; Helming idr., 2021; Javidan idr., 2024; Johnson & Ellozy, 2024; Krumm idr., 2022; Madathil idr., 2015a, 2015b; Mageto, 2019; Narayan idr., 2024; Onder & Zengin, 2023; Rapp idr., 2016; Rouhi idr., 2023; Samuel idr., 2017; Sánchez idr., 2024; Sharpe idr., 2023; Uprak & Ergenç, 2022; Uslu idr., 2024; Ward idr., 2019; Yan & Davies, 2020). Namen raziskave je analizirati mnenje študentov medicine o uporabi YouTube za izobraževanje na področju študija in posledično zapolniti vrzel v literaturi, ki je nastala z uporabo te platforme (Curran idr., 2020; Helming idr., 2021; Javidan idr., 2024).

Izkušnje učijo, da je YouTube vir znanja. Tako nas ne preseneča, da imajo na YouTube svoj kanal tudi najboljše medicinske šole, kot je npr. Harvard Medical School, katere kanal je dostopen na <https://youtube.com/@harvardmedicalschoool>. Na njem so mdr. objavljeni tudi videoposnetki, ki so namenjeni (samo)izobraževanju študentov medicine, zdravnikov in zdravljenecv (Azer idr., 2022; Barahona-Correa idr., 2023; Green idr., 2022; Javidan idr., 2023, 2024; Martinez idr., 2023; Safa idr., 2023), kar kaže na pomen YouTube za (samo)izobraževanje.

2 Metode

Raziskava, katere rezultate podajamo v naslednjem poglavju, temelji na uporabi metode anketiranja. Anketo o uporabi YouTube za izobraževanje med študenti medicine (gl. prilogo 1) smo izvedli med 19. februarjem 2024 in 19. majem 2024 s pomočjo 1KA. Anketirali smo 120 študentov Medicinske fakultete Univerze v Mariboru, od tega 26 moških (22 %) in 93 žensk (78 %), kar pomeni, da v vzorcu prevladujejo ženske in da moramo to upoštevati pri interpretaciji rezultatov. Povprečna starost anketirancev je bila 21,7 leta, kar pomeni, da v vzorcu prevladujejo pripadniki generacije Z in da moramo tudi to upoštevati pri interpretaciji rezultatov.

Slika 1: Število anketirancev po letniku študija



Vir: Lastni izračuni.

3 Rezultati

V tem poglavju podajamo 1. rezultate analize mnenja študentov medicine o uporabi YouTubea za izobraževanje na področju študija ter 2. rezultate faktorske in regresijske analize.

3.1 Analiza mnenja študentov medicine o uporabi YouTubea

Odločili smo se, da bomo strinjanje s trditvami analizirali v dveh delih. V prvem delu bomo analizirali prvih 21 trditve, v drugem pa drugih 21 trditve. S tem želimo povečati preglednost rezultatov. Tabela 1 vsebuje trditve, ki so na vrhu lestvice, tabela 2 pa trditve, ki so na dnu lestvice. Študenti medicine so svoje strinjanje ali nestrinjanje s trditvami o YouTubeu ocenjevali z oceno od 1 (sploh se ne strinjam) do 7 (povsem se strinjam).

Tabela 1: Povprečje in mediana stopnje strinjanja s trditvami (1. del)

Trditve	Povprečje	Mediana
Za uporabljanje YouTubea ni potrebnega veliko denarja.	6,5	7,0
Izobraževalne vsebine na YouTubeu s področja medicine so poučne.	6,5	7,0
YouTube je enostaven za uporabljanje.	6,5	7,0

Izobraževalne vsebine na YouTubeu s področja medicine so zanimive.	6,4	6,0
Za uporabljanje YouTubea ni potrebnega veliko znanja.	6,3	7,0
Izobraževalne vsebine na YouTubeu s področja medicine so raznovrstne.	6,2	6,0
Izobraževalne vsebine na YouTubeu s področja medicine so dobre.	6,1	6,0
Izobraževalne vsebine na YouTubeu s področja medicine so jasno predstavljene.	6,1	6,0
Za uporabljanje YouTubea ni potrebnih veliko izkušenj.	6,1	6,0
Izobraževalne vsebine na YouTubeu s področja medicine so razumljive.	6,0	6,0
Izobraževalne vsebine na YouTubeu s področja medicine so jasno podane.	5,9	6,0
Uporabljanje YouTubea za izobraževanje na področju medicine povečuje učinkovitost mojega izobraževanja.	5,8	6,0
Priporočam, da tudi drugi študenti medicine uporabljajo YouTube za izobraževanje na tem področju.	5,8	6,0
Izobraževalne vsebine na YouTubeu s področja medicine so koristne za opravljanje izpitov iz predkliničnih predmetov.	5,7	6,0
Uporabljanje YouTubea za izobraževanje na področju medicine povečuje uspešnost mojega izobraževanja.	5,6	6,0
Izobraževalne vsebine na YouTubeu s področja medicine so jasno opredeljene.	5,6	6,0
Izobraževalne vsebine na YouTubeu s področja medicine so usklajene z mojimi potrebami.	5,5	6,0
YouTube je primeren za izobraževanje na področju medicine.	5,5	5,5
Izobraževalne vsebine na YouTubeu s področja medicine so resnične.	5,5	6,0
Izobraževalne vsebine na YouTubeu s področja medicine so usklajene z mojimi pričakovanji.	5,5	6,0
Izobraževalne vsebine na YouTubeu s področja medicine so točne.	5,5	5,0

Vir podatkov: Lastni izračuni.

Iz tabele 1 je razvidno, da se anketiranci popolnoma strinjajo s trditvami »Za uporabljanje YouTubea ni potrebnega veliko denarja.«, »Izobraževalne vsebine na YouTubeu s področja medicine so poučne.« in »YouTube je enostaven za uporabljanje.« Tudi sicer je iz tabele 1 razvidno, da se študenti medicine, ki smo jih anketirali, strinjajo, da so izobraževalne vsebine na YouTubeu s področja medicine dobre, poučne, raznovrstne in zanimive, pa tudi resnične in točne.

Tabela 2: Povprečje in mediana (stopnje) strinjanja s trditvami (2. del)

Trditev	Povprečje	Mediana
Uporabljanje YouTubea za izobraževanje na področju medicine povečuje moje veselje do izobraževanja.	5,5	6,0
YouTube mi omogoča vpogled v tujo prakso na področju medicine.	5,4	6,0
Izobraževalne vsebine na YouTubeu s področja medicine so usklajene z mojimi zahtevami.	5,3	5,0

Izobraževalne vsebine na YouTubeu uporabljam za pripravlanje na izpite iz medicine.	5,3	5,5
Izobraževalne vsebine na YouTubeu uporabljam za pridobivanje osnovnega znanja s področja medicine.	5,2	6,0
Izobraževalne vsebine na YouTubeu s področja medicine so zaupanja vredne.	5,2	5,0
YouTube je pomemben vir izobraževalnih vsebin s področja medicine.	5,2	5,0
YouTube mi omogoča izobraževanje na področju medicine.	5,1	6,0
Uporabljanje YouTubea za izobraževanje na področju medicine mi prihrani čas.	5,0	5,0
Izobraževalne vsebine na YouTubeu s področja medicine so koristne za opravljanje izpitov iz kliničnih predmetov.	5,0	5,0
YouTube je pomemben vir znanja na področju medicine.	4,9	5,0
Uporabljanje YouTubea za izobraževanje na področju medicine mi prihrani delo.	4,9	5,0
YouTube je pomemben vir informacij na področju medicine.	4,8	5,0
Izobraževalne vsebine na YouTubeu uporabljam za pridobivanje naprednega znanja s področja medicine.	4,7	5,0
Predlagam, da se izobraževalne vsebine na YouTubeu s področja medicine vključijo v izobraževalni proces na fakulteti.	4,6	5,0
Uporabljanje YouTubea za izobraževanje na področju medicine mi prihrani skrbi.	4,3	4,0
YouTube je pomemben vir izkušenj na področju medicine.	4,1	4,0
Uporabljanje YouTubea za izobraževanje na področju medicine mi prihrani denar.	4,0	4,0
YouTube mi omogoča vpogled v domačo prakso na področju medicine.	3,0	3,0
Izobraževalne vsebine na YouTubeu uporabljam za pridobivanje osnovnega znanja s področja umetne inteligence v medicini.	2,8	2,0
Izobraževalne vsebine na YouTubeu uporabljam za pridobivanje naprednega znanja s področja umetne inteligence v medicini.	2,7	2,0

Vir: Lastni izračuni.

Iz tabel 1 in 2 izhaja, da študenti medicine, ki smo jih anketirali, večinoma pozitivno ocenjujejo uporabo YouTubea za (samo)izobraževanje na področju študija, kar je koristna informacija za visokošolske učitelje in sodelavce na Medicinski fakulteti Univerze v Mariboru, pa tudi druge, ki sodelujejo pri izobraževanju študentov medicine.

3.2 Faktorska in regresijska analiza

Po pregledu povprečnih vrednosti posameznih trditev smo izvedli eksplorativno faktorsko analizo z uporabo metode glavnih komponent. Z izračunom KMO-statistike ($KMO = 0,827$) in uporabo

Bartlettovega testa sferičnosti ($p < 0,001$) smo pokazali, da sta izpolnjena ključna pogoja za izvedbo faktorске analize.

Z eksplorativno faktorско analizo smo identificirali skupno šest komponent, ki skupaj pojasnijo 71,77 % skupne variance. Rezultate prikazujemo v tabeli 3.

Tabela 3: Rezultati eksplorativne faktorске analize (faktorске uteži in Cronbach α koeficienti)

Komponenta	Trditev	λ	α
1	Uporabljanje YouTube za izobraževanje na področju medicine povečuje učinkovitost mojega izobraževanja.	0,857	0,902
	Uporabljanje YouTube za izobraževanje na področju medicine povečuje uspešnost mojega izobraževanja.	0,831	
	Uporabljanje YouTube za izobraževanje na področju medicine povečuje moje veselje do izobraževanja.	0,747	
	Uporabljanje YouTube za izobraževanje na področju medicine mi prihrani čas.	0,711	
	Uporabljanje YouTube za izobraževanje na področju medicine mi prihrani delo.	0,696	
	Uporabljanje YouTube za izobraževanje na področju medicine mi prihrani denar.	0,689	
	Uporabljanje YouTube za izobraževanje na področju medicine mi prihrani skrbi.	0,654	
	Izobraževalne vsebine na YouTube uporabljam za pripravljane na izpite iz medicine.	0,653	
2	Izobraževalne vsebine na YouTube s področja medicine so jasno opredeljene.	0,863	0,910
	Izobraževalne vsebine na YouTube s področja medicine so jasno podane.	0,801	
	Izobraževalne vsebine na YouTube s področja medicine so jasno predstavljene.	0,762	
	Izobraževalne vsebine na YouTube s področja medicine so razumljive.	0,760	
	Izobraževalne vsebine na YouTube s področja medicine so resnične.	0,720	
	Izobraževalne vsebine na YouTube s področja medicine so točne.	0,690	
	Izobraževalne vsebine na YouTube s področja medicine so zaupanja vredne.	0,638	
3	YouTube je enostaven za uporabljanje.	0,833	0,799
	Za uporabljanje YouTube ni potrebnega veliko znanja.	0,800	
	Za uporabljanje YouTube ni potrebnih veliko izkušenj.	0,759	
	Za uporabljanje YouTube ni potrebnega veliko denarja.	0,711	
4	YouTube je pomemben vir izobraževalnih vsebin s področja medicine.	0,856	0,824
	YouTube je pomemben vir znanja na področju medicine.	0,714	
	YouTube mi omogoča vpogled v tujo prakso na področju medicine.	0,672	

	Izobraževalne vsebine na YouTubeu s področja medicine so koristne za opravljanje izpitov iz kliničnih predmetov.	0,619	
5	Izobraževalne vsebine na YouTubeu s področja medicine so usklajene z mojimi potrebami.	0,751	0,911
	Izobraževalne vsebine na YouTubeu s področja medicine so usklajene z mojimi pričakovanji.	0,733	
	Izobraževalne vsebine na YouTubeu s področja medicine so usklajene z mojimi zahtevami.	0,726	
6	Izobraževalne vsebine na YouTubeu uporabljam za pridobivanje osnovnega znanja s področja umetne inteligence v medicini.	0,940	0,914
	Izobraževalne vsebine na YouTubeu uporabljam za pridobivanje naprednega znanja s področja umetne inteligence v medicini.	0,914	

Opombe. 1 – Koristnost uporabe YouTubea; 2 – Kakovost izobraževalnih vsebin na YouTubeu; 3 – Enostavnost uporabe YouTubea; 4 – Uporabnost izobraževalnih vsebin na YouTubeu; 5 – Zadovoljstvo z YouTubeom kot izobraževalno platformo; 6 – Uporabnost UI izobraževalnih vsebin na YouTubeu.

Iz tabele 3 lahko razberemo šest unikatnih komponent: koristnost uporabe YouTubea (8 indikatorjev), kakovost izobraževalnih vsebin na YouTubeu (7 indikatorjev), enostavnost uporabe YouTubea (4 indikatorji), uporabnost izobraževalnih vsebin na YouTubeu (4 indikatorji), zadovoljstvo z YouTubeom kot izobraževalno platformo (3 indikatorji) in uporabnost UI izobraževalnih vsebin na YouTubeu (2 indikatorja). Vrednosti factorskih uteži za končni nabor trditev so v vseh primerih večje od 0,6, kar nakazuje močno povezanost med posameznimi faktorji in pripadajočimi indikatorji. Visoke vrednosti Cronbach α koeficientov ($\alpha > 0,7$) pa kažejo na visoko zanesljivost merjenja.

Pred izvedbo multiple regresijske analize smo želeli preveriti še naravo povezav med oblikovanimi komponentami. V ta namen v tabeli 4 predstavljamo rezultate korelacijske analize, ki jim pridružujemo še povprečne vrednosti komponent in pripadajoče vrednosti standardnih odklonov.

Tabela 4: Rezultati korelacijske analize, povprečne vrednosti in vrednosti standardnih odklonov

	1	2	3	4	5	6	M	SD
1	1						5,05	1,24
2	0,419**	1					5,67	0,78
3	0,117	0,324**	1				6,33	0,84
4	0,501**	0,476**	0,158	1			5,12	1,07
5	0,456**	0,653**	0,321**	0,464**	1		5,45	0,99

6	0,147	-0,011	-0,145	-0,015	0,048	1	2,77	1,59
---	-------	--------	--------	--------	-------	---	------	------

Opombe: 1 – Koristnost uporabe YouTube; 2 – Kakovost izobraževalnih vsebin na YouTube; 3 – Enostavnost uporabe YouTube; 4 – Uporabnost izobraževalnih vsebin na YouTube; 5 – Zadovoljstvo z YouTube kot izobraževalno platformo; 6 – Uporabnost UI izobraževalnih vsebin na YouTube. ** $p < 0,01$

Študenti medicine, ki so sodelovali v raziskavi, v povprečju ocenjujejo YouTube kot platformo, ki je enostavna za uporabo ($M = 6,33$; $SD = 0,84$), hkrati pa menijo, da so izobraževalne vsebine, dostopne na YouTube, kakovostne ($M = 5,67$; $SD = 0,78$). Kot razmeroma visoko ocenjujejo tudi zadovoljstvo z YouTube kot izobraževalno platformo ($M = 5,45$; $SD = 0,99$), nekoliko nižje ocene pa zasledimo pri ocenjevanju uporabnosti izobraževalnih vsebin ($M = 5,12$; $SD = 1,07$) in koristnosti YouTube ($M = 5,05$; $SD = 1,24$). Po drugi strani pa sodelujoči študenti medicine YouTube ne uporabljajo za pridobivanje znanj s področja umetne inteligence v medicini ($M = 2,77$; $SD = 1,59$), četrto tudi smo pri tej komponenti zabeležili največjo vrednost standardnega odklona, kar kaže na večjo razpršenost odgovorov kot v primeru preostalih komponent.

Pregled povezav med našimi komponentami pa razkriva naslednje: zadovoljstvo z YouTube kot izobraževalno platformo se statistično značilno ($p < 0,01$) povezuje z vsemi komponentami, razen s komponento 6 (uporabnost UI izobraževalnih vsebin na YouTube). Prav komponenta 6 je tudi edina, ki ni povezana z vsaj eno od preostalih komponent, zaradi česar smo jo iz nadaljnje analize izločili.

Za konec smo z uporabo multiple regresijske analize preverili še naše hipoteze, ki se glasijo:

- Koristnost uporabe YouTube pozitivno vpliva na zadovoljstvo študentov medicine z YouTube kot izobraževalno platformo.
- Kakovost izobraževalnih vsebin na YouTube pozitivno vpliva na zadovoljstvo študentov medicine z YouTube kot izobraževalno platformo.
- Enostavnost uporabe YouTube pozitivno vpliva na zadovoljstvo študentov medicine z YouTube kot izobraževalno platformo.
- Uporabnost izobraževalnih vsebin na YouTube pozitivno vpliva na zadovoljstvo študentov medicine z YouTube kot izobraževalno platformo.

Predhodno testiranje zbranih podatkov je pokazalo, da v modelu ni težav z avtokorelacijo med reziduali (Durbin-Watson = 2,248), vrednosti variantnega inflacijskega faktorja (VIF) pa v nobenem

od primerov niso presegale kritične vrednosti $VIF = 5$, s čimer smo izključili možnost multikolinearnosti.

Splošni rezultati multiple linearne regresije kažejo, da se model zadovoljivo prilega podatkom ($F = 27,868$; $p < 0,001$), z njim pa lahko pojasnimo 49 % zadovoljstva študentov medicine z YouTubom kot izobraževalno platformo ($R^2 = 0,492$). Doprinosi posameznih neodvisnih spremenljivk prikazujemo v tabeli 5.

Tabela 5: Rezultati multiple regresijske analize dejavnikov zadovoljstva z YouTubom kot izobraževalno platformo

Model 1	B	S.E.	β	t	p	95 % CI
Konstanta	-0,234	0,613	-	-0,382	0,704	[-1,448; 0,980]
Koristnost	0,141	0,063	0,177	2,242	0,027	[0,016; 0,266]
Kakovost vsebin	0,604	0,103	0,478	5,887	0,000	[0,401; 0,807]
Enostavnost	0,148	0,083	0,125	1,785	0,077	[-0,016; 0,313]
Uporabnost vsebin	0,118	0,076	0,128	1,563	0,121	[-0,032; 0,269]

Vir: Lastni izračuni.

Na podlagi rezultatov multiple regresijske analize, prikazanih v tabeli 5, lahko sklenemo, da je najpomembnejši dejavnik zadovoljstva z YouTubom kot izobraževalno platformo med študenti medicine kakovost objavljenih vsebin ($\beta = 0,478$; $p < 0,001$). Statistično značilni vpliv smo zabeležili še pri dejavniku koristnost ($\beta = 0,177$; $p < 0,05$), medtem ko se enostavnost uporabe in uporabnost vsebin nista izkazali za statistično značilna dejavnika zadovoljstva z YouTubom kot izobraževalno platformo ($p > 0,05$).

4 Razprava

Izkazalo se je, da študenti splošne medicine pogosto uporabljajo YouTube za samostojno izobraževanje na področju študija. Anketiranci se večinoma strinjajo, da uporaba YouTube ne zahteva veliko denarja, da je platforma enostavna za uporabo in da ne zahteva veliko predznanja ali izkušenj (prim. Azer idr., 2022; Chai idr., 2024; Cousins idr., 2020; Curran idr., 2020; Drozd idr., 2018; Gorgy idr., 2022; Green idr., 2022; Gupta idr., 2016; Helming idr., 2021; Javidan idr., 2024; Johnson & Ellozy, 2024; Krumm idr., 2022; Madathil idr., 2015a, 2015b; Mageto, 2019; Narayan idr., 2024;

Onder & Zengin, 2023; Rapp idr., 2016; Rouhi idr., 2023; Samuel idr., 2017; Sánchez idr., 2024; Sharpe idr., 2023; Uprak & Ergenç, 2022; Uslu idr., 2024; Ward idr., 2019; Yan & Davies, 2020). Prav tako se je večina študentov strinjala, da so izobraževalne vsebine s področja medicine poučne, zanimive, raznovrstne, jasno predstavljene in razumljive.

Zanimivo pa je, da se anketiranci večinoma ne strinjajo s trditvijo, da jim YouTube omogoča pridobivanje novega znanja o uporabi umetne inteligence v medicini. To je presenetljivo, saj je na YouTubu veliko videoposnetkov o tej temi, kar bi lahko vodilo do drugačnih rezultatov, zlasti glede na aktualnost tematike. Prav tako se večina anketirancev ni strinjala s trditvami, da jim YouTube omogoča vpogled v domačo prakso na področju medicine in da predstavlja pomemben vir izkušenj na tem področju. To bi lahko pojasnili z dejstvom, da je večina medicinskih vsebin pripravljena v skladu z anglosaško in ameriško medicinsko prakso, medtem ko strokovnih medicinskih video vsebin v slovenščini na YouTubu skorajda ni.

Pomembno je tudi poudariti, da so večji del anketirancev predstavljali študenti nižjih letnikov (1.–3. letnik), ki se v prvih dveh letih študija splošne medicine srečujejo predvsem s predkliničnimi vsebinami. Uporabnost YouTubovih video vsebin s področja klinične medicine je zato zanje manjša oziroma celo nerazumljiva. Med študijem v višjih letnikih (4.–6. letnik) pa, zaradi srečevanja s kliničnimi vsebinami in zaradi akumulacije ter povezovanja znanja predkliničnih in kliničnih veščin, YouTubove video vsebine pridobivajo na vrednosti, uporabnosti in koristnosti kot učni pripomoček. Med šestimi leti študija splošne medicine študenti namreč pridejo v stik z bolniki in kliničnim okoljem, kar zahteva aktivno participacijo, pridobivanje in implementacijo kliničnih veščin ter povezovanje s predhodno pridobljenim teoretičnim znanjem, pri čemer lahko YouTubove video vsebine igrajo ključno vlogo.

5 Sklep

Rezultati raziskave, ki smo jo izvedli, jasno kažejo, da je YouTube dober pripomoček za (samo)izobraževanje študentov (splošne) medicine na področju študija, kar smo pričakovali glede na rezultate drugih raziskav. To pomeni, da obstaja potreba po kakovostnih videoposnetkih na področju medicine, zlasti v slovenskem jeziku, ki bi lahko študentom Medicinske fakultete Univerze v Mariboru, pa tudi bolnikom, služili kot osnova za (samo)izobraževanje na določenem področju. Poleg tega bi lahko videoposnetki bolnikom služili tudi za nazoren prikaz poteka njihove bolezni, zdravljenja, operacije itd., zato menimo, da bi bilo smiselno anketo prilagoditi in jo izvesti tudi na vzorcu

bolnikov. Izkazalo se je, da obstaja na tem področju vrzel v literaturi, ki bi jo bilo treba zapolniti, zaradi česar predlagamo, da avtorji nadaljnjih raziskav analizirajo tudi mnenja bolnikov o uporabi YouTube za izobraževanje na področju njihove bolezni.

Na osnovi tega lahko sklepamo, da obstaja potreba po kakovostnih videoposnetkih v slovenskem jeziku, ki bi bili namenjeni slovensko govorečim študentom medicine, pa tudi slovensko govorečim zdravnikom in zdravljenecem. Poleg tega bi morali biti strokovno pregledani s strani strokovnjakov na področju medicine in dostopni tudi na drugih platformah, ne samo YouTube. To velja tudi za podkaste s področja medicine, ki so lahko tudi vir znanja.

Viri

Azer, S. A., AlKhawajah, N. M., & Alshamlan, Y. A. (2022). Critical evaluation of YouTube videos on colostomy and ileostomy: Can these videos be used as learning resources? *Patient Education and Counseling*, 105(2), 383–389. <https://doi.org/10.1016/J.PEC.2021.05.023>

Barahona-Correa, J. E., Rueda-Ortiz, C., Muñoz, O., García, Á. A., & Fernández-Ávila, D. G. (2023). YouTube® as a source of information for Spanish-speaking patients with rheumatoid arthritis. *Reumatología Clínica (English Edition)*, 19(10), 571–578. <https://doi.org/10.1016/J.REUMAE.2023.05.006>

Chai, B. S., Chae, T., & Huang, A. L. (2024). Evaluation of educational youtube videos for distal radius fracture treatment. *Journal of Hand Surgery Global Online*, 6(3), 382–387. <https://doi.org/10.1016/J.JHSG.2024.02.009>

Cousins, L., Davison, G. W., & O'Donnell, M. E. (2020). Social media and online surgical education: A content analysis and descriptive study on quality of vascular surgery information available on YouTube®. *European Journal of Vascular and Endovascular Surgery*, 60(2), e60. <https://doi.org/10.1016/J.EJVS.2020.03.036>

Curran, V., Simmons, K., Matthews, L., Fleet, L., Gustafson, D. L., Fairbridge, N. A., & Xu, X. (2020). YouTube as an educational resource in medical education: A scoping review. *Medical Science Educator*, 30(4), 1775–1782. <https://doi.org/10.1007/S40670-020-01016-W>

Drozd, B., Couvillon, E., & Suarez, A. (2018). Medical YouTube videos and methods of evaluation: Literature review. *JMIR Medical Education*, 20(2). <https://doi.org/10.2196/mededu.8527>

Gorgy, A., Hawary, H. El, Galli, R., MacDonald, M., Barone, N., & Thibaudeau, S. (2022). Evaluating the educational quality of surgical YouTube® videos: A systematic review. *Health Sciences Review*, 5, 100067. <https://doi.org/10.1016/J.HSR.2022.100067>

Green, L., Noll, D., Barbaro, A., Asokan, G., Hewitt, J., Ovenden, C., Kanhere, H., & Trochsler, M. (2022). YouTube—friend or foe? A closer look at videos on inguinal hernia surgery as a source for patient education. *Journal of Surgical Research*, 280, 510–514. <https://doi.org/10.1016/J.JSS.2022.07.024>

- Gupta, H. V., Lee, R. W., Raina, S. K., Behrle, B. L., Hinduja, A., & Mittal, M. K. (2016). Analysis of youtube as a source of information for peripheral neuropathy. *Muscle and Nerve*, 53(1), 27–31. <https://doi.org/10.1002/MUS.24916>
- Helming, A. G., Adler, D. S., Keltner, C., Igelman, A. D., & Woodworth, G. E. (2021). The content quality of youtube videos for professional medical education: A systematic review. *Academic Medicine*, 96(10), 1484–1493. <https://doi.org/10.1097/ACM.0000000000004121>
- Javidan, A., Nelms, M. W., Li, A., Lee, Y., Zhou, F., Kayssi, A., & Naji, F. (2023). Evaluating YouTube as a source of education for patients undergoing surgery: A systematic review. *Annals of Surgery*, 278(4), E712–E718. <https://doi.org/10.1097/SLA.0000000000005892>
- Javidan, A., Vignarajah, M., Nelms, M. W., Zhou, F., Lee, Y., Naji, F., & Kayssi, A. (2024). YouTube as a source of patient and trainee education in vascular surgery: A systematic review. *EJVES Vascular Forum*, 61, 62–76. <https://doi.org/10.1016/J.EJVSF.2024.01.054>
- Johnson, A., & Ellozy, S. (2024). The utilization of podcasts and other free open access medical education resources in vascular surgery. *JVS-Vascular Insights*, 100091. <https://doi.org/10.1016/J.JVSVI.2024.100091>
- Krumm, I. R., Miles, M. C., Clay, A., Carlos, W. G., & Adamson, R. (2022). Making effective educational videos for clinical teaching. *Chest*, 161(3), 764–772. <https://doi.org/10.1016/j.chest.2021.09.015>
- Madathil, K. C., Rivera-Rodriguez, A. J., Greenstein, J. S., & Gramopadhye, A. K. (2015a). Healthcare information on YouTube: A systematic review. *Health Informatics Journal*, 21(3), 173–194. <https://doi.org/10.1177/1460458213512220>
- Madathil, K. C., Rivera-Rodriguez, A. J., Greenstein, J. S., & Gramopadhye, A. K. (2015b). Healthcare information on YouTube: A systematic review. *Health Informatics Journal*, 21(3), 173–194. <https://doi.org/10.1177/1460458213512220>
- Mageto, Y. (2019). The increasing use of social media for medical information: Should healthcare providers be concerned? *Annals of the American Thoracic Society*, 16(5), 544–546. <https://doi.org/10.1513/AnnalsATS.201902-125ED>
- Martinez, V. H., Ojo, D., Gutierrez-Naranjo, J. M., Proffitt, M., & Hartzler, R. U. (2023). The most popular youtube videos about shoulder replacement are of poor quality for patient education. *Arthroscopy, Sports Medicine, and Rehabilitation*, 5(3), e623–e628. <https://doi.org/10.1016/J.ASMR.2023.03.001>
- Narayan, R. R., Kadri, H., Muhammad, H. A., & Qadan, M. (2024). Critical appraisal of content quality of YouTube Videos on the whipple pancreaticoduodenectomy. *Journal of Surgical Research*, 295, 690–698. <https://doi.org/10.1016/J.JSS.2023.11.066>
- Onder, M. E., & Zengin, O. (2023). Quality of healthcare information on YouTube: psoriatic arthritis. *Zeitschrift Fur Rheumatologie*, 82, 30–37. <https://doi.org/10.1007/s00393-021-01069-1>
- Rapp, A. K., Healy, M. G., Charlton, M. E., Keith, J. N., Rosenbaum, M. E., & Kapadia, M. R. (2016). YouTube is the most frequently used educational video source for surgical preparation. *Journal of Surgical Education*, 73(6), 1072–1076. <https://doi.org/10.1016/j.jsurg.2016.04.024>

- Rouhi, A. D., Roberson, J. L., Kindall, E., Ghanem, Y. K., Yi, W. S., Williams, N. N., & Dumon, K. R. (2023). Assessment of YouTube as an online educational tool in teaching laparoscopic Roux-en-Y gastric bypass: A LAP-VEGaS study. *Surgery in Practice and Science*, *14*, 100199. <https://doi.org/10.1016/J.SIPAS.2023.100199>
- Safa, A., De Biase, G., Gassie, K., Garcia, D., Abode-Iyamah, K., & Chen, S. G. (2023). Reliability of YouTube videos on robotic spine surgery for patient education. *Journal of Clinical Neuroscience*, *109*, 6–10. <https://doi.org/10.1016/J.JOCN.2022.12.014>
- Samuel, N., Alotaibi, N. M., & Lozano, A. M. (2017). YouTube as a source of information on neurosurgery. *World Neurosurgery*, *105*, 394–398. <https://doi.org/10.1016/j.wneu.2017.05.111>
- Sánchez, A., Rodríguez, O., Medina, M., Vegas, L., Couto, F., Mogollon, I., Inchausti, C., & Galvis, L. (2024). Is YouTube a reliable tool for approaching robotic assisted transabdominal preperitoneal surgery? A critical review of the available resources. *Cirugía Española (English Edition)*, *102*(4), 188–193. <https://doi.org/10.1016/J.CIRENG.2023.08.007>
- Sharpe, M. G., Crosby, D. R., Creary, J., Badrinathan, A., Kishawi, S. K., & Ho, V. P. (2023). Digital learning: The reach of podcasts and YouTube on trauma surgery education. *Surgery*, *174*(3), 535–541. <https://doi.org/10.1016/J.SURG.2023.05.012>
- Uprak, T. K., & Ergenç, M. (2022). Assessment of esophagectomy videos on YouTube: Is peer review necessary for quality? *Journal of Surgical Research*, *279*, 368–373. <https://doi.org/10.1016/J.JSS.2022.06.037>
- Uslu, E., Kendirkiran, G., & Yildirim, N. (2024). YouTube videos are a moderately comprehensive, reliable, and quality option to learn about “multiple sclerosis and sexuality.” *International Journal of Sexual Health*. <https://doi.org/10.1080/19317611.2024.2349597>
- Ward, M., Ward, B., Abraham, M., Nicheporuck, A., Elkattawy, O., Herschman, Y., Mammis, A., Liu, J. K., & Paskhover, B. (2019). The educational quality of neurosurgical resources on YouTube. *World Neurosurgery*, *130*, e660–e665. <https://doi.org/10.1016/j.wneu.2019.06.184>
- Yan, Q., & Davies, M. G. (2020). Quality of carotid endarterectomy videos on YouTube: viewer be aware. *Journal of the American College of Surgeons*, *231*(4), S355. <https://doi.org/10.1016/J.JAMCOLLSURG.2020.07.719>

Priloga: Anketni vprašalnik

Anketa o YouTubu kot digitalni izobraževalni platformi za študente medicine

Q1 - Spol

- Moški
- Ženski
- Drugo

Q2 - Starost v letih _____

Q3 - Letnik študija

- 1
- 2
- 3
- 4
- 5
- 6
- Absolvent

Q4 - Ocenite svoje strinjanje ali nestrinjanje s trditvami o YouTubu.

	Sploh se ne strinjam	Se ne strinjam	Delno se ne strinjam	Niti niti	Delno se strinjam	Se strinjam	Povsem se strinjam
Izobraževalne vsebine na YouTubu s področja medicine so dobre.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Izobraževalne vsebine na YouTubu s področja medicine so jasno opredeljene.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Izobraževalne vsebine na YouTubu s področja	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

medicine so jasno podane.							
Izobraževalne vsebine na YouTubeu s področja medicine so jasno predstavljene.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Izobraževalne vsebine na YouTubeu s področja medicine so poučne.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Izobraževalne vsebine na YouTubeu s področja medicine so raznovrstne.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Izobraževalne vsebine na YouTubeu s področja medicine so razumljive.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Izobraževalne vsebine na YouTubeu s področja medicine so resnične.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Izobraževalne vsebine na YouTubeu s področja medicine so točne.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Izobraževalne vsebine na YouTubeu s področja medicine so usklajene z mojimi potrebami.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Izobraževalne vsebine na YouTubeu s	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

področja medicine so usklajene z mojimi pričakovanji.							
Izobraževalne vsebine na YouTubeu s področja medicine so usklajene z mojimi zahtevami.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Izobraževalne vsebine na YouTubeu s področja medicine so zanimive.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Izobraževalne vsebine na YouTubeu s področja medicine so zaupanja vredne.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Uporabljanje YouTubea za izobraževanje na področju medicine povečuje učinkovitost mojega izobraževanja.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Uporabljanje YouTubea za izobraževanje na področju medicine povečuje uspešnost mojega izobraževanja.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Uporabljanje YouTubea za izobraževanje na področju medicine povečuje moje	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

veselje do izobraževanja.							
Uporabljanje YouTube za izobraževanje na področju medicine mi prihrani čas.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Uporabljanje YouTube za izobraževanje na področju medicine mi prihrani delo.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Uporabljanje YouTube za izobraževanje na področju medicine mi prihrani denar.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Uporabljanje YouTube za izobraževanje na področju medicine mi prihrani skrbi.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
YouTube je enostaven za uporabljanje.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Za uporabljanje YouTube ni potrebno veliko znanja.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Za uporabljanje YouTube ni potrebno veliko izkušenj.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Za uporabljanje YouTube ni potrebno veliko denarja.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
YouTube je primeren za izobraževanje na področju medicine.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

YouTube je pomemben vir informacij na področju medicine.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
YouTube je pomemben vir izobraževalnih vsebin s področja medicine.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
YouTube je pomemben vir znanja na področju medicine.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
YouTube je pomemben vir izkušenj na področju medicine.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
YouTube mi omogoča izobraževanje na področju medicine.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
YouTube mi omogoča vpogled v domačo prakso na področju medicine.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
YouTube mi omogoča vpogled v tujo prakso na področju medicine.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Izobraževalne vsebine na YouTubeu uporabljam za pridobivanje osnovnega znanja s področja medicine.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Izobraževalne vsebine na YouTubeu uporabljam za pridobivanje naprednega znanja s področja medicine.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Izobraževalne vsebine na YouTubeu uporabljam za pridobivanje osnovnega znanja s področja umetne inteligence v medicini.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Izobraževalne vsebine na YouTubeu uporabljam za pridobivanje naprednega znanja s področja umetne inteligence v medicini.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Izobraževalne vsebine na YouTubeu uporabljam za pripravljane na izpite iz medicine.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Izobraževalne vsebine na YouTubeu s področja medicine so koristne za opravljanje izpitov iz predkliničnih predmetov.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Izobraževalne vsebine na YouTubeu s	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

področja medicine so koristne za opravljanje izpitov iz kliničnih predmetov.							
Priporočam, da tudi drugi študenti medicine uporabljajo YouTube za izobraževanje na tem področju.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Predlagam, da se izobraževalne vsebine na YouTube s področja medicine vključijo v izobraževalni proces na fakulteti.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Katere so vodilne sile na področju umetne inteligence po poročanju ameriških kabelskih televizijskih postaj

Timotej Peter Valcl 

Univerza v Mariboru, Ekonomsko-poslovna fakulteta
Maribor, Slovenija

Dr. Dejan Romih 

Univerza v Mariboru, Ekonomsko-poslovna fakulteta
Maribor, Slovenija

Povzetek: V tem prispevku raziskujemo vprašanje, kdo so vodilne sile na področju umetne inteligence. Analiza kabelskih novic kaže, da so vodilna sila na tem področju Združene države Amerike, ki jim sledita Kitajska in Tajvan na drugem oz. tretjem mestu. Spremljanje kabelskih novic o umetni inteligenci je pomembno, ker omogoča vpogled v stanje na tem področju, kar je lahko koristno za raziskovalce in oblikovalce politike.

Ključne besede: kabelska novica, kabelska televizija, umetna inteligenca, Združene države Amerike

Who are the leading forces in the field of artificial intelligence according to US cable TV channels?

Timotej Peter Valcl 

University of Maribor, Faculty of Economics and Business
Maribor, Slovenia

Dejan Romih, PhD 

University of Maribor, Faculty of Economics and Business
Maribor, Slovenia

Abstract: In this paper, we explore the question of who the leading forces are in the field of artificial intelligence. An analysis of cable news shows that the leading power in this field is the United States, followed by China and Taiwan in second and third place, respectively. Monitoring cable TV news about artificial intelligence is important because it gives an insight into the state of play in the field, which can be useful for researchers and policy makers.

Keywords: cable news, cable TV, artificial intelligence, United States

1 Uvod

Izkušnje učijo, da se v zadnjem času, zlasti po uvedbi ChatGPT-ja, veliko govori in piše o umetni inteligenci ter njenem vplivu na družbo kot celoto. Izkazalo se je, da se umetna inteligenca uporablja na različnih področjih: v gospodarstvu, šolstvu, zdravstvu, znanosti (Ahmed, Wahed & Thompson, 2023). V tem prispevku analiziramo poročanje ameriških televizijskih hiš o umetni inteligenci, pri čemer nas zanima, katere države (sile) ob tem televizijski novinarji najpogosteje omenjajo. Glede na to, da se omejujemo na ameriške televizijske hiše, lahko upravičeno pričakujemo, da so na seznamu Združene države Amerike (ZDA), o katerih se tudi sicer veliko govori in piše, kar nas ne preseneča glede na njihov vodilni položaj v svetu, tudi kar se tiče umetne inteligence, za kar so zaslužna različna ameriška podjetja, kot so npr. Alphabet, IBM, Intel, Microsoft, Nvidia.

Namen tega prispevka je zapolniti vrzel v literaturi, ki je nastala z uvedbo ChatGPT-ja. Ta namreč predstavlja veliko prelomnico v razvoju umetne inteligence, kar je razvidno tudi iz literature. Dejstvo je, da so po novembru 2022 strokovnjaki na različnih področjih začeli veliko govoriti in pisati o umetni inteligenci, kar se odraža tudi v poročanju ameriških medijev. Zanimivo je, da umetna inteligenca omogoča tudi njegovo analiziranje. V ta namen so Hong idr. (2021) razvili analizator TV-novic (Stanford Cable TV News Analyzer), ki temelji na uporabi umetne inteligence.

Ta prispevek je strukturiran tako, da ima še štiri poglavja. V poglavju 2 podajamo metode, v poglavju 3 rezultate, v poglavju 4 razpravo, v poglavju 5 pa sklep, s čimer upoštevamo strukturo IMRaD (*Introduction, Methods, Results, and Discussion*).

2 Metode

V raziskavi, katere rezultate podajamo v naslednjem poglavju, smo uporabili podatke o času zaslona (angl. *screen time*), v katerem je bila v podnapisih izpisana beseda *artificial intelligence* ali *AI* in država (*China, France, Germany, India, Japan, South Korea, Taiwan, United Kingdom, United States*), pri čemer smo upoštevali 10-sekundni časovni interval, kar je razvidno s seznama vtipkov, ki smo jih uporabili. V raziskavi smo se omejili na televizijske hiše CNN, FOX in MSNBC, pri čemer smo uporabili analizator TV-novic, ki ga je razvila Univerza Stanford. Podatke, ki smo jih uporabili v raziskavi, smo pridobili tako, da smo v iskalno polje na <https://tvnews.stanford.edu/> vtipkali:

- `text="(artificial intelligence | AI) & China" AND textwindow=10,`
- `text="(artificial intelligence | AI) & France" AND textwindow=10,`

- text="(artificial intelligence | AI) & Germany" AND textwindow=10,
- text="(artificial intelligence | AI) & India" AND textwindow=10,
- text="(artificial intelligence | AI) & Japan" AND textwindow=10,
- text="(artificial intelligence | AI) & South Korea" AND textwindow=10,
- text="(artificial intelligence | AI) & Taiwan" AND textwindow=10,
- text="(artificial intelligence | AI) & (United Kingdom | UK | U.K.)" AND textwindow=10,
- text="(artificial intelligence | AI) & (United States | US | U.S.)" AND textwindow=10.

V raziskavi smo uporabili podatke od januarja 2010 do marca 2024 ter podatke, ki so navedeni v poročilih Univerze Stanford in podjetja Tortoise Media. Opisne statistike smo izračunali v SPSS-u, kar velja tudi za korelacijske statistike, grafikone pa smo narisali v Excelu.

3 Rezultati

Najprej podajamo opisne statistike za pare umetna inteligenca – država (gl. tabelo 1), pri čemer se mesečni podatki v tabeli nanašajo na čas zaslona.

Tabela 1: Opisne statistike

	CN	DE	FR	GB	IN	JP	KR	TW	US
Povprečje	120,97	1,80	3,06	5,48	2,68	4,32	0,94	8,69	364,57
Standardni odklon	230,59	6,94	9,97	26,07	11,22	23,04	6,21	42,67	729,76
Minimum	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00
Maksimum	1457,00	48,00	73,00	278,00	89,00	277,00	70,00	346,00	4630,00
Varianca	53.170,74	48,23	99,48	679,57	125,83	530,63	36,52	1820,54	532.499,69
Koeficient asimetrije	3,15	4,41	3,98	7,91	5,29	10,18	9,02	6,64	3,87
Koeficient sploščenosti	11,93	20,94	18,34	74,07	31,37	117,28	92,73	47,00	16,42

Opomba: CN = Kitajska, DE = Nemčija, FR = Francija, GB = Združeno kraljestvo, IN = Indija, JP = Japonska, KR = Južna Koreja, TW = Tajvan, US = ZDA.

Vir: Lastni izračuni.

Iz tabele 1 je razvidno, da je bil povprečni čas zaslona, v katerem je bila v podnapisih izpisana beseda *artificial intelligence* ali *AI* in država, najdaljši v primeru ZDA (364,57 sekunde), ki jim sledi Kitajska (120,97 sekunde). Najvišji standardni odklon ima par umetna inteligenca – ZDA (729,76),

kar pomeni velike razlike med vrednostmi časa zaslona, najnižjega pa par umetna inteligenca – Južna Koreja (6,21), kar pomeni majhne razlike med vrednostmi časa zaslona. Ameriške televizijske hiše so o paru umetna inteligenca – ZDA najdlje poročale maja 2023, ko je čas zaslona znašal 4630 sekund. Na drugem mestu je par umetna inteligenca – Kitajska (1457 sekund), ki mu sledijo pari umetna inteligenca – Tajvan (346 sekund), umetna inteligenca – Združeno kraljestvo (278 sekund) in umetna inteligenca – Japonska (277 sekund). Minimum v primeru vseh parov je 0, kar pomeni, da je v vseh primerih najmanjša vrednost 0. Največjo varianco ima par umetna inteligenca – ZDA (532.499,69), najnižjo pa par umetna inteligenca – Južna Koreja (36,52). Največjo pozitivno asimetrijo ima par umetna inteligenca – Japonska (10,18), najmanjšo pa par umetna inteligenca – Kitajska (3,15). Pozitiven koeficient asimetrije pomeni, da je porazdelitev nagnjena v desno, negativna pa, da je nagnjena v levo. Najvišji koeficient sploščenosti ima par umetna inteligenca – Japonska (117,28), najnižjega pa par umetna inteligenca – Kitajska (11,93). Višji koeficient pomeni, da je porazdelitev bolj koničasta, nižji pa, da je bolj ploščata.

V drugem delu podajamo koeficiente korelacije med pari umetna inteligenca – država (gl. tabelo 2).

Tabela 2: Koeficienti korelacije

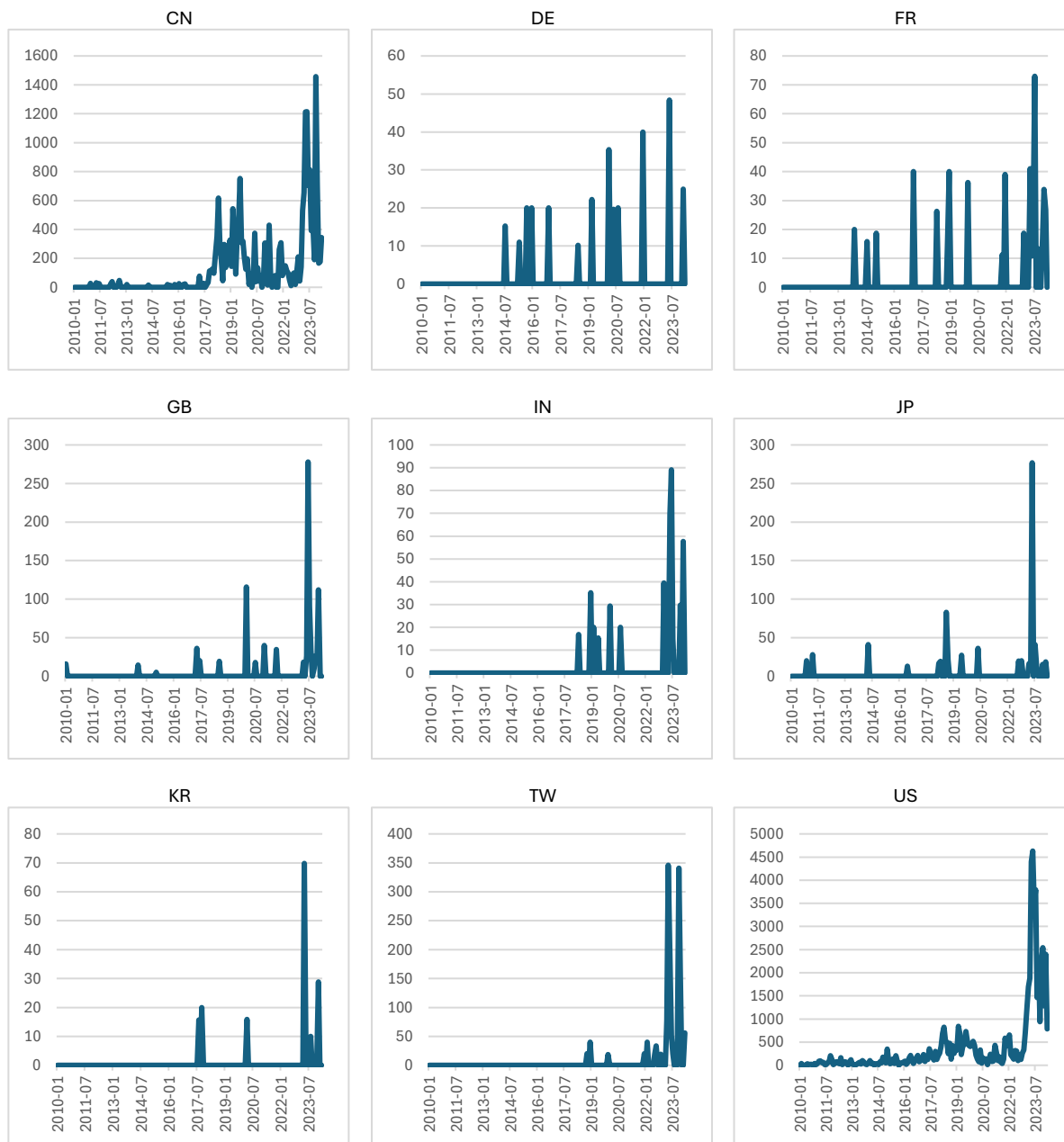
	CN	DE	FR	GB	IN	JP	KR	TW	US
CN	1,00								
DE	0,19	1,00							
FR	0,38	0,18	1,00						
GB	0,29	-0,01	0,32	1,00					
IN	0,44	0,33	0,32	0,60	1,00				
JP	0,45	0,49	0,14	0,08	0,46	1,00			
KR	0,32	-0,04	0,32	0,10	-0,04	0,02	1,00		
TW	0,76	0,17	0,29	0,14	0,28	0,37	0,51	1,00	
US	0,84	0,27	0,55	0,47	0,64	0,51	0,40	0,69	1,00

Vir: Lastni izračuni.

Iz tabele 2 je razvidno, da je stopnja povezanosti med paroma umetna inteligenca – Kitajska in umetna inteligenca – ZDA med vsemi pari največja. Koeficient korelacije znaša 0,84, kar pomeni, da sta pojava zelo močno povezana. Močna povezanost je tudi med pari CN – TW (0,76), TW – US (0,69), IN – US (0,64) in IN – GB (0,60).

V tretjem delu podajamo grafikone, ki kažejo gibanje časa zaslona, v katerem je bila v podnapisih izpisana beseda *artificial intelligence* ali *AI* in država.

Slika 1: Čas zaslona



Opomba: Os x kaže čas v mesecih, os y pa čas zaslona v sekundah. 2010-01 = januar 2010.

Vir: Hong idr. (2021), <https://tvnews.stanford.edu/>.

S slike 1 je razvidno, da se je v vseh primerih poročanje ameriških televizijskih hiš o paru umetna inteligenca – država povečalo, kar je razvidno tudi iz tabele 3. Res pa je, da so med državami velike

razlike glede pogostosti in trajanja poročanja. Lep primer so Francija, Južna Koreja in Nemčija, ki jih ameriški mediji redkeje omenjajo, ko poročajo o umetni inteligenci.

Tabela 3: Povprečni čas zaslona pred uvedbo ChatGPT-ja in po njej












	Povprečni čas zaslona pred uvedbo ChatGPT-ja		Povprečni čas zaslona po uvedbi ChatGPT-ja	
	Povprečje	Standardni odklon	Povprečje	Standardni odklon
CN	74,21	131,71	573,90	427,89
DE	1,51	5,94	3,31	13,24
FR	1,72	7,09	16,96	20,51
GB	2,06	10,95	38,53	72,01
IN	0,88	4,63	20,05	29,17
JP	2,23	9,23	24,54	68,25
KR	0,33	2,39	6,79	18,38
TW	1,36	6,19	79,72	119,59
US	171,29	182,43	2237,06	1251,92

Vir: Lastni izračuni.

V petem delu podajamo rezultate primerjave razvrstitve držav glede na povprečni čas zaslona in glede na različne kriterije, ki so navedeni v poročilu Univerze Stanford.

Tabela 4: Povprečni čas zaslona in različni kriteriji, ki so navedeni v poročilu Univerze Stanford
















































Povprečni čas zaslona, 2010–2024	Število modelov strojnega učenja, 2023	Število temeljnih modelov, 2023	Zasebne naložbe v umetno inteligenco (v milijardah USD), 2023	Zasebne naložbe v umetno inteligenco (v milijardah USD), 2013–2023	Število novih umetnointeligentnih podjetij, 2023	Število novih umetnointeligentnih podjetij, 2013–2023
 364,57	 61	 109	 67,22	 335,24	 897	 5509
 120,97	 15	 20	 7,76	 103,65	 122	 1446
 8,69	 8	 8	 3,78	 22,25	 104	 727
 5,48	 5	 2	 1,91	 10,35	 76	 391
 4,32	 4	 1	 1,69	 9,85	 58	 338
 3,06		 1	 1,39	 8,31	 45	 333

 2,68			 1,39	 7,25	 44	 319
 1,80			 0,68	 4,81	 42	 189
 0,94						

Vir podatkov: Maslej idr. (2024).

Iz tabele 4 je razvidno, da se razvrstitev ZDA in Kitajske glede na povprečni čas zaslona ujema z njuno razvrstitvijo glede na različne kriterije, ki so navedeni v poročilu Univerze Stanford. V nadaljevanju nas je zanimalo, ali to velja tudi za različne kriterije, ki so navedeni v poročilu podjetja Tortoise Media.

Tabela 5: Povprečni čas zaslona in različni kriteriji, ki so navedeni v poročilu podjetja Tortoise Media

Povprečni čas zaslona, 2010–2024	Skupaj	Raziskave	Infrastruktura	Delovno okolje	Talent	Vladna strategija	Komerciala
 364,57	 100	 100	 100	 99,7	 100	 93,9	 100,0
 120,97	 61,5	 80,6	 92,1	 92,4	 86,2	 93,5	 43,1
 8,69	 41,8	 48,8	 80,8	 91,4	 57,0	 91,9	 20,0
 5,48	 40,3	 29,3	 74,4	 91,1	 53,8	 90,3	 10,8
 4,32	 39,2	 24,3	 71,3	 90,7	 41,5	 89,2	 10,3
 3,06	 33,9	 21,4	 68,9	 84,2	 38,0	 87,3	 8,9
 2,68	 32,8	 18,6	 68,2	 82,8	 35,1	 80,3	 8,3
 1,80	 31,4	 13,6	 61,8	 79,5	 30,0	 56,0	 6,8
 0,94	 25,4	 12,0	 34,7	 71,4	 24,5	 51,4	 4,3

Vir podatkov: Cesareo & White (2023).

Iz tabele 5 je razvidno, da se razvrstitev ZDA in Kitajske glede na povprečni čas zaslona bolj ali manj ujema z njuno razvrstitvijo glede na različne kriterije, ki so navedeni v poročilu podjetja Tortoise Media, kar dopolnjuje naše dosedanje ugotovitve. Podatki kažejo, da ZDA vodijo na področju raziskav, infrastrukture, talenta in komerciala, Kitajska pa na področju delovnega okolja. Zanimivo je, da Kitajski na tem področju sledijo druge azijske države (Japonska, Južna Koreja, Indija), kar je

pomembno za njihovo konkurenčnost. Indija je med vodilnimi tudi na področju talenta, kar nas ne preseneča glede na talent Indijcev za informatiko, računalništvo, matematiko ipd.

4 Razprava

Umetna inteligenca je tema številka ena v gospodarstvu, družbi, politiki itd. (Noy & Zhang, 2023). Izkušnje iz ZDA učijo, kako pomembno je opazovati in spremljati trende ipd. (Ahmed, Wahed & Thompson, 2023). Tega se zavedajo tudi druge države, kot so npr. Brazilija, Indija, Kitajska, Malezija, Rusija, Singapur, Vietnam, ki bolj kot ne zaostajajo za ZDA. Deloma zaradi pomanjkanja denarja, deloma zaradi pomanjkanja znanja. Prednost ZDA je, da so razvile (edinstven) umetno-inteligenčni ekosistem, ki ga sestavljajo podjetja, naložbeniki (vlagatelji) in vozlišča (Deep Knowledge Group, 2024; gl. tudi <https://www.ai-ecosystem.org/usa-mindmaps>). Tako ne preseneča, da so vodilna (vele)sila na področju umetne inteligence, kar izhaja iz poročil ameriških kabelskih televizijskih postaj (časa zaslona) ter Univerze Stanford in podjetja Tortoise Media. To pomeni, da podatki o poročanju ameriških medijev odražajo dejansko stanje, kar lahko trdimo tudi za Kitajsko, ki se je uvrstila na drugo mesto, ne pa tudi za Tajvan, ki se je uvrstil na tretje mesto, in to predvsem po zaslugi poročanja ameriških novinarjev o vlogi Tajvana v dobavni verigi polprevodnikov.

5 Sklep

Ugotovili smo, da so televizijske hiše CNN, FOX in MSNBC pri poročanju o umetni inteligenci najpogosteje omenjale ZDA, kar smo pričakovali glede na to, da imajo vse tri svoj sedež v ZDA in da so ZDA po različnih kriterijih vodilne na področju umetne inteligence. Na drugem mestu je Kitajska, ki je njihova konkurentka za prvo mesto, kar se kaže tudi v poročanju ameriških televizijskih hiš. Strinjamo se, da obstaja potreba po dodatnih raziskavah, v okviru katerih bi raziskovalci poglobljeno analizirali poročanje ameriških medijev o umetni inteligenci. Predlagamo, da raziskovalci upoštevajo tudi druge novice, ne samo kabelskih (televizijskih), da upoštevajo tudi tuje medije, ne samo ameriških, da upoštevajo tudi druge besede in/ali besedne zveze, ne samo *artificial intelligence* oz. *AI*, da upoštevajo tudi druge države, ne samo Francije, Indije, Japonske, Južne Koreje, Kitajske, Nemčije, Tajvana, Združenega Kraljestva in ZDA, itd. To bi omogočilo boljši vpogled v stanje na tem področju, kar je pomembno za raziskovalce in oblikovalce politike. Poleg tega ne smemo pozabiti, da se umetna inteligenca ne uporablja samo v gospodarstvu, ampak tudi v vzgoji in izobraževanju, zdravstvu itd.

Viri

Ahmed, N., Wahed, M., & Thompson, N. C. (2023). The growing influence of industry in AI research. *Science*, 379, 884–886. <https://doi.org/10.1126/science.ade2420>

Cesareo, S., & White, J. (2023). *The global AI index*. Tortoise. <https://www.tortoisemedia.com/intelligence/global-ai/#rankings>

Deep Knowledge Group (2024). *AI industry in the United States: Landscape overview. February 2024*. <https://analytics.dkv.global/ai-ecosystem/usa/ai-industry.pdf>

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 J. Tang & T. Derr (ur.), *Proceedings of the 27th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining* (str. 3011–3021). <https://doi.org/10.1145/3447548>

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*. AI Index Steering Committee, Institute for Human-Centered AI, Stanford University. <https://aiindex.stanford.edu/report/2024>

Noy, S., & Zhang, W. (2023). Experimental evidence on the productivity effects of generative artificial intelligence. *Science*, 381, 187–192. <https://doi.org/10.1126/science.adh2586>

DIGITALNO PRAVO

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

(Ne)dopustnost profiliranja za namene oglaševanja na spletu

Kaja Lenart  

Univerza v Mariboru, Pravna fakulteta

Maribor, Slovenija

Jan Stajnkó 


Univerza v Mariboru, Pravna fakulteta

Maribor, Slovenija

Povzetek: Digitalizacija je v zadnjih desetletjih močno zaznamovala sodobno družbo, med drugim je pomembno vplivala tudi na področje varstva osebnih podatkov. Slednje je treba zagotoviti uporabnikom družbenih omrežij, kjer se oglaševalci pogosto poslužujejo tako imenovanega profiliranja. Takšen način upravljanja s podatki lahko služi analizi ekonomskega položaja, osebnega okusa ter analizi interesov posameznika. Proces profiliranja namreč omogoča ciljno oglaševanje, pri katerem so vsebine uporabnikom družbenih omrežij predstavljene na podlagi avtomatiziranega pridobivanja znanja z izvedbo analize obstoječih podatkov, s katerimi upravitelji podatkov oblikujejo predpostavke o posamezniku. Prispevek naslavlja pravno ureditev varstva osebnih podatkov posameznikov v okviru profiliranja, ki se izvaja preko družbenih omrežij, pri čemer analizira ureditev predmetnega področja v Splošni uredbi o varstvu osebnih podatkov in Aktu o digitalnih storitvah.

Ključne besede: profiliranje, ciljno oglaševanje, varstvo osebnih podatkov

(Im)permissibility of profiling for advertising purposes

Kaja Lenart  

University of Maribor, Faculty of Law
Maribor, Slovenia

Jan Stajniko 

University of Maribor, Faculty of Law
Maribor, Slovenia

Abstract: The modern society has been significantly marked by digitalization, which emphasized the urgency of ensuring the protection of personal data. Protection also needs to be ensured for users of social media platforms, where advertisers often resort to the so-called profiling. Such data management allows advertisers to conduct analysis of economic status, personal preferences, and individual interests. The profiling process enables targeted advertising. Advertisers can present social media users with content that is based on formulated assumptions about the individual, through the automated analysis of existing data. The article addresses the legal regulation of the protection of individuals' personal data within profiling for advertising purposes. It analyzes the regulation of the subject in the General Data Protection Regulation and the Digital Services Act.

Keywords: personal data protection, profiling, targeted advertising

1 Uvod

Izzivi, povezani z varovanjem osebnih podatkov, so privedli do poenotenja pravil varstva osebnih podatkov. Evropski zakonodajavec je prepoznal pomembnost zagotavljanja ustrezne ravni varnosti tako v resničnem kot tudi spletnem okolju in za potencialno problematičnega prepoznal tudi postopek oblikovanja profilov, ki ga vse pogosteje uporabljajo upravljavci podatkov, vključno z oglaševalci na družbenih omrežjih. Takšen postopek obdelave osebnih podatkov omogoča ciljno oglaševanje, pri čemer upravljavci na podlagi analize obstoječih podatkov ustvarjajo predpostavke o posameznikih ter jim nato prikazujejo prilagojene vsebine. Prispevek se osredotoča na pravno opredelitev postopka oblikovanja profilov in omejitev tovrstnega načina obdelave podatkov, hkrati pa opozarja na pravice, ki posamezniku pripadajo iz tega naslova.

2 Pravna opredelitev profiliranja

Profiliranje oz. oblikovanje profilov je postopek zbiranja informacij o posamezniku ali določeni skupini na podlagi ocenjevanja njihovih značilnosti ali vzorcev vedenja z namenom doseči uvrstitev določenih ljudi v posamično kategorijo. Razvrstitev je namenjena analizi posameznikovega predvidenega vedenja, zmožnosti ali interesa (Delovna skupina za varstvo podatkov iz člena 29, 2017, str. 7). Gre za proces, ki se uporablja na različnih področjih (kot so področje trženja, oglaševanja, bančništva ipd.), in je lahko koristen z vidika zagotavljanja večje učinkovitosti ter omogočanja varčevanja z viri. Vendar lahko ta proces izrazito negativno vpliva na temeljne pravice in svoboščine posameznikov (Delovna skupina za varstvo podatkov iz člena 29, 2017, str. 5). Postopek je lahko nepošten in lahko privede do diskriminatorne obravnave, saj posameznike ciljno usmerja do vsebine na podlagi zgolj določenih zbranih podatkov. Zaradi čedalje širšega obsega osebnih podatkov, ki so na voljo uporabnikom v digitalnem okolju, se lahko postopek profiliranja vse pogosteje uporablja z namenom hitrejšega doseganja specifičnih trgov ter zagotavljanja individualizirane ponudbe. Kljub temu ostaja problematično dejstvo, da se posamezniki pogosto ne zavedajo, zakaj jim je določena vsebina predstavljena in na kakšen način so uporabljeni njihovi osebni podatki.

Zaradi teh perečih vprašanj, ki se pojavljajo v okviru hitro razvijajoče se digitalne dobe, je nastala potreba po harmonizirani ureditvi varstva osebnih podatkov. Evropski zakonodajavec je na tem področju sprejel Uredbo Evropskega parlamenta in Sveta o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES (v nadaljevanju Splošna uredba o varstvu podatkov), ki v 4. členu smiselno obravnava oblikovanje profilov kot vsako

obliko avtomatizirane obdelave osebnih podatkov.¹ Takšna obdelava glede na uredbo vključuje uporabo osebnih podatkov za ocenjevanje nekaterih osebnih vidikov v zvezi s posameznikom, zlasti za analizo ali predvidevanje uspešnosti pri delu, ekonomskega položaja, zdravja, osebnega okusa, interesov, zanesljivosti, vedenja, lokacije ali gibanja določenega posameznika.

Oblikovanje profilov je lahko v osnovi izvedeno na tri načine: splošno oblikovanje profilov, sprejemanje odločitev na podlagi oblikovanja profilov ali pa zgolj avtomatizirano sprejemanje odločitev (ki vključuje oblikovanje profilov ter ima pravne ali znatne učinke na posameznika). Temeljna razlika med navedenimi načini profiliranja je v tem, da tisti postopki, ki so posledica zgolj avtomatiziranih oblikovanj profilov, potekajo brez kakršne koli človeške intervencije pri ocenjevanju pridobljenih informacij (Delovna skupina za varstvo podatkov iz člena 29, 2017, str. 9).

2.1 Razlikovanje med profiliranjem in avtomatiziranim sprejemanjem odločitev

Avtomatizirano sprejemanje odločitev omogoča zmožnost sprejemanja odločitev brez osebnega posredovanja, torej zgolj s tehnološkimi sredstvi. Glede na način obdelave podatkov pa lahko tak postopek preraste v postopek, ki temelji na oblikovanju profilov. Ključno pri postopku profiliranja je, da gre za izvedbo »ocenjevanja«, pri čemer je cilj postopka podati oceno posameznika. Razvrščanje na podlagi določenih lastnosti, kot je spol ali starost, namreč še ne pomeni oblikovanja profilov. Temeljni pokazatelj, da gre za postopek profiliranja, je izvedba razvrščanja, katerega cilj je ocenitev določenih značilnosti (Delovna skupina za varstvo podatkov iz člena 29, 2017, str. 8). Vzpostavitev profila posameznika, iz katerega lahko oglaševalci razberejo njegove interese, je ključnega pomena pri ciljnem oglaševanju izdelkov na spletnih platformah. S ciljnim oglaševanjem lahko oglaševalci zagotovijo boljše storitve svojim naročnikom in omogočijo, da oglasna sporočila dosežejo več potencialnih kupcev v primerjavi z oglasi, dostopnimi na primer v dnevnem časopisju, na televiziji, v strokovni periodiki ali drugih tiskanih medijih (Podpečan, 2019, str. 13-15).

2.2 Zakonitost postopka obdelave podatkov z izvedbo profiliranja

¹ Splošna uredba o varstvu podatkov v 1. odstavku 4. člena opredeljuje »osebne podatke« kot podatke, ki pomenijo katero koli informacijo v zvezi z določenim ali določljivim posameznikom. Določljiv posameznik je tisti, ki ga je mogoče neposredno ali posredno določiti, zlasti z navedbo identifikatorja, kot so ime, identifikacijska številka, podatki o lokaciji in spletni identifikator, ali z navedbo enega ali več dejavnikov, ki so značilni za fizično, fiziološko, genetsko, duševno, gospodarsko, kulturno ali družbeno identiteto tega posameznika.

Obdelava osebnih podatkov s postopkom profiliranja je dovoljena zgolj, kadar je v osnovi izvedena skladno z načeli Splošne uredbe o varstvu podatkov, kar pomeni, da mora biti obdelava celovita in zaupna. Zahteva se izvedba obdelave, ki zasleduje načelo zakonitosti, pravičnosti in preglednosti (oz. informiranosti) in je lahko namenjena le zbiranju podatkov za določene, izrecne in zakonite namene ob upoštevanju načela zajemanja najmanjšega obsega podatkov. Podatki morajo biti poleg navedenega skladno s 5. členom Splošne uredbe o varstvu podatkov točni in ustrezno posodobljeni, hkrati pa tudi shranjeni le toliko časa, kolikor je potrebno, da se doseže namen njihove obdelave.

V primeru neupoštevanja navedenih temeljnih načel lahko postopek oblikovanja profilov privede do diskriminacije. Konkretno je lahko zaradi obdelave zgolj določenih podatkov posamezniku onemogočena možnost pridobitve kredita, zavarovanja ali npr. pridobitev zaposlitve. Kadar izvedba postopka profiliranja ni smotrno omejena, pogosto privede tudi do usmeritve posameznika na pretirano tvegane izdelke oz. storitve (Delovna skupina za varstvo podatkov iz člena 29, 2017, str. 10).

Uporabniki morajo biti posebej previdni, kadar gre za osebne podatke občutljivejše narave. Lahko pa nastopi situacija, ko podatki sami po sebi sicer ne spadajo v posebno kategorijo podatkov, temveč se njihova občutljivejša narava vzpostavi v kombinaciji z obdelovanjem drugih podatkov, tj. z izvedbo oblikovanja profilov (npr. z vzpostavitvijo povezave o političnih ali verskih prepričanjih, vzpostavitvijo indikatorjev zdravstvenega stanja) (Delovna skupina za varstvo podatkov iz člena 29, 2017, str. 16).

Splošno upravljavci osebnih podatkov ravnajo zakonito le, kadar odločitev po obdelovanju podatkov temelji na določeni podlagi, predvideni v 6. členu Splošne uredbe o varstvu podatkov. Upravljavci lahko obdelavo utemeljijo na privolitvi posameznika, na katerega se nanašajo osebni podatki, ali pa je obdelava teh podatkov potrebna za izvajanje ali sklenitev pogodbe (kadar je ta posameznik stranka pogodbe). Obdelava je lahko potrebna tudi za izpolnitev zakonske obveznosti ali zaščito življenjskih interesov posameznika (na katerega se nanašajo osebni podatki ali druge fizične osebe). Obdelava je zakonita tudi, kadar potreba po obdelavi izhaja iz javnega interesa ali namena izvajanja javne oblasti, dodeljene upravljavcu ter kadar so podlaga zakoniti interesi, za katere si prizadeva upravljavec ali tretja oseba.

2.3 Pravice posameznikov, na katere se nanašajo osebni podatki

Posameznikom, na katere se osebni podatki nanašajo, Splošna uredba o varstvu podatkov priznava pravico do obveščенosti (upravljavci morajo jasno opredeliti, da bo postopek vključeval profiliranje), pravico do dostopa (dostopa do podatkov, uporabljenih za oblikovanje profilov), pravico do popravka,

pravico do izbrisa, pravico do omejitve obdelave ter pravico do ugovora obdelave (oz. do oblikovanja profilov). Pomembno je tudi poznavanje pravice iz 22. člena Splošne uredbe o varstvu podatkov, ki posamezniku, na katerega se nanašajo osebni podatki, v primeru izvajanja oglaševanja z izvedbo avtomatiziranih sprejemanj posameznih odločitev dodeljuje pravico, da se ta odloči, da zanj ne velja odločitev, ki je predstavljena na avtomatizirani obdelavi in vključuje profiliranje. Kot primer je v 71. točki uvodne izjave navedena "avtomatska zavrnitev spletne prošnje za posojilo ali prakse zaposlovanja prek spleta brez človekovega posredovanja". Uvodna izjava v tem delu pojasnjuje tudi, da 22. člena Splošne uredbe o varstvu podatkov ni možno uporabiti v okviru kakršnekoli obdelave, ki vključuje profiliranje, temveč zgolj za primere, ko obdelava pomeni sprejemanje individualiziranih odločitev o konkretnem posamezniku. Gre torej za preprečevanje uporabe odločitev, izhajajočih zgolj iz avtomatizirane obdelave, vključno z oblikovanjem profilov (Trstenjak, 2022, str. 902).

Iz 71. točke uvodne izjave Splošne uredbe o varstvu podatkov lahko razberemo tudi, da na splošno takšni postopki naj ne bi smeli zadevati otrok.

2.4 Primer Facebook in Cambridge Analytica

Nujnost omejitve zbiranja podatkov z namenom oblikovanja profilov je razvidna iz primera delovanja podjetja Cambridge Analytica, ki je nezakonito pridobivalo podatke od posameznih uporabnikov spletne platforme Facebook. S pomočjo oblikovanja profilov iz ogromne količine podatkov, ki jih zagotavlja spletna platforma Facebook, je podjetje Cambridge Analytica manipuliralo javno mnenje. Ta manipulacija se je izkazala za sporno predvsem v primeru pomembnih političnih prelomnic, kot so bile ameriške predsedniške volitve ter izstop Združenega kraljestva iz Evropske unije. Uporaba mehanizmov ni več predstavljala zgolj ciljnega informiranja, temveč je v tem primeru preseгла to funkcijo in dosegla možnost vpliva na izid pomembnih političnih odločitev, kar predstavlja grožnjo demokratičnemu sistemu. S takšnim pridobivanjem ter obdelavo podatkov je ogroženo svobodno izbiranje sprejemanja političnih odločitev. Ta primer je osvetlil pomembnost seznanitve posameznika v primeru izvedbe oblikovanja profilov, saj lahko zgolj ob upoštevanju pravil osebnih podatkov zagotovimo pravico do zasebnosti ter hkrati uresničujemo pravico do svobodnega odločanja (Informacijski pooblaščenec, 2018).

Spletna platforma Facebook se je izkazala za problematično sama po sebi, saj je razvila modele trženja, ki so vključevali oblikovanje profilov mladoletnih oseb. Vendar njihov postopek ni zadostil pričakovani

previdnosti glede tega, kakšni oglasi bodo dostopni mladoletnikom, ki predstavljajo ranljivo skupino med uporabniki (Reset Australia, 2021).

Zaradi novonastalih tveganj v povezavi z obdelavo osebnih podatkov je bila spletna platforma Facebook pozvana k celoviti prenovi, saj je dopuščala škodljivo ravnanje s podatki uporabnikov. Tovrstni sporni primeri so spodbudili tudi Evropsko unijo, da sprejme nove ukrepe, ki pripomorejo k zagotavljanju zasebnosti, sprejemanju demokratičnih odločitev in varstvu ranljivejših skupin.

3 Pravna opredelitev oglaševanja na družbenih omrežjih

Področje varstva osebnih podatkov je evropski zakonodajalec dopolnil s sprejetjem Uredbe Evropskega parlamenta in Sveta o enotnem trgu digitalnih storitev in spremembi Direktive 2000/31/ES (v nadaljevanju Akt o digitalnih storitvah), s katerim izpopolnjuje pravni okvir, ki prispeva k doseganju varnejšega digitalnega okolja v dobi, kjer uporabniki vstopajo na trg z novimi poslovnimi metodami, kot so družbena omrežja. Te platforme zahtevajo prilagojene varnostne mehanizme z namenom doseganja visoke ravni varstva pravic uporabnikov. Akt o digitalnih storitvah zajema vse vrste oglaševanja ter ustrezno dopolnjuje obstoječa pravila Splošne uredbe o varstvu podatkov in velja za vse platforme od 17. 2. 2024 dalje (Evropska komisija, 2024, str. 1 in 3). Poklicne in zasebne dejavnosti se v digitalnem okolju prepletajo in presegajo svoje teritorialne meje, kar predstavlja povsem nove izzive (Weber, 2017, str. 168).

Določbe Akta o digitalnih storitvah izhajajo iz načela, da je v digitalnem okolju nedopustno tisto, kar je na drugi strani nedopustno tudi v resničnem svetu. Upravljavcem na družbenih omrežjih nalagajo večjo odgovornost pri zaščiti uporabnikov ter nudijo izboljšane mehanizme za odstranjevanje lažnih ali nezakonitih vsebin. Predvidoma bodo določbe Akta o digitalnih storitvah učinkovito preprečevale tudi širjenje drugih nedopustnih vsebin. Sklepno gre za akt, ki zmanjšuje tveganja v digitalnem prostoru. Pravna predvidljivost namreč spodbuja konkurenčnost digitalnega gospodarstva ter boljšo preglednost nad spletnim oglaševanjem (Služba Vlade Republike Slovenije za digitalno preobrazbo, 2022).

Za izvedbo oglaševanja na družbenih omrežjih morajo sedaj ponudniki, ki predstavljajo svoje izdelke ali storitve na različnih platformah, ravnati v skladu s 26. členom Akta o digitalnih storitvah ter zagotoviti, da je posamezniku predstavljeno:

- a) da je informacija oglas, vključno s pomočjo vidnih označb, ki lahko upoštevajo standarde na podlagi člena 44;

- b) fizično ali pravno osebo, v imenu katere je oglas predstavljen;
- c) fizično ali pravno osebo, ki je plačala oglas, če to ni fizična ali pravna oseba iz točke (b);
- d) smiselne informacije, neposredno in preprosto dostopne prek oglasa, o glavnih parametrih, uporabljenih za določitev prejemnika, ki mu je oglas predstavljen, in po potrebi kako te parametre spremeniti.

Posameznikom mora biti skladno z 2. točko 26. člena Akta o digitalnih storitvah vedno predstavljeno, da je vsebina ponudnika na določeni platformi komercialno sporočilo oz. sporočilo, ki vsebuje komercialna sporočila. Poleg tega morajo potrošnikom, ki lahko sklepajo pogodbe na daljavo, zagotoviti ustrezne podatke o trgovcu. Izjemoma sledljivost trgovca kot ponudnika ni zahtevana za mikro oz. mala podjetja.

Zaradi znatnega vpliva na družbo Akt o digitalnih storitvah nalaga dodatne obveznosti tako imenovanim zelo velikim spletnim platformam, kot so: Facebook, Instagram, Pinterest, Snapchat, TikTok, Apple, Amazon Store, Google Shopping, Wikipedija, YouTube itd. Prav tako dodatne obveznosti nalaga zelo velikim spletnim iskalnikom, kot sta Bing in Google Search (Ministrstvo za digitalno preobrazbo, 2023). Merilo za razlikovanje platform je vzpostavljeno v 33. členu Akta o digitalnih storitvah, ki za velike spletne platforme in zelo velike spletne iskalnike smatra tiste platforme, ki na mesec dosejajo povprečno število vsaj 45 milijonov aktivnih uporabnikov. Zelo velike spletne platforme so se kar kmalu po uveljavitvi Akta o digitalnih storitvah izkazale za problematične, saj je Evropska komisija že pričela s presojo, ali platforma TikTok krši Akt o digitalnih storitvah z vidika zagotavljanja ustrezne zaščite mladoletnikov. Poleg tega je vprašljiva tudi zagotovitev preglednosti predstavljenega oglaševanja (Evropska komisija, 2024). Akt o digitalnih storitvah naj bi namreč urejal tudi poenostavljene postopke za prijavo takšnih kršitev, ki jih je možno zaslediti na različnih platformah ter vzpostavitev ustrežnejšega postopka odstranitve vsebin, ki so lažne oz. nezakonite (Ministrstvo za digitalno preobrazbo, 2023).

Z vidika ciljnega oglaševanja na spletnih platformah je sedaj v osnovi treba upoštevati dve temeljni omejitvi. Poglavitno, ciljno oglaševanje mladoletnikom na podlagi profiliranja načeloma ni dovoljeno (predvsem kadar lahko z razumno gotovostjo ugotovimo, da je prejemnik vsebine mladoleten). Poleg tega pa je prepovedano ciljno oglaševanje na podlagi profiliranja z uporabo posebnih kategorij osebnih podatkov (kot je politično ali versko prepričanje ipd.) Nova pravila zagotavljajo boljše razumevanje predstavljenih oglasov in uporabnikom omogočajo sprejetje bolj premišljenih ter samostojnejših

odločitev. S tem se vzpostavlja tudi lažje prepoznavanje sponzoriranih komercialnih vsebin, ki jih vse pogosteje na družbenih omrežjih zagotavljajo tudi vplivneži (Evropska komisija, 2024, str. 2).

4 Nadzorni organ

V primeru, da so posamezniki mnenja, da je pri obdelavi njihovih osebnih podatkov prišlo do kršitve njihovih pravic, imajo glede na 77. člen Splošne uredbe o varstvu podatkov možnost vložiti pritožbo pri nadzornem organu. Konkretnije Zakon o varstvu podatkov (v nadaljevanju ZVOP-2) v 1. točki 5. člena določa, da je nadzorni organ v Republiki Sloveniji informacijski pooblaščenec. Gre za samostojen in neodvisen državni organ, ki deluje kot pritožbeni, inšpekcijski ali prekrškovni organ, odvisno od vrste in značilnosti zadeve, med katere med drugim spadajo kršitve pravice do dostopa ali ponovne uporabe informacij javnega značaja, pravice do varstva osebnih podatkov ter pacientove pravice (Informacijski pooblaščenec, 2022a).

Funkcija informacijskega pooblaščenca je tudi ta, da podaja mnenja o upravičenosti obdelave, ki se izvaja v praksi. Tako je dne 21. 7. 2019 informacijski pooblaščenec podal mnenje glede posredovanja točno določenih izdelkov kupcu, izbranih na podlagi profiliranja posameznika, izhajajoč iz njegove privolitve. Informacijski pooblaščenec je poudaril, da mora upravljavec podatkov zagotoviti ustrezno predhodno informiranje, na podlagi katere je posamezniku podana dejanska možnost izbire glede obdelave njegovih podatkov pri uporabljanju storitev. Posameznik mora torej imeti možnost sprejeti ali zavrniti privolitev brez zanj škodljivih posledic (Informacijski pooblaščenec, 2019, str. 1). Mnoge spletne platforme pa še vedno ravna v nasprotju z zakonodajo, saj pogosto uporabnikom v primeru zavrnitve soglašanja s postopkom profiliranja onemogočajo ali močno omejujejo uporabo platforme.

Informacijski pooblaščenec je presojal tudi ustreznost pravne podlage za profiliranje kupcev na podlagi podatkov, zbranih v okviru kartice zvestobe. Odgovoril je na vprašanje, ali lahko upravljavec v tem primeru obdelavo podatkov utemelji na način, da zagovarja stališče, da se obdelava kupčevih podatkov izvaja na podlagi zakonitega interesa upravljavca. Zakoniti interes je namreč podan le, kadar zadosti testu tehtanja med zakonitim interesom upravljavca in posegom v interese ter temeljne pravice posameznika. Upravljavec mora presoditi, ali je profiliranje z namenom ugotovitve želja kupcev ali zagotovitve individualizacije ponudbe v njegovem zakonitem interesu. Informacijski pooblaščenec je v predmetnem primeru poudaril, da obstaja velika verjetnost, da gre v teh primerih za pretiran poseg v zasebnost, saj je treba upoštevati tudi možnost, da se profiliranje veže na osebne podatke občutljive narave. Profiliranja uporabnikov z uporabo kartice zvestobe zato načeloma ni dopustno izvesti na

podlagi zakonitega interesa upravljavca, saj je pri takšni obdelavi vprašljiva poštenost obdelave (Informacijski pooblaščenec, 2018, str. 1–3).

Nadalje je dne 7. 6. 2022 informacijski pooblaščenec odgovoril na vprašanje glede dopustnosti obdelave osebnih podatkov z namenom odobritve stanovanjskega kredita. V konkretnem primeru je banka kot enega izmed pogojev za obravnavo vloge za odobritev kredita zahtevala predložitev zadnjih dvanajstih bančnih izpiskov osebnega ter poslovnega računa. Pri tem ni vprašljivo, ali mora banka preveriti posameznikovo finančno sposobnost, temveč ali s pridobitvijo določenih podatkov pretirano posega v posameznikovo zasebnost. Obdelava podatkov bo namreč utemeljena, kadar bo banka svoje ravnanje utemeljila na podlagi relevantnega področnega zakona in s tem zakonito pridobila osebne podatke brez potrebe po privolitvi posameznika. Lahko pa obdelava temelji na podlagi privolitve ali nastopi zaradi sklenitve ali izvedbe pogodbe. Informacijski pooblaščenec je ob tem poudaril, da mora tudi banka ne glede na svojo vlogo dosledno spoštovati dejstvo, da se mora obdelava podatkov izvajati skladno z načelom najmanjšega obsega podatkov. To pomeni, da morajo biti podatki relevantni glede na namen uporabe. Posameznikom mora kot upravitelj podatkov zagotoviti vse ustrezne informacije o zahtevani pridobitvi oz. obdelavi podatkov. Vsekakor pa bi moral biti posameznik obveščen tudi o obstoju avtomatiziranega sprejemanja odločitev, ki vključuje profiliranje. V nasprotnem primeru banka krši določbe Splošne uredbe o varstvu podatkov, kot tudi v primeru, kadar za pridobivanje omenjenih podatkov ne bi bilo ustrezne podlage za obdelavo takšnega podatka (Informacijski pooblaščenec, 2022b, str. 1–2).

5 Sklep

Pravilna izvedba profiliranja lahko prinese številne koristi posameznikom, skupinam ali organizacijam, saj omogoča prilagojeno prikazovanje izdelkov ali storitev na družbenih omrežjih, ki natančneje ustrezajo posameznikovim potrebam. Neustrezna izvedba profiliranja oz. izvedba v nasprotju s predvidenimi varovalnimi mehanizmi, ki jih zagotavljata predvsem Splošna uredba o varstvu podatkov in Akt o digitalnih storitvah, pa lahko ima negativne posledice, predvsem za določene ranljive skupine. Vzpostavi se lahko tako neenakost pri dostopanju do izdelkov ali storitev kot tudi vplivanje na druge za posameznika pomembne odločitve. Profiliranje se ne sme uporabljati za vzpostavljanje situacij, v katerih lahko ranljive skupine postanejo tarča manj ugodnih ponudb, saj to vodi do dodatne socialne neenakosti; v nekaterih primerih pa lahko vodi tudi do vprašljive demokratičnosti.

Ključnega pomena je, da se postopek oblikovanja profilov tudi v okviru novodobnih oglaševalnih trendov izvaja odgovorno, v skladu z zakonodajo in z namenom, da ne prihaja do kršitev določb varstva osebnih podatkov.

Viri

Evropska komisija (2024). *Komisija začela formalni postopek proti TikToku na podlagi akta o digitalnih storitvah*. <https://digital-strategy.ec.europa.eu/si/news/commission-opens-formal-proceedings-against-tiktok-under-digital-services-act>

Evropska komisija (2024). *Vprašanja in odgovori o aktu o digitalnih storitvah*. https://ec.europa.eu/commission/presscorner/detail/en/QANDA_20_2348

Informacijski pooblaščenec (2018). *Zakoniti interesi kot podlaga za profiliranje*. <https://www.ip-rs.si/mnenja-zvop/zakoniti-interesi-kot-podlaga-za-profiliranje>

Informacijski pooblaščenec (2018). *Zaradi zlorabe osebnih podatkov v aferi "Cambridge Analytica" Facebooku grozi globa – ranljivost posameznikov pri personaliziranem prepričevanju v volilnih in referendumskih kampanjah*. <https://www.ip-rs.si/novice/6051f2192d8b2>

Informacijski pooblaščenec (2019). *Pošiljanje izbranih izdelkov kupcu*. <https://www.ip-rs.si/mnenja-gdpr/6048a38d3fa64>

Informacijski pooblaščenec (2022a). *Informacijski pooblaščenec*. <https://www.gov.si/drzavni-organi/drugi-drzavni-organi/informacijski-pooblascenec/>

Informacijski pooblaščenec (2022b). *Obdelava OP v namen odobritve stanovanjskega kredita*. <https://www.ip-rs.si/mnenja-gdpr/obdelava-op-v-namen-odobritve-stanovanjskega-kredita-1655723709>

Ministrstvo za digitalno preobrazbo (2023). *Akt o digitalnih storitvah: Evropska komisija objavila seznam zelo velikih spletnih platform in iskalnikov*. <https://www.gov.si/novice/2023-04-25-akt-o-digitalnih-storitvah-evropska-komisija-objavila-seznam-zelo-velikih-spletnih-platform-in-iskalnikov/>

Podpečan, M. (2019). Avtomatizirano odločanje in pravni položaj posameznika. *Pravna praksa*, 38(9-10), 13–15.

Trstenjak, V. (2022). Umetna inteligenca in pravo: kdaj in kako bo sodil robot. *Podjetje in delo*, 48(6-7), 902.

Reset Australia (2021). *Profiling children for advertising: Facebook's monetisation of young people's personal data*. <https://au.reset.tech/news/profiling-children-for-advertising-facebooks-monetisation-of-young-peoples-personal-data/>

Služba Vlade Republike Slovenije za digitalno preobrazbo (2022). *V veljavo stopil evropski Akt o digitalnih storitvah*. <https://www.gov.si/novice/2022-11-16-v-veljavo-stopil-evropski-akt-o-digitalnih-storitvah/>

Smernice o avtomatiziranem sprejemanju posameznih odločitev in oblikovanju profilov za namene Uredbe (EU) 2016/679, Delovna skupina za varstvo podatkov iz člena 29.

Weber, R. H. (2017). Challenges for communications in a changing legal landscape. V D. Weisenhaus in S. Young, *Media Law and Policy in the Internet Age*. Hart Publishing.

Pravna ureditev odgovornosti za škodo, povzročeno z umetno inteligenco v Sloveniji

Asja Lešnik  

Univerza v Mariboru, Pravna fakulteta

Maribor, Slovenija

Dr. Petra Weingerl 

Univerza v Mariboru, Pravna fakulteta

Maribor, Slovenija

Povzetek: Umetna inteligenca je hitro razvijajoča se skupina tehnologij, ki je družbi prinesla številne družbeno-ekonomske koristi, po drugi strani pa omogoča nastanek novih tveganj in negativnih posledic za posameznike in družbo. Veljavna nacionalna pravila o odškodninski odgovornosti po mnenju mnogih niso primerna za obravnavanje odškodninskih zahtevkov za škodo, ki jo povzroči umetna inteligenca. V luči tega je Evropska komisija pripravila Predlog direktive o prilagoditvi pravil o nepogodbni civilni odgovornosti umetne inteligence, ki bo harmonizirala nacionalne odškodninske sisteme in enotno uredila določena vprašanja odgovornosti za umetno inteligenca (vzročna zveza, razkritje dokazov). Prispevek obravnava pravno ureditev odškodninske odgovornosti za umetno inteligenca v Sloveniji, ki v določeni meri že temelji na pravilih EU, pri čemer analizira pozitivne in negativne vidike veljavne ureditve ter Bottom of Form/Top of Form novosti, ki jih bo prinesla predlagana evropska zakonodaja.

Ključne besede: umetna inteligenca, odškodninska odgovornost, vzročna zveza, dokazovanje, harmonizacija

Legal regulation of civil liability for damage caused by artificial intelligence in Slovenia

Asja Lešnik  

University of Maribor, Faculty of Law
Maribor, Slovenia

Dr. Petra Weingerl 

University of Maribor, Faculty of Law
Maribor, Slovenia

Abstract: Artificial intelligence is a set of enabling technologies which can contribute to a wide array of benefits across the entire spectrum of the economy and society. Conversely, it can generate risks and have negative consequences for individuals and society. Many legal experts argue that current national liability rules are not suited to handling liability claims for damage caused by AI-enabled products and services. In light of this, the European Commission has prepared a Proposal for a Directive on adapting non-contractual civil liability rules to artificial intelligence (AI Liability Directive), which will harmonize national civil systems and uniformly regulate certain issues of responsibility for artificial intelligence (causal link, disclosure of evidence). This Article examines the legal regulation of liability for artificial intelligence in Slovenia, which to some extent already relies on EU rules, analyzing the positive and negative aspects of the existing regulation and the changes that the proposed European legislation will bring.

Keywords: artificial intelligence, civil liability, causal link, evidence, harmonization

1 Uvod

Umetna inteligenca je v zadnjih letih doživela hiter razvoj in postala eden pomembnejših dejavnikov v številnih vidikih sodobnega življenja. Hkrati je pred nas postavila mnoge izzive, med drugim tudi vprašanje, kdo bo odgovarjal za škodo, ki jo bodo povzročili umetnointeligenčni sistemi. Odškodninska odgovornost za umetno inteligenco v Evropski uniji (EU) trenutno temelji na dveh stebrih: ureditvi v Direktivi 85/374 o približevanju zakonov in drugih predpisov držav članic v zvezi z odgovornostjo za proizvode z napako (v nadaljevanju Direktiva 85/374)¹ ter na drugih neharmoniziranih nacionalnih ureditvah odškodninske odgovornosti. Obstajajo pa tudi določene specialne področne ureditve, ki vplivajo na odškodninsko odgovornost za škodo, ki jo povzročijo umetnointeligenčni sistemi, npr. Splošna uredba o varstvu podatkov (GDPR)². Evropski zakonodajalec želi v luči tveganj, ki jih prinaša uporaba umetnointeligenčnih sistemov, prilagoditi obstoječo sekundarno zakonodajo in dodatno harmonizirati določene vidike nacionalnih odškodninskih sistemov, da bi se čim enotneje uredilo vprašanje odškodninske odgovornosti po celotni EU.

Pristop EU je osredotočen na tveganja, ki jih prinaša umetna inteligenca. V tem kontekstu je bila 13. 3. 2024 sprejeta Uredba Evropskega parlamenta in Sveta o določitvi harmoniziranih pravil o umetni inteligenci (v nadaljevanju Akt o umetni inteligenci)³, ki je zasnovana tako, da se tveganja, ki jih prinašata avtonomnost in nepreglednost sistemov umetne inteligence za nacionalna pravila odškodninskega prava, rešujejo na podlagi pristopa, ki temelji na stopnji tveganja. Akt o umetni inteligenci razlikuje med uporabami umetne inteligence, ki ustvarjajo (i) nesprejemljivo tveganje, (ii) veliko tveganje in (iii) majhno tveganje (Weingerl, 2023, str. 368).

Kljub naslavljanju tveganj, ki jih prinaša umetna inteligenca, pa se ta tveganja lahko uresničijo in s tem pride do škode. Za primer nastanka škode zaradi ravnanja umetnointeligenčnih sistemov je po veljavni ureditvi zaenkrat harmoniziran le vidik producerske odgovornosti za ravnanje

¹ Direktiva Sveta z dne 25. julija 1985 o približevanju zakonov in drugih predpisov držav članic v zvezi z odgovornostjo za proizvode z napako, Uradni list Evropske unije L 210, str. 29–33.

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), Uradni list Evropske unije L 119/1, str. 1–88.

³<https://www.europarl.europa.eu/news/sl/press-room/20240308IPR19015/akt-o-umetni-inteligenci-postanci-sprejeli-prelomno-zakonodajo>

umetnointeligentnih sistemov (z Direktivo 85/374), zato bo v prispevku najprej predstavljen ta vidik. V nadaljevanju prispevka bodo predstavljene predlagane spremembe na ravni EU glede obstoječe ureditve producerske (objektivne) odgovornosti, ki je v veljavi že skoraj 40 let in naj ne bi bila prilagojena novi realnosti, kot tudi predlagane novosti glede določenih vidikov krivdne odgovornosti. Prispevek bo naslovil tudi druge *lex specialis* ureditve odškodninske odgovornosti, kot je npr. odškodninska odgovornost v povezavi s kršitvijo GDPR.

Čeprav so predlogi evropskega zakonodajalca še v fazi sprejemanja, lahko pričakujemo, da bodo imeli pomembne posledice za pravno ureditev odškodninske odgovornosti za umetnointeligentne sisteme tako v Sloveniji kot v ostalih državah članicah EU.

2 Odgovornost proizvajalca za stvari z napako

Trenutni režim nepogodbene odškodninske odgovornosti za ravnanje umetne inteligence v slovenskem pravnem sistemu temelji na producerski odgovornosti, ki je urejena kot objektivna odgovornost proizvajalca za stvari z napako v prvem odstavku 155. člena Obligacijskega zakonika (v nadaljevanju OZ)⁴. Ta določa, da kdor da v promet kakšno stvar, ki jo je izdelal, pa pomeni zaradi kakšne napake škodno nevarnost za osebe ali stvari, odgovarja za škodo, ki nastane zaradi take napake. Za potrošnike se uporablja Zakon o varstvu potrošnikov (v nadaljevanju ZVPot-1)⁵, ki je implementiral Direktivo 85/374. Cilj te direktive je glede vprašanj, ki jih ureja, doseči popolno harmonizacijo zakonskih in drugih predpisov držav članic (C-285/08, 2009, točka 25), kar pomeni, da države članice razen v določenih izjemah ne smejo odstopati od ureditve v direktivi.

Iz njene osemnajste uvodne izjave pa je razvidno, da glede tega, kar presega okvir teh vprašanj, ni namenjena izčrpani harmonizaciji področja odgovornosti za proizvode z napako (Szpunar, 2018, str. 6). Direktiva je namreč ostala nespremenjena od njenega sprejema leta 1985, zaradi česar po mnenju mnogih ni prilagojena uporabi primerom odškodninske odgovornosti za umetno inteligenco (Koch, 2022, str. 28).

Direktiva 85/374 sicer določa objektivno odgovornost proizvajalca, pri čemer mora skladno z 61.

⁴ Uradni list RS, št. 97/07 – uradno prečiščeno besedilo, 64/16 – odl. US in 20/18 – OROZ631.

⁵ Uradni list RS, št. 130/22.

členom ZVPot-1 oškodovanec dokazati napako, škodo in vzročno zvezo med njima.⁶ Proizvajalec izdelka z napako mora skladno z 9. členom Direktive 85/374 plačati odškodnino za škodo za smrt in telesno poškodbo, ki jo povzroči izdelek z napako, ter tudi za škodo na zasebni lastnini, pri čemer je Evropski parlament izrazil stališče, da se škoda ne bi smela omejevati glede na vrsto in obseg ter glede oblike nadomestila škode, ki je nastala oškodovancu (Weingerl, 2020, str. 1195).

Za pripis odgovornosti proizvajalcu je pomembna opredelitev proizvoda. Proizvod oz. blago je skladno s 4. členom ZVPot-1 in 2. členom Direktive 85/374 vsaka premična stvar, tudi če je del druge premične stvari ali je povezana z nepremično stvarjo, vključno z električno energijo. Definicija proizvoda je že po trenutni ureditvi dokaj široka in lahko zajame tudi sisteme umetne inteligence, pri čemer pa je zaradi pravne varnosti treba definicijo proizvoda jasneje opredeliti (Weingerl, 2020, str. 1195).

Proizvod ima po 60. členu ZVPot-1 in 6. členu Direktive 85/374 napako, kadar njegova varnost ni takšna, kot jo potrošnik lahko upravičeno pričakuje, pri čemer je treba upoštevati zlasti predstavitev proizvoda glede na njegovo namembnost, predvidljivo uporabo proizvoda na razumen način in čas, ko je bil proizvod dan v promet. Dokazno breme tako glede napake na proizvodu kot nastale škode in vzročne zveze med njima po veljavni ureditvi nosi oškodovanec. Taka ureditev v primeru škode, ki jo povzroči umetna inteligenca, zaradi njene kompleksnosti ni primerna. Oškodovanci se bodo namreč soočali z velikimi težavami pri dokazovanju napake in vzročne zveze med napako in škodo (Ballell, 2023, str. 256).

V primeru ugotovljene napake je potrošnik, ki je o napaki obvestil prodajalca, upravičen, da zahteva od prodajalca brezplačno vzpostavitev skladnosti blaga. Če prodajalec tega ne stori, ima potrošnik pravico, da zahteva znižanje kupnine v sorazmerju z neskladnostjo ali odstopi od prodajne pogodbe in zahteva vračilo plačanega zneska.⁷ Pri tem je oškodovanec vezan na določene roke, ki so povezani predvsem s potrošnikovim obvestilom proizvajalcu o napaki (jamčevalni zahtevki namreč prenehajo v dveh letih od dneva, ko je potrošnik o neskladnosti blaga

⁶ ZVPot je v slovenski pravni sistem sicer implementiral Direktivo 85/374 o približevanju zakonov in drugih predpisov držav članic v zvezi z odgovornostjo za proizvode z napako.

⁷ To sicer velja le za potrošniške pogodbe, sklenjene po 26. 1. 2023. Za pogodbe, ki so bile sklenjene pred tem datumom, se uporablja ZVPot, ki v 37.c členu določa alternativne možnosti potrošnika, ki lahko od prodajalca zahteva, da odpravi napako na blagu ali vrne del plačanega zneska v sorazmerju z napako ali blago z napako zamenja z novim brezhibnim blagom ali vrne plačani znesek.

obvestil prodajalca) in z dnem, ko je bil proizvod dan v promet. 63. člen ZVPot-1 namreč določa, da je proizvajalec odgovoren za škodo, ki jo je povzročilo blago z napako, če je škoda nastala deset let od dneva, ko je blago z napako dal v promet. Vprašanje, ki bi se tukaj lahko postavilo, je, ali je objektivni 10-letni rok primeren tudi za umetnointeligenčne sisteme. Upoštevati je namreč treba dejstvo, da se umetna inteligenca ves čas spreminja, posodablja in razvija.⁸ Tako lahko bistveno spremeni lastnosti proizvoda, vključno z njegovimi varnostnimi značilnostmi, ta pa lahko povzročijo nova tveganja, ki niso bila prisotna, ko je bil sistem dan na trg (Weingerl, 2020, str. 1195). Zaradi navedenega ni smiselno, da bi se za proizvajalca, ki bo umetnointeligenčni sistem ves čas modificiral (in bi teoretično do napak lahko prišlo tudi pozneje), uporabljal 10-letni rok.

Pomembno je, da osebe, ki so utrpeli škodo, povzročeno zaradi uporabe umetne inteligence, uživajo enako raven zaščite kot osebe, ki utrpijo škodo zaradi uporabe drugih tehnologij. Navedeno je zaradi zapletenosti, povezljivosti, nepreglednosti, ranljivosti in avtonomije sistemov umetne inteligence oteženo, saj osebe, ki so utrpeli škodo zaradi sistemov umetne inteligence, pogosto nimajo ustreznega dostopa do informacij in s tem dokazov, da bi lahko dokazale svoj primer na sodišču. Dokazovanje napake in vzročne zveze med napako in nastalo škodo bo pogosto zahtevalo strokovni nasvet, stroški, ki bi zaradi tega nastali, pa lahko oškodovance odvrnejo od vložitve pravnega sredstva (Buiten et al., 2021, str. 55). Zaradi navedenega so lahko v primerjavi s škodo, ki jo povzročijo »tradicionalni« izdelki, zahtevki oškodovancev, ki jim je bila škoda povzročena zaradi umetnointeligenčnih sistemov, manj uspešni, v tej zvezi pa se v ospredje postavlja vprašanje učinkovitega dostopa do pravnega varstva. Vsled navedenemu so bile kljub sicer dobremu delovanju Direktive 85/374 potrebne določene prilagoditve, ki olajšujejo oškodovancev položaj in zmanjšujejo dokazno breme z uporabo razkritja in izpodbojnih domnev (Evropska komisija, 2022a, str. 10).

V nadaljevanju prispevka bodo predstavljene ključne novosti glede odškodninske odgovornosti za sisteme umetne inteligence v EU.

⁸ 7. člen Direktive 85/374 sicer določa t. i. obrambo razvojnega tveganja (angl. *development risk defence*), saj proizvajalec ni odgovoren za škodo, če dokaže, da raven znanosti in tehničnega napredka v času, ko je dal proizvod v promet, ni bila takšna, da bi bilo mogoče odkriti napako na proizvodu (Weingerl, 2020, str. 1195).

3 Novosti evropske zakonodaje

Veljavna nacionalna pravila o odgovornosti, zlasti tista na podlagi krivde, po mnenju mnogih niso primerna za obravnavanje odškodninskih zahtevkov za škodo, ki jo povzročijo umetnointeligentno omogočeni proizvodi in storitve, saj morajo oškodovanci v sistemu krivdne odgovornosti dokazati nezakonitost dejanja osebe, ki je povzročila škodo oz. nezakonitost opustitve njenega dejanja (Evropska komisija, 2022a, str. 1). To pa je pri škodi, ki jo povzročijo umetnointeligentni sistemi, izredno oteženo zaradi njihove kompleksnosti in stalne spremenljivosti (umetnointeligentni sistemi se namreč od svojega nastanka naprej ves čas spreminjajo in posodablajo), zaradi česar je precej bolj kompleksno dokazovanje obstoja napake (v času, ko je bil umetnointeligentni sistem dan v promet) ter vzročne zveze med napako in nastalo škodo (Kerkoč in Jager, 2023, str. 16–17). Zaradi navedenega bi lahko bili oškodovanci pri dokazovanju podvrženi nesorazmernim stroškom (npr. pritegnitve izvedencev), sodni postopki pa bi bili precej daljši kot v odškodninskih zadevah za škodo, ki je ne povzroči umetna inteligenca, zaradi česar bi se malokdo sploh odločil za vložitev odškodninske tožbe. Podobne pomisleke je navedel tudi Evropski parlament v svoji Resoluciji o umetnosti inteligenci v digitalni dobi z dne 3. 5. 2022.

Pred sprejemom evropske zakonodaje bodo nacionalna sodišča pri odškodninskih postopkih zaradi škode, povzročene zaradi umetne inteligence, najverjetneje prilagodila način uporabe obstoječih pravil na osnovi *ad hoc*, da bodo prišla do pravičnega rezultata za oškodovanca, kar pa bo povzročilo pravno negotovost, saj stranke ne bodo vnaprej vedele, na kakšen način bodo sodišča razlagala in uporabljala obstoječa nacionalna pravila o odgovornosti. Brez usklajenih pravil EU se bodo ponudniki, operaterji in uporabniki umetnointeligentnih sistemov na eni strani ter oškodovanci na drugi strani soočali s 27 različnimi ureditvami odgovornosti, kar bo privedlo tudi do različnih ravni varstva in izkrivljanja konkurence med podjetji iz različnih držav članic (Evropska komisija, 2022a, str. 2 in 6).

V luči navedenega je Komisija 28. 9. 2022 pripravila Predlog direktive o prilagoditvi pravil o nepogodbeni civilni odgovornosti umetne inteligence (v nadaljevanju Predlog direktive), ki bo harmonizirala nacionalne odškodninske sisteme in enotno uredila vprašanje odgovornosti za umetno inteligenco ter Predlog Direktive Evropskega parlamenta in Sveta o odgovornosti za proizvode z napako, ki bo razveljavila Direktivo 85/374/EGS.

3.1 Sprememba Direktive 85/374/EGS

Predlog Direktive Evropskega parlamenta in Sveta o odgovornosti za proizvode z napako razveljavnja Direktivo 85/374/EGS o približevanju zakonov in drugih predpisov držav članic v zvezi z odgovornostjo za proizvode z napako, pri čemer upošteva znatne spremembe sodobne družbe, med drugim izdelavo pametnih proizvodov in umetne inteligence. Tudi Predlog direktive o odgovornosti za proizvode z napako posega na področje odgovornosti za umetno inteligenco. Komisija je s tem uporabila celosten pristop k odgovornosti, tako da sta oba predloga direktiv tesno povezana, vendar pa se zahtevki, ki spadajo na njuno področje uporabe, nanašajo na različne vrste odgovornosti (Evropska komisija, 2022a, str. 3). Predlog direktive o odgovornosti za proizvode z napako namreč zajema nekrivdno odgovornost proizvajalca za proizvode z napako, ki privede do odškodnine za nekatere vrste škode, ki so jo utrpeli predvsem posamezniki, medtem ko Predlog direktive o prilagoditvi pravil o nepogodbeni civilni odgovornosti umetne inteligence zajema nacionalne odškodninske zahtevke, ki temeljijo predvsem na krivdi katerekoli osebe z namenom odškodnine za kakršnokoli škodo in katerokoli vrsto oškodovanca.

Oba predloga se tako dopolnjujeta in tvorita splošno učinkoviti sistem civilne odgovornosti. Ta pravila bodo skupaj spodbujala zaupanje v umetno inteligenco (in druge digitalne tehnologije), saj bodo zagotavljala, da oškodovanci prejmejo dejansko odškodnino, če škoda nastane kljub preventivnim zahtevam iz Akta o umetni inteligenci in drugim varnostnim pravilom (Evropska komisija, 2022a, str. 11).

3.2 Predlog direktive o prilagoditvi pravil o nepogodbeni civilni odgovornosti umetne inteligence

Predlog direktive prinaša novosti v zvezi z vprašanjem dokaznega bremena in posebnih značilnosti umetne inteligence. V zvezi s tem Predlog direktive zelo ciljno usmerjeno in sorazmerno zmanjšuje dokazno breme z uporabo razkritja dokazov in izpodbojnih domnev (Evropska komisija, 2022a, str. 11).

3.2.1 Razkritje dokazov in izpodbojna domneva o neizpolnjevanju dolžnosti

Za tiste, ki zahtevajo odškodnino, Predlog direktive določa možnost, da pridobijo informacije o umetno-inteligenčnih sistemih velikega tveganja, ki jih bo treba evidentirati in dokumentirati v skladu z Aktom o umetni inteligenci. Predlog direktive namreč v prvem odstavku 3. člena določa,

da lahko sodišče odredi razkritje zadevnih dokazov o specifičnih umetnointeligenčnih sistemih velikega tveganja, za katere se sumi, da so povzročili škodo. Sodišče zahtevo naslovi na ponudnika ali na uporabnika umetnointeligenčnega sistema⁹. Zahteva mora biti podprta z dejstvi in dokazi, ki zadostujejo za ugotovitev verodostojnosti predvidenega odškodninskega zahtevka in mora biti odrejena le v tolikšnem obsegu, kot je potreben za utemeljitev zahtevka, s čimer se omejuje razkritje dokazov, preprečuje splošne zahteve po razkritju in ščiti poslovne skrivnosti ali zaupne informacije. Drugi odstavek zadevnega člena določa, da lahko tožeča stranka od ponudnikov ali uporabnikov, ki niso tožene stranke, zahteva razkritje dokazov le, če so bili vsi sorazmerni poskusi zbiranja dokazov od tožene stranke neuspešni. Da bi bila sodna sredstva učinkovita, tretji odstavek določa, da lahko sodišče odredi tudi zavarovanje takih dokazov.

Nadalje peti odstavek vzpostavlja domnevo o neizpolnjevanju dolžnosti skrbnega ravnanja in določa, da če tožena stranka ne izpolni odredbe nacionalnega sodišča v odškodninskem zahtevku, naj razkrije ali zavaruje dokaze, ki jih ima na razpolago, nacionalno sodišče domneva, da tožena stranka ni izpolnila ustrezne dolžnosti skrbnega ravnanja. Tožena stranka ima pravico izpodbijati to domnevo s predložitvijo nasprotnih dokazov. Cilj ukrepa iz tega člena je spodbuditi razkritje, pa tudi pospešiti sodne postopke (Evropska komisija, 2022a, str. 13).

3.2.2 Domneva vzročne zveze v primeru krivde

Tožeča stranka mora za odškodninsko odgovornost dokazati krivdno ravnanje tožene stranke v skladu z nacionalnimi pravili ali veljavnimi pravili EU. Krivda v primeru odgovornosti za škodo, ki jo povzročijo umetnointeligenčni sistemi, pomeni neizpolnjevanje dolžnosti skrbnega ravnanja v skladu z Aktom o umetni inteligenci ali drugimi pravili.¹⁰ Tožeče stranke lahko imajo v praksi težave pri dokazovanju vzročne zveze med tovrstnim neizpolnjevanjem dolžnosti skrbnega ravnanja in izhodnimi podatki, ki jih ustvari (oz. jih ne ustvari) umetnointeligenčni sistem in ki povzročijo zadevno škodo. Predlog direktive v prvem odstavku 4. člena je zato vzpostavil

⁹ Akt o umetni inteligenci opredeljuje »ponudnika« kot fizično ali pravno osebo, javni organ, agencijo ali drugo telo, ki razvije umetnointeligenčni sistem ali ima umetnointeligenčni sistem, razvit za dajanje na trg ali v uporabo pod svojim imenom ali blagovno znamko, bodisi za plačilo bodisi brezplačno. »Uporabnik« pomeni vsako fizično ali pravno osebo, javni organ, agencijo ali drug organ, ki umetnointeligenčni sistem uporablja v svoji pristojnosti, razen kadar se umetnointeligenčni sistem uporablja v okviru osebne nepoklicne dejavnosti.

¹⁰ Sodišče lahko krivdo domneva tudi na podlagi neizpolnitve sodne odredbe za razkritje ali zavarovanje dokazov v skladu s petim odstavkom 3. člena Direktive (glej razdelek 3.1.1).

izpodbojno domnevo vzročnosti. Taka domneva je po mnenju predlagatelja Direktive najmanj obremenjujoči ukrep za obravnavanje potrebe po pravični odškodnini oškodovancu.¹¹ Kljub temu je primerno uvesti domnevo vzročnosti le, kadar se lahko šteje, da je dana krivda verjetno vplivala na zadevne izhodne podatke umetnointeligenčnega sistema ali dejstvo, da niso bili ustvarjeni, kar se lahko oceni na podlagi splošnih okoliščin primera. Hkrati mora tožeča stranka še vedno dokazati, da je umetnointeligenčni sistem (tj. njegovi izhodni podatki ali dejstvo, da izhodni podatki niso bili ustvarjeni) povzročil škodo (Evropska komisija, 2022a, str. 14).

4. člen Direktive torej v prvem odstavku določa domnevo vzročne zveze, če so izpolnjeni naslednji pogoji:

- (a) tožeča stranka je dokazala, ali je sodišče v skladu s členom 3(5) domnevalo krivdo tožene stranke ali osebe, za ravnanje katere je odgovorna tožena stranka, in sicer neizpolnjevanje dolžnosti skrbnega ravnanja, določene v pravu Unije ali nacionalnem pravu, ki je neposredno namenjena zaščiti pred nastalo škodo;
- (b) na podlagi okoliščin primera se lahko šteje za razumno verjetno, da je krivda vplivala na izhodne podatke, ki jih je ustvaril umetnointeligenčni sistem, ali na to, da umetnointeligenčni sistem ni ustvaril izhodnih podatkov;
- (c) tožeča stranka je dokazala, da so izhodni podatki, ki jih je ustvaril umetnointeligenčni sistem, ali dejstvo, da umetnointeligenčni sistem ni ustvaril izhodnih podatkov, povzročili škodo.

V primeru umetnointeligenčnega sistema velikega tveganja določa četrti odstavek 4. člena izjemo od domneve vzročnosti, kadar tožena stranka dokaže, da je tožeči stranki razumno na voljo dovolj dokazov in strokovnega znanja, da dokaže vzročno zvezo. Ta možnost lahko tožene stranke spodbudi k temu, da izpolnijo svojo obveznost razkritja (Evropska komisija, 2022a, str. 14).

V primeru umetnointeligenčnega sistema, ki ni umetnointeligenčni sistem velikega tveganja, se skladno s petim odstavkom 4. člena domneva vzročne zveze uporablja le, kadar nacionalno sodišče meni, da je za tožečo stranko vzročno zvezo pretirano težko dokazati.

¹¹ Evropski zakonodajalec se na drugi strani ni odločil k obrnitvi dokaznega bremena, saj ne želi, da bi bili ponudniki, operaterji in uporabniki umetnointeligenčnih sistemov izpostavljeni večjim tveganjem glede odgovornosti, saj bi to lahko zaviralno vplivalo na inovacije in razvoj umetnointeligenčnih sistemov (Evropska komisija, 2022a, str. 6–7).

V primerih, ko tožena stranka uporablja umetnointeligenci sistem v okviru osebne nepoklicne dejavnosti, šesti odstavek 4. člena določa, da se domneva vzročnosti uporablja le, če je tožena stranka bistveno posegla v pogoje delovanja umetnointeligence sistema ali če je bila tožena stranka zavezana in sposobna določiti pogoje delovanja umetnointeligence sistema, vendar tega ni storila. Ta pogoj je utemeljen s potrebo po uravnoteženju interesov oškodovancev in nepoklicnih uporabnikov, tako da se iz uporabe domneve vzročnosti izvzamejo primeri, v katerih nepoklicni uporabniki s svojim ravnanjem ne povečujejo tveganja (Evropska komisija, 2022a, str. 14).

4 Lex specialis ureditve odškodninske odgovornosti

4.1 Odškodninska odgovornost v povezavi s kršitvijo GDPR

Varstvo osebnih podatkov pri obdelavi osebnih podatkov je temeljna pravica, ki jo varuje že primarno pravo EU, natančneje 8. člen Listine EU o temeljnih pravicah in 16. člen Pogodbe o delovanju Evropske unije. Oba člena v prvem odstavku določata, da ima vsakdo pravico do varstva osebnih podatkov, ki se nanašajo nanj. V Republiki Sloveniji je varstvo osebnih podatkov urejeno z GDPR in ZVOP-2 (Weingerl, 2023, str. 368).

Tudi Akt o umetni inteligenci sega na področje varstva osebnih podatkov, in sicer vsebuje nekatera posebna pravila o varstvu posameznikov pri obdelavi osebnih podatkov v zvezi z omejitvami uporabe umetnointeligence sistemov za biometrično identifikacijo na daljavo v realnem času v javno dostopnih prostorih za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj, pri čemer se Akt o umetni inteligenci glede tega opira na člen 16 PDEU (Evropska komisija, 2021, str. 18–19).

V državah članicah EU je lahko obdelava osebnih podatkov, ki krši GDPR, podlaga za odškodninsko odgovornost po 82. členu GDPR. Ta v prvem odstavku določa, da ima vsak posameznik, ki je utrpel premoženjsko ali nepremoženjsko škodo kot posledico kršitve GDPR, pravico, da od upravljavca ali obdelovalca dobi odškodnino za nastalo škodo. Drugi odstavek istega člena določa, da je vsak upravljavec, vključen v obdelavo, odgovoren za škodo, ki jo povzroči obdelava, ki krši GDPR, in sicer le takrat, kadar ne izpolnjuje obveznosti iz GDPR, ki so posebej naslovljene na obdelovalce, ali kadar je prekoračil zakonita navodila upravljavca ali ravnal v nasprotju z njimi. Skladno s tretjim odstavkom 82. člena GDPR se lahko tako upravljavec

kot obdelovalec ekskulpirata odgovornosti, če dokažeta, da v nobenem primeru nista odgovorna za dogodek, ki je povzročil škodo.

Pri odškodninski odgovornosti v povezavi s kršitvijo GDPR gre za objektivno odgovornost, pri čemer pa GDPR ne določa izčrpnih pravil o predpostavkah odškodninske odgovornosti, zato imajo na tem področju države članice dopolnilno vlogo (Weingerl, 2023, str. 370–371). To področje zato ni popolnoma usklajeno na ravni EU, zaradi česar so možni tudi različni izidi v primerljivih primerih (Schutte, Majewski in Havu, 2021, str. 22–23).

5 Sklep

Pravna ureditev odškodninske odgovornosti za umetno inteligenco v Sloveniji temelji na producentni odgovornosti, kot jo določata ZVPot-1 in OZ. Zaradi pomanjkljivosti ureditve, ki ne upošteva specifičnosti in kompleksnosti umetnointeligentnih sistemov, je evropski zakonodajalec pripravil Predlog direktive o prilagoditvi pravil o nepogodbeni civilni odgovornosti umetne inteligence, ki prinaša novosti v zvezi z dokaznim bremenom z uporabo domneve vzročne zveze in razkritja dokazov. Predlog direktive namreč določa možnost, da oškodovanci pridobijo informacije o umetnointeligentnih sistemih velikega tveganja, poleg tega pa jim z vzpostavitvijo domneve vzročne zveze v primeru krivde olajšuje možnost uspeha z odškodninskimi zahtevki.

Direktiva o prilagoditvi pravil o nepogodbeni civilni odgovornosti umetne inteligence se ne bo uporabljala retroaktivno, temveč samo za odškodninske zahtevke, ki se bodo vložili od datuma prenosa direktive v nacionalni pravni sistem (Evropska komisija, 2022a, str. 12). Do sprejema evropske zakonodaje pa se bodo morala pred nacionalnimi sodišči za škodo, ki jo povzročijo umetnointeligentni sistemi, uporabiti veljavna pravila o nepogodbeni odškodninski odgovornosti.

Predlog direktive je bil sprejet skupaj s Predlogom direktive o odgovornosti za proizvode z napako, in sicer v svežnju, katerega namen je prilagoditi pravila o odgovornosti digitalni dobi in umetni inteligenci ter zagotoviti potrebno usklajevanje med tema dopolnjujočima se pravnima instrumentoma.

Viri

Buiten, M., de Streef A., Peitzl, M. (2021). *EU liability rules for the age of artificial intelligence*. Cerre.eu. https://cerre.eu/wp-content/uploads/2021/03/CERRE_EU-liability-rules-for-the-age-of-Artificial-Intelligence_March2021.pdf

Evropska komisija (2021). *Predlog uredbe Evropskega parlamenta in Sveta o določitvi harmoniziranih pravil o umetni inteligenci (Akt o umetni inteligenci) in spremembi nekaterih zakonodajnih aktov Unije*. <https://eur-lex.europa.eu/legal-content/SL/TXT/?uri=CELEX%3A52021PC0206>

Evropska komisija. (2022a). *Predlog direktive Evropskega parlamenta in Sveta o prilagoditvi pravil o nepogodbeni civilni odgovornosti umetni inteligenci (direktiva o odgovornosti na področju umetne inteligence)*. <https://eur-lex.europa.eu/legal-content/SL/TXT/?uri=CELEX%3A52022PC0496>

Evropska komisija. (2022b). *Predlog direktive Evropskega parlamenta in Sveta o odgovornosti za proizvode z napako*. <https://eur-lex.europa.eu/legal-content/sl/TXT/?uri=CELEX%3A52022PC0495>

Kerkoč, A., Jager, L. (2023). Predlog direktive EU za urejanje civilne odgovornosti umetne inteligence. *Pravna praksa*, 11–12, 16–17.

Koch, B. et al. (2022). Response of the European Law Institute to the public consultation on civil liability – adapting liability rules to the digital age and artificial intelligence. *Journal of European Tort Law*, 13(1), 25–63.

Rodriguez de las Heras Ballell, T., The revision of the product liability directive: a key piece in the artificial intelligence liability puzzle (2023). *ERA Forum* 24, 247–259.

Schütte, B., Majewski, L., Havu, K., Damages liability for harm caused by artificial intelligence – EU law in flux. *Helsinki Legal Studies Research Paper*, 69, 22–23.

Szpunar, M. (2018). *Sklepni predlogi generalnega pravobranilca Macieja Szpunarja v zadevi C-105/17*. <https://curia.europa.eu/juris/document/document.jsf?jsessionid=FE7B1C415DF2FA1B6A6FA371A49BDD8B?text=&docid=202421&pageIndex=0&doclang=SL&mode=lst&dir=&occ=first&part=1&cid=31071>

Weingerl, P. (2020). Novosti glede odškodninske odgovornosti za umetno inteligenco. *Podjetje in delo*, 6–7, 1195.

Weingerl, P. (2023). Odškodninska odgovornost za uporabo umetne inteligence v delovnem razmerju. *Delavci in delodajalci*, 4/2023/XXIII, 361–378.

(Proti)pravna ravnanja v virtualni resničnosti

Matej Makoter Rožmarin ✉ 

Univerza v Mariboru, Pravna fakulteta
Maribor, Slovenija

Kristjan Zahrastnik 

Univerza v Mariboru, Pravna fakulteta
Maribor, Slovenija

Povzetek: Britanska policija je pred kratkim prvič v svoji zgodovini uvedla preiskavo zoper neznane storilce zaradi storitve spolnega delikta posilstva, storjenega v virtualni resničnosti, pri čemer žrtev ni utrpela nobenih fizičnih poškodb, temveč zgolj duševne bolečine, ki pa naj bi bile povsem primerljive tistim, ki bi jih trpela oseba, če bi bil spolni delikt storjen v živo. V slovenski sodni praksi doslej takšnega primera še ni bilo moč zaslediti, zato se postavlja vprašanje, kakšno zaščito nam v predmetni zadevi sploh nudi slovenski pravni sistem. Prispevek se podrobneje ukvarja z učinkovitostjo in vidiki pravnega varstva v okviru dejanj, storjenih v virtualni resničnosti z vidika kazenskega prava, civilnega prava in ustavnega prava. V kazenskem pravu se kot bistveno postavlja vprašanje ustreznosti in primernosti zaščite, saj se pri spolnem deliktu posilstva zahteva prodorno spolno ravnanje, do česar pa pri v virtualni resničnosti storjenem dejanju ne more priti. Z vidika civilnega prava se prispevek osredotoča na vidik denarne odškodnine kot obliko povrnitve morebitne nastale škode, na področju ustavnega prava pa je v prispevku pojasnjeno, ali gre tudi za ustavno varovano kategorijo.

Ključne besede: virtualna resničnost, pravno varstvo, kazensko pravo, civilno pravo, ustavno pravo

(Il)legal acts in virtual reality

Matej Makoter Rožmarin  

University of Maribor, Faculty of Law
Maribor, Slovenia

Kristjan Zahrastnik 

University of Maribor, Faculty of Law
Maribor, Slovenia

Abstract: For the first time in its history, the British police launched an investigation into unidentified perpetrators for committing the sexual offence of rape in virtual reality, where the victim suffered no physical injuries, only mental anguish, which is said to be comparable to what a person would have suffered, if the sexual offence had been committed in real life. Such a case has not yet been seen in Slovenian case-law, which raises the question of what protection the Slovenian legal system offers us in the present case. The article highlights the effectiveness of legal protection in the context of acts committed in virtual reality from the perspective of criminal law, civil law and constitutional law. Regarding the criminal law, the question of the appropriateness of protection is a key issue, as the sexual offence of rape requires pervasive sexual conduct, which cannot occur in the case of an offence committed in virtual reality. From a civil law perspective, the paper focuses on the aspect of monetary damages as a form of compensation for any harm suffered, and from a constitutional law perspective, the paper clarifies whether this is also a constitutionally protected category.

Keywords: virtual reality, legal protection, criminal law, civil law, constitutional law

1 Uvod

Na začetku leta 2024 je britanska policija pričela s preiskovanjem domnevnega virtualnega posilstva. Gre za prvo tovrstno preiskavo, ki je bila sprožena zaradi obtožb žrtve, ki naj bi zaradi neljubega dogodka v virtualnem svetu ostala travmatizirana. Dekle, ki naj bi bilo po poročanju medijev staro okoli 16 let, je trdilo, da je njen avatar – njen digitalni lik (persona) v virtualni resničnosti Metaverse – skupinsko posilila skupina virtualnih spletnih neznancev (Camber, 2024). Žrtev, ki je nosila virtualno-resničnostna (VR) očala je sicer fizično nepoškodovana, saj ni prišlo do fizičnega napada, kljub temu pa naj bi doživela hud šok in utrpela enake duševne psihološke bolečine in strah kot oseba, ki je bila posiljena fizično, torej v resničnem svetu, saj je izkušnja virtualne resničnosti namreč zasnovana tako, da osebo čim bolj približa resničnosti (K. S., 2024).

Metaverse je internetna platforma naslednje generacije, ki si prizadeva ustvariti popolnoma potopni, hiper prostorsko-časovni in samovzdržen virtualni prostor za ljudi, namenjen delu, igri in druženju. To novo digitalno virtualno resničnost omogočajo nedavni napredki v tehnologijah, kot so razširjena realnost, umetna inteligenca in veriženje podatkovnih blokov. A tako kot pri kateri koli drugi novi tehnologiji tudi tukaj obstajajo vgrajena tveganja za zasebnost in varnost, ki jih je treba nasloviti, še preden se zagotovi široko sprejetje Metaversa (Wang idr., str. 319). Prispevek se zato v nadaljevanju ukvarja s tem, kako kazensko, ustavno in civilno pravo (če sploh) varujejo posameznika pred navedenimi ravnanji v virtualni resničnosti in kakšne so pravne možnosti potencialne žrtve.

2 Kazenskopravno varstvo

Že mednarodno kazensko pravo obravnava kazniva dejanja zoper spolno nedotakljivost. V tej luči je ključno omeniti Priporočilo (2002) 5 o varstvu žensk pred nasiljem (P(2002)5, 2002) ki predlaga sprejetje ukrepov na področju kazenskega prava, pa tudi na drugih področjih. V določbi 34. člena zadevnega Priporočila je tako določeno, da mora kazensko pravo inkriminirati vsako nasilje, še zlasti fizično in spolno nasilje. To nasilje mora pomeniti kršitev telesne, psihične in spolne svobode in ne zgolj kršitev morale, dostojanstva in časti (P(2002)5, 34. člen). Nadalje je v določbi 35. člena določeno, da morajo države zagotoviti primerne ukrepe in sankcije zoper storilce, zato je potrebna inkriminacija: 1. posilstva med zakoncema, zunajzakonskima partnerjema ter občasnim sostanovalcema; 2. kakršnegakoli spolnega dejanja zoper osebo, ki ni privolila vanj,

čeprav ni kazala znakov odpora, in 3. kakršnekoli penetracije s čimerkoli v osebo, ki v to ni privolila (P(2002)5, 35. člen). Ključno je v okviru mednarodnega kazenskega prava omeniti še Konvencijo o preprečevanju nasilja nad ženskami in nasilja v družini (Istanbulska konvencija) (MKPNZND, 2014), ki v določbi 36. člena, ki naslavlja spolno nasilje, vključno s posilstvom, in določa, da pogodbenice sprejmejo potrebne zakonodajne ali druge ukrepe za zagotovitev, da se naslednja naklepna dejanja opredelijo kot kazniva: 1. vaginalna, analna ali oralna spolna penetracija v telo druge osebe s katerim koli delom telesa ali predmetom brez njenega privoljenja; 2. izvajanje drugih spolnih dejanj z osebo proti njeni volji; 3. priprava druge osebe v neprostovoljna spolna dejanja s tretjo osebo. V drugem odstavku istega člena pa je določeno še, da mora biti privolitev dana prostovoljno kot izraz svobodne volje osebe, ocenjene v okviru danih okoliščin (MKPNZND, 1. in 2. odst. 36. člena). Navedeni mednarodni pravni viri so pomembni pri podaji ocene, ali je nacionalna ureditev kazenskopravne zakonodaje ustrezna in dejansko uresničuje določbe iz konvencije, ki jo je ratificirala tudi Republika Slovenija.

Za ugotovitev in oceno ustreznosti kazenskopravnega varstva v predmetni zadevi (za potrebe prispevka bo fokus na kaznivih dejanjih zoper spolno nedotakljivost) je, kot v vsakem konkretnem primeru, treba najprej določiti kazenskopravno dobrino, ki se v dotičnem primeru varuje. Kazenskopravna dobrina namreč predstavlja osnovni steber delovanja kazenskopravne represije. Predstavlja podstat, s pomočjo katerega kazensko pravo prepozna potrebe glede uveljavljanja represije in inkriminacije kaznivih dejanj za zaščito različnih vrednot, ki jih družba prepozna kot tiste, ki potrebujejo posebno – kazenskopravno – varstvo. Tako kazenskopravna dobrina po svoji definiciji služi kazenskopravnemu varstvu življenjskih in družbenih vrednot in situacij, za katere se je skozi zgodovinski in družbeni razvoj pojavila potreba po njihovem pravnem normiranju in končno tudi izvajanju represije za doseg določenih legitimnih varstvenih ciljev (Bavcon, 2017, str. 204–205). Za potrebe konkretnega prispevka se osredotočamo predvsem na kazenskopravne dobrine, varovane v okviru inkriminacije posilstva in spolnega nasilja.

Če nadaljujemo, torej kakor hitro zakonodajalec prepozna posamezno družbeno dobrino, za katero se ugotovi, da je vredna in tudi zahteva celotno težo kazenskopravne represije, uzakonjena inkriminacija, preko kazenskopravne dobrine, ki je zavarovana z inkriminacijo določenega ravnanja kot kaznivega dejanja, na koncu omogoča identificirati prepovedano posledico. Ali če v konkretni zadevi ponazorimo bolj plastično na kaznivem dejanju posilstva, ki je v slovenskem pravnem redu inkriminirano v 170. členu Kazenskega zakonika (KZ-1, 2012) (v nadaljevanju KZ-1),

ko je kazenskoppravna dobrina, tj. dovolj jasna spolna samoodločba človeka, ki jo inkriminacija posilstva varuje, s čimer je zato mogoče prepoznati prepovedano posledico, ki bi v navedenem primeru bila torej doseg spolnega občevanja z drugo osebo z uporabo sile, (ker zakon določa v dikciji 170. člena KZ: »prisili osebo«) morebiti na posebno grozovit način (Bavcon, 2017, str. 205).

Kazenskoppravna dobrina kaznivega dejanja posilstva je tako v slovenskem kazenskem pravu dovolj jasna spolna samoodločba človeka. Spolna samoodločba je sicer dobrina izrazito osebne narave (Korošec, 2008, str. 106) ki varuje vsakogar pred neutemeljenimi posegi drugih oseb v njegovo telo z različnimi spolnimi praktikami, ki so lahko tako prodrone ali neprodorne narave, posamezniku pa je priznana tudi, da se sam odloča, ali bo aktivno udeležen v spolnih ravnanjih, s kom vse bo vstopal v najrazličnejše spolne odnose in kakšni konkretno naj bodo ti odnosi, tj. katera ravnanja vse bodo obsegali, s čimer je tako posamezniku priznana pravica, da sam določa obseg in meje posegov, ki jih sam dovoljuje in ki se jim je tudi pripravljen podvreči (Korošec, 2008, str. 113–114). Pogosto je sicer mogoče srečati poudarek, da je poleg splošne spolne samoodločbe človeka posebna kazenskoppravna dobrina inkriminacije posilstva glede na njeno osredotočenost na prodorna spolna ravnanja še varovanje človekove notranjosti pred spolnim ponižanjem. Tudi v primeru kaznivega dejanja splošnega spolnega prisiljenja oz. spolnega nasilja po 171. členu KZ-1 je kazenskoppravna dobrina dovolj jasna spolna samoodločba človeka (Korošec, Novak & Zgaga Markelj, str. 1058).

Pogoj za kaznivost spolnega ravnanja po novem 170. členu KZ-1, noveliranega z novelo KZ-1H, tj. za potrebe posilstva ustrezno prodornega (imisivnega) spolnega ravnanja (občevanja), je odsotnost privolitve osebe, ki bo bodisi pasivno ali aktivno vključena v takšno spolno občevanje (Korošec, Novak & Zgaga Markelj, 2023, str. 1154). V predmetni zadevi, s katero se je soočila britanska policija, seveda gre več kot očitno za izostanek privolitve žrtve, katere avatar je bil skupinsko posiljen, sama pa po vsej verjetnosti česa takega v Metaversu tudi ni mogla pričakovati. Kljub temu da pri vseh novih tehnologijah obstajajo določena tveganja, verjetno ni nihče predvideval, da se bodo skupinska posilstva začela pojavljati tudi v virtualni resničnosti, saj Metaverse kot takšen temu prvenstveno zagotovo ni bil namenjen.

Ključno za ugotovitev, ali je t. i. virtualno posilstvo, kot ga pojmujejo mediji, mogoče zajeti v kazenskoppravno opredelitev posilstva, pa je opredelitev spolnega ravnanja, ki je tudi ključna razlika od splošneje opisanega kaznivega dejanja po 171. členu KZ. V teoriji spolnega kazenskega prava je tako implicitno opredeljen vstop v notranjost telesa, gre torej za prodorno (imisivno),

konkretnije medosebno prodorno spolno praktiko kot obliko najtežjega ponižanja človeka s spolnim ravnanjem. Kot vstopna točka v telo se (to velja npr. tudi za konkretni primer) največkrat omenja ženska nožnica, ni pa to nujno. Pravna teorija kot primere navaja tudi druge telesne odprtine, npr. usta ali zadnjik, ki že po naravi stvari niso samo ženska. Kot sredstvo vstopa pa se največkrat omenja moški spolni ud, to pa spet ni edini del človeškega telesa – po novejši kazenskopravni teoriji bi lahko prišle v poštev tudi druge stvari, če celotno dogajanje doseže standard spolnega ravnanja (Korošec, Novak & Zgaga Markelj, 2023, str. 1059). V primeru virtualnega posilstva seveda v nobenem primeru že iz narave stvari ni mogoče, da bi prišlo do imisivne oz. prodorne spolne praktike, zato bi iz navedenega sodeč konkretno dogajanje zelo težko kvalificirali za kaznivo dejanje posilstva, saj manjka ključno prodorno ravnanje storilca in vstop v notranjost telesa žrtve, s čimer odpade ključni opredelilni element kaznivega dejanja posilstva.

Nadalje se zato pojavi vprašanje, ali bi bilo mogoče opredeliti dogajanje virtualnega posilstva kot spolno nasilje, kot ga ureja določba 171. člena KZ-1. Kot že omenjeno, je tudi v primeru kaznivega dejanja spolnega nasilja kazenskopravna dobrina dovolj jasna spolna samoodločba posameznika (Korošec, Novak & Zgaga Markelj, str. 1154). V kaznivem dejanju spolnega nasilja so zajete vse alternativne oblike kaznivega dejanja spolnega nasilja in so že po določbi zakona (glej I. odst. 171. člena KZ-1, ki določa »kakšno spolno dejanje, ki ni zajeto v prejšnjem členu«) izrecno subsidiarne glede na primarno, kvalificirano obliko tega nasilja, imenovano posilstvo, urejeno v 170. členu KZ-1 (Korošec & Novak, 2023, str. 1174).

Bit kaznivega dejanja spolnega nasilja po določbi 171. člena KZ-1 zajema spolna ravnanja z medtelesnim stikom, kot tudi taka brez njega, pod pogojem, da so medosebna. Če ga primerjamo s primernim, specialnim, kvalificiranim kaznivim dejanjem posilstva, lahko ugotovimo, da spolno dejanje po 171. členu KZ-1 ne zajema klasičnega spolnega nožničnega prodornega (imisivnega) kontaktnega ravnanja. Tako je mogoče razumeti, da ostanejo spolnemu nasilju, opredeljenem v 171. členu, tehnično gledano neprodorna kontaktna medosebna spolna ravnanja in nekontaktna medosebna ravnanja, dokler jih je moč opredeliti za spolna (Korošec & Novak, 2023, str. 1183).

Pravna teorija za spolno ravnanje za potrebe kaznivega dejanja spolnega nasilja po določbi 171. člena KZ-1 zahteva telesnost. Upoštevajo se lahko tako zgolj ravnanja na telesu (ne nujno žrtvinim), vendar telesni stik za pojem spolnega ravnanja med osebami ni potreben. Glavni opredelilni element telesnosti pa torej pomeni, da npr. opolzko govorjenje, kazanje in opazovanje

še tako spolnih podob ali golo poziranje v opolzkih položajih ni spolno ravnanje (Korošec & Novak, 2023, str. 1185). Tako se v luči navedenega lahko sprašujemo, ali je virtualno »posilstvo« mogoče podrediti pod kaznivo dejanje spolnega nasilja. Manjka namreč element telesnosti, saj se je vse dogajalo na daljavo, tj. s pomočjo VR-očal, zato bi bilo problematično trditi, da je prišlo do kakršnega koli telesnega stika, ali okvalificirati celotno dogajanje za ravnanje na telesu, saj je kljub vsemu vse v virtualni resničnosti ustvarjeno z namenom ustvariti navidezni svet, ki pa se bo seveda čim bolj približal resničnemu. Podobno je, četudi ironično, mogoče razbrati tudi iz besed britanskega notranjega ministra Jamesa Cleverlyja, ki je zagovarjal policijsko preiskavo virtualnega posilstva in je tudi sam povedal: »Vem, da je zelo lahko odpraviti ta primer kot nekaj, kar ni resnično, ampak glavna značilnost teh virtualnih okolij je, da dajo neverjeten občutek resničnosti.« (K.S., 2024)

Za kaznivo dejanje spolnega nasilja gre tudi pri spolnih ravnanjih brez stika z drugim telesom, nemedtelesnih medosebnih ravnanjih, če jih je seveda mogoče opredeliti kot spolna ravnanja, kjer pa se značilno zahteva manipuliranje z lastnim telesom, npr. vtikanje predmetov v lastne telesne odprtine, dodatni pogoj, ki izhaja iz sodobnega spolnega kazenskega prava, pa je za spolna ravnanja pred žrtvijo, da mora žrtev dogajanje tudi zaznavati (Korošec & Novak, str. 1190). Iz vsega skupaj je zato mogoče izpeljati, da slovenska kazenskopravna ureditev vseeno tudi v tem primeru, tj. nemedtelesnih medosebnih ravnanjih, zahteva določeno mero telesnosti, tj. vsaj ravnanja na lastnem telesu, do česar pa seveda pri virtualnem posilstvu v nobenem primeru spet ne more priti. Kljub temu da je žrtev celotno dogajanje zaznavala, do njega pač ni prišlo neposredno v resničnosti.

Iz konkretnega dogodka pa prav tako ne izhaja, da bi bili izpolnjeni zakonski znaki za katero izmed preostalih kaznivih dejanj zoper spolno nedotakljivost v določbah členov 172–176., tj. spolna zloraba slabotne osebe, spolni napad na osebo, mlajšo od 15 let, pridobivanje oseb, mlajših od 15 let za spolne namene, kršitev spolne nedotakljivosti z zlorabo položaja, zloraba prostitucije ali prikazovanje, izdelava, posest in posredovanje pornografskega gradiva, s čimer zato ni mogoča subsumpcija konkretnega ravnanja, tj. virtualnega posilstva pod ta kazniva dejanja.

Slovenska nacionalna ureditev kazenskopravne zakonodaje je ustrezna in skladna s Priporočilom (2002) 5 o varstvu žensk pred nasiljem in Konvencijo o preprečevanju nasilja nad ženskami in nasilja v družini (Istanbulska konvencija). Navkljub temu pa se samoodločba človeka kot kazenskopravno varovana dobrina ne razteza na spolna ravnanja, ki so storjena v virtualnem

svetu, četudi gre za izostanek privolitve žrtve v takšna ravnanja. Seveda pa slednje ne pomeni, da takšna ravnanja niso protipravna v smislu ustavno- ali civilnopravnega varstva.

3 Ustavnopravno varstvo

V okviru ustavnopravnega varstva je najprej pomembno poudariti, da je bila pravna dobrina spolne samoodločbe kot kazenskopravne dobrine, ki je bila prej omenjena v zvezi s kaznivima dejanjema posilstva in spolnega nasilja, izrecno obravnavana v povezavi z dostojanstvom človeka, obravnavana tudi na ustavnosodni ravni. Ustavno sodišče je v odločbi Up-320/14, U-I-5/17, z dne 14. septembra 2017 navedlo, da izvršitev kaznivega dejanja zoper oškodovanca lahko pomeni hud poseg v njegovo pravno zavarovano dobrino in njegovo dostojanstvo. Še posebej to velja za tista kazniva dejanja, ki so bila predmet obtožbe v sprožilnem primeru in ki pomenijo poseg v dobrino varnosti, telesne in duševne celovitosti ter časti in dobrega imena posameznika (Up-320/14, U-I-5/17, tč. 21–23).

Vse zgoraj navedene pravice, kot tudi 34. člen Ustave Republike Slovenije (URS, 1991) (v nadaljevanju URS), ki določa pravico do osebnega dostojanstva in varnosti, spadajo v skupino temeljnih in izhodiščnih pravic ter skupino osebnostnih pravic in svoboščin. Slednje so namenjene varstvu človekovega osebnega dostojanstva, osebnostnih pravic, človekove zasebnosti in varnosti (glej U-I-25/95, tč. 32). 34. člen URS se sicer glede na ustavnosodno presojo najtesneje povezuje z določbami o varstvu osebnostnih pravic iz 35. člena URS. Osebnostne pravice so pravice, ki pripadajo človeku kot bitju in varujejo njegove temeljne dobrine ter njegovo osebnost. So individualne pravice, ki imajo osebno in nepremoženjsko naravo ter pripadajo človeku od rojstva naprej. So pravice, ki varujejo zoper vsakogar, ki vanje posega, zato jih prištevamo k absolutnim pravicam (Novak v Juhart idr., 2011, str. 117). Obstaja več vrst osebnostnih pravic, prof. dr. Finžgar tako navaja sledeče pravice: »Pravica do časti in dobrega imena, pravica do osebne identitete, pravica na lastni podobi, pravica do osebnega življenja, pravica do duševne integritete in druge.«(Finžgar, 1985, str. 65–136) Zanje je značilno, da gre za varstvo osebnih dobrin v razmerju do posameznika predvsem s sredstvi in metodami civilnega prava, posamezna pravna osebna dobrina pa je lahko tudi predmet varstva s predpisi drugih pravnih panog, npr. kazenskega prava (Pavčnik, Polajnar Pavčnik & Wedam Lukič, 1997, str. 150). Da bi se zagotovilo čim celovitejše varstvo človekove osebnosti, so osebnostne pravice v 35. členu URS varovane z generalno klavzulo, ponazorjeno s posamičnimi primeri osebnostnih

pravic, kot so npr. nedotakljivost človekove telesne in duševne celovitosti itd. (Avbelj, 2019, str. 341).

Določba 34. člena URS je namenjena varstvu posameznika tako v vertikalnih razmerjih (tj. država proti posamezniku) kot t. i. horizontalnih razmerjih (posameznik proti posamezniku). Državne oblasti, kot tudi vsi posamezniki, so tako brez izjem dolžni spoštovati pravico do osebnega dostojanstva in varnosti. V tej luči je tako pravica do osebnega dostojanstva in varnosti najprej obrambna pravica pred posegi državne oblasti in posameznikov (Šturm, 2002, str. 363). V odločbi U-I-25/95 je Ustavno sodišče še navedlo, da je v skladu z načelom, da je tu prepovedano vse, kar ni izrecno dovoljeno, po URS tako prepovedan vsak poseg v dostojanstvo, osebnostne pravice, zasebnost in varnost, razen tistih posegov, ki so izrecno dovoljeni (U-I-25/95 tč. 32).

Za človekovo pravico iz 34. člena URS v zvezi s pravico do varnosti Ustavno sodišče navaja, da ta v svojem bistvu pomeni, da nihče ne sme fizično ali psihično protipravno posegati v sfero posameznika, obenem pa je v zvezi s tem državi naložena dolžnost, da si aktivno prizadeva zagotavljati najvišjo mogočo stopnjo varnosti za svoje prebivalce (Up-1082/12, tč. 9). V zadevi U-I-109/10 je Ustavno sodišče še nadaljevalo, da gre člen 34. URS razumeti kot eno izmed določb, preko katere se človekovo dostojanstvo normativno konkretizira, in da človekovo dostojanstvo pomeni, da ima vsak človek enako in absolutno notranjo vrednost, ki mu pripada ravno zato, ker je človek (U-I-109/10 tč. 9). Seveda varstvo po določbah 34. in 35. člena URS ni brezmejno, ampak so pravice omejene s pravicami drugih, kar pomeni, da lahko pride do kolizije pravic. Pravna teorija je izoblikovala več rešitev, vendar je vsem skupno, da je metoda razreševanja konflikta tehtanje nasprotujočih si interesov. V okviru tehtanja je tako treba najprej ugotoviti, kateri pravici sta v konfliktu, nato pa opredeliti ustavno varovano vsebino vsake od njih. Sledi ugotavljanje, katere konkretne okoliščine obravnavanega (življenjskega) primera so pravno pomembne in katere iz človekovih pravic izvirajoče pravice in njih upravičenja so v koliziji. V zadnjem koraku pa se sodišče loti tehtanja v ožjem smislu, ki mora privedi do praktične konkordance (konkretne, praktične uskladitve obeh pravic, njuno uravnoteženje, določitev načina njunega sobivanja oz. na kratko oblikovanje pravila, veljavnega za konkreten primer) (Zobec, 2018, str. 37–39). Če strnemo vse navedeno in apliciramo na konkretni primer, lahko rečemo, da se pri virtualnem posilstvu v okviru praktične konkordance pravica do osebnega dostojanstva in duševne celovitosti žrtve zagotovo ne bo umaknila storilčevi svobodi ravnanja v virtualnem okolju.

Republika Slovenija sicer zagotavlja varnost, tudi preko inkriminacije posilstva in drugih kaznivih dejanj zoper spolno nedotakljivost, a se kljub temu v konkretni zadevi soočimo z zagato, saj virtualnega posilstva, kot je že bilo zapisano zgoraj, ni mogoče okvalificirati kot katerega izmed navedenih kaznivih dejanj. V navedenem primeru »virtualnega posilstva« pa je, navkljub temu da ne gre za kaznivo dejanje, skoraj z gotovostjo mogoče trditi, da je prišlo do posega v pravico do osebnega dostojanstva in varnosti, kot izhaja iz določbe 34. člena URS. Iz poročanj medijev pa lahko razberemo, da je bila prizadeta tudi duševna celovitost žrtve, ki jo ureja določba 35. člena URS (zagotovljena je nedotakljivost človekove telesne in duševne celovitosti, njegove zasebnosti ter osebnostnih pravic). Varstvo osebnostnih pravic se zagotavlja v okviru civilnopravnega varstva, ki bo podrobneje opisano v nadaljevanju.

4 Civilnopravno varstvo

S posegom v osebnostne pravice žrtve, ki je po dogajanju virtualnega posilstva njenega avatarja doživela travme in duševne bolečine, je prišlo do posega v njeno osebno sfero. V primeru, da ji je zaradi tega nastala negmotna škoda, ji pripada denarna odškodnina za nepremoženjsko obliko prikrajšanja. Tudi v slovenskem pravnem redu namreč žrtvi zaradi duševnih bolečin, posega v osebnostne pravice (v predmetni zadevi predvsem nedotakljivost duševne celovitosti in osebno dostojanstvo ter varnost) in za strah v skladu s prvim odstavkom 179. člena Obligacijskega zakonika (OZ, 2007) pripada denarna odškodnina. Duševne bolečine zaradi okrnitve osebnostnih pravic, ki jih je doživljala žrtev, so s tem umeščene med pravno priznane oblike nepremoženjske škode, ki upravičujejo prisajo pravične denarne odškodnine (VSRS II DoR 61/2012, tč. 3). Z umestitvijo zakonodajalec tudi dosledno izenačuje vse posamezne osebnostne pravice. V predmetni zadevi je mogoče trditi, da je žrtev trpela tudi občutek strahu. Strah spremljajo somatski, še posebej nevrovegetativni znaki in spremembe, ki jih oseba doživlja kot bolj ali manj močne čustvene doživljaje. V sodni praksi se je uveljavilo tudi razlikovanje med primarnim in sekundarnim strahom. S primarnim se označuje strah, ki nastane neposredno ob škodnem dogodku, s sekundarnim pa strah, do katerega je prišlo pozneje, a je njegov nastanek v vzorčni zvezi s škodnim dogodkom (VSC Cp 416/2019, tč. 8). Strah je sicer motnja človekovega čustvenega dožemanja. Pojavi se, ko je ogroženo življenje (VSL I Cp 1058/2019, tč. 10). Do navedenega je prišlo tudi v primeru virtualnega posilstva prizadete osebe, saj je žrtev, kot že zgoraj omenjeno, doživljala enake občutke, kot če bi doživela posilstvo v resničnem življenju.

Poseg v osebnostne pravice žrtve in povzročitev nematerialne škode tako pomeni civilni delikt, ki ima za posledico, kot že omenjeno, odškodninsko odgovornost. Na podlagi načela *neminem laedere* (10. člen OZ) se morajo posamezniki vzdržati ravnanja, iz katerega utegne drugemu nastati škoda. Kdor pa škodo povzroči, jo je dolžan povrniti, razen če dokaže, da ta ni nastala po njegovi krivdi (1. odstavek 131. člena OZ). Da pa bo odškodninska odgovornost povzročiteljev nastopila, bo morala žrtev, ki je utrpela duševne bolečine in strah v sled virtualnega posilstva dokazati predpostavke za nastop odškodninske odgovornosti. Za nastop odškodninske obveznosti povzročitelja morajo biti kumulativno izpolnjene štiri predpostavke, ki so 1. nedopustno ravnanje, ki izvira iz sfere povzročitelja, 2. škoda, 3. vzročna zveza med nedopustnim ravnanjem in nastalo škodo ter 4. krivda (VSRS II Ips 671/2008, tč. 4).

Pri presoji nedopustnega ravnanja se uporabijo merila dolžne skrbnosti iz 6. člena OZ na podlagi primerjave konkretnega ravnanja z abstraktnim tipom ravnanja. Z merili skrbnosti se presoja ustreznost strankinega prizadevanja v določeni smeri in ugotavlja, ali je ravnala tako, da ji ni mogoče očitati krivde. Slednja merila se pri presoji protipravnosti uporabljajo bolj objektivno, pri presoji krivde pa bolj subjektivno (Jadek Pensa, 1996, str. 596). Škoda je s pravnega vidika vsakršno prikrajšanje, ki nastane na podlagi zakona, zaradi posega v pravice in pravno zavarovane interese. Odgovoren je lahko le tisti, čigar nedopustnemu ravnanju je mogoče pripisati škodno posledico (vzročna zveza). Presoja vzročne zveze terjaja zgolj pravno relevantne vzroke za nastanek škode (Polajnar Pavčnik, 1993, str. 179) in se lahko izvede na podlagi tradicionalne ekvivalenčne teorije, tej sledeči teoriji *ratio legis* (po teoriji vzročnosti *ratio legis* je pravno odločilen le tisti vzrok, ki obenem pomeni kršitev pravne norme in ga pravna norma glede na svoj cilj šteje za vzrok (VSRS II Ips 588/99, tč. 5) in teoriji adekvatnosti (če zatrjevani škodni dogodek ni bil (objektivno) predvidljiva posledica (takšnega) nedopustnega ravnanja, potem dejanje povzročitelja škode ni v adekvatni (pravno zadostni) vzročni zvezi (VSL II Cp 1139/2012). OZ pozna in ločuje dve obliki odgovornosti, urejeni v 131. členu OZ, in sicer krivdno (subjektivno, deliktno), kjer krivda nastopa kot predpostavka odškodninske odgovornosti, in odgovornost na podlagi vzročnosti (objektivna), za katero se odgovarja ne glede na krivdo (Strohsack, 1996, str. 41). V našem pravnem redu je ustaljeno načelo krivdne odgovornosti z obrnjenim dokaznim bremenom, kar pomeni, da je breme dokazovanja neobstoja krivde na odgovorni osebi, medtem ko oškodovanca bremeni dokazovanje obstoja prvih treh predpostavk (Plavšak, 2003, str. 690 in 694). Po prvem odstavku 131. člena OZ je tisti, kdor drugemu povzroči škodo, le-to dolžan povrniti, če ne dokaže, da je škoda nastala brez njegove krivde. Krivda je podana, kadar oškodovalec povzroči škodo

namenoma ali iz malomarnosti (135. člen OZ). V predmetni zadevi bo tako morala žrtev virtualnega posilstva dokazati, da ji je zaradi protipravnega ravnanja povzročitelja tega virtualnega posilstva nastala nepremoženjska škoda v obliki duševnih bolečin kot pravno priznana oblika nepremoženjske škode in da je ravno ta škoda v vzročni zvezi, tj. kot posledica tega protipravnega ravnanja povzročitelja virtualnega posilstva. Breme dokazovanja neobstoja krivde pa bo doletelo povzročitelja virtualnega posilstva oz. povzročitelje, saj naj bi povzročiteljev, kot izhaja iz konkretnega primera, bilo več.

Seveda se v konkretni zadevi postavlja tudi vprašanje, kdo bi bil pasivno legitimirana stranka v konkretni pravdi. V nedavni zadevi Sanchez proti Franciji je Evropsko sodišče za človekove pravice (v nadaljevanju ESČP) posameznika tako izenačilo z urednikom oz. ponudnikom platforme, kajti kdor ustvari objavo npr. na Facebooku, pod katero lahko drugi komentirajo, vstopi v položaj urednika in je tako odgovoren za to vsebino. V predmetni zadevi sta sicer kazensko poleg Sancheza odgovarjala oba avtorja spornih komentarjev pod njegovo objavo, vendar je ESČP zatrdil, da gre za drugačno odgovornost in da je samo ravnanje avtorjev in pritožnika drugačno. Namen pri presoji pa je sicer ravno ta, da je ponudnik platforme sankcioniran šele po tem, ko avtorjev ni mogoče identificirati oz. ustrezno finančno oglobiti (Sanchez v. France 2023). Gre torej za obliko soodgovornosti, zato bi npr. v predmetni zadevi virtualnega posilstva Metaverse po vsej verjetnosti odgovarjala, a subsidiarno, če žrtvi torej ne bi uspelo identificirati storilcev. Podobno odgovornost je v primeru Delfi AS proti Estoniji vzpostavilo tudi Evropsko sodišče za človekove pravice, ki je odločilo, da multimedijski spletni portal odgovarja za žaljive komentarje, ki jih uporabniki objavijo na portalu (Delfi AS v. Estonia, 2013). Čeprav je seveda v konkretni zadevi ESČP-ja šlo za žaljive komentarje, v prispevku pa se ukvarjamo s protipravnimi ravnanji v virtualni resničnosti, bi vseeno lahko sklepali po analogiji *intra legem* (po t. i. argumentu *a simili ad simile* oz. s podobnega na podobno), saj bi Metaverse moral skrbeti za oz. vzpostaviti varnostne mehanizme, da ne pride do kršitev osebnostnih pravic uporabnikov.

5 Sklep

Prispevek je poskušal okvirno osvetliti področje pravnega varstva, ki ga nudi slovenski pravni sistem v primerih, ko se soočimo s (proti)pravnimi ravnanji v virtualnem svetu, v najhujšem primeru, kot se je zgodilo v Veliki Britaniji z virtualnim posilstvom. Ugotovimo lahko, da slovenski pravni sistem še ni povsem pripravljen na tovrstna tveganja, saj predvsem na področju

kazenskega prava še vedno ureditev ni prilagojena tveganjem, ki se pojavljajo v virtualnem svetu. Na tem mestu je sicer treba poudariti, da imamo ustrezno in zadostno kazenskopravno varstvo, ki ne obsega virtualnih dobrin. Kljub temu posameznik tudi v odsotnosti kazenskopravnega varstva v primeru virtualnih dobrin še vedno uživa varstvo na ustavnopravnem in civilnopravnem področju. Če bo žrtvi uspelo dokazati elemente odškodninske odgovornosti, bo seveda upravičena do odškodnine, čeprav bo seveda vprašljiva odgovornost spletne strani za tovrstna protipravna ravnanja.

Viri

Avbelj, M. (2019). *Komentar Ustave Republike Slovenije, Del. 1*. Ljubljana. Nova Univerza Evropska pravna fakulteta.

Bavcon, L. (2017). *Kazensko pravo splošni del*. Ljubljana. Uradni list Republike Slovenije.

Camber, R. (2024, Januar 1.). British police probe VIRTUAL rape in metaverse: Young girl's digital persona 'is sexually attacked by gang of adult men in immersive video game' - sparking first investigation of its kind and questions about extent current laws apply in online world. *Mail online news*. <https://www.dailymail.co.uk/news/article-12917329/Police-launch-investigation-kind-virtual-rape-metaverse.html>

Finžgar, A. (1958). *Osebnostne pravice*. Ljubljana. Slovenska akademija znanosti in umetnosti.

Juhart, M., Možina, D., Novak, B., Polajnar-Pavčnik, A. & Žnidaršič Skubic, V. (2011). *Uvod v civilno pravo*. Ljubljana. Uradni list Republike Slovenije.

K.S. (2024, Januar 4.). Britanska policija preiskuje prvo virtualno posilstvo v metaprostoru. *RTV SLO MMC*. <https://www.rtvlo.si/zabava-in-slog/zanimivosti/britanska-policija-preiskuje-prvo-virtualno-posilstvo-v-metaprostoru/693668>

Kazenski zakonik (KZ-1), Uradni list RS, št. 55/2008, 66/2008 - popr., 39/2009, 55/2009 - odl. US, 91/2011, 54/2015, 38/2016, 27/2017, 23/2020, 91/2020, 175/2020 - ZIUOPDVE, 195/2020, 95/2021, 186/2021, 206/2021 - ZDUPŠOP, 105/2022 - ZZNŠPP, 16/2023.

Korošec, D. (2008). *Spolnost in kazensko pravo*. Ljubljana. Uradni List Republike Slovenije.

Korošec, D., Filipčič, K., Devetak, H., ur., idr. (2023). *Veliki znanstveni komentar posebnega dela kazenskega zakonika (KZ-1), posodobljena izdaja 1. knjiga 100. do 176. člen*. Ljubljana. Uradni list Republike Slovenije.

Obligacijski zakonik (OZ), Uradni list RS, št. 83/2001, 32/2004, 28/2006 - odl. US, 40/2007, 64/2016 - odl. US, 20/2018.

Odločba Ustavnega sodišča RS U-I-109/10, z dne 26. 9. 2011.

Odločba Ustavnega sodišča RS U-I-25/95, z dne 27. 11. 1997.

Odločba Ustavnega sodišča RS Up-1082/12, z dne 29. 5. 2014.

Pavčnik, M., Polajnar-Pavčnik A., Wedam Lukič, D., (1997). *Temeljne pravice*. Ljubljana. Cankarjeva založba.

Pensa Jadek, D. (1996). Aktualni problemi odškodninskega prava. *Podjetje in delo*, 5–6, str. 593–600.

Plavšak, N., idr.. (2003). *Obligacijski zakonik s komentarjem, splošni del, 1. knjiga*. Ljubljana: GV Založba.

Polajnar Pavčnik, A. (1993). Vzročnost kot pravno vrednostni pojem. *Zbornik znanstvenih razprav Pravne fakultete v Ljubljani*, letnik LII.

Sodba Evropskega sodišča za človekove pravice Delfi AS proti Estoniji – 64569/09, z dne 16. 6. 2015.

Sodba Evropskega sodišča za človekove pravice Sanchez v. France [GC] – 45581/15, z dne 15. 5. 2023.

Strohsack, B., (1996). *Odškodninsko pravo in druge neposlovne obveznosti*. Ljubljana: Časopisni zavod Uradni list Republike Slovenije.

Svet Evrope Odbor ministrov, Priporočilo (2002) 5 o varstvu žensk pred nasiljem, 30. 4. 2002.

Svet Evrope, Konvencija o preprečevanju nasilja nad ženskami in nasilja v družini (Istanbulska konvencija) ISBN 978-92-871-7990-6, november 2014.

Šturm, L. (2002). *Komentar Ustave Republike Slovenije*. Ljubljana. Fakulteta za državne in evropske študije.

Ustava Republike Slovenije (URS), Uradni list RS/I, št. 33/1991, Uradni list RS, št. 42/1997 - UZS68, 66/2000 - UZ80, 24/2003 - UZ3a, 47, 68, 69/2004 - UZ14, 69/2004 - UZ43, 69/2004 - UZ50, 68/2006 - UZ121,140,143, 47/2013, 47/2013, 75/2016 - UZ70a, 92/2021 - UZ62a

Ustavna odločba Up-320/14, U-I-5/17, z dne 14. 9. 2017 Uradni list RS, št. 59/17 in Odl US XXII,9.

Višje sodišče v Celju, sodba Cp 416/2019, ECLI:SI:VSCE:2020:CP.416.2019, z dne 8. 1. 2020.

Višje sodišče v Ljubljani, sodba I Cp 1058/2019, ECLI:SI:VSLJ:2020:I.CP.2012.2019 z dne 23. 9. 2019.

Višje sodišče v Ljubljani, sodba in sklep II Cp 1139/2012, ECLI:SI:VSLJ:2012:II.CP.1139.2012, z dne 3. 10. 2012.

Vrhovno sodišče Republike Slovenije, ECLI:SI:VSRS:2008:II.IPS.671.2008, sodba II Ips 671/2008 z dne 20. 11. 2008.

Vrhovno sodišče Republike Slovenije, sklep II DoR 61/2012, ECLI:SI:VSRS:2012:II.DOR.61.2012, z dne 2.8.2012.

Vrhovno sodišče RS, sklep II Ips 588/99 z dne 31. 5. 2000.

Wang, Y., et.al. (2022). A survey on Metaverse: Fundamentals, security, and privacy. *IEEE Communications Surveys & Tutorials*, 25(1), 319–352. <https://doi.org/10.1109/COMST.2022.3202047>

Zobec, J. (2018). Praktična konkordanca v ustavnosodni presoji. *DIGNITAS Revija za človekove pravice*. Nova Univerza.
<https://doi.org/10.31601/dgnt/49/50-2>

Pravni položaj otrok vplivnežev

Amadeja Mlinar  

Univerza v Mariboru, Pravna fakulteta
Maribor, Slovenija

Dr. Katja Drnovšek 

Univerza v Mariboru, Pravna fakulteta
Maribor, Slovenija

Povzetek: V sodobni družbi je mogoče opaziti vedno večji razmah družbenih omrežij. V tem kontekstu ne govorimo le o komunikacijskih platformah, temveč tudi o tem, da postajajo družbena omrežja iz dneva v dan večji vir zaslužka. Družbena omrežja so še posebej priljubljena med mladimi, zato torej ni presenetljivo, da so tako med uporabniki kot tudi ustvarjalci tudi mladoletniki, kar posledično odpira določena pravna vprašanja. Eno od teh je, kako mladoletne zavarovati pred spolnim in verbalnim nasiljem na spletu. Starši mladoletnih otrok, ki sodelujejo pri ustvarjanju spletnih platform, se soočajo z vprašanji, kako zaščititi njihovo zasebnost in korist, hkrati pa zasledovati njihove premoženjske interese in jih učinkovito zastopati v pravnem prometu. Nujna je tudi ustrezna ureditev na področju delovnega prava in davčnih obveznosti, saj lahko družbene platforme predstavljajo tudi velik vir zaslužka.

Prispevek naslavlja nekaj najbolj perečih problematik ter se opredeljuje do obstoječih pravnih rešitev.

Ključne besede: vplivnostno trženje, otrokova korist, pravica do zasebnosti, omejena poslovna sposobnost, starševska skrb

Legal protection of kidfluencers

Amadeja Mlinar  

University of Maribor, Faculty of Law
Maribor, Slovenia

Katja Drnovšek, PhD 

University of Maribor, Faculty of Law
Maribor, Slovenia

Abstract: In modern society, social media plays an increasingly important role, not only in terms of communication platforms but also by becoming a growing source of income. Social media platforms are particularly popular among the youth; therefore, it is not surprising that both creators and users include minors, which raises certain legal issues. These issues include aspects, such as the protection of minors from sexual and verbal abuse online, the obligations and responsibilities of parents of these kidfluencers to protect their privacy and best interests while also pursuing their financial interests and effectively representing them in legal transactions, as well as adequate regulation in the areas of labour law and tax obligations, as social platforms can also represent a significant source of income. The article addresses some of the most pressing issues and evaluates the existing legal solutions.

Keywords: influencer marketing, child's best interest, the right to privacy, limited legal capacity, parental care

1 Uvod

Družbena omrežja so v zadnjih letih doživela velik razmah, tako zaradi naraščanja števila uporabnikov kot tudi zaradi nastanka novih spletnih platform. Trend naraščanja števila uporabnikov in soustvarjalcev na družbenih omrežjih še posebej izstopa med mladimi, katerih aktivno sodelovanje ni več presenetljivo. Zaradi soustvarjanja vsebin mladih se v pravu pojavljajo novi izzivi in vprašanja glede njihovih ustavno varovanih pravic, zlasti pa pravice do zasebnosti in osebnostnih pravic. Otroci so kot ena najranljivejših skupin izpostavljeni vplivom družbenih omrežij, ki lahko negativno vplivajo na njihov razvoj in samopodobo. Otroško vplivništvo na nek način predstavlja tudi novo obliko otroškega dela, ki zahteva ustrezno regulacijo na delovnopravnem in drugih področjih. Pri vplivništvu gre tudi za novo vejo marketinga, ki postaja vedno bolj priljubljena, sploh med mladimi, ki so še posebej dovzetni za razne oblike prikritega oglaševanja. Posebno hitro rast uporabe družbenih omrežij za marketing je bilo opaziti, ko so uporabniki izdelkov v zameno za njihovo promocijo pričeli prejemati plačila, s čimer se je razvil tako imenovani »marketinški poklic« (Schitton, 2018, str. 12–13). Otroški vplivneži se tako največkrat znajdejo v sodelovanju s podjetji, ki so vir promocij izdelkov, pogosto pa jih na spletne strani vključijo tudi njihovi starši ali skrbniki (Ovčak Kos, 2023, str. 120).

Sodobno okolje družbenih omrežij iz dneva v dan prinaša nove izzive glede varstva otrok na spletu, zato je ključnega pomena vzpostaviti celovit sistem regulacije, ki bo zagotovil varnost in zaščito mladoletnikov na teh platformah, obenem pa spoštoval njihove pravice in omogočal njihov nadaljnji razvoj v pozitivni smeri. Članek izhaja iz hipoteze, da trenutno veljavna pravna ureditev v Republiki Sloveniji zagotavlja omejeno varstvo koristi otrok vplivnežev na številnih področjih, ki bistveno posegajo v otrokove pravice, in opozarja na nekatera odprta vprašanja. Pri tem naslavlja najbolj pereče tematike s področij kaznivih dejanj, izvršenih na spletnih platformah, ureditve delovnih razmerij mladoletnih oseb in problematike razpolaganja z otrokovim premoženjem, ob polnem zavedanju, da gre za izjemno kompleksno problematiko, katere celovita obravnava bi presegala prostorske omejitve prispevka, je pa nedvomno vredna nadaljnje pozornosti (npr. področje oglaševanja, varstva osebnih podatkov ipd.).

2 Metode

Prispevek temelji na uporabi klasičnih metod pravnega raziskovanja. Na podlagi dogmatične metode so v vsakem poglavju ob uporabi jezikovne in logične analize najprej interpretirane pravne

norme, na podlagi normativne metode pa je izpeljana širša analiza trenutno veljavnega prava in njegovih funkcij. Za analizo obstoječe pravne ureditve je bila najprej uporabljena metoda kompilacije, s pomočjo katere so bila ob veljavni zakonodaji zbrana še razpoložljiva stališča v literaturi in sodni praksi, zbrane informacije, ki so predstavljene z metodo deskripcije, pa služijo kot temelj za kritično oceno trenutnega stanja na tem področju. Do zaključkov o ustreznosti trenutne ureditve in opozoril glede morebitnih neskladnosti je pripeljala uporaba tako induktivne kot tudi deduktivne metode. Zaradi narave uporabljenih metod in v izogib podvajanja je pregled literature smiselno vključen v razpravo in prepleten z ugotovitvami.

3 Rezultati in razprava

3.1 Spolno in verbalno nasilje na spletu

Zaskrbljujoče dejstvo, da je spletno okolje otroke izpostavilo novim nevarnostim in izjemno širokim možnostim, da se znajdejo v vlogi žrtve kaznivega dejanja, je že dolgo znano. Kljub ozaveščanju tako otrok kot njihovih staršev, pa tudi širšega družbenega diskurza in medijske pozornosti, se pojavnost tovrstnih dogodkov kvečjemu stopnjuje. Na spletu se s hitro rastjo uporabnikov širijo tudi vrste kibernetkega kriminala (Vintar idr., 2021, str. 27). Strokovnjaki iz teorije in prakse pri tem opozarjajo na nedoslednosti in pomanjkljivosti v obstoječi zakonodaji, ki kazenskopravne vidike delovanja na družbenih omrežjih pogosto naslavlja v okvirih splošnih oblik kaznivih dejanj, ki ne upoštevajo vseh posebnosti spletnega okolja, zaradi česar se rešitve pogosto vzpostavljajo v sodni praksi. Obravnava vseh kaznivih dejanj, v katerih so lahko udeleženi otroci vplivneži, bi bistveno presegala okvire tega prispevka, ki zato vključuje le pregled nekaterih najpogostejših vrst, kot so sovražni govor, spletno zalezovanje in nagovarjanje otrok k spolnosti.

3.1.1 Spletno/kibernetško nasilje

Eden od izzivov, s katerimi se srečujejo otroci v digitalni dobi, je razširitev medvrstniškega verbalnega nasilja v domače okolje, kjer so bili v preteklosti varni pred nadlegovanjem. Kibernetško nadlegovanje (angl. *cyberbullying*), ki obsega ustrahovanje, trpinčenje, tiraniziranje ali šikaniranje po internetu (npr. po e-pošti, spletnih straneh, blogih, klepetalnicah, forumih, spletnih družbenih omrežjih, straneh za izmenjavo multimedijskih vsebin), pa tudi po telefonu, ni posebej opredeljeno kot kaznivo dejanje (Završnik & Sedej, 2012, str. 263), čeprav bi bilo zaradi posebnosti tovrstnega ravnanja (predvsem potencialna intenzivnosti in nenehnosti) to smiselno. Namesto tega se lahko otroci vplivneži znajdejo v vlogi tako žrtve (npr. kot prejemniki neprimernih

sporočil ali komentarjev v odziv na objave) kot tudi storilca (zaradi neprimerne vsebine objav) kaznivih dejanj zoper čast in dobro ime, izsiljevanja, groženj idr.

Čeprav se v strokovnih, medijskih in drugih razpravah o odnosu med svobodo govora ter neprimernih in nezakonitih vsebinah spletnih objav pogosto uporablja izraz »sovražni govor«, slovenska kazenskopravna zakonodaja tega pojma kot takšnega ne opredeljuje (Korošec, Filipčič idr., 2023, str. 479–480). Namesto tega 297. člen KZ-1 obravnava kaznivo dejanje javnega spodbujanja sovraštva, nasilja ali nestrpnosti, ki ga med drugim stori, kdor spodbuja ali razpihuje sovraštvo, nasilje ali nestrpnost, ki temelji na kateri od primeroma naštetih osebnih okoliščin (narodnost, rasa, spol itd.), in je dejanje storjeno na način, ki lahko ogrozi ali moti javni red in mir, ali z uporabo grožnje, zmerjanja ali žalitev. Sovražni govor, ki je usmerjen zoper skupine (VSL Sodba VII Kp 32326/2021 z dne 25. 4. 2023), je na individualni ravni najpogostejše kaznivo dejanje razžalitve, storjene preko spletnega komunikacijskega portala (2. odstavek 158. člena KZ-1). Razžalitev je lahko izvršena pisno ali ustno, včasih celo simbolno, in jo je mogoče izvršiti tudi anonimno. Gre za izjavo žaljivih trditev o določeni osebi, v konkretnem primeru o otroku vplivnežu ali s strani otroka vplivneža, pri čemer se presoja, kako bo sporočilo dojemal prejemnik (Šepec, 2018, str. 269). Pri presoji žalitve je treba upoštevati vez med oškodovancem in storilcem, in okoliščine, v katerih je prišlo do razžalitve, ter vse skupaj tehtati s pravico do svobode izražanja. Pri razžalitvi gre namreč za kolizijo dveh ustavno varovanih človekovih pravic, zaradi česar bi razžalitev postala kaznivo dejanje šele, ko bi pravica do svobode izražanja prestopila mejo pravice do časti in dobrega imena (Korošec, Filipčič idr., 2023, str. 991–994). Smiselno je izpostaviti, da lahko kot storilec kaznivega dejanja odgovarja le otrok, ki je že dopolnil štirinajst let (21. člen Kazenskega zakonika, v nadaljevanju KZ-1), zaradi česar je možnost kazenskoopravnega ukrepanja v primerih verbalnega spletnega nasilja med osnovnošolci le omejena.

3.1.2 Spletno zalezovanje ali cyberstalking

Spletno zalezovanje zajema pojem ponavljajočega se opazovanja, zasledovanja in prizadevanja navezati stik na družbenem omrežju, pri čemer pa se povzročita strah in ogroženost zalezovane osebe (134.a člen KZ). Omenjeno kaznivo dejanje je nastalo na podlagi primerov iz sodne prakse, ki pred tem niso imeli kazenskoopravne podlage (Šepec, 2018, str. 308). Gre torej za primer normativne rešitve pravnega problema, ki ga je zaradi pomanjkljivosti dotedanje ureditve morala reševati sodna praksa. Tudi neželena komunikacija z otrokom se lahko kaže kot oblika zalezovanja v primeru, da pride do komunikacije z vsiljivim prizadevanjem vzpostaviti stik.

Prestrašenost in počutje ogroženosti morata kot posledica zalezovanja nastati pri otroku kot zalezovani osebi ali njegovem bližnjem sorodniku. V primeru storitve te vrste kaznivega dejanja ni pomembna minimalna starost žrtve. Zaradi navedenega je lahko žrtev zalezovanja tudi novorojeni otrok, kar pa povzroči vprašanje širine dometa obravnave tega člena (Korošec idr., 2023, str. 707–708, 712–715).

3.1.3 Nagovarjanje otrok k spolnosti ali child grooming

Kaznivo dejanje pridobivanja otrok, mlajših od 15 let, za spolne namene predpostavlja, da je pogoj za izvršitev kaznivega dejanja otroka nagovoriti preko komunikacijskega omrežja z namenom uresničitve srečanja ali izdelave slik in video pornografskih vsebin (173. a člen KZ). Gre za eno od novejših inkriminacij, ki se omejuje na spletno okolje, kjer se je zakonodajalec odzval na nove družbene izzive in tveganja, ki jih prinaša digitalizacija. Pri tem kaznivem dejanju gre relativno za proces vzpostavljanja stika z otrokom z namenom, da bi se pridobilo njegovo zaupanje in se ga lažje pripravilo k spolni zlorabi. Prvi zakonski znak je, da se storilcu lahko očita krivdo v primeru, da je prepričan, da se na družbenem omrežju pogovarja z otrokom. Če bi bil storilec prepričan, da gre za polnoletno osebo, pozneje pa se izkaže, da gre v bistvu za otroka, bi lahko prišla v poštev dejanska zmeta. Drugi zakonski znak kaznivega dejanja je nagovarjanje preko spletnega komunikacijskega kanala. Zoper storilca bo treba dokazati, da je imel pri srečanju z nagovorjenim otrokom namen storiti kaznivo dejanje spolnega napada ali proizvesti pornografske fotografije ali video vsebine ter da so nagovarjanju sledila še konkretna dejanja, iz katerih je razvidno, da se je storilec z otrokom že dogovarjal o času in kraju srečanja (Šepec, 2018, str. 229–231).

Pri omenjenem kaznivem dejanju je torej inkriminirano že nagovarjanje preko spletnih omrežij kot tako, ki pa mu pozneje sledijo konkretna dejanja za uresničitev dogovorjenega srečanja, pri čemer pa ni potrebno, da bi ob srečanju dejansko prišlo do spolnega nasilja (VSRS Sodba I Ips 10095/2011-62 z dne 31. 1. 2013).

3.1.4 Pomen ozaveščanja o ravnanju v primeru spolnega ali verbalnega nasilja na spletu

Čeprav nekatere spremembe v kazenskoopravni zakonodaji že naslavlajo izzive, s katerimi se srečujejo otroci vplivneži, je jasno, da gre za kompleksno tematiko, ki zahteva neprestano usklajevanje pravne ureditve z razvojem tehnologije in posledično družbe, pa tudi širši družbeni pristop, ki ne vključuje zgolj pravnikov, temveč tudi druge strokovne profile (sociologi, psihologi, kriminologi itd.). Najpomembnejšo vlogo pa ima nedvomno obveščanje uporabnikov o pasteh

delovanja v spletnem okolju. Opaziti je, da videoposnetki in fotografije otrok vplivnežev na družbenih omrežjih velikokrat prikazujejo celo intimni vidik otroške zasebnosti. Najpogosteje gre za objave otrok vplivnežev, ki prikazujejo družinska potovanja, praznovanja ali vsakdanje dogodke v domačem okolju. Otroci vplivneži so s spletnimi objavami izpostavljeni komentiranju, ki je velikokrat zelo negativno, kar pa lahko pri otroku povzroči stisko, slabo samopodobo in s tem tudi težavo pri nadaljnjem razvoju. Z objavami otrok na družbenih omrežjih pri tako nizki starosti se otroku onemogoči, da bi se sam pozneje v življenju odločil, kakšen pečat želi pustiti na ljudeh in na kakšen način bi rad to storil. Vse, kar se objavi, je na spletu namreč trajno dostopno in skoraj neizbrisljivo, kar pomeni, da se bo vsebina lahko delila še vrsto let. Otrok je lahko iz tega vidika izpostavljen tudi zasmehovanju in trpinčenju s strani sovrstnikov (Ovčak Kos, 2023, str. 120–123) ali še huje, številnim tveganjem, saj se s tem razkrivata otrokova identiteta in kraj, kjer se otrok zadržuje (Šepec, 2018, str. 19–22). Zaradi navedenih spletnih pasti je pomembno, da se starši ali zakoniti zastopniki z otrokom pogovarjajo o vsebinah, s katerimi se lahko srečajo na spletu, možnih rešitvah ter tem, na koga se obrniti v primeru, da se otrok s tem sreča v resničnem življenju (Vintar, Radšel idr., 2021, str. 27). Hkrati je treba poskrbeti za dobro ozaveščanje staršev, ki se morda tudi sami ne zavedajo vseh nevarnosti, o katerih bi se lahko pogovorili z otrokom (npr. pojav vedno novih in pogosto nevarnih izzivov), ali pa celo sami objavljajo vsebino, ki otroke izpostavi nevarnostim. Dobro pa se je zavedati, da so lahko otroci tudi ob dobri poučenosti o spletnih nevarnostih in odlični računalniški pismenosti izpostavljeni zanje škodljivim dogodkom, zaradi česar so nujne tudi ustrezne normativne rešitve.

3.2 Delovnopravna ureditev dela otrok vplivnežev

Redno ustvarjanje in objavljanje spletnih vsebin, še posebej v zameno za plačilo, je lahko sporno tudi z vidika zakonodaje, ki ureja delo otrok. Posebej varovana skupina mladoletnih otrok so otroci do 15. leta starosti. Za to skupino Zakon o delovnih razmerjih (v nadaljevanju ZDR-1) izrecno prepoveduje opravljanje dela z izjemo, ki mlajšim od 15 let dovoljuje sodelovanje pri snemanju filmov ter pripravi in izvajanju umetnostnih in scenskih aktivnosti na področju kulturne, športa in oglaševalne aktivnosti (2. odstavek 211. člena ZDR-1). Tovrstno delo lahko otrok opravlja po predhodnem dovoljenju inšpektorata za delo, ki se izda na predlog starša ali zakonitega zastopnika (2. člen Pravilnika o izdaji dovoljenj za delo otrok, mlajših od 15 let (v nadaljevanju Pravilnik)). Preden bi se izdala tovrstna dovoljenja, je dolžnost inšpektorata, da preveri, ali bi lahko delo, ki bi ga otrok opravljal, ogrožalo njegovo varnost, izobraževanje, moralo ali razvoj (7. člen Pravilnika). Po prosti presoji lahko inšpektor preveri tudi delovno okolje otroka, če pa tudi po tem

ne more opraviti konkretne odločitve o tem, ali je delo za otroka škodljivo, mora zahtevati mnenje pristojnega centra za socialno delo, šolske svetovalne službe ali druge pristojne institucije (Bečan idr., 2019, str. 1137). Zaradi zgoraj navedene izjeme od prepovedi dela bi otrok vplivnež, ki še ni dopolnil 15 let, načeloma lahko ustvarjal in objavljajal spletne vsebine ali sodeloval pri ustvarjanju vsebin, ki jih objavljajo njegovi starši, vendar morajo biti izpolnjeni tudi vsi naštetih pogoji. Ravno zaradi nepridobitve dovoljenja za delo otroka, mlajšega od 15 let, sta bila leta 2022 v Sloveniji že oglobljena prva vplivneža, ki sta s pomočjo svojih otrok v profilu na Instagramu promovirala izdelke (STA, Sa. B., 25. 11. 2022).

Mladoletniki, ki so že dopolnili 15 let, lahko sklenejo pogodbo o zaposlitvi (21. člen ZDR-1), samostojno pa lahko sklepajo tudi druge pravne posle, npr. pogodbo o sponzorstvu, pogodbo o delu, avtorsko pogodbo idr. Dovoljenje staršev potrebujejo le za sklepanje poslov, ki bistveno vplivajo na otrokovo življenje pred polnoletnostjo ali po njej (146. člen DZ). Po doseženem 15. letu starosti lahko otroci vplivneži torej samostojno vstopajo v pravne posle in sklepajo pogodbe, na podlagi katerih ustvarjajo vsebine in pridobivajo prihodke iz tega naslova. Vse tovrstne pogodbe, ki jih mladoletnik sklene pred 15. letom, so nične. Kljub temu da je delo otrok, ki so dopolnili starost 15 let, a še niso polnoletni, torej dovoljeno, se delodajalcu nalaga posebne obveznosti omejitve dela, s katerim se varuje varnost, zdravje in razvoj mladostnika (Bečan idr., 2019, str. 111). ZDR-1 posebej opredeljuje, da mladoletniku ni dovoljeno naložiti dela, ki bi objektivno presevalo njegove telesne in fizične sposobnosti (191. člen ZDR), prav tako pa jim ni dovoljeno opravljati dela v nočnem delovnem času (193. člen ZDR).

Če starši otroke pretirano silijo k delu in sodelovanju pri izdelavi objav za družbena omrežja, lahko rečemo, da gre za kaznivo dejanje (Bečan idr., 2019, str. 1133). Kazenskopravno definicijo prepovedanega otroškega dela vsebuje opis kaznivega dejanja zanemarjanja mladoletne osebe in surovega ravnanja in se nanaša na takšno delo otroka, ki bi ga prikrajšalo za otroštvo, mu preprečilo redno obiskovanje šole ali bi bilo zanj moralno ali socialno škodljivo. Starši, skrbniki, rejniki ali druge osebe, ki silijo mladoletno osebo k pretiranemu delu ali k delu, ki zanje ni primerno, kazensko odgovarjajo (2. odstavek 192. člena KZ-1). V sodni praksi se zaenkrat še niso izoblikovala stališča, kdaj bi delovanje na spletnih platformah predstavljalo takšno neprimerno otroško delo, tudi sicer pa je v praksi zelo težaven nadzor nad številom ur in pogoji, v katerih otrok delo opravlja.

Vsaka oseba, ki na družbenem omrežju opravlja pridobitno dejavnost, bi morala imeti to dejavnost

tudi ustrezno registrirano oz. bi si morala urediti status samostojnega podjetnika ali pravne osebe. V nasprotnem primeru bi lahko rekli, da gre za delo na črno, kar pa je prepovedano (Tržni inšpektorat, 2023). Kaznivo je tudi zaposlovanje na črno, za kar se šteje, če delodajalec omogoči delo posamezniku, s katerim ni sklenil pogodbe, na podlagi katere bi lahko opravljal delo, oz. ga ni prijavil v obvezna socialna zavarovanja (5. člen Zakona o preprečevanju dela in zaposlovanja na črno). Odvisno od okoliščin posameznega primera (predvsem kako pogosto vplivnež objavlja vsebine in v kakšni obliki prejema plačilo) lahko vključevanje otrok v plačano ustvarjanje spletnih vsebin predstavlja tudi delo na črno.

3.3 Ureditev upravljanja premoženjske koristi otrok vplivnežev

Soustvarjanje na družbenih platformah občasno s seboj prinese tudi ustvarjanje dobička. Spletne račune otrok vplivnežev v velikem deležu upravljajo starši ali njihovi zakoniti zastopniki (Ovčak Kos, 2023, str. 120). Zaradi navedenega je treba opredeliti tudi, kdo lahko upravlja s premoženjem mladoletnika, ki je rezultat njegovega delovanja na spletnih platformah. DZ določa, da v otrokovo korist z njegovim premoženjem upravljajo njegovi starši (147. člen DZ). Dohodke iz otrokovega premoženja smejo starši uporabljati predvsem za njegovo preživljanje, vzgojo in izobraževanje, za potrebe družinske skupnosti pa se sme otrokovo premoženje uporabiti le v primeru, da sami nimajo zadosti sredstev (148. člen DZ). Stvari iz premoženja svojega otroka (substancia premoženja) pa smejo starši odsvojiti ali obremeniti samo zaradi njegovega preživljanja, vzgoje in izobrazbe, ali če to zahteva kakšna druga njegova korist (1. odstavek 149. člena DZ). Do takrat, ko otrok dopolni 15 let in s tem pridobi omejeno poslovno sposobnost, lahko torej premoženje otroka vplivneža in dohodke iz tega premoženja v njegovo korist upravljajo njegovi starši. Da bi preprečili morebitne zlorabe glede sredstev, ki jih je vendarle s svojim delom zaslužil otrok, DZ vsebuje stroge omejitve glede pogojev in namena, za katerega se lahko ta sredstva porabijo.

Ker je finančna skrb za otroka ena temeljnih dolžnosti starša ali skrbnika, je jasno, da morajo slednji pokriti stroške za otrokove potrebe v prvi vrsti sami, v okviru dolžnosti preživljanja (Čujovič idr., 2019, str. 463–465). Šele če je njihova zmožnost preživljanja zmanjšana ali celo onemogočena, lahko posežejo tudi v substanco otrokovega premoženja (UPRS sodba I U 1284/2016-8 z dne 13. 6. 2017). Če obstaja nevarnost, da bodo starši z odsvojitvijo ali obremenitvijo premoženja svojega otroka ogrozili njegove premoženjske koristi, potem mora sodišče izreči ukrepe, ki jih za varstvo premoženjskih koristi otroka določa DZ (149. člena DZ), npr. staršem prepove odsvojitvev ali obremenitev otrokovega premoženja (drugi odstavek 171. člena

DZ). S premoženjem, ki izhaja iz sfere otroka, sta starša dolžna ravnati z ustrezno skrbnostjo (1. odstavek 6. člena Obligacijskega zakonika). Če nista dovolj skrbna, lahko otroku odgovarjata za škodo, ki bi nastala zaradi malomarnega upravljanja z njegovim premoženjem.

Trenutno veljavna ureditev torej natančno ureja pooblastila staršev glede upravljanja otrokovega premoženja, tudi tistega, ki ga pridobi otrok vplivnež z objavami na spletnih platformah. Medtem ko lahko otrok, ki je že dopolnil 15 let, v okviru svoje poslovne sposobnosti sam upravlja s svojimi dohodki in premoženjem (dokler to ne vpliva bistveno na njegovo življenje), pa tudi s svojo plačo (150. člen DZ), otrok, ki je mlajši od 15 let, ne more sklepati nobenih pravnih poslov in je torej v celoti prepuščen volji svojih staršev, ki lahko z njegovim premoženjem razpolagajo tudi proti njegovi volji (znotraj zgoraj omenjenih zakonskih omejitev). Čeprav so neskrbni starši otroku tudi odškodninsko odgovorni za morebitno škodo, ki so mu jo pri tem povzročili, sodišče pa jim lahko prepove nadaljnje upravljanje otrokovega premoženja, je lahko škoda v določenih primerih že nepopravljiva (npr. kadar starši zapravijo premoženje večje vrednosti, sami pa nimajo zadostnih sredstev, da bi otroku pozneje povrnili škodo). Do spora glede upravljanja otrokovega premoženja pa lahko pride tudi med staršema, ki starševsko skrb sicer izvajata sporazumno in v korist otroka. Če se starša ne moreta sporazumno odločiti o upravljanju premoženja otroka, jima pri iskanju skupne rešitve lahko pomaga center za socialno delo. Če se starša po tem še vedno ne moreta sporazumeti, bo o upravljanju premoženja otroka odločalo sodišče v nepravdnem postopku (151. člen DZ).

4 Sklep

Otroci vplivneži so otroci, ki na družbenih omrežjih sodelujejo v okviru profila svojih staršev ali v okviru profila podjetja, s katerim sodelujejo. Promocija izdelkov ali storitev običajno poteka preko fotografij ali videoposnetkov, ki so pozneje objavljeni na spletnih platformah. S tem, ko otroci vplivneži sodelujejo pri promociji izdelkov, so izpostavljeni različnim oblikam verbalnega in spolnega nasilja, ki jim grozi na spletu. Med njimi so razžalitev dobrega imena otroka ter zalezovanje in nagovarjanje otrok k spolnosti, ki so bolj ali manj ustrezno sankcionirani v veljavni kazenskopравни zakonodaji. Zaradi navedenega je treba otroke in njihove starše predvsem opozoriti na to, kje lahko najdejo pomoč, če se znajdejo v stiski, ključni pa so tudi nadaljnji normativni napori, usmerjeni v usklajevanje zakonodaje s tehnološkim in družbenim napredkom. Otroško vplivništvo predstavlja neke vrste novo obliko dela, za katero je nujno, da je ustrezno

urejena, saj gre v tem primeru za mladoletne otroke, ki nimajo poslovne sposobnosti. Največji problem na tem področju so predvsem otroci do 15. leta starosti, za katere je treba za delo pridobiti odobritev pristojnega organa in postaviti meje, ki določajo, kakšno delo lahko mladoletniki sploh opravljajo. S promoviranjem lahko otroci zaslužijo tudi kar nekaj denarja. Veljavna zakonodaja določa, da s premoženjem otrok upravljajo starši. Ker je ena temeljnih dolžnosti starša preživljanje otroka, morajo stroške za njegovo preživetje in izobraževanje v prvi vrsti kriti sami, če pa jim finančno stanje tega ne dopušča, se lahko izjemoma poseže v sfero otrokovega premoženja. Čeprav zakonodaja vsebuje številne varovalke pred izkoriščanjem otrok za lastne finančne koristi, te v praksi pogosto ne zadoščajo za celovito zaščito otrokove koristi.

Otroško vplivništvo torej poleg finančnih bonitet prinaša tudi zahteve po regulaciji različnih pravnih področij z namenom, da se mlade vplivneže ustrezno zaščiti. Potrebna je jasna postavitev meja, ki bodo otroke varovale pred morebitnim izkoriščanjem in negativnimi vplivi ter zagotovile najvišje možno varstvo načela otrokove največje koristi.

Viri

- Bečan, I., Belopavlovič, N., idr. (2019). *Zakon o delovnih razmerjih (ZDR-1): s komentarjem*. Lexpera, GV založba.
- Čujovič, M., Dolčič, T., idr. (2019). *Komentar Družinskega zakonika*. Uradni list Republike Slovenije.
- Korošec, D., Filipičič, K., idr. (2023). *Veliki znanstveni komentar posebnega dela kazenskega zakonika (KZ-1)*. Uradni list Republike Slovenije; Pravna fakulteta Univerze v Ljubljani.
- Ovčak Kos, M. (2023). Varstvo koristi otroka in vplivnostni marketing. V M. Repas (ur.), *Dileme sodobnega oglaševanja – izbrane teme* (str. 101–124). Univerza v Mariboru, Pravna fakulteta. <https://doi.org/10.18690/um.pf.6.2023>
- Schitton, D. (2018). Pravna vprašanja, povezana z vplivnostnim marketingom. *Pravna praksa*, 37(12/13), 15–17.
- STA, Sa. B. (2022, 25. november). *Slovenski vplivnež prejel kazen zaradi nezakonitega dela otrok*. <https://siol.net/trendi/svet-znanih/inspekcija-oglobila-vplivneza-ki-je-s-pomocjo-otrok-promoviral-izdelke-593152>
- Šepec, M. (2018). *Kibernetski kriminal: kazniva dejanja in kazensko-pravna analiza*, Univerzitetna založba Univerze v Mariboru. <https://doi.org/10.18690/978-961-286-160-5>
- Tržni inšpektorat RS (2023). *Vplivneži morajo imeti ustrezno urejeno poslovanje – to bo odslej podvrženo večjemu nadzoru*. <https://www.gov.si/novice/2023-06-26-vplivnezi-morajo-imeti-ustrezno-urejeno-poslovanje-to-bo-odslej-podvrzeno-vecjemu-nadzoru/>

Vintar Spreitzer, M., Baš, D., idr. (2021). *Smernice za uporabo zaslonov pri otrocih in mladostnikih: priročnik za strokovnjake*. <https://nijz.si/zivljenjski-slog/nekemicne-zasvojenosti/zasloni/>

Završnik, A. & Sedej, A. (2012). Spletno in mobilno nadlegovanje v Sloveniji. *Revija za kriminalistiko in kriminologijo*, 63(4), 263–280.

Pravna analiza e-športa s poudarkom na varstvu mladoletnikov

Žiga Rodošek ✉ 

Univerza v Mariboru, Pravna fakulteta

Maribor, Slovenija

Dr. Andreja Primec 

Univerza v Mariboru, Ekonomsko-poslovna fakulteta

Maribor, Slovenija

Povzetek: E-šport (tudi elektronski šport ali digitalni šport) je krovni izraz, ki se uporablja za opis tekmovanja v videoigrah in se ukvarja z videoigrami. Združenje eSport Bund Deutschland (ESBD), ustanovljeno februarja 2018, ga je v svojem statutu opredelilo kot »tekmovalno igranje računalniških ali videoiger, zlasti na računalnikih in konzolah, v skladu z določenimi pravili«. To področje se je razmahnilo, ko so mladi odrasli začeli ustvarjati in nadzorovati številne nove kulturne trende. Gledanost tradicionalnih športov upada, medtem ko gledanost e-športa strmo narašča. Vrednost globalnega trga e-športa je bila leta 2022 ocenjena z 1,45 milijarde ameriških dolarjev. Ker je e-šport razmeroma novo poslovno področje, zaradi bliskovitega razvoja trenutno ni standardizirane opredelitve tega pojava. Posledično je pomanjkljivo pravno urejeno. Prispevek se osredotoča na problematiko pravne ureditve tega področja in s tem v zvezi opozarja predvsem na varstvo mladoletnikov in morebitne zlorabe v obliki prikritih iger na srečo.

Ključne besede: E-šport, tekmovanje v videoigrah, varstvo mladoletnikov, zloraba, igre na srečo

Legal analysis of e-sports with a focus on the protection of minors

Žiga Rodošek ✉ 

University of Maribor, Faculty of Law
Maribor, Slovenia

Andreja Primec, PhD 

University of Maribor, Faculty of Economics and Business
Maribor, Slovenia

Abstract: E-sport (electronic or digital sport) is an umbrella term used to describe video game competition and is concerned with video games. The eSport Bund Deutschland (ESBD), founded in February 2018, defines it in its statutes as »the competitive playing of video or computer games, particularly on computers and consoles, following defined rules«. This field has exploded as young adults have begun to create and control many new cultural trends. Viewership of traditional sports is declining, while e-sports are rising rapidly. The global e-sports market was estimated to be worth around USD 1.45 billion in 2022. As e-sports is a relatively new business area, there is no standardised definition due to its rapid development. Consequently, there is a lack of legal regulation. This paper focuses on the problems of regulating this area, drawing attention in this respect, in particular to the protection of minors and possible abuse in the form of hidden gambling.

Keywords: e-sports, video game competition, protection of minors, abuse, gambling

1 Uvod

Elektronski šport (v nadaljevanju e-šport) je znan kot profesionalni šport ali tekmovanje, ki uporablja videoigre kot platformo za tekmovanje med dvema ali več posamezniki. Čeprav je za mnoge e-šport relativno nov pojav, segajo njegove korenine že na začetek razvoja računalniških sistemov. Prvo tekmovanje v videoigrah se je namreč odvijalo že leta 1972 na Univerzi Stanford pod imenom »Intergalactic Spacewar Olympics«. Elektronski športi so doživeli izjemno rast v številu gledalcev in denarnih nagradah, saj sta se v letih od 2000 do 2012 povečala tako obseg kot število turnirjev s približno 10 na 700 (Hiltscher, 2013). Leta 2020 je po ocenah Forbese globalni prihodek industrije e-športa znašal 1,1 milijona dolarjev in pritegnil pozornost 495 milijonov ljudi po vsem svetu (Newzoo, 2019 v Chan idr., 2022). V svetu e-športa se je zaradi združevanja tekmovalnosti in digitalnih kompetenc pojavil kritičen diskurz do presečišča prava in zaščite mladih. Zaradi rasti e-športa se potreba po trdnih pravnih okvirih za zaščito dobrobiti mladoletnikov močno veča, in sicer od zaščite mladoletnikov pred izkoriščevalskimi pogodbami do obravnave zapletenega področja spletnega nadlegovanja in vprašanja prikritih iger na srečo. Poleg tega se je okoli e-športa pojavilo vprašanje prikritih iger na srečo, saj se virtualni igralni predmeti, znani kot »kože« (skins), uporabljajo kot valuta za sklepanje stav na različnih spletnih straneh e-športa. O omenjenih novih oblikah iger na srečo je zaenkrat malo informacij, čeprav se zaskrbljenost, da lahko ti izdelki nekatere ranljive potrošnike (npr. mlade) izpostavijo tveganju škode, povezane z igrami na srečo, povečuje (Greer idr., 2019). Najpogostejša oblika iger na srečo so t. i. loot boxi oz. predmeti v videoigrah, ki jih je mogoče kupiti z dejanskim denarjem. Formalna podobnost med loot boxi in igrami na srečo je vzbudila zaskrbljenost, da bi ti lahko predstavljali »vstopno točko« za igre na srečo pri otrocih (Zendle idr., 2020). Omenjeni vidiki predstavljajo potrebo po kritični presoji že obstoječih pravnih okvirov znotraj področja e-športa in potencialnih izboljšavah v korist mladih (in ostalih uporabnikov).

Prispevek obravnava problematiko pomanjkljive pravne ureditve e-športa. Ker ta najbolj pritegne pozornost mladoletnikov, se kot osrednje raziskovalno vprašanje izpostavlja analiza posameznih vsebin e-športa do te starostne skupine in vprašanje njihovega pravnega varstva. Predstavljena bo tudi pomembnost e-športa kot samostojne športne discipline, učinkovitost starostnih ocen za igranje videoiger ter povezava med prikritimi igrami na srečo v videoigrah in nastankom odvisnosti od iger na srečo pri mladoletnikih.

2 Opredelitev e-športa

Pojem e-šport se nanaša na tekmovanje med ljudmi s pomočjo različnih računalniških ali videoiger. Ker je e-šport razmeroma novo poslovno področje, trenutno ni standardizirane opredelitve tega pojava. V praksi se v svetu videoiger pojavljajo posamezne igre, ki jih proizvajalci kategorizirajo kot »pripravljene za e-šport« (ready for e-sport). Od prvega tekmovanja v videoigrah na Univerzi Stanford je do danes prišlo do mnogih sprememb, med drugim do modernizacije računalniških programov, ki so bili podlaga za igranje videoiger in posledično e-športa. S programsko opremo za osebne računalnike so podjetja izdajala igre, specifično namenjene tekmovanjem v e-športu. Tehnologija je z razvojem omogočala simulacije, ki so vključevale podrobna 3D-okolja in številne igralce ter nastanek novih žanrov iger, kot so prvoosebne strelske igre oz. FPS (first person shooter, npr. Call of Duty). Konkurenca med igralci videoiger v poznih devetdesetih letih prejšnjega stoletja je prav tako imela veliko koristi od uporabe interneta v razvitih državah, kot so Združene države (Snavey, 2014). Če je igralec imel dostop do interneta, so lahko igralne konzole in računalniki povezali igralce z različnih fizičnih lokacij, da so hkrati igrali v eni virtualni areni.

Medtem ko so organizatorji dogodkov na Zahodu še naprej prirejali pretežno fizične turnirje v videoigrah, se je v Južni Koreji razvijala kultura, ki se poslužuje omrežne infrastrukture in digitalne tehnologije (Jin in Chee, v Snavey, 2014). Z uporabo interneta so igralci v Južni Koreji že pred letom 2000 preživeli veliko časa ob igranju videoiger in prirejali razna tekmovanja. Ta dejavnost je postala tako priljubljena, da je ustvarila industrijo, ki je lahko podpirala profesionalne igralce s prirejanjem glavnih e-športnih dogodkov, ki so bili privlačni za sponzorje. Južna Koreja zaradi organizacije ogromnih nacionalnih in mednarodnih igralnih turnirjev, kot je World Cyber Games, predstavlja začetnico in vodilno državo profesionalnega igranja iger, kar ji je leta 2009 prineslo 1,4 milijarde dolarjev zaslužka (Jin in Chee, v Snavey, 2014). Pri njih so za razliko od igralnih konzol (kot so npr. Playstation, Nintendo, Xbox), kjer več igralcev igra na isti konzoli v fizični oz. neposredni bližini, v ospredju računalniški sistemi, kjer so igralci fizično ločeni in igrajo z različnih lokacij. Razcvet digitalnega gospodarstva je v Južni Koreji povzročil nastanek edinstvenega trga e-športa, ki državi prinaša številne gospodarske prednosti, predvsem dobičkonosnost.

Čeprav v azijskih državah priznavajo e-športe kot uveljavljeno športno disciplino, na zahodu (ZDA in EU) še ni tako. Pristaši tradicionalnega športa in osebe z bolj konservativnimi pogledi so namreč mnenja, da e-šport ne more biti enakovreden tradicionalnim športnim disciplinam. Zaradi dobičkonosnosti e-športov pa prihaja tudi v Evropi do vse večje integracije e-športov v pojem športnih

tekmovanj. S tem se tudi povečuje potreba po enotni definiciji e-športa, njegovi pravni ureditvi ter uvrščanju na področje športa. Po Tiedemannu je »šport« kulturno področje dejavnosti, na katerem ljudje prostovoljno vstopajo v odnos z drugimi z zavestnim namenom razvijanja svojih sposobnosti in dosežkov (zlasti na področju spretnih gibov) in primerjave z drugimi ljudmi v skladu s pravili, ki so jih postavili sami ali jih sprejeli, ne da bi sebi ali drugim namerno škodovali (Wagner, 2006). Ta definicija je dovolj široka, da lahko zajame tudi e-šport. Zagovorniki ideje, da je e-šport šport, poudarjajo dejstvo, da ta temelji na tekmovanju z močno čustveno komponento, ki je prav tako značilna za ostala športna tekmovanja – od nogometa do pikada ali šaha. E-šport ne predstavlja več le oblike preživljanja prostega časa, temveč odpira nove poklicne možnosti ter prepoznavnost in ugled v svetu (Gunia, 2018).

3 Metode

Uporabljene so bile uveljavljene metode za pravno raziskovanje, ki jih ponuja pravna epistemologija (Novak, 2010). V največji meri je bila uporabljena avtonomno pravna oz. normativno dogmatična metoda za preučitev trenutne pravne ureditve e-športa, pri čemer je poudarek na varstvu mladoletnikov in težavah, ki se pojavljajo na tem področju. Primerjalno pravna metoda je bila uporabljena za pojasnitev pravne ureditve prirejanja e-športnih dogodkov, prikritih iger na srečo v igrah in pojasnitev varstva mladoletnikov kot splošnega pojma, predvsem v Nemčiji, ki je urejeno v Zakonu o varstvu mladoletnikov (Jugendschutzgesetz), ter za pojasnitev povezave e-športa z varstvom mladoletnikov. V nadaljevanju je bila uporabljena tudi vrednostna metoda z namenom analize prakse in drugih pravnih varovalk, ki naj bi preprečevale zlorabe.

4 Raziskava

4.1 Vsebina raziskave

S pomočjo študija literature, dosedanjih raziskav na področju e-športa in pravnih virov na tem področju je raziskava potekala v treh smereh. Prva se je nanašala na razvoj e-športa in njegovo pravno ureditev v treh izbranih državah (Sloveniji, Avstriji in Nemčiji), druga je proučevala pomen in funkcijo oznak PEGI in USK na videoigrah, tretja pa se je osredotočila na problematiko prikritih iger na srečo, ki se pojavljajo v svetu videoiger.

4.2 Razvoj in pravna ureditev e-športa v Sloveniji

V Sloveniji je področje e-športa precej mlado in v primerjavi z drugimi državami (npr. Avstrijo in Nemčijo) manj razvito. Razlog je v pomanjkanju sredstev za organizacijo športnih dogodkov zaradi majhnega števila sponzorjev in neučinkovitega oglaševanja s strani državnih medijev. (Zavašnik, 2020). Začetki e-športa v Sloveniji so se pojavljali v obliki organiziranih lokalno omrežnih ali LAN-dogodkov (angl. local area network), kjer so se udeleženci fizično zbrali z osebnimi računalniki ali združljivimi igralnimi konzolami in se povezali s pomočjo lokalne omrežne povezave. Na takih dogodkih je bilo fizično prisotnih do 50 igralcev, so se pa v Sloveniji zgodili tudi večji dogodki, in sicer leta 2003 Lethal LAN XXI z 240 tekmovalci v strelskih igrah in leta 2008 Grand LAN z 270 tekmovalci ter denarnim skladom v vrednosti 13.000 evrov (Zavašnik, 2020). Po tem je področje e-športa v Sloveniji stagniralo zaradi pomanjkanja sponzorjev in spodbud s strani državnih organov. Leta 2012 se je v Portorožu odvil odmeven e-športni turnir priljubljene videoigre Counter Strike: Global Offensive, ki je bil označen za najslabši turnir v celotni zgodovini e-športnih tekmovanj. Negativen vtis naj bi pustilo pomanjkanje denarne nagrade za zmagovalce ter dostopa do ustrezne opreme. Nekaterim igralcem so zaplenili tudi potne liste, ker organizatorji niso plačali njihove hotelske nastanitve (Lewis, 2016 v Zupančič, 2023). Do leta 2020 sta v Sloveniji bila aktivna predvsem dva redna organizatorja e-športnih turnirjev, to sta nepridobitno Društvo za elektronske športe (spid.si, b. d.) in agencija Legit marketing, d. o. o. Spid.si je prirejal več turnirjev, društvo pa je znano po organizaciji LAN-tekmovanj Epicenter LAN, ki so veljala za serijo največjih e-športnih dogodkov v Sloveniji. Potekali so večkrat letno, imeli pa so udeležbo do kar 400 igralcev ter denarni sklad nad 15.000 evrov. Na dogodkih so bile predstavljene tudi nove igre, ki so jih obiskovalci lahko preizkusili ter spoznavali znane osebnosti s področja e-športa (Zavašnik, 2020).

Leta 2020 je bila v Sloveniji ustanovljena enotna organizacija E-športna zveza Slovenije (EŠZS). EŠZS je neprofitna organizacija za promocijo e-športa v Sloveniji, ki s pomočjo sponzorjev in članov prireja veliko e-športnih dogodkov ter ima svoj statut. EŠZS ima svojo definicijo e-športa: »e-šport (tudi elektronski šport, tekmovalno igričarstvo in profesionalno igričarstvo) je krovni izraz, ki se uporablja za opis tekmovanja v videoigrah med poklicnimi igralci« (E-Športna Zveza Slovenija, b. d.). Igralci pa navadno pripadajo določenemu moštvu ali športni organizaciji, ki jih sponzorirajo različna podjetja, pri čemer prevladuje organizacijski model e-športa v takšni obliki, da si jih lahko navijači ogledajo v živo in s pomočjo živega prenosa v različnih spletnih medijih (Twitch ali YouTube), hkrati pa sodelujejo komentatorji za lažje sledenje igri (Pisk, 2021). Koristi, ki jih prinaša

EŠZS za razvoj e-športa na slovenskih tleh, so razvidne že iz statuta: »E-športna zveza Slovenije je združenje e-športnih društev, ki se ukvarjajo z e-športi, organizacijo e-športnih dogodkov, nudijo pomoč e-športnim organizacijam ter so kakorkoli povezani s področjem e-športa. Namen ustanovitve E-športne zveze Slovenije je uveljavitev in regulacija e-športa na državni ravni.« (Statut EŠZS, 1.člen) Z vse večjim oglaševanjem, prirejanjem rednih turnirjev, celo v obliki državnih prvenstev, večjimi denarnimi skladi, vodenjem enotne evidence e-športnikov, upravljanjem e-športnih ekip ter usklajevanjem pravil na državni ravni (tudi s šolanjem sodnikov) EŠZS pripomore k razširitvi e-športa v Sloveniji in povečuje število e-športnikov in e-športnih ekip v domačem prostoru (Pisk, 2021).

Zaviralni vpliv na področju e-športa v Sloveniji je tudi pomanjkljiva pravna ureditev. Pogoji za prireditve manjših LAN- ali večjih, medijsko odmevnih turnirjev s področja e-športa je po 7. členu Zakona o javnem zbiranju (v nadaljevanju ZJZ) obvestitev policije glede dogodka. Če pa se prireja mednarodna športna prireditev ali prireditev z več kot 3000 obiskovalci, mora po 13. členu ZJZ organizator tudi pridobiti dovoljenje pristojne upravne enote. V Sloveniji se področje organizacije e-športnih dogodkov lahko ureja na podlagi določil Obligacijskega zakonika (v nadaljevanju OZ), in sicer z najemno pogodbo dvorane, s čimer organizatorji upoštevajo splošne pogoje in pravilnike najemodajalca in Zakon o javnem zbiranju (ZJZ).

S težavo pa v Sloveniji obravnavamo tudi problematiko t. i. loot boxov (podrobneje opisano v poglavju 4.5) ali drugih prikritih iger na srečo, ki se pojavljajo v videoigrah. 137. člen OZ določa, da otroci do sedmega leta starosti ne odgovarjajo za povzročeno škodo in ne veljajo za opravilno sposobne osebe, zato ne morejo sklepati pogodb, razen če se s tem strinjajo starši ali zakoniti zastopniki. Po slovenski zakonodaji otroci do sedmega leta ne morejo sklepati pogodb, kot so nakupi v digitalni aplikaciji ali na spletnih mestih. Tudi mladoletnik od sedmega do 14. leta ne odgovarja za nastalo škodo, razen če se dokaže njegovo zmožnost razsojanja. V obeh primerih gre za mladoletnike do največ 14. leta starosti; po dopolnjenem 14. letu mladoletnik odgovarja po splošnih pravilih o odgovornosti za škodo. Problem se pojavi, saj so osebe nad 14. letom starosti še vedno mladoletniki, razvijalci videoiger pa spretno izkoriščajo njihovo neizkušenost in nevednost s ponujanjem loot boxov (Ministrstvo za gospodarstvo, kulturo in šport, 2021).

Kadar želi mladoletna oseba v fizični trgovini v večini držav Evropske Unije kupiti videoigro, neprimerno starostni skupini, lahko prodajalec preveri starost kupca in zavrne nakup (v Sloveniji tovrstnih omejitev ni). Za razliko od tega se loot boxi predstavljajo kot digitalna vsebina v videoigrah, na

raznih spletnih mestih ali aplikacijah. V primeru nezaželenega nakupa loot boxov potrošniki niso upravičeni niti do odstopa pogodbe v 14 dneh, kakor to velja za ostale spletne nakupe. Tako poteka regulacija področja digitalnih vsebin in storitev v okviru digitalne strategije, s prenosom direktiv EU 2019/770, 2019/771 in direktive Omnibus 2019/2161 v nacionalne zakonodaje pa so napovedane spremembe v potrošniški zakonodaji (Ministrstvo za gospodarstvo, kulturo in šport, 2021). S to spremembo naj bi se za digitalne nakupe in uporabo digitalnih storitev zagotovilo učinkovitejšo zaščito v primerih, ko ponudnik ne zagotovi dogovorjene storitve ali zagotovi takšno storitev z napako.

Po sodbi sodišča v Šmohorju (nem. Hermagorju) (podrobneje opisano v poglavjih 4.3 in 4.5) se tudi v Sloveniji ponuja možnost, da lahko potrošniki za loot boxe zahtevajo povračilo denarja. Kot je bilo omenjeno že v prejšnjem podnaslovu, loot boxi temeljijo na aleatornem elementu, pri čemer igralec kupi loot box z valuto videoigre, za to pa uporabi resničen denar. Definicijo loot boxov lahko povežemo z 2. členom Zakona o igrah na srečo (v nadaljevanju ZIS), ki določa, da je temeljna lastnost igre na srečo enaka možnost zadeti dobiček ob plačilu določenega zneska. Izid igre je odvisen od naključja. 3. člen ZIS nadalje določa, da lahko igre na srečo prireja izključno Republika Slovenija ali koncesionar, ki je od pristojnega organa pridobil dovoljenje za njihovo izvajanje. Razvijalci videoiger pa dovoljenja za izvajanje iger na srečo od Republike Slovenije nimajo, zato lahko kupec od ponudnika zahteva povračilo denarja.

4.3 Razvoj in pravna ureditev e-športa v Avstriji in Nemčiji

V drugih evropskih državah, kot sta Nemčija in Avstrija, se je e-šport razvil bistveno hitreje. Že pred dvajsetimi leti so igralci organizirali turnirje, ki so primerljivi z današnjimi nacionalnimi in mednarodnimi tekmovanji v e-športu. Nemčija ima danes že več kot tri milijone e-športnih igralcev, svojo e-športno zvezo eSport-Bund Deutschland (ESBD) so ustanovili leta 2017 (Gözl, 2020). ESVÖ ali eSport Verband Österreich pa deluje v Avstriji že od leta 2007, kjer so leta 2018 priredili enega izmed največjih e-športnih turnirjev v Evropi, na katerem je sodelovalo kar 5000 tekmovalcev (ESVOE).

Organizatorji e-športnih dogodkov v Nemčiji potrebujejo v skladu z veljavno nemško sodno prakso dovoljenje za igralni salon v skladu s členom 33i Trgovinskega zakonika ali t. i. Gewerbeordnung (GewO). Dovoljenje je povezano s številnimi resnimi omejitvami za e-šport, npr. da je dostop mo-

goč šele od dopolnjenega 18. leta starosti. Za razmeroma mlado ciljno skupino, ki jo e-šport privlači, je za mnoge e-športne prireditve v Nemčiji omenjena ureditev omejevalna (Gunia, 2018). V Avstriji pa so edina pravila za prirejanje takšnih dogodkov v Spodnjeavstrijskem zakonu o prireditvah (državnopravno konsolidirano) ali v nemščini Niederösterreich Veranstaltungsgesetz (NÖ Veranstaltungsgesetz), ki določa, da mora organizator prireditev prijaviti pristojni upravni enoti (WKO, 2023). V Nemčiji na področju zaščite mladoletnikov pride v poštev tudi Zakon o varstvu mladoletnikov oz. Jugendenschutzgesetz (JuSchG).

Na področju boja proti prikritim igram na srečo v videoigrah je v ospredju sodba okrožnega sodišča Šmohor (nem. Hermagor) v Avstriji, ki je odločilo, da mora razvijalec igre FIFA Electronic Arts (EA) tožniku povrniti denar, ki ga je porabil za nakup paketov FIFA, v obliki loot boxov. Igralec je namreč z resničnim denarjem kupil igralno valuto »FIFA Points« v znani nogometni simulacijski igri FIFA, ki jo je mogoče zamenjati za t. i. pakete FIFA. Ti vsebujejo naključno izbrane kartice igralcev različne redkosti za tekmovanje. Kartice igralcev, ki so »izvlečene« iz paketa, lahko igralec uporabi v svoji ekipi ali jih proda drugim igralcem na sekundarnem trgu za igralno valuto. Igralec je družbo Sony (Sony je matično podjetje podjetja EA) obtožil, da je kršila monopol na področju iger na srečo v Avstriji, saj zasnova paketov FIFA predstavlja igre na srečo in Sony nima koncesije oz. dovoljenja za prirejanje iger na srečo. Okrožno sodišče v Šmohorju je 26. februarja 2023 izdalo prvostopenjsko sodbo in družbi Sony naložilo, naj povrne 338,26 evra. Ugotovili so, da je vsebina kupljenih paketov FIFA bila odvisna od naključja in je predstavljala tudi denarno korist, kar pomeni, da je šlo za igro na srečo v smislu člena 2. avstrijskega Zakona o igrah na srečo ali t. i. Glücksspielgesetz (GlückG). Potemtakem je pakete FIFA mogoče opredeliti kot igro na srečo, s čimer je Sony kršil državni monopol na področju iger na srečo. Posledično so bile pogodbe o nakupu loot boxov nične in tožnik je bil upravičen do vračila kupnine (Dimov, 2023).

4.4 Pomen oznak PEGI in USK za varstvo mladoletnikov

E-šport nima enotnega priznanja, opredelitve ali uvrstitve med tradicionalne športe, je pa potreba po pravni ureditvi vse večja, predvsem zaradi povezanosti z otroki in mladostniki. Povezanost izhaja iz dejstva, da je e-šport oblika računalniške ali videoigre, torej je v svojem temelju igra, ki je neizogiben del odraščanja. V sodobnem svetu se otroška in mladostniška igra vse bolj digitalizirata, s čimer se povečuje uporaba videoiger. Več kot 90 % otrok, starejših od dveh let, igra videoigre, tri četrtine ameriških gospodinjstev pa imajo konzolo za videoigre (Aldanko, 2023). Leta 2019 se je število srednjih šol v Združenih državah Amerike, ki sodelujejo v e-športih, razširilo z 200 na

več kot 1200. Starostna skupina udeležencev e-športov je tako bila sestavljena iz najstnikov, srednješolcev in študentov (Hennick v Zhong idr., 2022). Otroška raba informacijsko komunikacijske tehnologije je lahko pojmovana kot del kulturnega razvoja, vključenost mlajših generacij v svet e-športa pa neizogibna. S tem se temeljna pravna vprašanja pojavljajo v zvezi z otroki in mladostniki in ne z odraslimi in profesionalnimi igralci videoiger. Kljub ugotovljenim pozitivnim učinkom videoiger, kot so izboljšanje kognitivnih sposobnosti ter bralnih in komunikacijskih spretnosti (Franceschini idr., 2022), se največ dilem pojavlja na področju zlorab otrok in mladostnikov, ki so neizkušeni in brez popolne opravilne sposobnosti in s tem povezane zaščite mlajših igralcev. Dileme se pojavljajo tudi pri vsebini tako vojnih, strelskih in borbenih kot tudi drugih videoiger, predvsem glede kulturnega in političnega vpliva in duševnega zdravja mladostnikov.

Eden izmed načinov preprečevanja zlorab in kontrole vsebine videoiger predstavljata organizaciji USK (Unterhaltungssoftware Selbstkontrolle) in PEGI (Pan-European Game Information). USK je nemška organizacija, odgovorna za ocenjevanje videoiger, PEGI pa je širši evropski sistem ocenjevanja vsebin videoiger. Vzpostavljen je bil z namenom pomoči in informiranja evropskih potrošnikov glede starostne primernosti in vsebinskih opisov videoiger ter aplikacij na trgu. Razvila ga je Evropska zveza za interaktivno programsko opremo (ISFE), uporabljati pa se je začel aprila 2003, ko je številne nacionalne sisteme ocenjevanja starosti nadomestil enoten evropski sistem.

V nekaterih državah (npr. Združenem kraljestvu) je uporaba oznake PEGI na videoigrah pravno zavezujoča, v Sloveniji in večini drugih evropskih držav se priporoča, uporablja in priznava, zaradi odsotnosti njene zakonske podlage pa ni obvezna. Neučinkovito regulacijo v obliki oznak PEGI in USK so predvidevale že prve raziskave ob ustanovitvi PEGI-ja, saj kritične ocene videoiger, podane z oznakami, nasprotujejo komercialnim interesom proizvajalcev (Xlao, 2023). S tem se poraja vprašanje o učinkovitosti takih oznak, če niso pravno zavezujoče.

Prireditelje e-športnih dogodkov v Sloveniji zavezuje le Zakon o javnih zbiranjih (ZJZ). Splošna dolžnost organizatorja je namreč, da mora shod oz. prireditve organizirati tako, da bo poskrbljeno za red, varnost in zdravje udeležencev ali drugih oseb, da ne bo ogrožen javni promet in da ne bo nedopustne obremenitve okolja (povzeto po 10. členu ZJZ). V Nemčiji je ocenjevanje videoiger z oznakami zakonsko urejeno le v 14. členu nemškega Zveznega združenja za interaktivno zabavno programsko opremo (nem. Bundesverband Interaktive Unterhaltungssoftware). Tekmovanja v e-športu ne glede na spornost vsebin pa nimajo nobenih omejitev. Sicer je v Nemčiji področje zaščite mladoletnikov dobro razvito, saj so sprejeli poseben zakon, namenjen specifično zaščit

mladoletnikov. Gre za Jugendschutzgesetz (JuSchG), s katerim vse bolj učinkovito s kogentnimi normami posegajo v avtonomijo prirediteljev e-športnih tekmovanj in proizvajalcev videoiger.

Oznake USK in PEGI na videoigrah niso obvezne, poleg tega pa imajo kopico pomanjkljivosti. Za potrošnike v večini evropskih držav, kot tudi v Sloveniji, predstavljajo zgolj usmeritev, natančnejše ocene in strokovna priporočila pa morajo osebe (predvsem starši) opraviti sami. Do potrebnih informacij lahko dostopajo na različnih spletnih mestih, do katerih se morajo dokopati sami. Poleg tega problem predstavlja slaba informiranost staršev o pomenu posameznih oznak in opisov. Zabeleženi so bili podatki o napačnem razumevanju oznak, pri čemer so potrošniki bili prepričani, da določena oznaka pomeni oceno težavnosti, pomenila pa je starostno oceno (Morris, 2012). Pomanjkljivost oznak USK in PEGI je tudi v označevanju starostnih mej. USK ločuje starostne skupine nad 0, 6, 12 in 18 let, PEGI pa nad 3, 7, 12, 16 in 18, pri čemer so pravno zavezujoče le ocene od 12 naprej (pri državah, ki že imajo zavezujoče ocene). Do nejasnosti prihaja tudi, kadar je igra zasnovana po filmu ali televizijski oddaji. Ti imajo ločene sisteme za ocenjevanje starostne primernosti, ki jih postavlja ameriško združenje za filme MPAA. Starostne ocene pri filmih se velikokrat ne skladajo z ocenami pri igrah. Primer takega neskladja je World Wrestling Entertainment (WWE) oz. profesionalna ameriška rokoborba, ki ima svojo televizijsko oddajo. Ta ima starostno oznako PG (parental guidance), kar pomeni, da jo lahko gledajo mlajši otroci v spremstvu staršev. Videoigra, ki je nastala po oddaji, pa je ocenjena s PEGI 16 in označuje prikaz nasilja in spolne aktivnosti, podobne tisti v realnem življenju, rabo neprimerne jezika, tobaka, alkohola in prepovedanih drog (Morris, 2012). Neuskladenost starostnih ocen lahko pri potrošnikih povzroči zmedo in vodi v nakup starostno neprimernih iger za otroke in mladostnike.

4.5 Prikrite igre na srečo

Vse večji problem na področju e-športa so tudi prikrite igre na srečo, ki jih ponujajo proizvajalci videoiger v obliki t. i. loot boxov. Gre za igralno mehaniko v videoigrah, s katero lahko igralci pridobijo naključne virtualne predmete, največkrat za nadgradnjo igralnih predmetov (orožja, opreme) ali likov, kar predstavlja prednost v igri – napredovanje ali izboljšanje položaja tekmovalca (Zendle, 2020). Predmeti so običajno razdeljeni v različne kakovostne razrede, ki so barvno označeni glede na pogostost oz. redkost pojavljanja (od »običajnih« do »redkih« in »legendarnih«). Barvne označbe so za mladostnike bolj vabljive in povečujejo željo po pridobitvi loot boxov (Woodhouse, 2023).

Izvajanje loot boxov pa ni homogeno, kar otežuje natančno definiranje in zavira izdajo enotne zakonodaje glede te problematike; trenutno obstaja mnogo različic, ki se med seboj razlikujejo glede uporabe, verjetnosti pridobitve redkega predmeta ob večkratnih nakupih in možne uporabe osvojene vsebine. V nasprotju z drugimi mikrotransakcijami, kot so razširitve iger v obliki dodatkov DLC, je pri loot boxih poudarek predvsem na aleatornem elementu. Iz tega lahko izpeljemo povezavo med loot boxi in igrami na srečo. Pred nakupom posameznega loot boxa so igralcu večinoma predstavljene potencialne pridobitve. Algoritem videoigre pa naključno določi, kateri predmet/nadgradnja bo kupec loot boxa dobil. Naključen izbor algoritma lahko dojemamo kot srečo. Kritike loot boxov se nanašajo na to, da znatno povečujejo problem sistema »Pay2Win« (»kupi si zmago/plačaj za zmago«). Da bi videoigro lahko uvrstili v kategorijo »Pay2Win«, mora imeti igralec možnost nakupa izboljševalnega igralnega dodatka z realnim denarnim sredstvom, kar se sklada s principom nakupa loot boxov.

Novo raziskave kažejo, da lahko zabavni in na videz neškodljivi nakupi loot boxov pri igranju videoiger v mladostništvu vodijo v tvegano vedenje v odraslosti npr. v odvisnost od iger na srečo. Zaradi pogoste vključenosti mehanizmov loot boxov v priljubljene otroške igre (npr. franšizo Pokemon) morajo starši poznati tveganja, ki jih prinaša njihova raba, ter spremljati otrokovo posluževanje omenjenih vsebin. Nevarnosti vse pogostejše vključenosti mehanizmov loot boxov v videoigre, ki jih igrajo mladostniki, se zaveda tudi mnogo raziskovalcev. Na univerzi Central Queensland so ugotovili, da večina najbolj prodajanih iger vsebuje loot boxe in da mladostniki, stari od 12 do 24 let igrajo igre, ki vsebujejo te mehanizme. Zanje naj bi povprečen mladostnik porabil od 50 do 72 dolarjev na mesec (Osbourne, 2023). Zendle idr. (2018) so v najobsežnejši raziskavi s 14.182 udeleženci empirično dokazali korelacijo med uporabo mehanizmov loot boxov in odvisnostjo od iger na srečo. Ugotovili so močnejšo korelacijo z odvisnostjo od iger na srečo kot s prej ugotovljeno zlorabo alkohola in prepovedanih drog. Več denarja ko naj bi igralci porabili za nakup loot boxov, hujše naj bi bile njihove težave z igrami na srečo. Zaradi formalnih značilnosti, ki si jih loot boxi delijo z drugimi oblikami iger na srečo, bi lahko med igralci delovali kot vstop v nadaljnje, problematično igranje iger na srečo. V zadnjih letih je na tem področju bila najbolj preudarna sodba okrožnega sodišča Šmohor v Avstriji, ki je ugodilo tožniku, da mu mora tožena stranka EA, ki je proizvajalec igre FIFA, vrniti denar, ki ga je tožnik porabil na loot boxih. Tožnik je uspešno argumentiral, da je posledica kupljenega loot boxa odvisna od naključja. Tožnik je lahko od EA zahteval povračilo denarja, saj tožena stranka nima koncesije za prirejanje iger na srečo.

Pri loot boxih lahko govorimo tudi o spornosti pravne definicije v večini državah, in sicer glede možnosti subsimiranja loot boxov pod pojem iger na srečo. Po Zakonu o igrah na srečo so igre na srečo »igre, pri katerih imajo udeleženci za plačilo določenega zneska enake možnosti zadeti dobitke, izid igre pa je izključno ali pretežno odvisen od naključja ali kakšnega negotovega dogodka« (ZIS, 2. člen). Z omenjeno definicijo se v svojem principu skladajo tudi loot boxi, ki jih potem takem v Sloveniji lahko obravnavamo kot obliko iger na srečo. Pri e-športnih tekmovanjih (npr. FIFA), kjer je izid tekmovanja rezultat veččin »ekipe« igralnih likov, ki jo sestavi igralec oz. tekmovalec, so nadgradnje v obliki loot boxov edini sporni vidik teh tekmovanj. Sicer obstajajo videoigre, kjer vsebina loot boxov ne predstavlja povečane možnosti za zmago oz. napredka, temveč prihranek v času igralca (npr. igra Heroes of the Storm podjetja Activision-Blizzard), prevladuje pa mnenje, da imajo vsebine loot boxov temeljni vpliv na igranje. Tako je predvsem v strateških in gradbenih igrah – primer take videoigre je Travian. Naraščajoče kritike zaradi vse bolj izkoriščevalske narave mehanike loot boxov za uporabnike so dosegle vrhunec leta 2017 z izdajo videoigre Star Wars: Battlefront II. Proizvajalec te igre EA je moral po pritožbah kupcev iz igre odstraniti sistem mikrotransakcij. Pritožbe so se nanašale na dejstvo, da so igralci, ki ne investirajo v loot boxe, za približno 40 ur igranja v zaostanku v primerjavi z igralci, ki te mehanizme kupijo. Loot boxi in podobni mehanizmi videoiger so povzročili, da nakup videoiger ni več le enkratno, temveč gre bolj za storitev, kjer je igra sprva lahko tudi brezplačna, nato pa za uspešno in učinkovito igranje priporoča (ali celo zahteva) nakup loot boxov (Hern, 2017).

Tudi po poročilu Zvezne komisije za trgovino (angl. Federal Trade Commission ali FTC) loot boxi predstavljajo predmet zaskrbljenosti zaradi njihove podobnosti s stavami in igrami na srečo ter zaradi principa delovanja, ki spodbuja zasvojenost tudi mladoletnih potrošnikov (Osbourne, 2023). Zaradi tega sta leta 2020 Odbor za ocenjevanje zabavne programske opreme (ESRB) in PEGI napovedala, da bodo igre, ki vsebujejo loot boxe in druge oblike transakcij v igri z naključnimi elementi, označene z novo oznako »nakupi v igri (vključuje naključne predmete)«. Ena od študij, ki so proučevale učinkovitost igralnih oznak (kot sta PEGI in USK), pa je pokazala, da 71 % priljubljenih iger, ki vsebujejo loot boxe, v trgovini Google Play ni imelo omenjene oznake (Xiao, 2023), s čimer se ponovno izgubi njen pomen.

Mehanizmi loot boxov so prisotni pri vse več videoigrah, ki se pojavljajo na tekmovanjih v e-športu. Posledično postajajo del teh tekmovanj in sodelujočim omogočajo razne prednosti, tj. povečujejo možnosti za zmago. Zaradi povezanosti posluževanja mehanizmov loot boxov in tveganih vedenj

se s popularizacijo e-športov širi tudi stavna industrija, tudi na področju stav glede rezultatov v e-športu. Svetovni trg e-športnih stav je leta 2020 dosegel 17,2 milijarde dolarjev (Roberts, 2021, v Zupančič, 2023).

5 Razprava in sklep

E-šport je razmeroma mlado področje, ki zaradi hkratnega pomanjkanja pravne ureditve in naraščajoče priljubljenosti ter dobičkonosnosti odpira mnogo dilem, vprašanj in zahtev. Porast e-športa v našem okolju se je zgodil na začetku 21. stoletja, zaradi tehnološkega napredka in populacije mladostnikov, ki jih je svet videoiger najbolj zanimal, pa se je ekspanzivno razširil tudi v domače okolje. Razširjenost in preprost dostop do e-športnih vsebin sta prav tako odprla možnosti za zlorabe in izkoriščanje mladostnikov, s čimer se vse bolj povečuje zahteva po učinkovitejši pravni ureditvi področja e-športa.

E-šport kljub nasprotnikom in kritikom zaradi svoje priljubljenosti oblikuje prihodnost sodobnega tekmovanja in zabave. Definiranje in ureditev e-športa kot samostojne športne discipline bi omogočila priznavanje e-športa kot uradne oblike tekmovanja, kar bi lahko vodilo k boljši zaščiti igralcev in omogočalo enostavnejše prirejanje e-športnih dogodkov. Tudi enotna in jasna pravna definicija bi olajšala upravljanje in nadzor nad industrijo e-športa, kar bi lahko prispevalo k večji preglednosti, transparentnosti in dolgoročni trajnostnosti tega področja. S tem bi se prav tako vzpostavili pravni standardi, ki bi predstavljali stalne zahteve na področju e-športa. Problem predstavlja dejstvo, da je e-šport globalni pojav, zaradi česar je težko doseči konsenz med različnimi državami in jurisdikcijami glede pravil in regulativ. E-šport namreč obsega širok spekter dejavnosti, vključno z organizacijo tekmovanj, varstvom mladoletnikov, sponzorstvi, razvijanjem videoiger in delom igralcev, kar zahteva kompleksno pravno ureditev, ki upošteva vse vidike industrije. Tako je ključno, da se vključijo vsi relevantni na tem področju, torej igralci, organizatorji, predstavniki mladoletnikov, zakonodajalci in strokovnjaki za pravo za oblikovanje celovite pravne ureditve e-športa. Zadostna pravna ureditev bi vodila tudi do zagotavljanja integritete e-športa in spodbujala zdrav razvoj e-športne industrije (Gunia, 2018).

Zaradi velike nevarnosti, ki so ji izpostavljeni mladoletniki kot najpogostejši uporabniki videoiger, je eno najpomembnejših področij v e-športu njihova zaščita. Zakonska podlaga na tem področju se med posameznimi državami razlikuje. Za najrazvitejšo velja Nemčija, saj so tam sprejeli poseben zakon, namenjen varstvu mladoletnikov – Jugendenschutzgesetz (JuSchG), ki je glede na študij

literature in zakonske podlage najučinkovitejši za svoj namen. V Nemčiji so računalniške igre, kot tudi filmi, podvržene zakonski regulaciji. 14. člen JuSchG zahteva, da so filmi in igre ustrezno označeni glede na vsebino, pri čemer lahko to označevanje izvajajo državni organi ali regulativna organizacija USK. Ta določa označevanje igralnih vsebin v petih kategorijah, vključno z označevanjem starostne meje, ki je prisotna na embalažah videoiger. S takšnim označevanjem postavlja meje in orientacijske točke, katerih upoštevanje naj bi preprečilo, da bi vsebina škodovala razvoju mladoletnikov. Njim škodljivi mediji so uvrščeni na poseben seznam, kar pomeni, da morajo biti za otroke in mladostnike javno nedostopni. Distribucija takih medijev mladoletnikom je kaznivo dejanje. Zaščita te populacije se v Nemčiji šteje za zgledno na mednarodni ravni, tudi ker zakonodaja določa stroge meje glede prikazovanja nasilnih vsebin mladoletnikom. V 131. členu nemškega Kazenskega zakonika ali Strafgesetzbucha so določene zakonske meje dovoljenega ravnanja. V skladu z njim sta tako razširjanje kot dajanje na voljo prikazov nasilja osebam, mlajšim od 18 let, kaznivi dejanji (Zimmermann, 2008). V Sloveniji ugotavljamo prav nasprotno: pomanjkljivo oz. nezadostno pravno ureditev, saj niti uporaba starostnih ocen z oznakami PEGI ali USK za nakup videoiger ni pravno zavezujoča. Vse bolj se kaže potreba po varstvu mladoletnikov zaradi izkoriščevalskih namenov razvijalcev videoiger, kar bi lahko dosegli s sprejemom posebnega zakona po vzoru Nemčije ali z novelo Kazenskega zakonika RS.

Naslednja dilema, ki jo je treba poudariti, je nakupovanje loot boxov v videoigrah, ki predstavlja kompleksen problem zaradi etičnih, ekonomskih in regulatornih vidikov. Soočeni s hitrim razvojem digitalnega igralnega okolja, so loot boxi postali predmet razprav in kritik glede svoje podobnosti z igranjem na srečo. Najspornejše je dejstvo, da je naključni element v loot boxih dovolj podoben elementom, ki opredeljujejo tradicionalne igre na srečo, da bi lahko bili obravnavani kot oblika le-teh. Čeprav mnogi igralci uživajo v presenečenju, ki ga ponujajo loot boxi, obstaja resna zaskrbljenost zaradi potencialnih škodljivih učinkov, zlasti na mlade in dovzetne posameznike. Zasojejenost, finančna izčrpanost in pomanjkanje transparentnosti glede verjetnosti dobivanja železih nagrad so le nekateri od problemov, ki jih prinaša ta praksa. Regulatorji in industrija se soočajo z izzivom, kako najbolje uravnotežiti svobodo potrošnikov, inovacije in varstvo igralcev. Mnoge države so že uvedle ali razmišljajo o uvedbi regulativnih ukrepov, kot so obvezno razkritje verjetnosti, starostne omejitve in prepovedi za mladoletnike ter označevanje iger z loot boxi kot »nakupi v igri« (Xiao, 2023). Rešitev predstavlja popolna ukinitvev loot boxov kot takih. Poleg tega pa se pojavljajo alternativni modeli monetizacije, ki odpravljajo potrebo po nakupovanju loot boxov, npr. neposredna prodaja predmetov ali vsebine v videoigrah za točno določeno (fiksno) ceno. Čeprav loot boxi

ostajajo donosen posel za industrijo iger, je jasno, da bo njihova prihodnost verjetno odvisna od nadaljnjega razvoja regulativnih okvirov in sprememb v preferencah potrošnikov.

Čeprav je na področju e-športa dosežen že opazen napredek, še vedno ostaja veliko izzivov, ki zahtevajo dodatno raziskovanje. Razvoj e-športa je vzbudil navdušenje in pritegnil veliko pozornosti, vendar ostaja potreba po dodatnem razvoju, da bi ta sektor postal bolj transparenten, reguliran in pravičen. Nadaljnje raziskave so ključnega pomena za razumevanje številnih vidikov e-športa, vključno z vplivom na varstvo mladoletnikov, gospodarskim doprinosom ter vplivom na družbo kot celoto. Le s temeljitim in sistematičnim pristopom k raziskovanju lahko ustvarimo trdne temelje za razvoj e-športa kot trajnostne in spoštovane dejavnosti. Poleg tega je treba raziskati tudi pravne in etične vidike, da bi se vzpostavili ustrezni okvirji in smernice za delovanje tako dinamičnega sektorja. Z vztrajnimi prizadevanji za nadaljnje raziskovanje in sodelovanje lahko e-športi postanejo še bolj urejen, dostopnejši in varnejši prostor za igralce, organizatorje, gledalce ali obiskovalce takih prireditev.

Viri

Alanko, D. (2023). The health effects of video games in children and adolescents. *Pediatrics in review*, 44(1), 23–32. <https://doi.org/10.1542/pir.2022-005666>

Chan, G., Huo, Y., Kelly, S., Leung, J., Tisdale, C., & Gullo, M. (2022). The impact of eSports and online video gaming on lifestyle behaviours in youth: A systematic review. *Computers in Human Behavior*, 126, 106974. <https://doi.org/10.1016/j.chb.2021.106974>

Dimov, V. (2023). Gaming: Glücksspiel-Urteil in Österreich – Sony muss Lootbox-Kaufpreis erstatten. <https://haer-tung.de/wissen/gaming-gluecksspiel-urteil-in-oesterreich-sony-muss-lootbox-kaufpreis-erstatten/>

E-športna zveza Slovenije. (2021). Statut E-športna zveza Slovenije. https://www.eszs.si/?lang_id=1&page_id=21

Franceschini, S., Bertoni, S., Lulli, M., Pievani, T., & Facoetti, A. (2022). Short-term effects of video-games on cognitive enhancement: The role of positive emotions. *Journal of Cognitive Enhancement*, 1–18. <https://doi.org/10.1007/s41465-021-00220-9>

Glücksspielgesetz (GSpG). (1989). BGBl. Nr. 620/1989. <https://www.ris.bka.gv.at/Geltende-Fassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10004611>

Gözl, J. (2020). *E-Sports in Deutschland: eine Konzeption zur Steigerung der Akzeptanz* (Bachelor's thesis).

Greer, N., Rockloff, M., Browne, M., Hing, N., & King, D. L. (2019). Esports betting and skin gambling: A brief history. *Journal of Gambling Issues*, 43. <https://doi.org/10.4309/jgi.2019.43.8>

- Gunia, H. (2018). *Die Anerkennung eSports als Sportart* (Seminararbeit).
- Hern, A. (2017). Star Wars Battlefront II and the problem with paid-for video game rewards. *The Guardian*. <https://www.theguardian.com/games/shortcuts/2017/nov/26/how-much-star-wars-battlefront-ii-and-the-problem-with-paid-for-video-game-rewards>
- Hiltscher, J. (2013). A short history of esports. *eSports yearbook*, 14, 9–14.
- Jugendschutzgesetz (JuSchG). (2002). BGBl. I S. 2730. <https://www.gesetze-im-internet.de/juschg/BJNR273000002.html>
- Novak, M. (2010). Uvod v pravo. *Evropska pravna fakulteta v Novi Gorici*, 433–449.
- MGTŠ. (2021). Video igre in varstvo mladih. <https://www.epc.si/si/novica/video-igre-varstvo-mladih>
- Morris, I. (2012). The problems with PEGI. <https://www.outcyders.net/article/the-problems-with-peg>
- Osborne, Jason W. (2023). How Loot Boxes In Children’s Video Games Encourage Gambling. *Forbes*. <https://www.forbes.com/sites/jasonwosborne/2023/05/25/how-loot-boxes-in-childrens-video-games-encourage-gambling/?sh=30b23bd45653>
- Pisk, J. (2021). Ali je e-šport nova športna panoga? Razmislek o športnosti e-športov. *Revija Šport*.
- Reitman, J. G., Anderson-Coto, M. J., Wu, M., Lee, J. S., & Steinkuehler, C. (2020). Esports research: A literature review. *Games and Culture*, 15(1), 32–50. <https://doi.org/10.1177/1555412019840892>
- Scholz, T. M., & Scholz, T. M. (2019). A short history of esports and management. *eSports is Business: Management in the World of Competitive Gaming*, 17–41. https://doi.org/10.1007/978-3-030-11199-1_2
- Snavely, T. L. (2014). *History and analysis of eSport systems* (Doctoral dissertation).
- Wagner, M. G. (2006, June). On the Scientific Relevance of eSports. *In International conference on internet computing* (str. 437–442).
- WKO. (2023). Organisation von Veranstaltungen. <https://www.wko.at/noe/tourismus-freizeitwirtschaft/freizeit-sport-betriebe/organisation-von-veranstaltungen/>
- Woodhouse, J. (2023). Loot boxes in video games. Commons Library Research Briefing Paper, CBP-8498. <https://commonslibrary.parliament.uk/research-briefings/cbp-8498/>
- Xiao, L. Y. (2023). Beneath the label: unsatisfactory compliance with ESRB, PEGI and IARC industry self-regulation requiring loot box presence warning labels by video game companies. *Royal Society Open Science*, 10(3), 230270. <https://doi.org/10.1098/rsos.230270>

Zakon o igrah na srečo (ZIS). (1995). *Uradni list RS*, št. 14/11, 108/12, 11/14 – popr. in 40/14 – ZIN-B. <http://pisrs.si/Pis.web/pregledPredpisa?id=ZAKO409>

Zakon o javnih zbiranjih (ZJZ). (2002). *Uradni list RS*, št. 64/11. <http://pisrs.si/Pis.web/pregledPredpisa?id=ZAKO1455>

Zavašnik, S. (2020). *Ešporti kot oglaševalska platforma v Sloveniji* (Doctoral dissertation, Univerza v Ljubljani, Fakulteta za družbene vede).

Zendle, D., & Cairns, P. (2018). Video game loot boxes are linked to problem gambling: Results of a large-scale survey. *PloS one*, 13(11), e0206767. <https://doi.org/10.1371/journal.pone.0206767>

Zendle, D., Meyer, R., Cairns, P., Waters, S., & Ballou, N. (2020). The prevalence of loot boxes in mobile and desktop games. *Addiction*, 115(9), 1768–1772. <https://doi.org/10.1111/add.14973>

Zhong, Y., Guo, K., Su, J., & Chu, S. K. W. (2022). The impact of esports participation on the development of 21st century skills in youth: A systematic review. *Computers & Education*, 191, 104640. <https://doi.org/10.1016/j.compedu.2022.104640>

Zimmermann, O., & Geissler, T. (Eds.). (2008). Streitfall Computerspiele: Computerspiele zwischen kultureller Bildung, Kunstfreiheit und Jugendschutz. *Deutscher Kulturrat*.

Zupanič, Ž. (2023). *Organizacijski in pravni vidiki prepoznavanja športne panoge e-šport* (Doctoral dissertation, Univerza v Mariboru, Fakulteta za organizacijske vede).

Problemi uporabe z umetno inteligenco obdelanih dokazov v kazenskem postopku

Oskar Peče 

Univerza v Mariboru, Pravna fakulteta

Maribor, Slovenija

Povzetek: V stalni debati glede tega, ali, in v kakšni meri, digitalni dokazi zahtevajo posebno obravnavo v okviru kazenskega postopka, prihaja do pogostega trenja med postulati poštenega postopka in stanjem tehnologije. Uporaba dokazov, obdelanih s pomočjo umetne inteligence, lahko posega v načela kazenskega postopka, ustaljene doktrine in pravice obdolženca. Sistemi umetne inteligence lahko dokaze obdelujejo na tri načine, tj. analitično brez vrednostnih zaključkov, analitično z vrednostnimi zaključki in za izboljšavo dokazov. Analitična obdelava brez vrednostnih zaključkov predstavlja izjemen poseg v zasebnost tako preiskovanih kot tudi drugih posameznikov, pri čemer se zaradi nadomestitve človeških čutov pri tovrstni uporabi pod vprašanje postavlja ustreznost doktrine plain view. Analitična obdelava z vrednostnimi zaključki ponuja rezultate, ki v kazenskem postopku niso dokazi, saj so primerljivi s strokovnim mnenjem, ki ga pridobijo stranke. Dokazi, obdelani s sistemi umetne inteligence za izboljšavo njihove predstavitve kakovosti, prenehajo biti dokaz, saj tovrstna obdelava kritično poseže v njihovo integriteto in zanesljivost njihove vsebine. Pravo ima pred sabo izjemen izziv, in sicer konkretno ureditev različnih načinov uporabe umetne inteligence v kazenskem postopku. Glede na dejstvo, da uporaba po navadi prehiti pravno ureditev, je razumno pričakovati, da bo velik del predmetne regulacije posledica sodne prakse, ki bo obravnavala primere neprimerne in prekomerne uporabe.

Ključne besede: digitalni dokazi, kazenski postopek, obdelava dokazov, umetna inteligenca

The challenges of using AI-processed evidence in criminal proceedings

Oskar Peče ✉

University of Maribor, Faculty of Law

Maribor, Slovenia

Abstract: In the ongoing debate about whether and to what extent digital evidence requires special consideration in criminal proceedings, there is frequent friction between the principles of fair procedure and the state of technology. The use of evidence processed through artificial intelligence can intrude upon the fundamental principles of criminal procedure, established doctrines, and the rights of the accused. Artificial intelligence systems can process evidence in three ways: analytically without value judgments, analytically with value judgments, and for the enhancement of evidence. Analytical processing without value judgments represents a significant intrusion into the privacy of both the investigated and other individuals, questioning the appropriateness of the plain view doctrine due to the replacement of human senses in such usage. Analytical processing with value judgments yields results that are not evidence in criminal proceedings, as they are comparable to expert opinions obtained by parties. Evidence processed by artificial intelligence systems to enhance their presentation quality ceases to be evidence, as such processing critically impinges on their integrity and the reliability of their content. Law faces a significant challenge: to concretely regulate the various uses of artificial intelligence in criminal proceedings. Given that the application often precedes legal regulation, it is reasonable to expect that much of this regulation will result from case law addressing cases of improper and excessive use.

Keywords: digital evidence, criminal procedure, evidence processing, artificial intelligence

1 Uvod

Bliskovit razvoj umetne inteligence (v nadaljevanju UI) na dnevni ravni vzbuja tako čudenje in pričakovanje kakor tudi strah in zgražanje v širši javnosti. Dnevno prihaja do razvoja tehnologije, ki na naša življenja vpliva tako zaradi naše voljne uporabe kakor tudi proti naši volji in pogosto brez našega zavedanja. Ne glede na mnoge koristi, ki jih ta tehnologija prinaša, moramo do nje vselej pristopati z zavedanjem, da njena uporaba predstavlja tveganje za temeljne pravice posameznikov (Council of the European Union, 2024). Problem je, da so nam koristi te tehnologije po navadi znane precej hitreje kot tveganja, saj nove tehnologije UI pogosto uporabljajo posamezniki, podjetja in celo države, še preden so deležne ustreznega nadzornega pregleda in preveritve (Grimm, Grossman & Cormack, 2021, str. 84). Ocena tveganj, povezanih s sistemi UI, je tudi ob previdnem in dobronamernem postopanju sicer problematična, saj ti sistemi podatke pogosto obdelujejo na način, ki posameznikom ni razumljiv, zaradi česar nam ti sistemi predstavljajo svojevrstne »črne škatle« (Chen & Tseng, 2023, str. 85).

Uporaba UI za forenzične namene ni povsem nova, saj je že uveljavljena in pogosta za namen avtomatizacije procesa ekstrakcije in prečiščevanja DNK-vzorcev. Kot nove v ospredje prihajajo razne tehnike uporabe UI za namene digitalne forenzike oz. odkrivanja in obdelave digitalnih dokazov, med njimi nekatere, ki so nekoliko sporne, kot npr. sistemi za prediktivno napoved kriminalne dejavnosti¹ in prepoznavo obraza (Grimm, Grossman & Cormack 2021, str. 36). Tovrstni načini uporabe so sporni, saj je vprašljiva ustreznost njihove uporabe z vidika človekovih pravic, pri čemer njihovo legitimno uporabo (oz. zaupanje vanjo) otežuje pomanjkanje ustrezne in konkretne zakonodajne ureditve.

V tem prispevku bom opredelil pravne probleme, povezane z uporabo umetne inteligence pri obdelavi dokazov v kazenskem postopku, ter predstavil relevantno pravno ureditev uporabe predmetne tehnologije. Vsebinsko je prispevek omejen na obdelavo predhodno obstoječih digitalnih dokazov in ne obravnava kreacije povsem novih (lažnih) vsebin. Obravnavana tema se navezuje na uporabo modernih digitalnih forenzičnih orodij, ki temeljijo na UI, za iskanje, kategorizacijo, razlago, predstavitev in izboljšanje digitalnih dokazov. V veliki meri gre za

¹ Ti sistemi skušajo na podlagi analitičnih metod ugotoviti čas in kraj povečanega tveganja kriminala z namenom učinkovitega razporejanja policijskih sredstev.

digitalizacijo človeškega miselnega procesa in izboljšavo njegovih zaznavnih in senzoričnih sposobnosti za namen forenzičnega in posledično kazenskega postopka.

2 Vrste uporabe

Za namene tega članka in analize pravnih problemov, povezanih z uporabo UI v kazenskem postopku, bomo uporabo tovrstne tehnologije razdelili na tri vrste: analitično brez vrednostnih zaključkov, analitično z vrednostnimi zaključki in izboljšavo digitalnih dokazov. Tovrstna kategorizacija je za namen teme predmetnega članka koristna, saj si omenjene tri kategorije v predstavljenem zaporedju sledijo glede na stopnjo problematičnosti. Pri tem se ne ocenjuje teža posameznih problemov v vsaki kategoriji, temveč se upošteva število problemov in spornih točk, ki so značilni za posamezno kategorijo. Problemi, ki so navedeni v posamezni kategoriji, so lahko prisotni tudi v naslednji kategoriji. Namen tovrstne kategorizacije je strukturiran pregled posameznih problemov in izogibanje ponavljanju opredelitve problemov, ki se pojavljajo v več kategorijah, ter smiselna primerjava različne uporabe umetne inteligence za obdelavo dokazov.

3 Analitična obdelava dokazov brez vrednostnih zaključkov

Pod vrsto uporabe za analitične namene brez vrednostnih zaključkov sodijo sistemi UI za iskanje relevantnih dokazov in njihovo kategorizacijo. Gre za najpogostejši način uporabe umetne inteligence v preiskavi, pri katerem so uporabljena forenzična orodja na podlagi UI, ki so namenjena zbiranju dokazov ali obdelavi predhodno zbranih oz. zavarovanih podatkov (Du, Lin, Lv, Liu & Ding, 2022, str. 1546). Pogosti primeri teh tehnologij so orodja za lažjo preiskavo zaseženih elektronskih naprav z analizo in primerjavo podatkov, orodja za prepoznavo znakov spolnih zlorab na fotografijah in orodja za zbiranje in obdelavo podatkov z namenom premagovanja ekripcije (Quezada-Tavárez, Vogiatzoglou & Royer, 2021, str. 1–2). Tukaj moramo upoštevati, da so na osnovni ravni tudi tovrstni sistemi sposobni »presoje« v smislu kategorizacije podatkov in smiselne prepoznave relevantnih informacij v določenih datotekah, vendar iz zbranih podatkov ne ustvarjajo vrednostnih zaključkov. Ta orodja služijo zbiranju (oz. odkrivanju) in predstavitvi dokazov na ljudem lažje razumljiv način z namenom, da posameznik kot dejanski ocenjevalec (in posledično odločevalec) na podlagi pregleda zbranih in predstavljenih podatkov oceni njihovo dokazno vrednost in vsebino ter samostojno ustvari vrednostni zaključek, v smislu potrditve nekega zatrjevanega dejstva ali odkritja novega dejstva. Gre za orodja, ki so pretežno uporabljena v postopku preiskave elektronskih naprav.

3.1 Preiskava elektronskih naprav in poseg v komunikacijsko zasebnost

Obdelava digitalnih dokazov predstavlja poseg v zasebnost posameznikov, na katere se podatki, zajeti v teh dokazih, nanašajo. V kontekstu preiskave elektronskih naprav (in z njo povezane obdelave digitalnih dokazov) primarno govorimo o posegu v komunikacijsko zasebnost imetnikov in uporabnikov naprav, na katerih se ti dokazi nahajajo oz. na katerih so bili odkriti. Pravico do komunikacijske zasebnosti določa 37. člen Ustave Republike Slovenije (Ustava Republike Slovenije, 1991) (v nadaljevanju URS), skladno s katerim je zaščiten tajnost pisem in drugih občil. V skladu s 37. členom URS ni varovana zgolj vsebina komunikacije, temveč tudi okoliščine in dejstva, povezana s komunikacijo (Ustavno sodišče Republike Slovenije, odločba Up-106/05-27 z dne 2. 10. 2008). Poseg v to pravico je dovoljen zgolj, kadar je predpisan z zakonom, za določen čas in če je nujen za uvedbo ali potek kazenskega postopka ali za varnost države, pri čemer mora konkreten poseg temeljiti na odločbi sodišča. Skladno s tem je preiskava elektronskih naprav v kazenskem postopku urejena v 219.a (in 223.a) členu Zakona o kazenskem postopku (Zakon o kazenskem postopku, 1995) (v nadaljevanju ZKP), ki določa, da je za preiskavo elektronske naprave potrebna odredba sodišča, ter preiskavo časovno omejuje. Preiskava elektronskih naprav in posledična analiza digitalnih dokazov predstavlja poseg v pravico do komunikacijske zasebnosti tudi v kontekstu Evropske konvencije o človekovih pravicah (Zakon o ratifikaciji Konvencije o varstvu človekovih pravic in temeljnih svoboščin) (v nadaljevanju EKČP), in sicer kot poseg v pravico do zasebnosti dopisovanja, ki je določena v 8. členu EKČP (Ivanshchenko proti Rusiji, 2011). Določilo 8. Člena EKČP sicer skupaj obravnava tako komunikacijsko zasebnost kakor tudi splošno varstvo zasebnosti (Klemenčič, 2011), kar URS sicer določa v 35. členu. Skladno s prakso Evropskega sodišča za človekove pravice (v nadaljevanju ESČP) je pri preiskavi osebnih elektronskih naprav, kot so pametni telefoni, zahtevana še večja zaščita v okviru posameznikove pravice do zasebnosti (Quezada-Tavárez, Vogiatzoglou in Royer, 2021, str. 6).

Obdelava oz. analiza digitalnih dokazov v okviru preiskave elektronskih naprav se navezuje na predhodno zavarovane podatke². S tem je analiza omejena na v konkretnem primeru zavarovano količino podatkov. Kljub omejenemu obsegu je tovrstna analiza pogosto zahtevna zaradi izjemne količine zavarovanih podatkov. Za preiskavo zavarovanih podatkov se že dolgo uporabljajo

² Pred dejansko analizo in pregledom podatkov, ki se nahajajo na preiskovani napravi, je ustvarjena istovetna kopija teh podatkov, pri čemer analiza v okviru preiskave poteka na tej, za namen preiskave ustvarjeni, istovetni kopiji podatkov.

posebna programska orodja za lažjo in učinkovito analizo, odkritje in kategorizacijo relevantnih podatkov s pomočjo iskalnih nizov in filtracije podatkov v skladu z določenimi lastnostmi. Tovrstna forenzična orodja, ki uporabljajo UI, so lahko še učinkovitejša, saj so poleg iskanja relevantnih datotek na podlagi metapodatkov in neposrednega besedilnega ujemanja z iskalnimi nizi znotraj besedilnih datotek zmožna prepoznavanja in razumevanja vsebine analiziranih podatkov.

Medtem ko podatkovni oz. tehnični obseg analize smiselno določa opredelitev preiskovane naprave v odredbi za preiskavo³, je primarni vsebinski obseg preiskave določen s pogojem za izvedbo preiskave elektronske naprave, in sicer da se nanaša na konkretno kaznivo dejanje, za katerega so podani utemeljeni razlogi za sum, da je bilo storjeno. Ta pogoj ni pomemben zgolj z vidika preprečevanja arbitrarnega odrejanja tovrstnih preiskav, temveč je ključnega pomena za presojo sorazmernosti posega v pravice imetnika naprave. Presoja razumnega razmerja sorazmernosti med uporabljenimi sredstvi in ciljem predstavlja test ustreznosti izvedenega zasega in preiskave elektronskih naprav, ki ga je ESČP utemeljilo v zadevi *Kruglov in drugi proti Rusiji* (Kruglov in drugi proti Rusiji, 2020). Preiskava elektronske naprave je namenjena zgolj iskanju dokazov v zvezi s konkretnim kaznivim dejanjem, za preiskavo katerega je bila odrejena, zaradi česar se njena ustreznost (tako obstoj preiskave kot njen vsebinski obseg) presojata z vidika tega konkretnega kaznivega dejanja.

Analizirati je treba tudi drugi vsebinski pogoj, ki izhaja iz vsebine predloga in odredbe o preiskavi elektronske naprave. Ta mora namreč vsebovati opredelitev vsebine iskanih podatkov⁴. Gre za pomembno sestavino odredbe, saj določa sekundarno vsebinsko omejitev preiskave, ki je za razliko od predhodno omenjene primarne vsebinske omejitve konkretnejša. Ne nanaša se na specifične datoteke ali shranjevalne lokacije, temveč na specifično vsebino in vrsto datotek. Smiselni namen te določbe je omejiti poseg v komunikacijsko zasebnost imetnikov in uporabnikov preiskovanih naprav ter preprečiti splošen oz. nediskriminatoren pregled podatkovne vsebine, ki v skrajni obliki predstavlja zlorabo preiskave v obliki »fishing ekspedicije« (Peče, 2022, str. 24). Od oseb, ki opravljajo konkretno preiskavo, seveda ni mogoče pričakovati,

³ Skladno s 3. odstavkom 219.a člena ZKP morata predlog in odredba o preiskavi elektronske naprave vsebovati (med drugim) podatke, ki omogočajo identifikacijo elektronske naprave, ki se bo preiskala. S tem je zahtevana konkretizacija preiskovanih naprav.

⁴ To je določeno v 3. odstavku 219.a člena ZKP.

da bi pred preiskavo poznali imena relevantnih datotek, njihovo vsebino in lokacijo na napravi. Realno se v sklopu preiskave pregledujejo datoteke širom naprave, za katere se sklepa, da lahko vsebujejo relevantno oz. iskano vsebino. Omejitev preiskovane vsebine torej smiselno ne omejuje analize kot take, temveč uporabo najdene vsebine.

Analiza podatkov v sklopu preiskave elektronske naprave je omejena na podatkovni obseg (zavarovani podatki) in vsebino, določeno v odredbi za preiskavo. Medtem ko uporaba umetne inteligence ne širi obsega preiskovanih podatkov (omejena je na enak obseg podatkov kakor človek preiskovalec), uporaba te tehnologije močno vpliva na kakovost in vsebinski obseg analize. Namen uporabe umetne inteligence za preiskavo sklopov podatkov je iskanje predvidene vsebine širom vseh zbranih podatkov (oz. datotek), česar človek v vlogi preiskovalca v primerih ogromne količine podatkov oz. datotek, v doglednem času, ni sposoben storiti. Zaradi dejanske zmožnosti pregleda vseh datotek v danem podatkovnem obsegu tovrstna analiza digitalnih dokazov smiselno predstavlja večji poseg v komunikacijsko zasebnost posameznikov, saj predstavlja vsebinsko obsežnejšo analizo.

3.2 Ustreznost doktrine *plain view*

Pri analizi zavarovanih podatkov z uporabo UI se pod vprašaj postavlja tudi veljavnost doktrine *plain view*. Kot je bilo do sedaj pojasnjeno, določitev preiskovane vsebine v odredbi zaradi narave analize učinkovito ne omejuje preiskovalnega vpogleda v napravo, temveč uporabo najdene vsebine. Pri preiskavi se pogosto odprejo in pregledajo tudi s preiskovano vsebino nepovezane datoteke. Zaradi tega lahko pri tovrstni preiskavi pride tudi do »odkritja« podatkov, ki niso povezani s preiskovanim kaznivim dejanjem. Odkriti podatki, ki v okviru konkretne preiskave sicer niso bili iskani, so lahko povezani z drugim kaznivim dejanjem. Gre za podatkovno vsebino, ki je absolutno izven odredbe o preiskavi elektronske naprave, na kateri temelji konkretna odredba. Za takšne situacije je v 12. odstavku 219.a člena ZKP določeno ustrezno ukrepanje oz. ravnanje s takšnimi podatki. To določilo sicer določa ustrezno ravnanje s tovrstno odkritimi podatki, vendar ne določa zakonitosti tako pridobljenih dokazov. Zakonitost tovrstne pridobitve dokazov se v konkretnem primeru ocenjuje z vidika doktrine *plain view* (Višje sodišče v Ljubljani, V Kp 55723/2018, 9. 4. 2020). Pri tem ne gre za presojo, ali ti podatki sodijo v vsebinski obseg odredbe, v okviru katere so bili pridobljeni, temveč gre za vprašanje obstoja pravnega temelja za izvedbo dela preiskave, v katerem so ti podatki bili odkriti.

Doktrina *plain view* določa izjemo zahteve predhodnega obstoja odredbe oz. odstop od njenih omejitev glede pridobivanja dokazov, ki jih policisti naključno najdejo (Hooper in Masters, 2017, str. 379). Kriterije za presojo dovoljenosti uporabe tako pridobljenih dokazov v kazenskem postopku je slovenska sodna praksa razvila v povezavi z ameriško sodno prakso⁵. Naključno najden dokaz je v skladu z doktrino *plain view* uporaben, če se je policist na mestu zasega dokaza (v času zasega), ki ima domnevno obremenilni značaj (kaže na drugo kaznivo dejanje), nahajal zakonito ter je najdba dokaza bila nenamerna in nepričakovana (Višje sodišče v Ljubljani, V Kp 55723/2018, 9. 4. 2020). Glede vprašanja, ali je uporaba doktrine *plain view* zaradi specifične narave digitalnih dokazov sploh ustrezna v povezavi s preiskavo elektronskih naprav, sta se v ZDA razvila dva mnenjska pola, pri čemer prvi digitalnim dokazom ne priznava posebne narave (koncept elektronske naprave kot »škatle dokumentov«), s čimer dopušča uporabo doktrine *plain view*, medtem ko drugi opozarja na obsežnejši podatkovni potencial digitalnih dokazov in njihovih nosilcev, kakor tudi na dejstvo, da doktrina *plain view* temelji na empiričnem konceptu vizualnega opazovanja, ki v fizičnem svetu ni dvoumen, v virtualnem pa je odvisen od metode preiskave. Pri tem izpostavljajo bistveno lastnost digitalnih dokazov, in sicer da za seznanitev s podatkovno vsebino naprave ni zadosten zgolj fizičen pogled na shranjevalno enoto, temveč je treba uporabiti elektronsko napravo⁶, da se pregleda vsebina te shranjevalne enote (Ward, 2011, str. 1169–1170). To posebno značilnost digitalnih dokazov, da je za njihovo odkritje treba napravo najprej odpreti in jo s tem narediti dostopno človeškemu čutom, je izpostavilo tudi Višje sodišče v Ljubljani v sklepu V Kp 55723/2018 z dne 9. 5. 2020, kjer je odločalo o ustreznosti uporabe doktrine *plain view* pri preiskavi elektronske naprave. Izpostavili so tudi, da je za oceno naključnosti odkritja treba ugotoviti, ali je policist ravnal v skladu s prvotno preiskavo, torej s prvotno odredbo. Sodišče je v predmetni sodbi kljub izpostavi posebnih lastnosti digitalnih dokazov zavzelo stališče, skladno s konceptom elektronske naprave kot škatle dokumentov, in potrdilo, da je doktrina *plain view* ustrezna pri preiskavi elektronskih dokazov.

Uporaba doktrine *plain view* je nekoliko spornejša, kadar se navezuje na preiskavo elektronske naprave, kjer je za analizo podatkovne vsebine bila uporabljena UI. V skladu z ameriško sodno prakso doktrina *plain view* ni uporabna v primerih, kjer je bila na zaščiteneh območjih uporabljena

⁵ Zaradi tega je za razumevanje doktrine *plain view* in vprašanj, ki se nanjo navezujejo, smiselno upoštevati ameriško sodno prakso.

⁶ Praviloma drugo elektronsko napravo (in ne tiste, ki je vir podatkov), sicer gre za t. i. živo analizo, ki zaradi potrebe po zagotovitvi integritete podatkov ni ustrezna.

»tehnologija za izboljšanje čutil« (npr. termalne kamere ali visoko zmogljivi teleskopi) (Hooper & Masters, 2017, str. 380). S tega vidika je vprašljiva že uporaba forenzičnih programov (npr. X-ways Forensics), ki preiskavo olajšajo z različnimi funkcijami, kot sta odkrivanje izbranih datotek in odkrivanje datotek po ključu iskalnih nizov. Kadar se za tovrstne namene uporabi UI, ne govorimo zgolj o izboljšanju čutil preiskovalca, temveč govorimo o nadomestitvi njegovih čutil s sistemom, ki ima s človekom neprimerljivo višjo raven sposobnosti odkrivanja in analize podatkovne vsebine. Uporaba forenzičnega programa, ki za analizo podatkovne vsebine uporablja umetno inteligenco skladno z argumentom *a minore ad maius*, upoštevajoč ameriško sodno prakso, ni skladna s konceptom doktrine *plain view*.

Pri uporabi tovrstnih sistemov se pojavlja tudi drug problem, in sicer ali je odkritje podatkov pri uporabi programov, ki od uporabnika zahtevajo specifikacijo iskane podatkovne vsebine, sploh lahko naključno. Forenzični programi, kot je Cellebrite⁷, od uporabnika zahtevajo določitev iskane vsebine (DiSilvio, 2023). Upošteva, da je predvidena vsebina preiskave določena v odredbi, je preiskovalec glede izbora iskane vsebine dejansko omejen na obseg, določen v odredbi. S tega vidika je »izgovor« odpiranja naključnih datotek ali datotek z majhno verjetnostjo relevance s preiskovano vsebino, zaradi »narave tovrstne preiskave«, smiselno močno omejen. Od preiskovalca, ki uporablja funkcije forenzičnega programa, ki temeljijo na UI, se skladno s povedanim pričakuje, da pri uporabi tega programa iskalna navodila v kontekstu in obsegu odredbe čim bolj konkretizira, pri čemer odstopanja od teh navodil ne morejo biti upravičljiva z doktrino *plain view*.

3.3 Tajnost podatkov

Pomemben vidik uporabe umetne inteligence, ki ga moramo upoštevati pri analizi podatkov z UI, je tajnost. Zagotavljanje ustrezne tajnosti podatkov s strani sodišča, organov pregona in odvetnikov je kritična za pravičen kazenski postopek, kakor tudi zaščito zasebnosti udeležencev postopka. Omenjena tajnost podatkov je lahko ogrožena s tem, ko različni udeleženci kazenskega postopka (ali drugi, ki imajo dostop do teh podatkov) uporabijo storitve, ki temeljijo na umetni inteligenci in se izvajajo na tujih strežnikih, ki ne pripadajo uporabniku. Tako namreč poteka uporaba več tovrstnih sistemov (npr. ChatGPT), ki uporabnikove zahteve in posredovane podatke obdelajo na strežnikih ponudnikov te storitve (ali strežnikih drugih ponudnikov strežniških

⁷ Forenzični program Cellebrite v ZDA policija pogosto uporablja kot orodje za preiskavo pametnih telefonov.

storitev) in ne na napravi, s katero uporabnik dostopa do te storitve. Drugače povedano: tovrstna uporaba omenjenih sistemov pomeni, da uporabnik obdelovane podatke pošilja na tuj računalnik. Na ta problem je nedavno opozorila Komisija za etiko odvetniške zbornice na Floridi v mnenju o uporabi generativne umetne inteligence s strani odvetnikov (Board Review Committee on Professional Ethics, 2023). Izpostavila je, da uporaba tujih sistemov UI predstavlja tveganje razkritja zaupnih podatkov, pri čemer je opozorila, da tudi »in house« rešitve, čeprav vsekakor zmanjšajo možnost razkritja zaupnih podatkov, najbrž vseeno zahtevajo informirano soglasje strank. Opozorila je, da morajo odvetniki pri uporabi sistemov UI, ki se izvajajo na drugih strežnikih, postopati podobno skrbno kot pri uporabi storitev v oblaku, torej pri odročnem shranjevanju podatkov. Izpostavila je tudi potrebo po razumevanju, ali se ti sistemi UI sami učijo, saj tovrstne funkcije predstavljajo dodatno tveganje za tajnost podatkov.

3.4 Sistemi za prepoznavo obraza

Do sedaj smo govorili o sistemih, namenjenih analizi podatkov, zavarovanih iz določenih zaseženih elektronskih naprav, vnaprej pa se moramo opredeliti tudi glede sistemov, ki UI uporabljajo za izvajanje nadzora. Klasifikacija tehnologije za prepoznavo obraza kot analitične obdelave dokazov brez vrednostnih zaključkov je na prvi pogled vprašljiva. Tukaj vsekakor ne gre zgolj za splošno iskanje znotraj neke gmote podatkov, temveč gre za analizo obrazov in povezovanje s primerjavo biometričnih lastnosti. Ti sistemi na podlagi analize ustvarijo nek zaključek, torej prepoznavo (določitev identitete osebe na posnetku), vendar je za predmetno klasifikacijo pomembna preverljivost rezultata. Program na posnetku sicer prepozna osebo, vendar je ta rezultat analize preprosto preverljiv.⁸ Nekateri sistemi za prepoznavo obraza imajo postopek človeške potrditve rezultatov celo integriran v postopek uporabe. Takšen je npr. Interpolov sistem za prepoznavo obrazov⁹, ki na podlagi primerjave analizirane slike z v sistemu shranjenimi profili izvrše seznam kandidatov, katerih vizualni profil se z analizirano sliko najbolj ujema. Temu sledi analiza ujemanja predlaganih kandidatov s strani kvalificiranih Interpolovih uradnikov. (Interpol, n. d.) Podobno poteka tudi uporaba sistema Face Trace na slovenski policiji, in sicer tako, da se v sistem vstavi fotorobot ali posnetek¹⁰ neznane osebe, pri čemer sistem

⁸ Sodnik lahko npr. sam z lastnim vidom primerja videz osebe na posnetku in obdolženca ter presodi, ali gre za isto osebo.

⁹ Interpolov sistem za prepoznavo obraza vsebuje fotografije obrazov iz več kot 179 držav. (Interpol, n. d.)

¹⁰ Uporabljen je lahko tudi posnetek iz videonadzornega sistema.

opravi avtomatsko primerjavo s fotografijami iz Evidence fotografiranih oseb. Sistem po analizi izvrše seznam oseb, razvrščenih po podobnosti iskani osebi iz vstavljenega posnetka. Končno identifikacijo na podlagi tega rezultata opravi strokovnjak za primerjavo obraznih značilnosti (Informacijski pooblaščenec, 2021).

Z vidika odločanja sodnika v večini primerov ni velike razlike, ali je storilca na posnetku identificiral program ali oseba, saj končno presojo opravi sodnik sam. Problematici so primeri, kjer je identiteta osebe na posnetku dvomljiva. Tukaj lahko nastopi problem vpliva tehnološke ocene, kjer v primeru nesigurnosti obstoj predhodnega rezultata vpliva na človekovo oceno natančnosti in verodostojnosti rezultata. V teh primerih bi sodnik načeloma moral ravnati v smeri dvoma. Kljub temu je treba izpostaviti, da imajo napačne prepoznave obraza lahko izjemno negativne učinke za posameznike, tudi če napaka pri prepoznavi ne vodi do napačne obsodbe. Tovrstne posledice so jasno vidne v primeru iz Detroita, kjer je policija na podlagi napačne avtomatizirane prepoznave obraza aretirala nedolžnega moškega in ga pridržala za 30 ur. Tožilstvo je zoper njega opustilo pregon zgolj dva tedna pozneje, s pojasnilom, da je policija ukrepala na podlagi nezadovoljivih dokazov (Harwell, 2021). Iz tovrstnih primerov izhaja jasna potreba po stalni človeški verifikaciji tovrstnih rezultatov.

Sistemi za prepoznavo obraza predstavljajo izjemen poseg v zasebnost posameznikov, pri čemer v teh primerih ne govorimo o posegu v komunikacijsko zasebnost, kot smo jo predhodno opredelili, temveč splošno zasebnost, zaščiten v 35. členu URS in 8. členu EKČP. Z vidika EKČP je treba pojasniti, da ESČP pri presoji posega v pravico do zasebnosti ločuje med tehnologijo, namenjeno nadzoru, in tehnologijo, katere primarni namen ni nadzor. Skladno s prakso ESČP sistemi UI, namenjeni preprečevanju, zaznavi in preiskavi kriminala, štejejo za tehnologijo, namenjeno nadzoru (Quezada-Tavárez, Vogiatzoglou & Royer, 2021, str. 6–7). Kadar je sistem, namenjen nadzoru, uporabljen na način, ki ni skladen z regulacijo, ki ureja uporabo tovrstnega nadzornega sistema, takšna uporaba krši pravico do zasebnosti posameznikov. Uporaba tovrstne tehnologije brez ustrezne pravne ureditve predstavlja poseg v pravico do zasebnosti tudi zaradi nepredvidljivosti. Pogoji za tovrstne posege v zasebnost posameznikov morajo biti v skladu s prakso ESČP dovolj jasni, da državljanom nudijo predstavo o okoliščinah in pogojih za njihovo uporabo.

Pri presoji ustreznosti uporabe sistemov za prepoznavo obrazov je potrebna analiza Konvencije o varstvu posameznika glede na avtomatsko obdelavo osebnih podatkov (Zakon o ratifikaciji

konvencije o varstvu posameznikov glede na avtomatsko obdelavo osebnih podatkov, 1994) (v nadaljevanju KVPAOP), vključno s Protokolom o spremembi Konvencije o varstvu posameznikov glede avtomatske obdelave osebnih podatkov (Protocol, 2018), ki skupaj tvorita »Posodobljeno KVPAOP« (Council of Europe Committee of Ministers, 2018). Glede uporabe tega akta v povezavi s sistemi prepoznavne obraza je Posvetovalni odbor Konvencije za zaščito posameznikov glede avtomatske obdelave osebnih podatkov sprejel Smernice za (tehnologijo) prepoznavne obraza (angl. Guidelines on facial recognition) (Guidelines on facial recognition, 2021). Te smernice nudijo napotke glede uporabe tehnologije za prepoznavo obrazov, ki v okviru KVPAOP predstavlja obdelavo biometričnih podatkov, ki so opredeljeni kot občutljivi podatki. Poudarek smernic je na potrebi po spoštovanju pravice do zasebnosti in varstva osebnih podatkov pri avtomatski obdelavi slik za identifikacijo posameznikov. Pri tem opozarjajo, da integracija teh tehnologij v nadzorne sisteme predstavlja tveganje za zasebnost in temeljne pravice, še posebej če se uporabljajo brez vednosti ali sodelovanja posameznikov.

Zaveznice te konvencije so dolžne zagotavljati standarde uporabe tehnologije za prepoznavo obrazov, ki ustrezajo uveljavljenim načelom EKČP. Ker prepoznavna obraza predstavlja obdelavo občutljivih (biometričnih) podatkov posameznika, mora v skladu s 6. členom KVPAOP temeljiti na ustrezni pravni podlagi. Ustrezna pravna ureditev za uporabo takšnih tehnologij mora vsebovati kategorizacijo različnih namenskih uporab teh tehnologij, pri čemer mora predmetna zakonodajna ureditev obdelave biometričnih podatkov za vsak kategorizirani način vsebovati natančen opis posebne uporabe in njenega namena, minimalno zanesljivost in točnost uporabljenega algoritma, trajanje hrambe uporabljenih fotografij, možnost revidiranja teh meril, sledljivost postopka in ustrezne varovalne mehanizme (Guidelines on facial recognition, 2021, str. 7).

Uporabo sistemov za prepoznavo obrazov je ESČP nedavno obravnavalo v zadevi *Glukhin proti Rusiji* (Glukhin proti Rusiji, št. Zadeve: 11519/20 z dne 4. 7. 2023), v kateri je presodilo, da je uporaba sistema za prepoznavo obraza preko videonadzora v konkretnem primeru kršila pritožnikovo pravico do zasebnosti. Ta zadeva se je nanašala na uporabo tehnologije za prepoznavo obraza za identificiranje posameznika, ki je protestiral v prostorih podzemne železnice v Moskvi. Ruski organi pregona so pritožnika aretirali in obtožili upravnega prekrška, pri čemer so v postopku uporabili zbrane dokaze, vključno s posnetki videonadzornega sistema z moskovske podzemne železnice in posnetki zaslona z družbenega omrežja Telegram. ESČP je v

tej zadevi opozorilo, da, medtem ko je izvajanje videonadzora s strani policije sicer bilo zakonsko urejeno, uporaba tehnologije za prepoznavo obraza ni bila jasno in natančno določena v predmetni zakonodaji, pri čemer ni bilo ustreznih varoval pred tveganjem zlorab in samovoljne uporabe. ESČP je izrazilo dvom o skladnosti ruskih zakonskih določb z zahtevo »kakovosti zakona«, pri čemer je posebej opozorilo na široko formulacijo zakonov, ki dovoljujejo obdelavo biometričnih podatkov v sodnih postopkih, brez jasnih omejitev ali postopkovnih varoval pri uporabi tehnologije za prepoznavo obrazov. Pojasnilo je, da čeprav je bil namen uporabe te tehnologije kot preprečitev kriminala ustrezen, v konkretnem primeru uporaba te tehnologije ni zadovoljila merila »nujnosti v demokratični družbi«. ESČP pri ocenjevanju »nujnosti v demokratični družbi« obdelave osebnih podatkov v okviru preiskave upošteva naravo in težo obravnavanih kaznivih dejanj. V obravnavani zadevi je bil pritožnik obtožen zgolj storitve upravnega prekrška in ne kaznivega dejanja. S tem pogoj »nujnosti v demokratični družbi« ni bil izpolnjen.

Kot smo omenili, tudi slovenska policija uporablja sistem za prepoznavo obrazov Face Trace, ki za razliko od drugih sistemov, kot je Clearview, ne omogoča identifikacije, temveč zgolj primerjavo podobnosti opisanemu storilcu. Sistem Face Trace deluje le znotraj policijskega informacijskega sistema, pri čemer za namene avtomatske prepoznave obraza ne uporablja fotografij, ki bi se nahajale na spletu ali kje drugje izven sistema policije, temveč zgolj fotografije obrazov posameznikov v Evidenci fotografiranih oseb, ki jih je policija fotografirala v skladu z 2. odstavkom 149. člena ZKP¹¹. Avtomatizirano obdelavo biometričnih podatkov iz teh fotografij policija skladno s 1. odstavkom 112. člena ZNPPol izvaja zgolj pri odkrivanju in preiskovanju kaznivih dejanj, če je to glede na okoliščine storitve konkretnega kaznivega dejanja nujno in potrebno. Informacijski pooblaščenec je leta 2021 v okviru inšpekcijskega postopka zoper policijo ocenil uporabo sistema Face Trace pri slovenski policiji, pri čemer ni odkril sistemskih nepravilnosti pri njegovi uporabi. Kljub temu je izpostavil, da je kljub vzpostavljenim varovalkam sistem Face Trace mogoče zlorabiti, pri čemer je izpostavil uporabo tega sistema za identifikacijo udeležencev protestnih shodov ter takšno uporabo označil kot nezakonito. Takšna uporaba bi namreč presegla pravno podlago, saj postopek prepoznave obraza slovenska zakonodaja predvideva samo za namen odkrivanja in preiskovanja kaznivih dejanj.

¹¹ Policija sme fotografirati tistega, za kogar obstajajo razlogi za sum, da je storil kaznivo dejanje.

Uporabo sistemov UI za prepoznavo obrazov ureja tudi nova Uredba Evropskega parlamenta in Sveta o določitvi harmoniziranih pravil o umetni inteligenci (Uredba 2024/1689)¹² (v nadaljevanju Akt o UI), ki v točki h 1. odstavka 5. člena prepoveduje uporabo te tehnologije za oddaljeno prepoznavo obrazov »v realnem času« v javno dostopnih prostorih za namene kazenskega pregona, razen v strogo nujnih primerih. Primeri, v katerih je tovrstna uporaba ustrezna, so usmerjeno iskanje žrtev ugrabitve, trgovine z ljudmi in spolne zlorabe, iskanje pogrešanih oseb, preprečevanje konkretnih, obsežnih in neposrednih groženj življenju ali varnosti ljudi ter terorističnih napadov, kakor tudi za lokalizacijo ali identifikacijo oseb, osumljenih kaznivih dejanj. 2. odstavek 5. člena Akta o UI uporabo tega sistema dalje pogojuje s tehtanjem med potencialnim obsegom škode, ki bi nastal v odsotnosti uporabe tega sistema, in posegom v pravice in svoboščine prizadetih oseb. Prav tako zahteva, da uporaba poteka skladno z zakonskimi varovali in pogoji nacionalne zakonodaje za uporabo tovrstnih sistemov, še posebej časovnih, geografskih in osebnih omejitev. Uporaba tovrstnih sistemov je prav tako pogojena s tem, da so organi pregona, pristojni za uporabo tega sistema, predhodno opravili preizkus vpliva na temeljne pravice posameznikov iz 27. člena te uredbe in da so uporabljeni sistem registrirali v bazo, določeno v 49 členu. Uporaba teh sistemov je dovoljena zgolj ob predhodni avtorizaciji s strani sodnika ali neodvisne administrativne avtoritete na podlagi predloga. Brez predhodne avtorizacije je tovrstni sistem dovoljeno uporabiti zgolj v utemeljenih primerih nujnosti, vendar mora ustrezna avtorizacija biti izdana v 24 urah od začetka uporabe sistema. Avtorizacija za uporaba takšnega sistema je dovoljena zgolj ob prepričanju izdajalca, da je njegova uporaba nujna in sorazmerna za doseganje določenih ciljev in omejena glede na čas, kraj in osebe. O vsaki uporabi tovrstnega sistema je treba obvestiti pristojni organ za nadzor trga in nacionalni organ za varstvo osebnih podatkov.¹³

Akt o UI v točki g 1. odstavka 5. člena prav tako prepoveduje dajanje na trg in uporabo sistemov, ki posameznike na podlagi njihovih biometričnih lastnosti kategorizirajo z namenom sklepanja o njihovi rasi, političnem prepričanju, članstvu v sindikatu, verskih ali filozofskih prepričanjih,

¹² 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).

¹³ To je določeno v 3. odstavku 5. člena Akta o UI.

spolnem življenju ter spolni usmerjenosti.¹⁴ Gre za pomembno prepoved z vidika izjemne nevarnosti, tako namerne kot nenamerne diskriminacije pri uporabi umetne inteligence. Pri obravnavi problema diskriminacije pri uporabi UI moramo vedno upoštevati, da učenje UI poteka na podlagi zgodovinskih podatkov, zaradi česar lahko ti sistemi prevzamejo oz. ohranjajo različne oblike pristranskosti, ki se jim z uporabo tovrstne tehnologije načeloma želimo izogniti. Pogost razlog za ta pojav je nereprezentativnost ciljne populacije v podatkih, uporabljenih za učenje (Grimm, Grossman & Cormack, 2021, str. 42). Uporaba programov za prepoznavo obrazov se je v preteklosti namreč izkazala za nevarno z vidika diskriminacije. Raziskave, ki so jih opravili Tehnološki inštitut Massachusettsa (MIT), Microsoft Research in Nacionalni inštitut za standarde in tehnologijo ZDA (NIST), so pokazale odstopanja v natančnostih prepoznave obraza v relaciji z raso preiskovanih oseb. Ugotovili so, da so ti sistemi bili manj natančni pri prepoznavi obrazov temnopoltih in azijskih posameznikov, pri čemer so bile napačne prepoznave teh posameznikov 10- do 100-krat pogostejše kot pri belcih. Ta odstopanja so delno pripisali manjši zastopanosti teh demografskih skupin v bazah podatkov, iz katerih se tovrstni sistemi umetne inteligence učijo (Grimm, Grossman & Cormack, 2021, str. 38).

Problem diskriminacije izpostavlja potrebo po skrbi ne samo glede pogojev in namena uporabe sistemov za prepoznavo obraza, temveč tudi glede tega, na podlagi katerih podatkov so ti sistemi bili razviti.

4 Analitična obdelava z vrednostnimi zaključki

Pod vrsto analitične uporabe z vrednostnimi zaključki uvrščamo uporabo umetne inteligence za analitično obdelavo podatkov, rezultat katere je vrednostni zaključek oz. nek nov »izveden dokaz« (profil, ocena, prepoznani vzorec, mnenje). V veliki meri gre za uporabo generativne umetne inteligence oz. sistemov, ki so sposobni na podlagi učnih podatkov generirati navidezno nove, smiselne vsebine, kot so besedila, slike in zvok. Teh sistemov ni mogoče uporabiti le za produkcijo »umetniških del«, temveč so kot inteligentni sistemi sposobni tudi ljudem odgovarjati na vprašanja (Feuerriegel idr., 2024, str. 1). Omogočajo vnos podatkov in njihovo analizo, katere

¹⁴ Ta prepoved se ne nanaša na označevanje ali filtriranje zakonito pridobljenih biometričnih podatkov v okviru kazenskega pregona.

rezultat lahko vsebinsko predstavlja mnenje, ki temelji na predhodno določenih kriterijih ali kriterijih, ki jih je določil uporabnik.

Pri tovrstni uporabi umetne inteligence moramo prvotno ločiti dve vrsti uporabe, ki se med seboj razlikujeta po rezultatu. Pomembna je ločitev med rezultati, ki temeljijo na osebnih podatkih posameznikov, in drugimi, saj ta ločitev predstavlja kritičen vidik določitve zakonodajnih okvirov uporabe tovrstne tehnologije. Za tovrstno avtomatsko obdelavo podatkov se v pravnih virih najpogosteje uporablja izraz »oblikovanje profilov«. Ta je v 4. točki 3. člena Direktive EU o varstvu posameznikov pri obdelavi osebnih podatkov, ki jih pristojni organi obdelujejo za namene preprečevanja, preiskovanja, odkrivanja ali pregona kaznivih dejanj (Direktiva 2016/680), definiran kot vsakršna oblika »avtomatizirane obdelave osebnih podatkov, ki vključuje uporabo osebnih podatkov za ocenjevanje nekaterih osebnih vidikov v zvezi s posameznikom, zlasti za analizo ali predvidevanje uspešnosti pri delu, ekonomskega položaja, zdravja, osebnega okusa, interesov, zanesljivosti, vedenja, lokacije ali gibanja tega posameznika«. ¹⁵ Iz te definicije je razvidno, da profil opredeljujeta dva kritična elementa, in sicer da se nanaša na konkretnega posameznika ter da temelji na obdelavi njegovih osebnih podatkov.

Namen ureditve oblikovanja profilov v pravu EU je posameznikom zagotoviti pravico, da zanj ne veljajo odločitve, ki temeljijo zgolj na avtomatizirani obdelavi in imajo zanj škodljive pravne učinke ali nanj znatno vplivajo. Omenjena direktiva (Direktiva 2016/680) v 11. členu določa dolžnost držav članic, da »zagotovijo, da je sprejemanje odločitev izključno na podlagi avtomatizirane obdelave, vključno z oblikovanjem profilov, ki ima lahko negativen pravni učinek za posameznika, na katerega se nanašajo osebni podatki, ali ga zelo prizadene, prepovedano, razen če to dovoljuje pravo Unije ali države članice, ki se uporablja za upravljavca in ki zagotavlja ustrezno zaščito pravic in svoboščin posameznika, na katerega se nanašajo osebni podatki, vsaj pravice do osebnega posredovanja upravljavca.« Tudi če ta pravica ni absolutna, je predvidena potreba po ustreznih zaščitnih ukrepih, vključno s seznanitvijo posameznika s konkretnim odločanjem. ¹⁶

Temu dosledno sledi Akt o UI, ki v 5. členu prepoveduje postavitve na trg in uporabo sistemov, ki ocenjujejo ali napovedujejo tveganje fizične osebe za storitev kaznivega dejanja, ki temelji izključno na profiliranju fizične osebe ali na ocenjevanju njenih osebnostnih lastnosti in

¹⁵ Na to definicijo se glede uporabe pri organih pregona sklicuje tudi Akt o UI.

¹⁶ To izhaja iz 38. uvodne izjave te direktive. (Direktiva 2016/680)

značilnosti (Council of the European Union, 2024). Ta prepoved sicer ne velja za sisteme UI, ki se uporabljajo za podporo človeškemu ocenjevanju vpletenosti osebe v kaznivo dejanje, ki je že utemeljeno na objektivnih in preverljivih dejstvih, neposredno povezanih s kaznivo dejavnostjo (točka d 1. odstavka 5. člena, Akt o UI). Izjema smiselno konkretizira oz. razlaga predhodno obstoječo zahtevo iz 11. člena Direktive EU o varstvu posameznikov pri obdelavi osebnih podatkov, ki jih pristojni organi obdelujejo za namene preprečevanja, preiskovanja, odkrivanja ali pregona kaznivih dejanj (Direktiva 2016/680), da odločitve, ki vplivajo na posameznike, ne temeljijo zgolj na avtomatizirani obdelavi osebnih podatkov. Akt o UI tej omejitvi dodaja drug pogoj, tj. da je vpletenost osebe v preiskovano kaznivo dejanje že utemeljena na objektivnih in preverljivih dejstvih, neposredno povezanih s konkretnim kaznivim dejanjem. Gre za pogoj, ki omejuje »slepo« iskanje oz. ocenjevanje posameznikov s tem, da uporabo tovrstnih sistemov omejuje (vsaj) na osebe, ki so v konkretni zadevi že osumljenci¹⁷. Gre za osebe, katerim skladno s 4. odstavkom ZKP pripadajo procesna jamstva, na katera jih mora opozoriti policija. Razumevanje predmetne omejitve zgolj kot prepovedi nediskriminatornega ocenjevanja z vezavo na osumljence uporabo tovrstne tehnologije veže na obstoj razlogov za sum, ki sicer predstavlja najnižji dokazni standard oz. stopnjo verjetnosti, ki je sicer potrebna za začetek delovanja policije. Glede na to, da omejitev iz Akta o UI govori o utemeljenosti z objektivnimi in preverljivimi dejstvi, bi le-to bilo bolj smiselno razumeti kot vezanost na dokazni standard utemeljenih razlogov za sum, ki pomenijo »višjo stopnjo suma od razlogov za sum in se približuje utemeljenemu sumu, ki pomeni visoko stopnjo artikulirane konkretne in specifične verjetnosti, da je določena oseba storila kaznivo dejanje« (Vrhovno sodišče Repunlike Slovenije, sodba I Ips 340/2006 z dne 26. 10. 2006).

4.1 Vrednostni zaključek kot dokaz

Sedaj ko smo opredelili zakonodajni okvir obravnavane tehnologije, je treba opredeliti, kakšno vrsto dokaza rezultat tovrstnih sistemov predstavlja oz. ali je tovrsten rezultat sploh dokaz v smislu kazenskega procesnega prava. Dokaze lahko oblikovno ločimo na ustno pričanje, dokumente in fizične dokaze oz. predmete. Ob tej razmejitvi se po navadi pogosto iz vsebinskih razlogov kot ločeno kategorijo obravnava demonstrativne dokaze (izvedenska mnenja,

¹⁷V 144. členu ZKP je osumljenec definiran kot oseba, zoper katero je pred uvedbo kazenskega postopka pristojni državni organ opravil določeno dejanje ali ukrep zaradi obstoja razlogov za sum, da je storila ali sodelovala pri storitvi kaznivega dejanja.

zemljevidi, grafi, modeli, itd.). Ti dokazi bi oblikovno sicer sodili v katero od prej naštetih kategorij, vendar njihovo posebno kategorizacijo opredeljuje njihov poseben namen predstavitve in pojasnitve dejstev in dokazov (Ho, 2021). Formalno gledano so dokazi v kazenskem postopku zagovor obdolženca, izpoved priče, mnenje izvedenca, posnetki, pridobljeni s tehnično registracijo, dokumenti ter listine (Vrhovno sodišče Republike Slovenije, sodba I Ips 42731/2010-66 z dne 28. 2. 2013).

Klasifikacija z UI oblikovanih profilov ali drugih vrednostnih zaključkov je težavna, saj ne zajema le lastnosti različnih oblik dokazov, temveč tudi ni določena oblika predstavitve teh zaključkov. Z vidika, da UI predstavlja emulacijo človeškega kognitivnega mišljenja, se poraja vprašanje, ali tovrstne rezultate ustrezno opredeliti in ocenjevati kot pričanje, strokovno oz. izvedensko mnenje ali zgolj kot tehnološko izvedeno meritev (Grimm, Grossman & Cormack, 2021, str. 79) (s čimer bi rezultat meritve najbrž zavzel obliko dokumenta). Na podlagi smiselne analize vsebinskih lastnosti obravnavanih rezultatov ugotovimo, da so ti najbolj primerljivi s strokovnimi oz. izvedenskimi mnenji. Oblikovanje obravnavanih vrednostnih zaključkov temelji na tem, da sistemi UI analizirajo predhodno zbrane dokaze in predstavljena dejstva ter na podlagi predhodnega znanja te z izvedenim rezultatom predstavijo in pojasnijo. Gre za enako učinkovito funkcijo, kot jo imajo sodni izvedenci – torej izdelavo izvida ali mnenja, za katerega je potrebno posebno strokovno znanje, ki je nujno za ugotovitev ali presojo kakšnega pomembnega dejstva.¹⁸

Do predstavljene ugotovitve pridemo tudi s primerjalno analizo. Rezultati sistemov UI z vsebinskega vidika ne predstavljajo pričanja, saj njihovo delovanje v poglavitnem smislu predstavlja analizo in ne vir podatkov. Priče so skladno z 234. členom ZKP osebe, ki so (oz. je zanje verjetno, da bodo) sposobne kaj povedati o kaznivem dejanju, storilcu ali drugih pomembnih okoliščinah, pri čemer (vsaj v teoriji) ni sporno, da te osebe izpovedujejo o svojih čutnih zaznavah (Gorkič, 2016). S tem se bistveno razlikujejo od zaključkov sistemov UI, saj so vir in ne obdelovalec informacij oz. podatkov. Ta primerjava je sicer vprašljiva v primerih sistemov, ki temeljijo na UI in so sposobni določene zaznave oz. meritve ali beleženja. Smiselni primer za obravnavo tega vprašanja je varnostni informacijski sistem, ki beleži prometne podatke in komunikacijo na varovanih informacijskih sistemih ter na podlagi obdelave teh podatkov zaznava razne oblike kibernetičnih kaznivih dejanj. Na prvi pogled tovrstni sistem oz. njegov rezultat predstavlja nov vir informacij, ki temeljijo na njegovi zaznavi, primerljiv s pričanjem. Pri pa

¹⁸ To izhaja iz 248. člena ZKP.

moramo upoštevati, da opredelitev rezultatov tovrstnih sistemov kot pričanje ni ustrezna, saj je »zaznava« teh sistemov (beleženje prometnih in drugih podatkov) empirična in posledično objektivno preverljiva. Zaradi tega bi bilo pri tovrstnih sistemih rezultate njihovega delovanja smiselno ločiti na zbrane podatke, ki imajo naravo dokumentov, in analizo teh podatkov, ki je vsebinsko primerljiva s strokovnim oz. izvedenskim mnenjem.

Sedaj ko smo opredelili vsebinsko naravo vrednostnih zaključkov sistemov UI, je treba odgovoriti na vprašanje, ali so tovrstne vrednostne sodbe lahko dokaz v kazenskem postopku. Odgovor se nanaša na vprašanje, kdo bi v postopku lahko uporabil to tehnologijo in predstavil njen rezultat. Sodnik za razjasnitev dejstev, za katera bi potreboval strokovno znanje, tovrstne tehnologije ne more uporabiti, saj mu ZKP za ta namen v 248. členu ekskluzivno določa postavitev izvedenca ustrezne stroke. Sodnik torej ne le, da nima (s teoretičnega vidika) potrebe po uporabi tovrstne tehnologije, temveč je zakonsko omejen na konkretno določeno rešitev (postavitev izvedenca). Postavljeno vprašanje, ali je vrednostna sodba dokaz, analiziramo torej z vidika, da je tovrstni sistem uporabila stranka v postopku in predložila rezultat. Ob upoštevanju ugotovitve, da tovrstne vrednostne sodbe vsebinsko ustrezajo strokovnemu oz. izvedenskemu mnenju, je vprašanje opredelitve vrednostnih zaključkov UI kot dokaza treba analizirati z vidika teh dveh oblik mnenj. Kot izhaja iz ustaljene sodne prakse (Vrhovno sodišče Republike Slovenije, sodba I Ips 6330/2016 z dne 14. 5. 2020), je dokaz z izvedencem oz. izvedensko mnenje dokaz, kadar ga odredi sodišče, mnenje strokovnjaka (kot pomočnika stranke), ki ga pridobi in predloži stranka, pa predstavlja del strankinih navedb. Skladno s povedanim obravnavani vrednostni zaključki v okviru kazenskega postopka niso dokaz, temveč so lahko zgolj del navedb strank.

Neustreznost upoštevanja vrednostnih zaključkov UI kot dokaza izhaja tudi iz narave procesa oblikovanja teh zaključkov. ESČP je v preteklosti večkrat opozorilo na zahtevo, da ima obdolženec v postopku efektivno možnost izpodbijati tako avtentičnost kot uporabo posameznega spornega dokaza. Pravica do poštenega postopka namreč zajema pravico zadostnega časa za pripravo in dostop do ustreznih sredstev za pripravo obrambe. Uporaba rezultatov UI kot dokaza je problematična iz dveh razlogov, in sicer objektivne možnosti izpodbijanja takšnih rezultatov in obdolženčeve (osebne) sposobnosti izpodbijanja rezultatov.

Prvi problem se nanaša na nepreglednost pri sistemih UI, ki temeljijo na strojnem učenju oz. na problemu »črne škatle« (angl. black box), ki predstavlja eno glavnih ovir za transparentnost v UI (Quezada-Tavárez, Vogiatzoglou & Royer, 2021, str. 8–16). Za razliko od programske kode, ki jo je

mogoče pregledati za »hrošče« (angl. bugs), pri modelih, ki temeljijo na strojnem učenju, pogosto ni mogoče ugotoviti oz. razumeti, kako so ti bili razviti oz. kako delujejo. Dodaten problem predstavlja dejstvo, da ti modeli UI niso statični, temveč se skozi čas stalno spreminjajo in dopolnjujejo (Grimm, Grossman in Cormack, 2021, str. 48) Zaradi navedenih tehničnih lastnosti, ki onemogočajo ustrezno transparentnost delovanja teh sistemov, bi uporaba rezultata UI kot dokaza nasprotovala obdolženčevi pravici do poštenega sojenja, saj tega ni mogoče preizkusiti.

Drug problem se navezuje na primere, kjer bi rezultat sicer bilo mogoče preizkusiti, vendar obdolženec tega ne zmore, saj za to nima ustreznega znanja, sredstev ali pa dostop do ustreznih orodij ni dosegljiv širši javnosti. Ta problem se poleg zahteve, da ima obdolženec v kazenskem postopku efektivno možnost izpodbijati in preveriti dokaze, ki ga bremenijo, nanaša tudi na načelo enakosti orožja. Skladno z načelom enakosti orožja mora imeti obdolženec enake možnosti predstaviti svoje navedbe in dokaze, ki so mu v prid, brez pomembne slabosti v primerjavi s tožilcem. Pomen tega načela je še posebej izrazit v državah, kjer tožilec vodi preiskavo, saj služi uravnoteženju razlike moči med tožilcem in obdolžencem ter s tem zagotavlja, da obdolženec ni prikrajšan za svoje temeljne procesne pravice (Mrčela, 2017, str.17–18).

5 Izboljšava dokazov

Zadnja vrsta uporabe UI za obdelavo dokazov je izboljšanje dokazov. V tem smislu govorimo o izboljšanju predstavitvene vrednosti dokazov za namen lažje zaznave njihove vsebine s človeškimi čuti. Primer tega je izboljšanje ločljivosti slike ali videoposnetka z namenom lažje prepoznave obraza ali manjših podrobnosti na sliki. Medtem ko koncept sintetične povečave ločljivosti slik in videoposnetkov ni nov in je ta tehnologija že prilagojena v vsakodnevnih napravah (npr. velik del pametnih televizorjev ima to funkcijo¹⁹), je ta do sedaj, skladno z zmogljivostmi, bila pretežno namenjena izboljšavi zabavnih vsebin in ne preiskovalni in analitični uporabi.²⁰

V zadnjih letih je prišlo do izjemnega razvoja sistemov umetne inteligence, ki temeljijo na generativnih adversarnih mrežah (angl. generative adversarial networks) ali GANs. Gre za vrsto

¹⁹ Tovrstne funkcije so verjetno aktivne tudi v nekaterih televizorjih, ki so v sodnih dvoranah namenjeni pregledu dokazov. S tem po vsej verjetnosti v primeru nekaterh slik in videoposnetkov v strogo tehničnem smislu prihaja do prikazovanja »izboljšanih« oz. spremenjenih verzij dokazov.

²⁰ Trditev popolnoma ne drži za tehnologijo, namenjeno izboljšavi razločnosti zvočnih posnetkov.

umetne inteligence, ki je sestavljena iz dveh nevronske mreže, tj. generatorja in diskriminatorja. Medtem ko generator ustvarja nove vzorce na podlagi že obstoječih (vnešenih), diskriminator ocenjuje avtentičnost teh vzorcev, kar sistemu omogoča učinkovito generiranje slik, besedil in drugih podatkov. Ti sistemi niso praktični zgolj zaradi izjemne sposobnosti izboljšave kakovosti obstoječih vsebin (kot je ločljivost slike), temveč v primerjavi z drugimi vrstami umetne inteligence zahtevajo manjše število vnesenih vzorcev za učenje (Tian idr., 2022, str. 3–4). Kljub izjemnim zmogljivostim te tehnologije ne gre za nezmotljive sisteme. Ti sistemi pri rekonstrukciji slik pogosto izpuščajo cele razrede objektov²¹, zaradi česar njihova uporaba zahteva ustrezno previdnost, še posebej pri uporabi za generiranje sintetičnih vsebin za tvegane namene (Martineau, 2019).

Pri izboljšavi dokaza z UI obstaja možnost, da je ta izboljšava napačna. Tudi človek, ki skuša interpretirati informacijo v posnetku slabe kakovosti (prepoznati osebo na podlagi fotografije s slabo ločljivostjo), se lahko zmoti. Pomembna razlika pa je, da pri prepoznavi s strani človeka vemo, da gre za njegovo subjektivno presojo slike, pri čemer lahko upoštevamo tudi druge dejavnike, ki so lahko botrovali njegovi presoji, kot npr. predhodno seznanitev s podobo osumljenca ali predhodno obstoječe predsodke. Pri izboljšavi z UI nam ni jasno, zakaj je izboljšava takšna, kot je, in kaj je nanjo vplivalo, kljub temu pa zaradi tehnološke narave oblikovanja te presoje takšna izboljšava ustvarja vtis objektivnosti.

5.1 Omejitev uporabe generativne umetne inteligence

V uporabo tehnologije za izboljšavo dokazov je posegel Akt o UI. V okviru tega akta je tovrstna obdelava dokazov klasificirana kot »deep fake«, kar Akt o UI sicer definira kot z umetno inteligenco generirano ali manipulirano vsebino v obliki slike, zvoka ali videa, ki spominja na obstoječe osebe, objekte, kraje ali druge entitete ali dogodke in pri osebah napačno ustvarja vtis avtentičnosti ali resničnosti.²² Uporabnikom tovrstne tehnologije je Akt o UI v 4. odstavku 50. člena določil obveznost transparentnosti, skladno s katero mora uporabnik sistema UI, ki generira ali manipulira slikovno, zvočno ali video vsebino, ki predstavlja »deep fake«, razkriti, da je bila vsebina umetno generirana ali manipulirana. V tem odstavku je določil tudi izjemo te obveznosti, tj. kadar je uporaba po zakonu dovoljena za odkrivanje, preprečevanje, preiskovanje in pregon

²¹ Sem sodijo tudi ljudje oz. njihovi deli, kakor tudi teksture in podobno.

²² Definicija je navedena v 60. odstavku 3. člena Akta o UI.

kaznivih dejanj. S tem AKT o UI državam članicam EU daje možnost, da z zakonom uredijo netransparentno uporabo tovrstne tehnologije. Postavi se vprašanje, za kakšne namene bi bila netransparentna uporaba tehnologije za generacijo in modifikacijo vsebin ustrezna v kazenskem postopku in ali bi takšna vsebina lahko služila kot dokaz.

Uporabo te tehnologije in pogoje za njeno netransparentno uporabo bo zakonodajalec vsekakor moral urediti, saj ima ta tehnologija velik potencial pri policijskem delu, zaradi česar je razumljivo pričakovati željo organov pregona po ureditvi ustrezne zakonske podlage, ki bi takšno uporabo omogočala. Uporabo te tehnologije lahko predvidimo kot orodje pri izvajanju prikritih preiskovalnih ukrepov, kjer policija osumljenca namerno spravi v zмотo, kot je ukrep navideznega odkupa, navideznega sprejemanja oz. dajanja daril ali navideznega jemanja oz. dajanja podkupnine²³ ter ukrep tajnega delovanja²⁴, v okviru katerega tajni delavec uporablja tajno identiteto. V teh primerih bi uporaba predmetne tehnologije bila uporabljena kot orodje za tajno delovanje in ustvarjanje tajne identitete ter izvedena pod pogoji in v obsegu, določenem za izvajanje teh ukrepov, ter skladno s pogoji o pripravi prirejene identitete. V okviru teh ukrepov bi bila neustrezna uporaba modificiranih vsebin pri policiji na način, da osumljenca izzove h kriminalni dejavnosti. Ali je bila kriminalna dejavnost izzvana, se presoja z vidika, ali bi ukrep na način, kot je bil izveden, napeljal k storitvi kaznivega dejanja osebo, ki tovrstnega kaznivega dejanja sicer ne bi bila pripravljena storiti (3. odstavek 155. člena ZKP). Če je kriminalna dejavnost bila izzvana, to predstavlja okoliščino, ki izključuje kazenski pregon za kaznivo dejanje, ki se preiskuje. Zaradi pojasnjene je pomembno, da se tajni policijski delavec pri izvrševanju ukrepa omeji na preiskovanje kriminalne dejavnosti obdolženca na način, ki je v bistvenem pasiven (Višje sodišče v Mariboru, Sklep V Kp 10935/2021 z dne 2. 6. 2022).

Smiselno bi bilo, da bi zakonodajalec pri zakonski ureditvi uporabe predmetne tehnologije pri policiji določil enako »sankcijo« v primerih, kjer je policija kriminalno dejavnost izzvala z uporabo z UI generirane vsebine izven omenjenih prikritih preiskovalnih ukrepov, saj lahko tudi takšna uporaba smiselno izzove kriminalno dejavnost preiskovanega posameznika.

Ne glede na siceršnjo možnost uporabe te tehnologije v kazenskem postopku pa vsebine, ki so bile manipulirane z uporabo UI, ne morejo biti uporabljene kot dokaz v kazenskem postopku. Da

²³ Ti ukrepi so določeni v 155. členu ZKP.

²⁴ Ta ukrep je določen v 155.a členu ZKP.

je dokaz zanesljiv, ne sme biti dvoma o njegovi avtentičnosti in integriteti. To pomeni, da mora biti izvor tega dokaza nedvoumen in dokaz med zbiranjem in njegovim nadaljnjim ravnanjem ne sme biti manipuliran. Ker izboljšava digitalnega dokaza z uporabo UI po smislu pomeni manipulacijo z dokazom na način dodajanja vsebine, ki je originalni dokaz predhodno ni vseboval (dodajanje predhodno neobstoječih slikovnih točk za izboljšanje ločljivosti), tovrstna izboljšava dejansko pomeni ustvarjanje sintetičnega oz. lažnega dokaza, ki ne ustreza merilom zanesljivega in ustreznega dokaza v kazenskem postopku. Pri tem je treba poudariti, da skladno s tretjim odstavkom 285. člena KZ-1 predložitev lažnih ali ponarejenih dokazov (za katere storilec ve, da so lažni) z namenom preprečitve ali otežitve dokazovanja v kazenskem postopku pomeni kaznivo dejanje preprečitve dokazovanja. Skladno s prakso (Višje sodišče v Ljubljani, Sklep II Kp 52330/2018 z dne 6. 5. 2022) je to kaznivo dejanje lahko izvedeno ne le v kazenskem, temveč tudi predkazenskem postopku oz. pred začetkom kazenskega postopka.

6 Sklep

Uporaba umetne inteligence za namen preiskave v kazenskem postopku ni le praktična, temveč zaradi digitalizacije življenja verjetno celo potrebna. Kljub praktičnim vidikom te tehnologije pa ne smemo prezreti njenih negativnih posledic ter stremeti k ustrezni ureditvi, ki uporabo te tehnologije omejuje na nujne primere in preprečuje tako sistemske kot individualne zlorabe. Da gre za problematično področje uporabe umetne inteligence, pričajo razni mednarodni akti, ki to področje že urejajo, čeprav pretežno na načelni ravni, oz. ponujajo zgolj okvir, znotraj katerega morajo to področje konkretno urediti zakonodajalci na ravni posameznih držav. Pri tem na žalost vidimo podoben, v uvodu omenjeni trend industrije umetne inteligence²⁵, tj. uporabo te tehnologije še pred sprejemom ustrezne zakonske ureditve in s tem ustreznih varoval.

Uporaba UI v kazenskem postopku za obdelavo dokazov ni problematična zgolj z vidika kršitev pravic obdolženca, temveč zadeva tudi naše razumevanje in uporabo dokazov. Postulati koncepta dokaza v dobi digitalizacije prihajajo pod vprašanje, saj se z vedno težjo ločitvijo resničnega od sintetičnega ruši koncept dokaza kot objektivnega in resničnega sredstva za ugotavljanje (oz. presojo) dejanskega stanja. Digitalni svet, ki je do nedavnega predstavljal binarno preslikavo fizičnega sveta, z razvojem umetne inteligence posega v realnost našega sveta z ustvarjanjem vzporedne realnosti, pri čemer je odstopanje med obema svetoma pogosto

²⁵ Uporaba novih tehnologij umetne inteligence pred ustreznim preizkusom tveganj.

težko ali celo nepreverljivo. V prihodnosti lahko zaradi izjemne dostopnosti tehnologije za manipulacijo in generacijo novih dokazov, v odsotnosti ustrezne tehnologije za zaznavo lažnih dokazov, morda pričakujemo celo razvoj predpostavljenega dvoma o predstavljenem dokaznem gradivu.

Viri

Board Review Committee on Professional Ethics. (2023). *Proposed Advisory Opinion 24-1*. The Florida Bar Board of Governors. <https://aboutblaw.com/bcnO>

Chen, C. Y.-F., in Tseng, P. (2023). The boundary of artificial intelligence in forensic science. *DIALOGO*, 10, 83–90. <https://doi.org/10.51917/dialogo.2023.10.1.5>

Council of Europe (2018). *Protocol amending the Convention for the Protection of Individuals with regard to automatic processing of personal data*. Council of Europe Committee of Ministers, Convention 108 +. https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/LIBE/DV/2018/09-10/Convention_108_EN.pdf

Council of Europe (2021). *Consultative Committee of the Convention for the protection of individuals with regard to automatic processing of personal data, Guidelines on facial recognition*. <https://rm.coe.int/guidelines-facial-recognition-web-a5-2750-3427-6868-1/1680a31751>

Council of the European Union. (2024). *Proposal for Regulation of the European Parliament and the Council laying down harmonised rules on the artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts – Analysis of the final compromise text with a view to agreement*. <https://data.consilium.europa.eu/doc/document/ST-5662-2024-INIT/en/pdf>

Direktiva 2016/680. Direktiva (EU) 2016/680 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov, ki jih pristojni organi obdelujejo za namene preprečevanja, preiskovanja, odkrivanja ali pregona kaznivih dejanj ali izvrševanja kazenskih sankcij, in o prostem pretoku takih podatkov ter o razveljavitvi Okvirnega sklepa Sveta 2008/977/PNZ. <https://eur-lex.europa.eu/legal-content/SL/ALL/?uri=celex%3A32016L0680>

DiSilvio, G. (2023). *Siri, is this admissible in court? Five steps to challenging warrants for digital evidence*. Lawline. <https://blog.lawline.com/siri-is-this-admissible-in-court-six-steps-to-challenging-warrants-for-digital-evidence>

Du, Y., Lin, S., Lv, H., Liu, X., in Ding, N. (2022). A review of the application of artificial intelligence in criminal investigation. 3rd International Conference on Artificial Intelligence and Education, 1544–1548. Atlantis Press. https://doi.org/10.2991/978-94-6463-040-4_232

Feuerriegel, S., Hartmann, J., Janiesch, C. in Zschech, P. (2024). Generative AI. *Business Information Systems Engineering*, 66, 111–126. <https://doi.org/10.1007/s12599-023-00834-7>

Glukhin proti Rusiji, št. Zadeve: 11519/20 z dne 4. julija 2023

Gorkič, P. (2016). Izvedena priča. *Pravna praksa*, (6). <https://www.insolvinfo.si/medijsko-sredisce/v-srediscu/175937>(<https://www.insolvinfo.si/medijsko-sredisce/v-srediscu/175937>)

Grimm, P. W., Grossman, M. R. in Cormack, G. V. (2021). Artificial intelligence as evidence. *Northwestern Journal of Technology and Intellectual Property*, 19 (1).

Harwell, D. (2021, 13. April). *Wrongfully arrested man sues Detroit police over false facial recognition match*. The Washington Post. <https://www.washingtonpost.com/technology/2021/04/13/facial-recognition-false-arrest-lawsuit/>

Ho, H. L. (2021). *The legal concept of evidence*. V E. N. Zalta (ur.), The Stanford Encyclopedia of Philosophy. <https://plato.stanford.edu/archives/win2021/entries/evidence-legal/>

Hooper, M. K., in Masters, R. E. (ur.). (2017). *The criminal justice system* (druga izdaja). Salem Press Inc, a division of EBSCO Information Services, Inc.; Grey House Publishing.

Informacijski pooblaščenec. (2021). Policijski sistem Face Trace sicer temelji na biometrični obdelavi osebnih podatkov, a ne omogoča identifikacije, Informacijski pooblaščenec. <https://www.ip-rs.si/novice/policijski-sistem-face-trace-sicer-temelji-na-biometrični-obdelavi-osebnih-podatkov-a-ne-omogoča-identifikacije>

Interpol. (b.d.). *Facial Recognition*, Interpol. <https://www.interpol.int/en/How-we-work/Forensics/Facial-Recognition>

Ivanshchenko proti Rusiji, št. zadeve: 61064/2011, 5. oktober 2011

Klemenčič, G. (2011). *Splošno o komunikacijski zasebnosti, Razmerje med 35. in 37. členom*. V Komentar Ustave Republike Slovenije, Človekove pravice in temeljne svoboščine. <https://e-kurs.si/komentar/razmerje-med-35-in-37-clenom/>

Kruglov in drugi proti Rusiji, št. zadeve: 11264/04, 4. februar 2020

Martineau, K. (2019). Visualizing an AI model's blind spots. *MIT News*. <https://news.mit.edu/2019/visualizing-ai-models-blind-spots-1108>

Mrčela, M. (2017). Adversarial principle, the equality of arms and confrontational right – European Court of Human Rights recent jurisprudence. *EU and Comparative Law Issues and Challenges Series (ECLIC)*, 1. <https://doi.org/10.25234/ecllic/6519>

Peče, O. (2022). *Preiskava enkriptiranih elektronskih naprav in nosilcev elektronskih podatkov v kazenskem postopku; problem nezmožnosti dostopa do podatkovne vsebine naprave in prisila razkritja šifrirnega gesla*, Magistrsko delo, Univerza v Mariboru.

Quezada-Tavárez, K., Vogiatzoglou, P. in Royer, S. (2021). Legal challenges in bringing AI evidence to the criminal courtroom. *New Journal of European Criminal Law*, 12(4), 531–551. <https://doi.org/10.1177/20322844211057019>

Tian, C., Zhang, X., Lin, J., Zuo, W., in Zhang, Y. (2022). Generative adversarial networks for image super-resolution: A survey. <https://doi.org/10.48550/arXiv.2204.13620>

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)

Ustava Republike Slovenije (URS). (1991). Uradni list RS, št. 33/91-I, 42/97 – UZS68, 66/00 – UZ80, 24/03 – UZ3a, 47, 68, 69/04 – UZ14, 69/04 – UZ43, 69/04 – UZ50, 68/06 – UZ121,140,143, 47/13 – UZ148, 47/13 – UZ90,97,99, 75/16 – UZ70a in 92/21 – UZ62a. <https://pisrs.si/pregledPredpisa?id=USTA1>

Ustavno sodišče Republike Slovenije, odločba Up-106/05-27 z dne 2. oktober 2008

Višje sodišče v Ljubljani, sklep II Kp 52330/2018 z dne 6. maj 2022

Višje sodišče v Ljubljani, sklep V Kp 55723/2018 z dne 9. april 2020

Višje sodišče v Mariboru, sklep V Kp 10935/2021 z dne 2. junij 2022

Vrhovno sodišče Republike Slovenije, sodba I Ips 42731/2010-66 z dne 28. februar 2013

Vrhovno sodišče Republike Slovenije, sodba I Ips 6330/2016 z dne 14. maj 2020

Vrhovno sodišče Repunlike Slovenije, sodba I Ips 340/2006 z dne 26. oktober 2006

Ward, K. B. (2011). The plain (or not so plain) view doctrine: Applying the plain view doctrine to digital seizures. *University of Cincinnati Law Review*, 79*(3), 1163–1187.

Zakon o kazenskem postopku (ZKP). (1995). Uradni list RS, št. 176/21 – uradno prečiščeno besedilo, 96/22 – odl. US, 2/23 – odl. US in 89/23 – odl. US. <https://pisrs.si/pregledPredpisa?id=ZAKO362>

Zakon o ratifikaciji Konvencije o varstvu človekovih pravic in temeljnih svoboščin. (1994). Zakon o ratifikaciji Konvencije o varstvu človekovih pravic in temeljnih svoboščin, spremenjene s protokoli št. 3, 5 in 8 ter dopolnjene s protokolom št. 2 ter njenih protokolov št. 1, 4, 6, 7, 9, 10 in 11 (Uradni list RS – Mednarodne pogodbe, št. 7/94). <https://pisrs.si/Pis.web/evrovocTematskoKazaloRSPrikazRezultatov?evrovoc=5326&tez=12&treid=5143>

Zakon o ratifikaciji konvencije o varstvu posameznikov glede na avtomatsko obdelavo osebnih podatkov (MKVP). (1994).Uradni list RS – Mednarodne pogodbe, št.11/94 in Uradni list RS, št. 86/04 – ZVOP-1. <https://pisrs.si/pregledPredpisa?id=ZAKO741>

