Usklađivanje zahtjeva OUZP-a s izazovima umjetne inteligencije

Šegović, Dorian

Pravni fakultet Sveučilišta u Zagrebu

Katedra za pravo informacijskih tehnologija

Dorian Šegović

Usklađivanje zahtjeva OUZP-a s izazovima umjetne inteligencije

Diplomski rad

Mentor: izv. prof. dr. sc. Tihomir Katulić

Zagreb

2024.

Izjava o izvornosti

Ja, Dorian Šegović, pod punom moralnom, materijalnom i kaznenom odgovornošću, izjavljujem da sam isključiv autor diplomskog rada te da u radu nisu na nedozvoljen način (bez pravilnog citiranja) korišteni dijelovi tuđih radova te da se prilikom izrade rada nisam koristio drugim izvorima do onih navedenih u radu.

_____

Dorian Šegović, v.r.

Sažetak

Zaštita podataka stekla je izrazitu važnost s pojavama novih tehnologija poput umjetne inteligencije (UI). U tom segmentu vrlo je naglašena zaštita temeljnih ljudskih prava poput prava na privatnost i prava na zaštitu osobnih podataka. Kroz to vodi *Opća uredba o zaštiti podataka* (OUZP), njezin okvir i najrelevantniji članci. OUZP daje zakonodavni okvir kako bi pravilan i pošten postupak obrade podataka trebao izgledati. Pretpostavka je da, iako odredbe OUZP-a ostavljaju prostora za interpretaciju novih tehnologija, brojna pitanja vezana uz zaštitu podataka, a u vezi s umjetnom inteligencijom, nemaju izričit odgovor u OUZP-u. To može dovesti do neizvjesnosti i troškova te može nepotrebno ometati razvoj aplikacija umjetne inteligencije. U radu se analizira kako se obveze voditelja obrade odražavaju na poslovanje organizacije, konkretni učinci ljudskog nadzora automatiziranih odluka UI-ja, načela transparentnosti, minimizacije, zakonitosti, točnosti, nepristranosti, obveze informiranja i ispunjavanja prava ispitanika, pristup utemeljen na riziku, kategoriziranje sustava UI-ja prema predloženom *Aktu o umjetnoj inteligenciji* i koje su potrebne tehničke i organizacijske mjere poduzete za očuvanje privatnosti od strane organizacija, poput anonimnosti i pseudonimnosti, te korištenje postupaka certificiranja za dokazivanje usklađenosti prema propisima EU-a.

Ključne riječi: *Opća uredba o zaštiti podataka*, umjetna inteligencija, tehničke i organizacijske mjere zaštite podataka

Summary

Data protection has become extremely important with the emergence of new technologies such as artificial intelligence. In this segment, the protection of fundamental human rights such as the right to privacy and the right to the protection of personal data is highly emphasized. The General Data Protection Regulation, its framework and the most relevant articles guide us through this. The GDPR provides a legislative framework for what a proper and fair data processing procedure should look like. The assumption is that, although the provisions of the GDPR leave room for the interpretation of new technologies, many questions related to data protection and artificial intelligence do not have an explicit answer in the GDPR. This can lead to uncertainty and cost, and can unnecessarily hinder the development of AI applications. The paper analyzes how the processing manager's obligations reflect on the organization's operations, the concrete effects of human supervision of automated AI decisions, the principles of transparency, minimization, legality, accuracy, impartiality, obligations to inform and fulfill the rights of respondents, a risk-based approach, categorization of the AI system according to the proposed Act on artificial intelligence and the necessary technical and organizational measures taken to preserve privacy by organizations such as anonymity and pseudonymity and the use of certification procedures to demonstrate compliance with EU regulations.

Key words: General data protection regulation, artificial intelligence, tehnical and organizational data protection measures

Sadržaj

1. UVOD

Nove tehnologije duboko su promijenile način na koji organiziramo i živimo svoje živote. Konkretno, nove tehnologije koje se temelje na podacima potaknule su razvoj umjetne inteligencije uključujući povećanu automatizaciju zadataka koje obično obavljaju ljudi. Umjetna inteligencija (dalje u tekstu UI) postala je jedan od najmoćnijih pokretača društvene transformacije mijenjajući ekonomiju, politiku i preoblikujući živote i interakcije građana. U posljednjem desetljeću umjetna inteligencija doživjela je brz razvoj, zdravstvena kriza izazvana bolešću COVID-19 potaknula je usvajanje UI-ja i dijeljenje podataka stvarajući nove prilike, ali i izazove i prijetnje ljudskim temeljnim pravima. Umjetna inteligencija stekla je čvrstu znanstvenu osnovu i proizvela mnoge uspješne primjene poput gospodarskog, društvenog i kulturnog razvoja, energetske održivosti, bolje zdravstvene zaštite i širenja znanja. Razvoj UI-ja privukao je veliku pozornost medija, civilnog društva, akademske zajednice, tijela za ljudska prava i kreatora politika. Velik dio te pozornosti usmjeren je na njezin značaj da podrži gospodarski rast, dok se manje pozornosti posvećuje tome kako različite tehnologije mogu utjecati na temeljna prava. Osobni podaci postali su novo sredstvo informacijske moći. Prikupljanje golemih količina osobnih podataka potiče moderno gospodarstvo informacijskog doba. Kroz opsežno i često osjetljivo profiliranje, subjekti podataka i njihovi osobni podaci objektiviziraju se, često se njima trguje i razmjenjuju ih čak i najsavjesniji sudionici u podatkovnoj ekonomiji, a kamoli oni koji na osobne podatke gledaju kao na sirovi industrijski resurs na neki način odvojen od života i briga ispitanika od kojih su podaci prikupljeni. [1] Umjetna inteligencija napravila je impresivan korak naprijed otkako se počela fokusirati na primjenu strojnog učenja na masovne količine podataka. Industrija UI-ja u Hrvatskoj, kao i u mnogim drugim zemljama, bilježi vrlo brz rast i razvoj te je broj tvrtki i stručnjaka koji ulaze u to područje u velikom porastu. U Hrvatskoj rješenja iz područja UI-ja razvija čak više od 130 *startupova*. [2] Sustavi strojnog učenja otkrivaju korelacije između podataka i izgrađuju odgovarajuće modele, koji povezuju moguće ulaze s pretpostavljenim

[1] Katulić, T., Protrka, N.: *Information Security in Principles and Provisions of the EU Data Protection Law*. // 42nd International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO) Opatija: IEEE, 2019. pp. 1420–1426 (predavanje, međunarodna recenzija, cjeloviti rad [in extenso], znanstveni).

[2] Umjetna inteligencija u Hrvatskoj postaje već ozbiljan globalni biznis, 16. kolovoza 2023. https://lidermedia.hr/tehno/umjetna-inteligencija-u-hrvatskoj-postaje-vec-ozbiljan-globalni-biznis-152504, prema stanju na dan 12. 9. 2023.

ispravnim odgovorima predviđanjima. U aplikacijama za strojno učenje, sustavi UI-ja uče predviđati nakon što su obučeni na golemim skupovima primjera. Stoga je UI postao gladan podataka, a ta je glad potaknula prikupljanje podataka, u samojačajućoj spirali razvoja sustava UI-ja temeljenih na strojnom učenju, pretpostavlja i potiče stvaranje golemih skupova podataka, to jest velike količine podataka. Integracija UI-ja i velikih podataka može donijeti mnoge koristi za gospodarski, znanstveni i društveni napredak. Od, primjerice, pametnih gradova, pa sve do pronalaska lijeka protiv raka. Međutim, on također pridonosi rizicima za pojedince i cijelo društvo, kao što su sveprisutni nadzor i utjecaj na ponašanje građana, polarizacija i fragmentacija u javnoj sferi, što također predstavlja zadiranje u pojedinčevu privatnost. Tehnologija koja mijenja pravila, poput UI-ja sa svojim brojnim mogućnostima i mnogim rizicima, treba učinkovit i stabilan pravni okvir koji definira materijalni opseg odgovornosti za sve one koji su uključeni u razvoj i implementaciju ove tehnologije u nove inovativne usluge i proizvode ili zamjenu postojeće informacijske infrastrukture u uslugama koje se danas koriste.[3]

Međutim, ovaj brzi napredak prati neodgodiva briga očuvanja privatnosti pojedinca i njegovih podataka, a iako digitalne tehnologije, uključujući UI, pružaju sve veće mogućnosti i koristi, njihovo osmišljavanje, razvoj, uvođenje i zloupotreba također mogu sadržavati rizike za temeljna prava, demokraciju i vladavinu prava. Danas je izuzetno teško, ako ne i nemoguće, za pojedinca koji koristi online ili povezane proizvode ili usluge, izbjeći sustavan digatlni nadzor kroz većinu aspekata njihovog života.[4] Kako sustavi UI-ja postaju sveprožimajući i sofisticiraniji, gubi se linija između inovacija i zadiranja postavljajući važna etička, pravna i socijalna pitanja korištenja podataka. U ovom radu autor će istražiti zapetljan odnos privatnosti podataka i izazova koje donosi UI, ispitivanjem višestranih pitanja koja se pojavljuju dok društvo plovi neistraženim vodama nevidljive revolucije vođene podacima. Od mogućnosti algoritamske pristranosti do implikacija masovnog nadzora, uspostavljanje ravnoteže između tehnološkog napretka i prava pojedinca na privatnost imperativ je koji zahtijeva pažljivo istraživanje. Dok se društvo bori sa složenošću ovog digitalnog krajolika, postaje jasno da zaštita privatnosti podataka u doba UI-ja nije samo tehnički izazov već

[3]Katulić, T.: *Towards the Trustworthy AI: Insights from the Regulations on Data Protection and Information Security*, str. 13, Medijska istraživanja, Zagreb, 2020.
[4]King, J., Meinhardt, C.: *Rethinking Privacy in the AI Era Policy Provocations for a Data-Centric World* , Stanford HAI, Stanford, str 20, 2024.

i temeljni test naše predanosti ljudskom dostojanstvu i demokratskim vrijednostima. U digitalnom svijetu složenost današnje regulative ne odnosi se samo na provedbu zakona već također na sučelje ljudskog i strojnog ponašanja kroz institucionalna i društvena sredstva.[5]

Do danas još nema velike količine empirijskih dokaza o širokom rasponu prava koja UI implicira ili o zaštitnim mjerama potrebnim kako bi se osigurala uporaba UI-ja u skladu s temeljnim pravima u praksi. Ovim radom autor želi istražiti kako se pravni okvir zaštite podataka iz *Opće uredbe o zaštiti podataka* (Uredba [EU] 2016/679, dalje u tekstu OUZP) uklapa sa zahtjevima i izazovima koje donosi UI. Ubrzanim razvojem tehnologije zaštita podataka dobila je na značajnosti te se predviđa da će se taj trend samo nastaviti. Iako postoje već brojna teoretska istraživanja i nagađanja kako će točno UI utjecati na naše živote, autor smatra kako manjak empirijskih istraživanja poziva na potrebu provjere praktičnih učinaka OUZP-a na poslovanje organizacija koje koriste UI. Današnji sustavi UI-ja trenirani su na golemim količinama podataka kako bi postigli najbolje rezultate. Neki dijelovi tog razvoja još nisu razjašnjeni, a naizgled prkose zahtjevima OUZP-a. Predstavlja li organizacijama koje koriste sustave UI-ja izazov dosljedno provođenje načela OUZP-a? Mogu li organizacije jasno i precizno pružati ispitanicima informacije kako se obrađuju njihovi podaci? Kako je moguće transparentno prikazati obradu podataka sustava UI-ja? Zadovoljavaju li organizacije tehničke i organizacijske mjere pri obradi podataka kako od njih zahtijeva OUZP? Brinu li organizacije o očuvanju privatnosti podataka koje obrađuju? Ovo su primjeri samo nekolicine pitanja kojima će se autor baviti u ovom radu, a sve s ciljem utvrđivanja pruža li OUZP dovoljan regulativni okvir na izazove UI-ja s kojima se nose organizacije, iako još ne postoji njegova zasebna regulacija. Razumijevanje navedenih izazova važno je zato što još nije donesena sveobuhvatna regulacija za UI, a on postaje neizbježan dio naše svakodnevice. Nalazi se ga svugdje, a kako bi se mogao integrirati u sve segmente društva bitno je informirati se kako utječe na ostala ljudska prava, primjerice ona navedena u OUZP-u, te mogu li se te prava ostvariti u sustavima UI-ja unatoč nekim naizgled očitim suprotnostima.

[5]Pagallo, U., Casanovas, P., Madelin, R.: *The middle-out approach: assessing models of legal governance in data protection, artificial intelligence, and the Web of Data*, The Theory and Practice of Legislation, 7:1, 1–25, Routledge, 2019.

Rad se nastavlja korištenom metodologijom istraživanja, nakon čega slijedi objašnjenje osnovnih i relevantnih pojmova OUZP-a i UI-ja. Zatim slijedi pregled dosadašnjih istraživanja s temom zaštite podataka i utjecaja UI-ja na njih. Potom će se podrobnije opisati kako točno UI utječe na okvir zaštite podataka i privatnosti i utvrditi koje prepreke za organizacije proizlaze iz toga. Na kraju će se analizirati rezultati ankete provedene među organizacijama koje se koriste UI-jem te će se utvrditi jesu li im pretpostavljene prepreke uistinu izazovi. Uz to, u zaključku će autor dodati prijedloge za pouzdaniju i učinkovitiju buduću regulaciju.

Pri izradi ovog rada korištene metode istraživanja su analiza sekundarnih izvora podataka, analiza sadržaja i anketa. Analizirani su relevantni članci, izvješća i dokumenti, a cilj analize je prepoznati izazove koje donosi UI i dobiti uvid kako ti izazovi utječu na postojeći pravni okvir OUZP-a te koje su posljedice za organizacije koje koriste UI. U radu je istraživano aktualno stanje zaštite podataka i primjena OUZP-a u organizacijama koje se bave obradom podataka. Uz to su istraženi i izazovi UI-ja s kojima se društvo suočava, a vezani su uz obradu podataka, a još se ne naziru njihova jasna rješenja. Također je tijekom srpnja i kolovoza 2023. provedena dvodijelna kvalitativna anketa putem Google obrasca s organizacijama čije poslovanje obuhvaća UI, s obzirom na to da su navedene organizacije najprikladniji ispitanici za ovo istraživanje. Prvi dio ankete sastoji se od 9 tvrdnji vezanih uz osviještenost i usklađenost organizacija s OUZP-om i obvezama koje iz njega proizlaze. Za svaku od ponuđenih tvrdnji organizacije su imale mogućnosti odabira jednog odgovora s kojim se najviše ili najmanje slažu. Ponuđeni odgovori na tvrdnje su: *Uopće se ne slažem*, *Uglavnom se ne slažem*, *Niti se slažem niti se ne slažem*, *Uglavnom se slažem* i *U potpunosti se slažem*. Prvom dijelu ankete pristupilo je 12 organizacija. Drugi dio ankete također se sastoji od 9 tvrdnji koje su više posvećene izazovima UI-ja, kao i tehničkim i organizacijskim mjerama koje organizacije poduzimaju unutar svog djelovanja, a na koje organizacije mogu odgovoriti istim odgovorima kao i u prvom dijelu ankete. Drugom dijelu ankete pristupilo je 5 organizacija. Anketa je bila anonimna kako bi se zaštitile organizacije od pokušaja identificiranja danog odgovora s određenom organizacijom. Dobiveni rezultati ankete analizirani su i predstavljeni tekstualno te uspoređeni s dosadašnjim istraživanjima kako bi ukazali na nove probleme ili potvrdili već dokazane činjenice.

2. ZAŠTITA PODATAKA

2.1. Pravo na privatnost i zaštitu podataka kao temeljna ljudska prava

Temeljna su ljudska prava univerzalna, nedjeljiva, međuovisna i međusobno povezana. Zaštita i promicanje temeljnih prava i temeljne ideje ljudskog dostojanstva u središtu su antropocentričnog pristupa UI-ja.[6] Korištenje tehnologijama vođenih UI-jem često podrazumijeva računalnu obradu velikih količina osobnih podataka. EDPB i EDPS naglašavaju da su prava na privatnost i na zaštitu osobnih podataka, koja su protivna pretpostavci da strojevi samostalno donose odluke, a na kojoj se temelji načelo UI-ja, okosnica vrijednosti EU-a priznatih u *Općoj deklaraciji o ljudskim pravima* (čl. 12.), *Europskoj konvenciji o ljudskim pravima* (čl. 8.) i *Povelji Europske unije o temeljnim pravima* (dalje u tekstu Povelja) (čl. 7. i 8.).[7] Pravo na poštivanje privatnog života i zaštita osobnih podataka (čl. 7. i 8. Povelje) u središtu su rasprava o temeljnim pravima oko upotrebe UI-ja.[8] Iako su usko povezana, prava na poštivanje privatnog života i zaštitu osobnih podataka su različita, samostalna prava. Opisuju se kao "klasično" pravo na zaštitu privatnosti i "modernije" pravo, pravo na zaštitu podataka. Privatnost se obično definira kao pravo građana na nadziranje osobnih podataka i odlučivanja o tome kako postupiti s njima.[9] Koncept "privatnog života" ili "privatnosti" složen je i širok te nije podložan iscrpnoj definiciji. Važno je istaknuti interes zaštite podataka i privatnosti, odnosno interes za zakonitom i razmjernom obradom osobnih podataka koji su predmet nadzora. To je teško kompatibilno s internetskim okruženjem u kojem se prati svaka radnja, a rezultirajući podaci koriste se za izvlačenje daljnjih informacija o dotičnim pojedincima izvan njihove kontrole i za obradu tih informacija na načine koji mogu biti u suprotnosti s njihovim interesima. Iako je privatnost već dulje vrijeme afirmirana kao ljudsko pravo, tek je nedavno stupila na globalnu scenu te svi akteri počinju shvaćati njezinu važnost. Zaštita podataka ključna je u razvoju i korištenju UI-jem. Članak 8. st. 1. Povelje i čl. 16. st. 1. *Ugovora o funkcioniranju*

[6] Predsjedništvo Vijeća Europske unije, Zaključci predsjedništva: *Povelja o temeljnim pravima u kontekstu umjetne inteligencije i digitalnih promjena*, str. 9, Bruxelles, 2020.
[7] EDPB-EDPS: *Zajedničko mišljenje 5/2021 o Prijedlogu uredbe Europskog parlamenta i Vijeća o utvrđivanju usklađenih pravila o umjetnoj inteligenciji (Akt o umjetnoj inteligenciji)*, str. 7, Bruxelles, 2021.
[8] Čl. 7. Povelje Europske unije o temeljnim pravima.
[9] Kurbalija, J., Murphy, M.: *An introduction to internet governance*, str. 211, DiploFoundation, Geneva, 2016.

Europske unije propisuju da svatko ima pravo na zaštitu svojih osobnih podataka.[10] OUZP i *Direktiva o provedbi zakona* (Direktiva [EU] 201/680) dodatno razrađuju ovo pravo i uključuju mnoge odredbe primjenjive na korištenje UI-jem. Uz pravnu stečevinu EU-a o zaštiti podataka, europsko pravo protiv diskriminacije ključno je za zaštitu temeljnih prava u kontekstu upotrebe UI-ja i povezanih tehnologija. Članak 2. *Ugovora o Europskoj uniji* propisuje da je nediskriminacija jedna od temeljnih vrijednosti EU-a, a čl. 10. UFEU-a zahtijeva od Europske unije borbu protiv diskriminacije na više osnova.

Uporaba UI-ja s njegovim specifičnim karakteristikama netransparentnosti, složenosti, ovisnosti o podacima i njegovo autonomno ponašanje mogu nepovoljno utjecati na brojna temeljna prava utvrđena u Povelji. Prijedlog *Akta o umjetnoj inteligenciji* ističe kako se uredbom želi osigurati visoka razina zaštite tih temeljnih prava i nastoje se riješiti različiti izvori rizika s pomoću jasno definiranog pristupa koji se temelji na riziku.[11] Zahvaljujući skupu zahtjeva za pouzdanim UI-jem i proporcionalnim obvezama za sve sudionike lanca vrijednosti, prijedlogom će se poboljšati i promicati zaštita prava zaštićenih Poveljom, primjerice pravo na ljudsko dostojanstvo (čl. 1.), poštovanje privatnog života i zaštitu osobnih podataka (čl. 7. i 8.), nediskriminaciju (čl. 21.) te ravnopravnost žena i muškaraca (čl. 23.). Obveze koje se odnose na *ex-ante* ispitivanje, upravljanje rizikom i ljudski nadzor isto će tako olakšati poštovanje drugih temeljnih prava, jer će se rizik od pogrešnih ili pristranih odluka potpomognutih UI-jem u važnim područjima, kao što su obrazovanje i osposobljavanje, zapošljavanje, kazneni progon i sudstvo, svesti na najmanju moguću mjeru. Ako i dalje bude kršenja temeljnih prava, trebalo bi omogućiti djelotvornu pravnu zaštitu za pogođene osobe tako što bi se osiguralo transparentnost i sljedivost sustava UI-ja u kombinaciji sa snažnim *ex-post* kontrolama. Ovaj okvir temeljnih prava pruža normativnu osnovu i mjerila za dizajn, razvoj i implementaciju alata UI-ja.

[10]Čl. 16. Ugovora o funkcioniranju Europske unije, Službeni list Europske unije, Bruxelles, 2016.
[11]Europska komisija: *Prijedlog Uredbe Europskog parlamenta i Vijeća o utvrđivanju i usklađivanju pravila o umjetnoj inteligenciji (Akt o umjetnoj inteligenciji) i izmjeni određenih zakonodavnih akata Unije, obrazloženje 3.5. Temeljna prava,* Bruxelles, 2021.

2.2. Zaštita podataka u zakonskom okviru OUZP-a

Središnji dio sekundarnog prava EU-a u kontekstu UI-ja jest *Opća uredba o zaštiti podataka* (OUZP – Uredba[(EU] 2016/679). Za razliku od Direktive o zaštiti podataka iz 1995., OUZP sadrži neke pojmove koji se odnose na internet poput društvenih mreža, web stranica, poveznica i drugih, ali ne sadrži pojam "umjetna inteligencija" ni bilo koji izraz koji izražava srodne koncepte, kao što su inteligentni sustavi, autonomni sustavi, strojno učenje ili čak veliki podaci.[12] To odražava činjenicu da je OUZP usredotočen na izazove koji se pojavljuju za internet, a nisu razmatrani u Direktivi o zaštiti podataka iz 1995., ali su bili dobro prisutni u vrijeme kada je OUZP sastavljen, a ne na nova pitanja koja se odnose na UI, a koja dobivaju društveni značaj posljednjih godina. OUZP sadrži važna prava za korisnike u vezi s bilo kojom obradom njihovih osobnih podataka, kao i obveze izvršitelja obrade koje će oblikovati način na koji će se UI razvijati i primjenjivati. OUZP se primjenjuje kako u fazi razvoja UI-ja tako i u pogledu njegove upotrebe za analizu i donošenje odluka o pojedincima. Posebno su relevantne za okruženje UI-ja odredbe koje se odnose na područje primjene, pravne osnove, načela zaštite podataka i automatizirano donošenje odluka.[13] Međutim, kao što će se vidjeti, mnoge odredbe OUZP-a vrlo su relevantne za UI. U tom kontekstu potrebno je pozabaviti se izazovima kao što su netransparentnost, složenost, pristranost, određeni stupanj nepredvidivosti i djelomično autonomno ponašanje kako bi se osigurala usklađenost automatiziranih sustava s temeljnim pravima i olakšala provedba pravnih propisa.

Članak 5. stavak 1. točka (c) navodi načelo smanjenja količine podataka prema kojem bi osobni podaci trebali biti primjereni, relevantni i ograničeni na ono što je nužno u odnosu na svrhe u koje se obrađuju.[14] Načelo smanjenja količina podataka također je sadržano u uvodnoj izjavi 78., koja zahtijeva „smanjenje količine obrade osobnih podataka" kao organizacijsku mjeru za zaštitu podataka prema dizajnu i prema zadanim postavkama. Članak 5., stavak 1. točka (b) utvrđuje načelo ograničenja svrhe prema kojem se osobni podaci trebaju prikupljati u „posebne, izričite i zakonite svrhe te se dalje ne smiju obrađivati na način koji nije u skladu s tim svrhama; daljnja obrada

[12]Think tank: European Parliament: *The impact of the General Data Protection Regulation (GDPR) on Artificial Intelligence*, str. 35, Bruxelles, 2020.
[13]Mitrou, L.: *Data Protection, Artificial Intelligence and Cognitive Services: Is the General Data Protection Regulation (GDPR)'Artificial Intelligence-Proof'?*, str. 28, 2018.
[14]Čl. 5. st. 1. t. (c). OUZP.

u svrhe arhiviranja u javnom interesu, svrhe znanstvenog ili povijesnog istraživanja ili statističke svrhe, u skladu s člankom 89. stavkom 1., ne smatra se neusklađenom s prvotnim svrhama".[15] Koncept svrhe također se nalazi u čl. 6. OUZP-a koji uspostavlja vezu između svrhe postupaka obrade i njihove pravne osnove. Pojam svrhe izričito se spominje u čl. 6. samo u odnosu na prvu pravnu osnovu, naime, privolu, koja se treba dati „za jednu ili više specifičnih svrha" te za posljednju pravnu osnovu.[16] Privola je svako dobrovoljno, posebno, informirano i nedvosmisleno izražavanje želje ispitanika kojom on izjavom ili jasnom potvrdnom radnjom daje pristanak za obradu osobnih podataka koji se na njega odnose.[17] Članak 6. OUZP-a navodi da svaka obrada osobnih podataka zahtijeva pravnu osnovu. Ova je ideja prvi put uvedena u Direktivi o zaštiti podataka iz 1995., a kasnije je konstitucionalizirana u članku 8. Povelje, prema kojem se osobni podaci moraju obrađivati pošteno, u utvrđene svrhe i na temelju suglasnosti osobe o kojoj je riječ ili na nekoj drugoj legitimnoj osnovi utvrđenoj zakonom.[18] Obrada osobnih podataka u kontekstu primjene UI-ja postavlja neka pitanja koja se odnose na postojanje valjane pravne osnove. Kako bi se odredilo kada pravna osnova može podržati obradu temeljenu na UI-ju, potrebno je zasebno razmotriti pravne osnove navedene u članku 6. OUZP-a, koji navodi da je obrada osobnih podataka zakonita samo pod sljedećim uvjetima: (a) pristanak subjekta podataka ili (b) nužnost za obavljanje ili sklapanje ugovora, (c) za poštivanje zakonske obveze, (d) za zaštitu vitalnih interesa, (e) za obavljanje zadaće u javnom interesu ili u izvršavanju javnih vlasti ili (f) zbog legitimnog interesa. Konačno, pojam svrhe također se pojavljuje u člancima 13. stavku 1. točki (c) i 14. stavku 1. točki (c), koji zahtijevaju od voditelja obrade pružanje informacija o svrhama obrade za koje su osobni podaci namijenjeni, kao i pravnog temelja za obradu. Načelo točnosti navedeno je u članku 5. stavku 1. točki (d) OUZP-a koji zahtijeva da podaci budu „točni i prema potrebi ažurni" i da se mora poduzeti svaka razumna mjera radi osiguravanja da se osobni podaci koji nisu točni, uzimajući u obzir svrhe u koje se obrađuju, bez odlaganja izbrišu ili isprave.[19] Ovo se načelo također primjenjuje na osobne podatke koji se koriste kao ulazni podaci za sustav UI-ja, posebno kada se osobni podaci koriste za donošenje zaključaka ili

[15]Čl. 5. st. 1. t. (b). OUZP.
[16]Čl. 6. OUZP.
[17] Dragičević, D., Gumzej, N., Jurić M., Katulić, T., Lisičar, H.: *Pravna informatika i pravo informacijskih tehnologija*, str. 127, NN, Zagreb, 2015.
[18]Čl. 8. st. 2. Povelje Europske unije o temeljnim pravima.
[19]Čl. 5. st. 1. t. (d). OUZP.

odluka o subjektima podataka. Netočni podaci mogu izložiti subjekte podataka šteti, kad god ih se razmatra i s njima postupa na načine koji ne odgovaraju njihovom identitetu.

Informacije o automatiziranom donošenju odluka članka 13. stavka 2. točke (f) i 14. stavka 2. točke (g) OUZP-a bave se ključnim aspektom aplikacija UI-ja, to jest automatiziranim odlučivanjem. Voditelj obrade ima obvezu pružiti: (a) informacije o „postojanju automatiziranog donošenja odluka uključujući profiliranje, iz članka 22. stavka 1." i (b) „barem u tim slučajevima smislene informacije o uključenoj logici, kao i značaj i predviđene posljedice takve obrade za nositelja podataka." Automatizirano donošenje odluka prema članku 22. OUZP-a i članku 11. Direktive o zaštiti podataka pri izvršavanju zakonodavstva (Direktiva [EU] 2016/680) općenito su zabranjeni, što znači svaku „odluku koja se temelji isključivo na automatiziranoj obradi, uključujući profiliranje, koja proizvodi pravne učinke u vezi s njim ili njom ili na sličan način značajno utječe na njega ili nju".[20] Prema članku 22. OUZP-a, izričit pristanak potreban je kada su odluke isključivo automatizirane i imaju pravni ili sličan značajan učinak na ljude te ako takvo automatizirano donošenje odluka nije dopušteno zakonom. Odobrenje prema pravu Unije ili nacionalnom pravu jedini je preduvjet prema članku 11. Direktive o zaštiti podataka pri izvršavanju zakonodavstva.[21] Kako se odluka ne bi smatrala potpuno automatiziranom, oba instrumenta zahtijevaju ljudski pregled od strane upravljačke jedinice. Članak 22., koji govori o automatiziranom donošenju odluka, najrelevantniji je za UI. Kao što će se vidjeti u nastavku, ova odredba kombinira opću zabranu automatiziranog donošenja odluka, uz velike iznimke. Članak 22. stavak 1. OUZP-a propisuje opće pravo da se ne podliježe potpuno automatiziranim odlukama koje značajno utječu na ispitanika. Ispitanik ima pravo ne podlegnuti odluci koja se temelji isključivo na automatiziranoj obradi, uključujući profiliranje, koja proizvodi pravne učinke u odnosu na njega ili nju ili na sličan način značajno utječe na njega ili nju. Iako se ova odredba odnosi na pravo, ona ne predviđa pravo prigovora na automatizirano donošenje odluka, naime, ne pretpostavlja da je automatizirano donošenje odluka općenito dopušteno sve dok se nositelj podataka tome ne protivi.

[20]Čl. 22. OUZP.

[21]Direktiva (EU) 2016/680 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka od strane nadležnih tijela u svrhe sprečavanja, istrage, otkrivanja ili progona kaznenih djela ili izvršavanja kaznenih sankcija i o slobodnom kretanju takvih podataka o stavljanju izvan snage Okvirne odluke Vijeća 2008/977/PUP.

Umjesto toga uvodi zabranu za voditelje obrade te su zabranjene automatizirane odluke koje utječu na subjekte podataka, osim ako se uklapaju u jednu od iznimaka navedenih u stavku 2. Prema Radnoj skupini za članak 29. u pravilu postoji opća zabrana potpuno automatiziranog individualnog donošenja odluka uključujući profiliranje koje ima pravni ili sličan značajan učinak.[22] Za primjenu zabrane utvrđene člankom 22. stavkom 1. potrebna su četiri uvjeta: (1) mora se donijeti odluka, (2) mora se temeljiti isključivo na automatiziranoj obradi, (3) mora uključivati profiliranje, (4) mora imati pravni ili bilo kako značajan učinak.[23] Mnoge odluke koje danas donose sustavi UI-ja pripadaju opsegu članka 21. stavka 1., jer se algoritmi UI-ja sve više koriste pri zapošljavanju, davanju zajmova, pristupu osiguranju, zdravstvenim uslugama, socijalnom osiguranju, obrazovanju. Korištenje UI-ja čini sve više vjerojatnim temeljenje odluka „isključivo" na automatiziranoj obradi. Provođenje učinkovitog pregleda može biti nemoguće ili može zahtijevati pretjerane napore, osim ako je sustav učinkovito projektiran za transparentnost, što u nekim slučajevima može biti iznad najnovijeg stanja tehnike. Stoga, posebno kada se koristi neproziran sustav velikih razmjera, ljudi će vjerojatno samo izvršavati automatizirane prijedloge UI-ja, čak i kada su formalno nadležni. Štoviše, ljudska intervencija može biti spriječena postojećom strukturom troškova i poticaja. Ljudi vjerojatno neće značajno preispitati automatiziranu odluku kada trošak uključenja u reviziju iz perspektive pojedinca ili institucije premašuje značaj odluke.

Članak 17. OUZP-a: pravo na brisanje (ili biti zaboravljenim) sastoji se od prava ispitanika da „od voditelja obrade ishode brisanje osobnih podataka koji se odnose na njega ili nju bez nepotrebnog odgađanja", kada ispunjeni uvjeti za zakonitu obradu prestanu.[24] Takvi uvjeti navedeni su u članku 17. stavku 1. Relativno moderno pravo nastalo odlukom španjolskog suda C-131/12 Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD) i Mario Costeja González, također sadrži određene izazove u sustavima UI-ja.[25] Primjerice, sustavi UI-ja, poput neuronskih mreža, nemaju sposobnost zaboravljanja na isti način kao ljudi. Mreža može prilagoditi svoje težine kako bi bolje odgovarala novim podacima, što bi moglo rezultirati različitim predviđanjima za isti unos. Međutim, to nije isto što i zaboravljanje u smislu

[22]Radna skupina za zaštitu podataka iz članka 29: *Smjernice o automatiziranom pojedinačnom donošenju odluka i izradi profila za potrebe Uredbe 2016/679*, str. 19, 2018.
[23]Čl. 22. st. 1. OUZP.
[24]Čl. 17. OUZP.
[25]C-131/12 Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD) i Mario Costeja González.

da mreža još uvijek ima pristup svim informacijama koje je prethodno naučila, samo daje viši prioritet novim informacijama.[26] Još jedan problem je pitanje odnosi li se pravo na zaborav i na izvedene osobne podatke kao što su podaci korišteni za obuku algoritamskog modela, koji bi kao posljedica obveze brisanja prikupljenih osobnih podataka trebali biti brisani jer su omogućili izvođenje takvih zaključaka. Međutim, brisanje podataka korištenih za izradu algoritamskog modela može otežati ili onemogućiti demonstraciju ispravnosti tog modela.

OUZP je povezan s Direktivom o provedbi zakona koja se odnosi na policijsku i pravosudnu suradnju u kaznenim stvarima. Oba instrumenta EU-a uključuju brojne odredbe o zaštiti osobnih podataka određujući ključna načela obrade podataka kao što su zakonitost, poštenje i transparentnost. Primjenjuje li se zakonodavstvo EU-a o zaštiti podataka ovisi o tome obrađuju li se osobni podaci. Neke aplikacije koje pokreću UI ne koriste osobne podatke, dok druge koriste anonimizirane podatke. U tim slučajevima zakoni o zaštiti podataka ne vrijede ili njihova primjenjivost nije sasvim jasna. Granica između osobnih i neosobnih podataka je zamagljena jer postoji određeni rizik da se anonimizirani podaci mogu „ponovno identificirati" te tako poništiti proces anonimizacije. Međutim, ponovna identifikacija obično je nezakonita. Osim toga, osobe koje ponovno identificiraju podatke obično moraju uložiti velike napore i potencijalno trebaju pristup dodatnim informacijama o pojedincima koji bi mogli biti uključeni u anonimizirani skup podataka za ponovnu identifikaciju. Široka uporaba UI-ja može, kako se tehnologije nastavljaju razvijati, pokrenuti neistražena pitanja i nove brige o pravu na poštivanje privatnog života. Tehnologije koje pokreću UI mogu promijeniti način na koji razmišljamo o privatnosti. Algoritamski alati mogu predvidjeti i otkriti informacije o ponašanju ljudi na dosad neviđene načine, a da ljudi uopće ne shvate da odaju takve informacije. Važno je prepoznati da mnoga pitanja zadiru u različita prava. Na primjer, potencijalno pristrana odluka koju donosi algoritam mogla bi uključivati pravo na nediskriminaciju, zaštitu osobnih podataka i pravo na učinkovit pravni lijek. Slično tomu, određeno pitanje može se promatrati iz perspektive različitih prava. Na primjer, dobro objašnjenje odluke koju je donio algoritam zahtijeva se prema

[26]We Forgot To Give Neural Networks The Ability To Forget https://www.forbes.com/sites/ashoka/2023/01/25/we-forgot-to-give-neural-networks-the-ability-to-forget/?sh=44424d816853, prema stanju na dan 27. 9. 2023.

pravu na zaštitu osobnih podataka, pravu na dobru upravu i pravu na učinkovit pravni lijek i pošteno suđenje.

2.3. Umjetna inteligencija

Umjetna inteligencija znanstvena je disciplina koja pokušava stvoriti strojeve i sustave sposobne izvršavati zadatke koji obično zahtijevaju ljudsku inteligenciju. Počeci umjetne inteligencije datiraju iz sredine 20. stoljeća, kada su znanstvenici i istražitelji postavili temelje ove revolucionarne grane. Osnovu UI-ja možemo pronaći već u 1940-ima, kada je došlo do velikog napretka računalne tehnologije. Alan Turing, britanski matematičar, često smatran jednim od ključnih pionira UI-ja, u svojoj publikaciji *Computing Machinery and Intelligence*, raspravlja o konceptu Turingoa testa koji razmatra može li stroj primijeniti inteligentno ponašanje koje bi bilo nerazlučivo od onog čovjekovog.[27] Nadalje, jedan od najznačajnijih doprinosa bila je ideja neuronske mreže Warrena McCullocha i Waltera Pittsa 1943. u njihovoj objavi *A Logical Calculus of Ideas Immanent in Nervous Activity*, u kojoj su predložili računalni model neuronske mreže.[28] To je pak bila osnova za konekcionizam, znanost koja proučava povezanosti mreža, jednostavnijih procesnih elemenata koji obavljaju složenije zadatke. U kasnim 50-ima te ranim 60-ima koncept perceptrona razvio se kao bitan napredak UI-ja. Perceptroni su bili zamišljeni kao umjetni neuroni, slično kako biološki neuroni djeluju u ljudskom mozgu. Frank Rosenblatt, psiholog i računalni znanstvenik, zaslužan je za stvaranje algoritma perceptrona. U svom djelu *The Perceptron: A Perceiving and Recognizing Automaton* demonstrirao je potencijal umjetnih neuronskih mreža u zadacima prepoznavanja uzoraka.[29] No početni entuzijazam koji je pratio perceptrone ubrzo je nestao zbog ograničenja u njihovim mogućnostima. Otkriveno je da mogu raditi samo s linearno odvojenim uzorcima te tako nisu bili podobni za složenije zadatke. Unatoč izazovima iz 60-ih, istraživanje UI-ja nastavilo se te kroz 1980-e i ponovno oživjelo interes za neuronskim mrežama, često zvanim drugim valom UI-ja. Snažan razvoj snage računala i dostupnost velikih baza podataka u 21. stoljeću omogućili su izvanredno napredovanje u polju dubokog učenja

[27]Turing, A. M.: *Computing machinery and intelligence*, str. 59, Mind, 1950.
[28]Mcculloch, W., Pitts, W.: *A Logical Calculus of Ideas Immanent in Nervous Activity. Bulletin of Mathematical Biophysics*, str. 5, 1943.
[29]Rosenblatt F.: *The perceptron – A perceiving and recognizing automaton*, Technical Report 85-460-1, Cornell Aeronautical Laboratory, Ithaca, New York, 1957.

i primjene sustava UI-ja uključujući prepoznavanje zvuka i slika, autonomna vozila i obradu prirodnog jezika. Dok su perceptroni i rane neuronske mreže bili suočeni s ograničenjima tog razdoblja, kasniji prodori u dubokom učenju i konekcionizmu postavili su put za sofisticirane sustave UI-ja koji se koriste danas. Znanstvenici Geoffrey Hinton, Yann LeCun i Yoshua Bengio značajno su pridonijeli razvoju arhitektura neuronskih mreža koje su nadvladale ograničenja perceptrona.[30] Povećana količina i raznolikost podataka, koji su ponekad dostupni gotovo u stvarnom vremenu putem interneta, često se nazivaju velikim podacima. Važan element za korištenje UI-ja u velikim razmjerima je pristup velikim količinama podataka. Za razvoj UI-ja potrebno je koristiti velike količine podataka koji se obrađuju i čine osnovu za učenje algoritama.[31] Tehnologije strojnog učenja i povezani algoritmi, uključujući dubinsko učenje, imaju goleme koristi od ove povećane računalne snage i dostupnosti podataka, a njihov razvoj i upotreba cvjetaju. Većina rasprava i stvarna upotreba UI-ja uključuju primjenu tehnologija strojnog učenja. Duboko učenje područje je strojnog učenja koje se zasniva na neuronskim mrežama s više slojeva (*deep neural networks*). Mnoge su tehnike primijenjene u strojnom učenju kao stabla odlučivanja, statistička regresija, stroj potpornih vektora, evolucijski algoritmi i metoda za pojačano učenje. Neuronske mreže sastoje se od skupa čvorova, zvanih neuroni, raspoređenih u više slojeva i povezanih vezama. Tako su zvani jer reproduciraju neke aspekte ljudskog živčanog sustava, koji se doista sastoji od međusobno povezanih specijaliziranih stanica, bioloških neurona, koji primaju i prenose informacije. Različiti pristupi strojnom učenju razlikuju se u svojoj sposobnosti pružanja objašnjenja. Na primjer, ishod stabla odlučivanja može se objasniti nizom testova koji vode do tog ishoda. Za razliku od stabla odlučivanja, neuronska mreža ne pruža objašnjenja svojih ishoda. Međutim, ove informacije ne pokazuju obrazloženje koje je značajno za ljude, ne govore zašto je dan određeni odgovor. Postoje mnogi pristupi davanju objašnjenja ponašanja neuronskih mreža i drugih neprozirnih sustava koji se nazivaju i crne kutije. No napredak čovjeku razumljivog objašnjenja neuronskih mreža do sada je još uvijek prilično ograničen.

Ne postoji univerzalno prihvaćena definicija UI-ja. Umjesto da se odnosi na konkretne primjene, ona odražava najnovija tehnološka dostignuća koja obuhvaćaju

[30]Fathers of the Deep Learning Revolution Receive ACM A.M. Turing Award (https://www.acm.org/media-center/2019/march/turing-award-2018), prema stanju na dan 27. 9. 2023.
[31]Mazurek, G., Małagocka, K.: *Are we down to zero-one code? Perception of privacy and data protection in the context of the development of artificial intelligence*, str. 10, Journal of Management Analytics, 2019.

različite tehnologije.[32] No unatoč tomu potrebna je definicija kako bi se znalo što točno čini UI i koje bi zakonske odredbe trebalo primijeniti. Uspoređujući početnu definiciju koju je dala Stručna skupina na visokoj razini za umjetnu inteligenciju: „Umjetna inteligencija (UI) odnosi se na sustave koji pokazuju inteligentno ponašanje analizirajući svoje okruženje i poduzimajući radnje uz određeni stupanj autonomije za postizanje određenih ciljeva. Sustavi koji se temelje na umjetnoj inteligenciji mogu biti isključivo bazirani na softveru, djelujući u virtualnom svijetu (npr. glasovni asistenti, softver za analizu slike, tražilice, sustavi za prepoznavanje govora i lica) ili UI može biti ugrađen u hardverske uređaje poput primjerice naprednih robota, autonomnih vozila, dronova ili aplikacija Internet of Things“[33] i definiciju koju sadrži prijedlog Akta o UI-ju: „UI sustav” znači strojni sustav dizajniran za rad s promjenjivim razinama autonomije i koji nakon uvođenja može pokazati prilagodljivost te koji, za eksplicitne ili implicitne ciljeve, iz ulaznih vrijednosti koje prima, zaključuje kako generirati izlazne vrijednosti kao što su predviđanja, sadržaj, preporuke ili odluke koji mogu utjecati na fizička ili virtualna okruženja“, može se vidjeti kako je u prvoj definiciji naglasak stavljen na okupljanje što više tehnologija koje koriste UI, dok je iz druge definicije vidljiva sklonost užem i preciznijem definiranju karakteristika UI-ja.[34] Sustavi UI-ja razlikuju se i prema potencijalnoj šteti koja bi mogla proizaći iz pogrešne odluke temeljene na upotrebi UI-ja. Ovisno o području primjene, pogrešne odluke temeljene na pogrešnim rezultatima iz sustava mogu imati različite učinke o UI-ju. Prema predloženom Aktu o umjetnoj inteligenciji razlikuju se pravila za različite razine rizika. Da bi proveli procjenu rizika, organizacije trebale bi identificirati i rangirati rizike kao neprihvatljiv, visoki, ograničeni ili minimalni, procjeniti vjerojatnost štete implementirati mjere ublažavanja za smanjenje ili uklanjanje rizika i dokumentirati procjenu rizika kako bi se dokazala odgovornost.[35] Neprihvatljiv rizik donose sustavi koji se smatraju prijetnjom ljudima i takvi sustavi će biti zabranjeni. Među njima su kognitivno-bihevioralno manipuliranje osobama ili određenim ranjivim skupinama, primjerice glasovno aktivirane igračke koje potiču opasno ponašanje kod djece,

[32]Agencija Europske unije za temeljna prava: *Getting the future right – Artificial intelligence and fundamental rights*, str. 19., Beč, 2020.
[33]High level expert group on artificial intelligence (HLEG AI): *A definition of Artificial Intelligence: main capabilities and scientific disciplines*, str. 1, Bruxelles, 2018.
[34]Europska komisija: *Prijedlog Uredbe Europskog parlamenta i Vijeća o utvrđivanju i usklađivanju pravila o umjetnoj inteligenciji (Akt o umjetnoj inteligenciji) i izmjeni određenih zakonodavnih akata Unije, članak 3. točka 1.* Bruxelles, 2021.
[35] Kourinian, A., Brown, M.: *Conducting an AI risk assessment,* Bloomberg Law, str. 2, 2024.

bodovanje i klasifikacija ljudi na temelju ponašanja, socioekonomskog statusa, osobnih obilježja, sustavi biometrijske identifikacije u stvarnom vremenu i daljinski sustavi za biometrijsku identifikaciju, kao što je prepoznavanje lica. Neke iznimke mogu biti dopuštene, poput korištenja sustava za daljinsku biometrijsku identifikaciju u kojima se identifikacija odvija sa znatnim kašnjenjem, a koristi se nakon odobrenja suda za kazneni progon kod počinjenja teških kaznenih djela. Visok rizik predstavljaju sustavi koji negativno utječu na sigurnost ili temeljna prava. Ti rizici podijeljeni su u dvije skupine. Prvu skupinu čine sustavi koji se upotrebljavaju u proizvodima obuhvaćenima zakonodavstvom EU-a o sigurnosti proizvoda. Oni uključuju igračke, zrakoplovstvo, automobile, medicinske uređaje i dizala. Drugoj skupini pripadaju sustavi iz osam posebnih područja koji će morati biti registrirani u bazi podataka EU-a, a odnose se na biometrijsku identifikaciju i kategorizaciju fizičkih osoba, upravljanje kritičnom infrastrukturom i njezin rad, obrazovanje i strukovno osposobljavanje, zapošljavanje, upravljanje radnicima i pristup samozapošljavanju, pristup i korištenje osnovnih privatnih i javnih usluga, provedbu zakona, upravljanje migracijama, azilom i nadzorom granica i pomoć u pravnom tumačenju i primjeni zakona. Svi visokorizični sustavi UI-ja trebaju se procijeniti prije stavljanja na tržište i tijekom njihova životnog ciklusa, dok će sustavi s ograničenim rizikom trebati ispunjavati minimalne zahtjeve transparentnosti koji korisnicima omogućavaju donošenje informiranih odluka. Nakon interakcije s aplikacijama korisnik može odlučiti hoće li ih nastaviti koristiti. Korisnici trebaju znati kada su u interakciji s UI-jem. To uključuje sustave koji generiraju ili manipuliraju slikom, audiosadržajem ili videosadržajem. Za sustave niskog ili minimalnog rizika vrijede najmanja ograničenja kako bi se izbjegla prekomjerna regulacija i potaknula njihova inovacija. Iako mnogi sustavi UI-ja predstavljaju minimalan rizik, potrebno ih je procijeniti. Za UI-sustave koji nisu visokorizični nameću se samo vrlo ograničene obveze u pogledu transparentnosti, koje se, primjerice, odnose na davanje upozorenja kad se UI-sustav kad koristi u interakciji s ljudima. Za visokorizične UI-sustave nužni su zahtjevi u pogledu visokokvalitetnih podataka, dokumentacije i sljedivosti, transparentnosti, ljudskog nadzora, točnosti i otpornosti kako bi se smanjili rizici za temeljna prava i sigurnost koji proizlaze iz UI-ja i koji nisu obuhvaćeni drugim postojećim pravnim okvirima. [36] Prijedlog Akta o UI-ju

[36] Europska komisija: *Prijedlog Uredbe Europska Parlamenta i Vijeća o Utvrđivanju i usklađivanju pravila o umjetnoj inteligenciji (Akt o umjetnoj inteligenciji) i izmjeni određenih zakonodavnih akata Unije, obrazloženje 2.3. Proporcionalnost,* Bruxelles, 2021.

naglašava dosljednost i komplementarnost s drugim zakonodavstvom i inicijativama Unije. Također predviđa znatno jačanje uloge Unije u oblikovanju globalnih normi i standarda te promicanju pouzdanog UI-ja koji je dosljedan vrijednostima i interesima Unije.[37] Kao najveće prijetnje Akt ima one u vidu sprječavanja udvostručavanja, proturječnih obveza i prekomjernih popisa koji bi mogli dovesti do fragmentacije unutarnje tržišta Unije. Iako je promicanje i poticanje inovacija spomenuto na više mjesta u Aktu o UI-ju, postoje mnogi sudionici koji su skeptični te ističu kako će on ugroziti sposobnost europskih tvrtki da se natječu s drugim konkurentima. U otvorenom pismu Europskoj komisiji koje je potpisalo više od 150 europskih poduzeća upozoravaju da bi predloženi Akt o UI-ju imao katastrofalne posljedice za europsku konkurentnost.[38]

2.4. Pregled dosadašnje literature

Globalni fenomen UI-ja poznaje više pristupa u rješavanju problema njegove regulacije. Uz europski, kojem će biti posvećeno najviše pozornosti, valja spomenuti pristupe Kine i SAD-a koji zastupaju liberalniji pristup te dopuštaju više slobode u istraživanju i samokontrole s manjim naglaskom na zaštiti podataka te tako ugrožavaju konkurentnost europskih poduzeća.[39] Europski pristup karakterizira čuvanje temeljnih ljudskih prava i prilaženje problemu na više osnova poput zaštite podataka i nediskriminacije. Navedeni dokumenti čine analize i naputke relevantne za tehnologiju UI-ja s komplementarnošću s načelima zaštite podataka prema OUZP-u počevši s Etičkim smjernicama za pouzdanu umjetnu inteligenciju koje sadrže listu zahtjeva poveznica između UI-ja, zaštite podataka i privatnosti. Prema Smjernicama, pouzdan UI ima tri sastavnice koje trebaju biti ispunjene tijekom cijelog životnog ciklusa sustava: a) trebao bi biti zakonit i poštovati sve primjenjive zakone i propise, b) trebao bi biti etičan i osigurati poštovanje etičkih načela i vrijednosti i (c) trebao bi biti otporan i iz tehničke i iz socijalne perspektive, jer sustavi UI-ja čak i s dobrim namjerama mogu uzrokovati nenamjernu štetu.[40] Prvi zahtjev odnosi se na integraciju ljudskog kadra i nadzora. Svrha ovog zahtjeva je, između ostalog, osigurati ljudski nadzor nad

[37]Ibid.
[38]https://techcrunch.com/2023/06/30/european-vcs-tech-firms-sign-open-letter-warning-against-over-regulation-of-ai-in-draft-eu-laws/, prema stanju na dan 24. 9. 2023.
[39]Europski parlament: *Izvješće o umjetnoj inteligenciji u digitalnom dobu*, Bruxelles, 2020.
[40]Europska komisija, Directorate-General for Communications Networks, Content and Technology: *Etičke smjernice za pouzdanu umjetnu inteligenciju*, str. 2, Publications Office, 2019.

usklađenošću temeljnih ljudskih prava i sloboda kroz razvoj i korištenje UI-ja. Etičke smjernice nadalje naglašavaju kvalitetu i integritet podataka obrađenih podataka UI-jem. U pogledu kvalitete, pozivaju na detaljnu pozornost na takozvane „pristrane" skupove podataka poput socijalno izazvane pristranosti, netočnosti, pogrešaka i zabluda koje za posljedice mogu imati diskriminatorne odluke. Posebno dokument naglašava da korišteni postupci i skupovi podataka moraju biti testirani i zabilježeni na svakome koraku planiranja, obuke, testiranja i implementacije.[41] Cjeloživotna briga u svim ciklusima obveza u skladu je s načelom točnosti sadržanom u članku 5. stavku 1. podstavku (d) OUZP-a. U Smjernicama se spominju načela točnosti i transparentnosti, koja su važna kako bi se dalje razumjela istraživačka pitanja u anketi. Načelo točnosti zahtijeva veću točnost podataka u kontekstu specifične svrhe obrade, dok načelo transparentnosti zahtijeva da odluke UI-ja moraju biti sljedive i objašnjive. Posljednje smjernice zahtijevaju kvalificirano upravljanje pravima i obvezama voditelja obrade unutar organizacije koja koristi sustav UI-ja. Prema Smjernicama, potrebno je osigurati da cijeli životni ciklus UI-sustava ispunjava zahtjeve za njegovu pouzdanost, što uključuje: *(1) ljudsko djelovanje i nadzor, (2) tehničku otpornost i sigurnost, (3) privatnost i upravljanje podacima, (4) transparentnost, (5) raznolikost, nediskriminaciju i pravednost, (6) dobrobit društva i okoliša, (7) odgovornost, a posebno regulira zahtjeve tehničke otpornosti i sigurnosti.* Smjernice pružaju uvid u to kako treba poštovati i provoditi načela za uspješan i pouzdan UI.[42]

Nastavak donosi više o *Bijeloj knjizi o umjetnoj inteligenciji. Europski pristup izvrsnosti i izgradnji povjerenja.* Bijela knjiga ističe, prije svega, da je europska pravna kultura izgrađena na poštovanju temeljnih prava i sloboda uključujući vrijednosti sadržane u tim pravima i slobodama. Komisija naglašava regulatorni pristup usmjeren na ulaganja s dvojakim ciljem uvođenja UI-ja i suzbijanja rizika povezanih s određenim načinima upotrebe te nove tehnologije.[43] Posebno se spominju rizici povezani sa zaštitom privatnosti, osobnih podataka i nediskriminacijom, koji mogu proizaći iz nedovoljnog ljudskog nadzora i pristranih podataka koje obrađuje sustav UI-

[41]Andraško, J., Mesarčík, M., Hamuľák, O.: *The regulatory intersections between artificial intelligence, data protection and cyber security: challenges and opportunities for the EU legal framework*, str. 9, Bratislava, Olomouc, 2020.
[42]European Commission, Directorate-General for Communications Networks, Content and Technology: *Etičke smjernice za pouzdanu umjetnu inteligenciju*, str. 16, Publications Office, 2019.
[43]Europska komisija: *Bijela knjiga o umjetnoj inteligenciji – Europski pristup izvrsnosti i izgradnji povjerenja*, str. 1, Bruxelles, 2020.

ja. U pogledu obrade podataka, Bijela knjiga identificira niz područja u kojima UI stoji kao poseban čimbenik. Prvo područje odnosi se na količinu i kvalitetu podataka o obuci, odnosno podataka korištenih u razvoju UI-ja u smislu rizika koji takva obrada može predstavljati u budućnosti. Drugo područje bavi se vođenjem evidencije i dokumentiranjem korištenih podataka, kao i samim čuvanjem podataka. Treći aspekt odnosi se na transparentnost i pružanje informacija o obradi podataka. Prema Bijeloj knjizi, ovaj zahtjev nadilazi obvezu općeg informiranja prema OUZP-u, s obzirom na to da zahtijeva pružanje specifičnih informacija o funkcioniranju i mogućnostima UI-ja. Sljedeći je aspekt naglasak na ljudskom nadzoru. U praksi bi to trebalo značiti da bi svaku automatiziranu odluku trebali pregledati ljudi, kao i mogućnost ljudske intervencije u proces donošenja odluka ili implementacije preventivnih mehanizama u fazi razvoja UI-ja. Uz zahtjeve temeljnih prava, uključujući zaštitu osobnih podataka, privatnosti i nediskriminaciju, Bijela knjiga identificira pitanja sigurnosti i odgovornosti kao glavne rizike povezane s korištenjem UI-jem. Bijela knjiga jasno zahtijeva da „kako bi umjetna inteligencija bila pouzdana, sigurna i u skladu s europskim vrijednostima i pravilima, nadležna nacionalna i europska tijela te uključene strane moraju poštovati važeće pravne zahtjeve u praksi i učinkovito ih provoditi”.[44] U tu svrhu Komisija predlaže uvođenje prethodne ocjene sukladnosti i s tim povezan sustav certificiranja i označavanja. OUZP već odražava neke od potreba regulacije UI-ja i dotiče se pitanja koja je istaknula Europska komisija u Bijeloj knjizi i drugim dokumentima. Bijela knjiga o UI-ju ukazuje na sklonost Komisije tomu da mogući novi regulatorni okvir slijedi pristup temeljen na riziku, u kojem bi se obvezni zahtjevi u načelu primjenjivali samo na visokorizične aplikacije.

Vrlo sveobuhvatan izvještaj također je *Getting the future right* Agencije Europske unije za temeljna prava. Izvještaj zaključuje da već postoji sveobuhvatni okvir temeljnih prava koji se primjenjuje na korištenje UI-ja u EU-u, a sastoji od Povelje kao i *Europske konvencije o ljudskim pravima*. Korištenje sustava UI-ja uključuje širok raspon temeljnih prava, bez obzira na područje primjene. Pritom bi se EU i njegove države članice trebali oslanjati na čvrste dokaze o utjecaju UI-ja na temeljna prava kako bi osigurali da sva ograničenja određenih temeljnih prava poštuju

[44]Ibid., str. 21.

načela nužnosti i proporcionalnosti.[45] Zakonom je potrebno predvidjeti relevantne mjere za učinkovitu zaštitu od proizvoljnog uplitanja u temeljna prava i za pružanje pravne sigurnosti i razvojnim programerima i korisnicima UI-ja. Teme temeljnih prava koje su se pojavile u istraživanju opetovano se primjenjuju na većinu slučajeva UI-ja te uključuju potrebu da se osigura nediskriminirajuća upotreba UI-ja (pravo da se ne bude diskriminiran), zahtjev za zakonitom obradom podataka (pravo na zaštitu osobnih podataka) i mogućnost žalbe na odluke temeljene na UI-ju i traženja pravne zaštite (pravo na učinkovit pravni lijek i pošteno suđenje). Postoji visoka razina nesigurnosti u vezi sa značenjem automatiziranog donošenja odluka i prava na ljudski pregled koji je povezan s upotrebom UI-ja i automatiziranim odlučivanjem. S obzirom na poteškoće u objašnjavanju složenih sustava UI-ja, EU bi, zajedno s državama članicama, trebao razmotriti razvoj smjernica za podršku naporima za transparentnost u ovom području. Pritom bi se trebao oslanjati na stručnost nacionalnih tijela za ljudska prava i organizacija civilnog društva aktivnih u ovom području. Zaključno, voditelji obrade koji se bave obradom temeljenom na UI-ju trebali bi podržati vrijednosti OUZP-a i usvojiti odgovoran pristup usmjeren na rizik. Međutim, s obzirom na složenost materije i praznine, nejasnoće i dvosmislenosti prisutne u OUZP-u, voditelji obrade ne bi trebali biti prepušteni sami sebi u ovoj vježbi. Institucije trebaju promicati široku društvenu raspravu o primjenama UI-ja i pružiti indikacije na visokoj razini.

Završno će biti pregledano najtemeljitije i sveobuhvatno istraživanje vezano uz učinke OUZP-a na UI, izvještaj Panela za znanost i tehnologiju pripremljeno za Europski parlament *The impact of the General Data Protection Regulation on artificial intelligence.* Izvještaj smatra da OUZP općenito pruža smislene naznake za zaštitu podataka u odnosu na aplikacije UI-ja te se može tumačiti i primjenjivati tako da ne ometa korisnu primjenu UI-ja na osobne podatke i da ne stavlja poduzeća iz EU-a u nepovoljniji položaj u usporedbi s neeuropskim konkurentima.[46] Stoga se čini da OUZP ne zahtijeva nikakvu veću promjenu kako bi se pozabavio UI-jem. Unatoč tomu, OUZP nema eksplicitan odgovor na brojna pitanja zaštite podataka povezanih s UI-jem, što može dovesti do nesigurnosti i troškova te može nepotrebno ometati razvoj aplikacija

[45]Agencija Europske unije za temeljna prava: *Getting the future right – Artificial intelligence and fundamental rights*, str. 7, Beč, 2020.
[46]Think tank: European Parliament: *The impact of the General Data Protection Regulation (GDPR) on Artificial Intelligence,* str. 3, 2020.

UI-ja.[47] Izvještaj ističe kako se rasprava treba pozabaviti pitanjima određivanja standarda koji bi se trebali primjenjivati na UI-obradu osobnih podataka, posebno kako bi se osigurale prihvatljivost, pravednost i razumnost odluka o pojedincima. Za to su potrebna pravno obvezujuća pravila, s obzirom na to da je OUZP usredotočen na pojedinačna prava i ne uzima u obzir šire društvene učinke masovne obrade. Izvještaj također upozorava na to da postoji napetost između tradicionalnih načela zaštite podataka ograničenja svrhe, minimiziranja podataka, posebnog tretmana „osjetljivih podataka", ograničenja automatiziranih odluka i pune primjene snage UI-ja i velikih podataka. Potonje podrazumijeva prikupljanje golemih količina podataka u vezi s pojedincem i njegovim društvenim odnosima te obradu takvih podataka u svrhe koje nisu bile u potpunosti određene u trenutku prikupljanja. Međutim, postoje načini tumačenja, primjene i razvoja načela zaštite podataka koji su u skladu s korisnim korištenjem UI-ja i velikih podataka. Voditelji obrade također bi trebali imati obvezu davanja pojedinačnih objašnjenja, u mjeri u kojoj je to moguće prema usvojenoj tehnologiji UI-ja i razumno prema troškovima i koristima. Potrebno je specificirati sadržaj obveze voditelja obrade da pruži informacije i odgovarajuća prava ispitanika o svrsi sustava UI-ja, s odgovarajućim primjerima, a s obzirom na različite tehnologije. Zaključno, voditelji obrade koji se bave obradom temeljenom na UI-ju trebali bi podržati vrijednosti OUZP-a i usvojiti odgovoran pristup usmjeren na rizik te bi to trebali moći učiniti na način koji je kompatibilan s dostupnim tehnologijama i ekonomskom isplativošću.[48]

Iz pregleda se može uočiti pozivanje na iste probleme i izazove, što potvrđuje ozbiljnost navedenih nedostataka. Načelo točnosti, načelo transparentnosti, zaštita temeljnih prava privatnosti i zaštita osobnih podataka naglašeni su kao osnovna načela kojih se treba pridržavati kod implementacija novih sustava UI-ja kako bi bili sigurni za korištenje te imali povjerenje korisnika. Od velikog je značaja i dosljednost pristupu utemeljenom na procjenama rizika. Vidljiva je potreba za jasnim i razumljivim smjernicama, dok bi istovremeno trebalo izbjeći previše regulacije kako bi tehnološka scena ostala konkurentna. Sve veće pozivanje na temeljna prava u ovim raspravama ukazuje na osviještenost postojanja okvira temeljnih prava uz druge pravne okvire. UI je nužan za procjenu brojnih prilika i izazova koje donose nove tehnologije, učinkovitu

[47]Ibid., str. 3.
[48]Ibid., str. 4.

i usklađenu s ljudskim pravima. Mnoge postojeće inicijative UI-ja vođene su etičkim okvirima koji su obično dobrovoljni. Ipak, sustavi o kojima je riječ mogu biti zasta složeni. I oni koji se koriste sustavima UI-ja i oni koji su odgovorni za reguliranje njihove uporabe priznaju da ih ne razumiju uvijek u potpunosti.[49] Važno je napomenuti da navedeni dokumenti ne čine cjelokupnu analizu te postoje još i drugi dokumenti i propisi koji bi se trebali spomenuti, poput *Europske strategije za zaštitu podataka*, *Strategije Europske unije za kibersigurnost, Akta o digitalnim uslugama*, *Akta o digitalnim tržištima* i *Akta o upravljanju podacima* koji također pružaju pravnu infrastrukturu za učinkovito djelovanje UI-ja. Također se mogu uočiti sličnosti izazova s prethodnim tehnologijama koje su nedavno stekle popularnost, poput *Internet of Things* (dalje u tekstu IoT). Kako ističe Katulić: „Brojni su autori prepoznali nekoliko ključnih točaka u vezi s primjenom GDPR-a na obradu IoT-a, uglavnom se fokusirajući na pitanja u vezi utvrđivanja odgovarajuće pravne osnove (kao što je prevladavajuća i često neprikladna upotreba privole koja nije prikladna za mnoge IoT situacije), borba operatera IoT usluga s načelima zaštite podataka sadržanih u Uredbi kao što su načela transparentne, poštene i zakonite obrade, minimizacija podataka i sigurnost podataka, povjerljivost i integritet“.[50] Izniman razvoj tehnologije prate slični problemi u vidu zakonite i poštene obrade podataka koje koriste te UI nije iznimka.

2.5. Načela obrade podataka u UI-ju

2.5.1. Načelo transparentnosti

Postoje brojne napetosti između upotrebe UI-ja kao tehnologije velikih podataka i zahtjeva za ograničenjem svrhe, transparentne obrade i izbjegavanja

[49]Agencija Europske unije za temeljna prava: *Getting the future right – Artificial intelligence and fundamental rights*, str. 1, Beč, 2020.

[50] Vojković, G., Milenković, M., Katulić, T.: *IoT and Smart Home Data Breach Risks from the Perspective of Croatian Data Protection and Information Security Law*. // Proceedings of the ENTRENOVA -ENTerprise REsearch InNOVAtion Conference / Milković, Marin; Seljan, Sanja; Pejić Bach, Mirjana; Peković, Sanja; Perovic, Djurdjica (ur.). Rovinj: Udruga za promicanje inovacija i istraživanja u ekonomiji "IRENET", Zagreb, 2019. pp. 298–308. (https://www.bib.irb.hr/1020078) (predavanje, međunarodna recenzija, cjeloviti rad [*in extenso*], znanstveni).

pristranosti, primjerice. Zbog toga je potrebno uspostaviti odgovarajuće zaštitne mjere kako bi se osigurale primjene u skladu sa zakonima o zaštiti i privatnosti podataka, posebno s OUZP-om i nacionalnim zakonima o zaštiti podataka te s drugim temeljnim pravima. Osnovni je zahtjev da zaštita podataka bude integrirani element obrade podataka. Načelo integrirane zaštite podataka zahtijeva od voditelja obrade osiguravanje kroz odgovarajuće tehničke i organizacijske mjere da se integriranim načinom kao početna i zadana vrijednost obrađuju samo osobni podaci nužni za svaku posebnu svrhu, na količinu, opseg obrade, razdoblje pohrane i njihovu dostupnost.[51] Pristup zaštiti podataka temeljen na riziku usmjeren je na sprječavanje štete, a ne na davanje pravnih ovlasti pojedinačnim subjektima podataka nad obradom njihovih podataka. Ključnu ulogu u tom smislu ima članak 25. OUZP-a, *Zaštita podataka projektirano i prema zadanim postavkama*, koji zahtijeva usvajanje tehničkih i organizacijskih mjera za provedbu načela zaštite podataka i integraciju zaštitnih mjera u obradu. Tom se odredbom ponajprije želi zajamčiti primjerena i učinkovita zaštita podataka, uz poštivanje njezinih tehničkih i integriranih elemenata, što znači da bi voditelji obrade trebali moći dokazati da imaju uspostavljene odgovarajuće i zaštitne mjere kako bi osigurali učinkovitost načela zaštite podataka te prava i slobode ispitanika.[52] Ostale odgovarajuće mjere ovise o okolnostima obrade, no one mogu uključivati provođenje procjene učinka na zaštitu podataka, primjenu tehnika pseudonimizacije na predmetne podatke, smanjenje količine prikupljenih podataka i razdoblja pohrane podataka te provođenje tehničkih i organizacijskih mjera radi osiguravanja visoke razine zaštite.[53] U predloženom *Aktu o umjetnoj inteligenciji*, s obzirom na podatkovno intenzivnu narav brojnih primjena UI-ja, trebalo bi promicati usvajanje pristupa tehničke i integrirane zaštite podataka na svakoj razini, čime se jamči učinkovita provedba načela zaštite podataka kako je predviđeno člankom 25. OUZP-a i člankom 27. *Europske uredbe o zaštiti podataka* s pomoću najnovijih tehnoloških dostignuća.[54]

[51] EPDB, Europski odbor za zaštitu podataka: *Smjernice 4/2019 o članku 25. Tehnička i integrirana zaštita podataka*, str. 11, 2020.
[52]Ibid., str. 5.
[53]Radna skupina iz članka 29: *Smjernice o transparentnosti na temelju Uredbe 2016/679*, str. 32, 2018.
[54]EDPB-EDPS: *Zajedničko mišljenje 5/2021 o Prijedlogu uredbe Europskog parlamenta i Vijeća o utvrđivanju usklađenih pravila o umjetnoj inteligenciji (Akt o umjetnoj inteligenciji)*, str. 7, Bruxelles, 2021.

Složenost obrade temeljene na UI-ju i činjenica da se takva obrada ne može u potpunosti predvidjeti, osobito kada se temelji na strojnom učenju, posebno otežava osiguranje transparentnosti. Pitanje transparentnosti može se pojaviti u dvjema vremenskim točkama, kada se podaci subjekta podataka unose u informacijski sustav koji uključuje algoritme UI-ja (*ex-ante* transparentnost) ili nakon što je algoritamski model sustava primijenjen na subjekt podataka, na dane specifične rezultate u vezi s njim (*ex-post* transparentnost).[55] U OUZP-u postoji inherentna suprotnost između zahtjeva, s jedne strane, za pružanje sveobuhvatnih informacija ispitanicima na temelju te uredbe i, s druge strane, za pružanje tih informacija u sažetom, transparentnom, razumljivom i lako dostupnom obliku.[56] Načela pravednosti i transparentna obrada zahtijevaju da ispitanik bude obaviješten o postojanju postupka obrade i njegovoj svrsi. Korisnicima bi također trebalo pružiti dovoljno informacija za donošenje informirane procjene o prikladnosti modela za njihov slučaj upotrebe. Informacije o rizicima, provednim protumjerama, preostalim rizicima ili ograničenjima trebaju biti jasno priopćene.[57] Voditelj obrade trebao bi ispitaniku pružiti sve daljnje informacije potrebne za osiguranje poštene i transparentne obrade uzimajući u obzir posebne okolnosti i kontekst u kojem se osobni podaci obrađuju. U OUZP-u se mogu razlikovati dva različita koncepta pravednosti. Prvi, koji možemo nazvati „pravednošću informacija“, strogo je povezan s idejom transparentnosti**.** Zahtijeva da subjekti podataka ne budu prevareni ili dovedeni u zabludu u vezi s obradom svojih podataka, kao što je objašnjeno u uvodnoj izjavi (60): „informacijska pravednost postavlja specifična pitanja u vezi s umjetnom inteligencijom i velikim podacima zbog složenosti obrade koja je uključena u aplikacije umjetne inteligencije, neizvjesnosti njezina ishoda i višestrukih svrha“.[58] Nova dimenzija načela odnosi se na objašnjivost automatiziranih odluka. U odnosu na aplikacije i usluge UI-ja, značajke sustava za obradu podataka moraju omogućiti subjektima podataka da stvarno razumiju što se događa s njihovim podacima, bez obzira na pravnu osnovu obrade. U svakom slučaju, načelo pravednosti nadilazi obveze transparentnosti.[59] Poseban aspekt transparentnosti u kontekstu

[55]Think tank: European Parliament: *The impact of the General Data Protection Regulation (GDPR) on Artificial Intelligence*, str. 53, 2020.
[56]Radna skupina iz članka 29: *Smjernice o transparentnosti na temelju Uredbe 2016/679*, str. 19, 2018.
[57] Federal office of Information security: *Generative AI Models Opportunities and Risks for Industry and Authorities*, str. 28, 2024.
[58]Uvodna izjava 60, OUZP.
[59]Mitrou, L.: *Data Protection, Artificial Intelligence and Cognitive Services: Is the General Data Protection Regulation (GDPR) 'Artificial Intelligence-Proof'*?, str. 42, 2018.

strojnog učenja odnosi se na pristup podacima, posebno skupu za obuku sustava. Pristup podacima može biti potreban kako bi se identificirali mogući uzroci nepoštenosti koji proizlaze iz neadekvatnih ili pristranih podataka ili algoritma obuke. Ovo je osobito važno kada je naučeni algoritamski model netransparentan, tako da se mogući nedostaci ne mogu otkriti njegovim pregledom. Materijalna pravednost u uvodnoj izjavi (71) ukazuje na drukčiju dimenziju pravednosti, to jest na ono što možemo nazvati suštinskom pravednošću koja se odnosi na pravednost sadržaja automatiziranog zaključivanja ili odluke, prema kombinaciji kriterija koji se mogu sažeti pozivanjem na prethodno spomenuti standard prihvatljivosti, relevantnosti i pouzdanosti. [60] Upravo načelo transparentnosti, odnosno primjena tog načela u relevantnim odredbama, omogućuje subjektima podataka lakši uvid u postupke obrade osobnih podataka te, na temelju toga i načela odgovornosti, pozivanje voditelja obrade i izvršitelja obrade na odgovornost.[61] Ispitanici uvijek trebaju biti obaviješteni o tome da se njihovi podaci koriste kako bi se sustavima UI-ja omogućilo učenje, predviđanje, o pravnoj osnovi za takvu obradu te trebaju dobiti opće objašnjenje logike postupka i informacije o opsegu sustava UI-ja. U tom pogledu, u tim slučajevima uvijek treba biti zajamčeno pravo pojedinca na ograničenje obrade (čl. 18. OUZP-a i čl. 20. *Europske uredbe o zaštiti podataka*), kao i na brisanje podataka (čl. 16. OUZP-a i čl. 19. *Europske uredbe o zaštiti podataka*). [62] Pristup UI-ja usmjeren na temeljna prava podupire zakonska regulativa, pri čemu je odgovornost za poštivanje, zaštitu i ispunjavanje prava na državi. To bi trebalo jamčiti visoku razinu pravne zaštite od moguće zlouporabe novih tehnologija. Također, pristup pruža jasnu pravnu osnovu iz koje se može razviti UI, gdje je pozivanje na temeljna prava i njihovu primjenu u praksi u potpunosti ugrađeno. U slučajevima iz članka 22. stavka 2. točaka (a) i (c) OUZP-a kada je automatizirana odluka potrebna za ugovor ili izričitu suglasnost, članak 22. stavak 3. zahtijeva odgovarajuće zaštitne mjere: voditelj obrade podataka provodi odgovarajuće mjere zaštite subjektovih prava i sloboda te legitimnih interesa, najmanje prava na ljudsku intervenciju voditelja obrade, izražavanje vlastitog stajališta i prava na osporavanje odluke. Prema Radnoj skupini za članak 29., neke od ovih mjera odnose

[60]Uvodna izjava 71, OUZP.
[61]Katulić, A., Katulić, T., Hebrang Grgić, I.: *Application of the principle of transparency in processing of European national libraries patrons' personal data*, str. 7, // Digital Library Perspectives, 2022.
[62]EDPB-EDPS: *Zajedničko mišljenje 5/2021 o Prijedlogu uredbe Europskog parlamenta i Vijeća o utvrđivanju usklađenih pravila o umjetnoj inteligenciji (Akt o umjetnoj inteligenciji)*, str. 19., Bruxelles, 2021.

se na smanjenje rizika. Primjeri su provjere osiguranja kvalitete, algoritamska revizija, minimizacija podataka i anonimizacija ili pseudonimizacija te mehanizmi certificiranja. S obzirom na zahtjeve za tehničku i integriranu zaštitu podataka, mehanizmi transparentnosti trebali bi se ugraditi u sustave obrade na samom početku, tako da se svi izvori osobnih podataka koje je organizacija primila mogu pratiti i da se njihov izvor može utvrditi u bilo kojem trenutku ciklusa obrade podataka.[63]

2.5.2. Načelo minimizacije

Također, postoji napetost između načela minimizacije i same ideje velikih podataka i analitike podataka, što uključuje korištenje UI-ja i statističkih metoda za otkrivanje novih neočekivanih korelacija u golemim skupovima podataka. Ova napetost može se smanjiti sljedećim razmatranjima. Prvo, ideju minimiziranja treba povezati s idejom proporcionalnosti.[64] Minimiziranje ne isključuje uključivanje dodatnih osobnih podataka u obradu, sve dok dodavanje takvih podataka pruža korist, u odnosu na svrhe obrade, koja nadmašuje dodatne rizike za subjekte podataka. Čak i korisnost buduće obrade može opravdati zadržavanje podataka, sve dok postoje odgovarajuće sigurnosne mjere. Konkretno, pseudonimizacija kao mjera obrade osobnih podataka služi kako se ti podaci više ne bi mogli pripisati određenom ispitaniku bez uporabe dodatnih informacija, pod uvjetom da se te informacije drže odvojeno te da podliježu tehničkim i organizacijskim mjerama, kako bi se osiguralo da se osobni podaci ne mogu pripisati pojedincu čiji je identitet utvrđen ili se može utvrditi, u kombinaciji s drugim sigurnosnim mjerama može pridonijeti ograničavanju rizika i stoga povećati kompatibilnost zadržavanja sa smanjenjem.[65] Načelo minimizacije podataka također se može shvatiti tako da se omogući korisna primjena UI-ja. Minimiziranje može zahtijevati, u nekim kontekstima, smanjenje osobnosti dostupnih podataka, a umjesto količine takvih podataka može se zahtijevati smanjenje, putem mjera kao što je pseudonimizacija. Mogućnost ponovne identifikacije ne bi trebala značiti da se svi

[63]Radna skupina iz članka 29: *Smjernice o transparentnosti na temelju Uredbe 2016/679*, str. 31, 2018.
[64]Think tank: European Parliament: *The impact of the General Data Protection Regulation (GDPR) on Artificial Intelligence*,str. 47, 2020.
[65]Dragičević, D., Gumzej, N., Jurić M., Katulić, T., Lisičar, H.: *Pravna informatika i pravo informacijskih tehnologija*, str. 129, NN, Zagreb, 2015.

podaci koji se mogu ponovno identificirati smatraju osobnim podacima koje treba minimizirati. Umjesto toga, ponovnu identifikaciju ispitanika treba smatrati stvaranjem novih osobnih podataka koji bi trebali podlijegati svim primjenjivim pravilima. Ponovna identifikacija trebala bi biti strogo zabranjena, osim ako nisu ispunjeni svi uvjeti za zakonito prikupljanje osobnih podataka, i trebala bi biti kompatibilna sa svrhama za koje su podaci izvorno prikupljeni i naknadno anonimizirani. Zahtjev za ograničenjem svrhe može se razumjeti na način koji je kompatibilan s UI-jem i velikim podacima, kroz fleksibilnu primjenu ideje kompatibilnosti koja dopušta ponovnu upotrebu osobnih podataka kada to nije nespojivo sa svrhama za koje su podaci bili izvorno prikupljeni. Štoviše, pretpostavlja se da je ponovna uporaba u statističke svrhe kompatibilna te bi stoga općenito bila dopuštena, osim ako uključuje neprihvatljive rizike za nositelja podataka. Jasno razgraničenje svrhe važno je ne samo kako bi se subjektima podataka omogućilo učinkovito ostvarivanje njihovih prava već i za definiranje ukupne usklađenosti sa zakonom i za njegovu procjenu.[66] Provođenje minimizacije podataka i svrhe načela , u teoriji bi trebalo voditi savjesnom i promišljenom prikupljanju podataka. Međutim u nedostatku dogovora o tome što čini previše podataka, biti će izazov za regulatore ustvrditi prakticira li organizacija dovoljno načelo minimizacije izuzev teških kršenja.[67]

Kombinacija UI-ja i velikih podataka omogućuje automatizirano donošenje odluka, čak i u domenama koje zahtijevaju složene izbore na temelju višestrukih čimbenika i bez unaprijed definiranih kriterija. Također je važno razmotriti da više podataka ne znači nužno i bolja rješenja. Testiranje algoritama korištenjem minimzacije podataka može pomoći u određivanju najmanje potrebne količine podataka za održivi slučaj upotrebe.[68] Posljednjih godina vodila se široka rasprava o izgledima i rizicima algoritamskih procjena i odluka u vezi s pojedincem. Neki su znanstvenici primijetili da su automatizirana predviđanja i odluke u mnogim područjima ne samo jeftinije već i preciznije i nepristranije od ljudskih. Sustavi UI-ja mogu izbjeći tipične zablude ljudske psihologije kao što su pretjerano samopouzdanje, nesklonost gubitku, sidrenje, pristranost potvrde, heuristika reprezentativnosti i raširena ljudska nesposobnost obrade

[66]Mitrou, L.: *Data Protection, Artificial Intelligence and Cognitive Services: Is the General Data Protection Regulation (GDPR) 'Artificial Intelligence-Proof'?*, str. 47, 2018.
[67] King, J., Meinhardt, C.: *Rethinking Privacy in the AI Era Policy Provocations for a Data-Centric World* , Stanford HAI, Stanford, str 23, 2024.

[68]CEDPO AI Working Group; *Generative AI: The Data Protection Implications*, str. 19, 2023.

statističkih podataka, kao i tipične ljudske predrasude u vezi s, primjerice, etničkom pripadnošću, spolom ili društvenim podrijetlom.[69] U drugim slučajevima, pogreške i diskriminacije mogu se odnositi na pristranosti sustava strojnog učenja ugrađene u prediktore. Sustav može raditi nepravedno jer koristi povoljan prediktor koji se odnosi samo na članove određene skupine. Nepoštenost također može proizaći iz uzimanja pristranih ljudskih prosudbi kao prediktora, poput pisma preporuke. Primjene koje se temelje na UI-ju pružaju mogućnosti za procjenu poštovanja temeljnih prava, među ostalim u području jednakosti. Pri utvrđivanju načina treniranja algoritama UI-ja, voditelj obrade trebao bi imati točne podatke za postizanje preciznih rezultata. Stoga bi voditelj obrade trebao osigurati točnost podataka koji se upotrebljavaju za treniranje algoritama UI-ja.[70]Odluke koje se temelje na algoritamskim sustavima s unaprijed definiranim pravilima i točnim i odgovarajućim podacima prikladnima za tu svrhu mogle bi biti manje podložne pristranim rezultatima nego ljudske odluke. Istodobno, upotrebom UI-ja u određenim slučajevima može se perpetuirati i pojačati diskriminacija uključujući strukturne nejednakosti. Podaci koji se upotrebljavaju za treniranje sustava UI-ja moraju stoga biti točni i svrsishodni, a potrebno je pozabaviti se potencijalnim oblicima pristranosti uz istodobno omogućivanje dovoljne fleksibilnosti u istraživanju i razvoju radi daljnjeg razvoja tih sustava. U tom pogledu važno je naglasiti načela jednakosti i nediskriminacije u osmišljavanju, razvoju, uvođenju, upotrebi i evaluaciji UI-ja, osobito u sustavima u kojima je integrirano strojno učenje, te osiguravanja podlijeganja takvih sustava odgovarajućim zaštitnim mjerama i nadzoru, među ostalim nadzoru tržišta.[71] OUZP dopušta razvoj UI-ja i velikih podatkovnih aplikacija koje uspješno balansiraju zaštitu podataka i druge društvene i ekonomske interese, ali pruža ograničene smjernice o tome kako postići taj cilj. Svaka tvrtka koja koristi UI, razvija tehnologiju ili je primjenjuje u poslovanju trebat će specijalizirano osoblje koje će biti u skladu s regulativom, što očito povećava troškove, ali i ne potiče ulaganja u ovo područje. Također, postoji sve više dokaza da velik broj malih i srednjih poduzeća ima problema s razumijevanjem i primjenom propisa. Stoga mogu biti otporni na iskorištavanje prednosti UI-ja kada se suoče s

[69]Kahneman, D.: *Thinking: fast and slow*, Farrar, Straus and Giroux, New York, 2011.
[70]EPDB, Europski odbor za zaštitu podataka: *Smjernice 4/2019 o članku 25. Tehnička i integrirana zaštita podataka*, str. 24, 2020.
[71]Predsjedništvo Vijeća Europske unije, Zaključci predsjedništva: *Povelja o temeljnim pravima u kontekstu umjetne inteligencije i digitalnih promjena*, str. 11, Bruxelles, 2020.

rizikom i nađu se na meti pravnih radnji.[72] OUZP doista obiluje nejasnim klauzulama i otvorenim standardima čija primjena često zahtijeva balansiranje suprotstavljenih interesa. U slučaju primjene UI-ja i velikih podataka, neizvjesnosti su pogoršane novošću tehnologija, njihovom složenošću i širokim opsegom njihovih pojedinačnih i društvenih učinaka.

3. ANKETNA PITANJA

Razumijevanje najbitnijih pojmova i načela nužno je za shvaćanje anketnih pitanja te interpretacije odgovora i učinaka UI-ja na poslovanje organizacija. Prvi dio ankete usmjeren je na obveze organizacije koje proizlaze iz OUZP-a, dok je u drugom

[72]Mazurek, G., Małagocka, K.: *Are we down to zero-one code? Perception of privacy and data protection in the context of the development of artificial intelligence*, str. 10, Journal of Management Analytics, 2019.

dijelu pozornost posvećena konkretnim tehničkim i organizacijskim mjerama koje organizacije provode kako bi uskladile svoje proizvode sa zahtjevima sigurnog i pouzdanog UI-ja. Ponuđeni odgovori iskazani su brojčanom vrijednošću od 1 do 5, gdje 1 označuje *Uopće se ne slažem*, 2 *Uglavnom se ne slažem*, 3 *Niti se slažem niti se ne slažem*, 4 *Uglavnom se slažem* i 5 *U potpunosti se slažem.*

3.1. Prvi dio ankete

1. Vaša organizacija (društvo, tvrtka) u potpunosti razumije i primjenjuje osnovna načela zaštite podataka prema *Općoj uredbi o zaštiti podataka* (OUZP) (od 1 do 5).

Odgovori:

- 5 *U potpunosti se slažem*,
- 6 *Uglavnom se slažem*,
- 1 *Niti se slažem niti ne slažem*.

Većina ispitanika u potpunosti se slaže ili se uglavnom slaže da razumiju i primjenjuju osnovna načela zaštite podataka prema OUZP-u, dok se samo jedan ispitanik niti slaže niti se ne slaže s tvrdnjom. Odgovori sugeriraju kako sudionici shvaćaju ulogu i svrhu načela zaštite podataka. Treba naglasiti da je bitno razumjeti načela kako bi se ona mogla pravilno primijeniti. Također, u odgovoru sudionici tvrde kako primjenjuju osnovna načela u djelovanju svoje organizacije.

2. Vaša organizacija je ispravno identificirala pravne osnove obrade osobnih podataka koje obrađuje u okviru svojih aktivnosti (od 1 do 5).

Odgovori:

- 5 *U potpunosti se slažem,*
- 6 *Uglavnom se slažem*,
- 1 *Uglavnom se ne slažem*.

Većina ispitanika u potpunosti se slaže ili se uglavnom slaže da su ispravno identificirali pravne osnove obrade osobnih podataka koje obrađuju u okviru svojih aktivnosti, a tek se jedan ispitanik uglavnom ne bi složio s tvrdnjom. Iz odgovora možemo zaključiti kako je većina ispitanika shvatila koncept pravnih osnova na kojima obrađuju podatke. Shvaćanje pravne osnovne važno je kako bi ispitanici mogli pravilno obavijestiti korisnike o tome na kojem temelju i kako se obrađuju njihovi podaci.

3. U vašoj organizaciji postoji adekvatna dokumentacija o provedbi postupaka ispunjavanja prava ispitanika (od 1 do 5).

Odgovori:

- 4 *U potpunosti se slažem*,
- 5 *Uglavnom se slažem*,
- 1 *Niti se slažem niti se ne slažem*,
- 2 *Uglavnom se ne slažem*.

Većina ispitanika u potpunosti se slaže ili se uglavnom slaže da u njihovoj organizaciji postoji adekvatna dokumentacija o provedbi postupaka ispunjavanja prava ispitanika, dok se tri ispitanika uglavnom ne slažu ili niti se slažu niti se ne slaže. Smjernice obvezu ispunjavanja prava ispitanika i čuvanje odgovarajuće dokumentacije smatraju ključnim elementom ostvarenja načela transparentnosti. Postupci ispunjava prava ispitanika trebali bi sadržavati načine i pojašnjenja kako pojedinci mogu ostvariti zaštitu i ispunjenje svojih prava navedenih u člancima OUZP-a.

4. Vaša organizacija adekvatno ispunjava obveze o informiranju ispitanika prema OUZP-u (od 1 do 5).

Odgovori:

- 5 *U potpunosti se slažem*,
- 4 *Uglavnom se slažem*,
- 2 *Niti se slažem niti se ne slažem*,
- 1 *Uglavnom se ne slažem*.

Većina ispitanika u potpunosti se slaže ili se uglavnom slaže da ispunjavaju obveze o informiraju ispitanika prema OUZP-u, dok se trećina ispitanika ne slaže s tvrdnjom. Navedene informacije moraju sadržavati upute o tome u koje će se svrhe koristiti njihovi podaci, kako i kome se korisnik može obratiti za zaštitu i ostvarenje svojih prava. Informiranje ispitanika mora biti pravodobno i potpuno kako bi učinkovito ispunili načela transparentnosti. Prema prijedlogu uredbe, sve organizacije koje koriste sustave UI-ja imat će obvezu obavijestiti korisnika sustava kako je u interakciji s UI-jem.

5. Zaposlenici organizacije adekvatno su obučeni o tehničkim aspektima zaštite podataka (od 1 do 5).

Odgovori:

- 3 *U potpunosti se slažem*,
- 5 *Uglavnom se slažem*,
- 2 *Niti se slažem niti se ne slažem*,
- 1 *Uglavnom se ne slažem*,
- 1 *Uopće se ne slažem*.

Većina ispitanika u potpunosti se slaže ili se uglavnom slaže da su zaposlenici njihove organizacije adekvatno obučeni o tehničkim aspektima zaštite podataka, dva ispitanika niti se slažu niti ne slažu, jedan se ispitanik uopće ne slaže, kao što se jedan uglavnom ne slaže. Tehnička zaštita podataka trebala bi biti integrirana u cjeloživotni ciklus sustava UI-ja. Trećina sudionika ne bi se složila kako je primjena tehničkih mjera u njihovoj organizaciji adekvatna.

6. Organizacija u potpunosti razumije i provodi obveze kao voditelj obrade prema OUZP-u (od 1 do 5).

Odgovori:

- 5 *U potpunosti se slažem*,
- 3 *Uglavnom se slažem*,
- 3 *Niti se slažem niti se ne slažem*,
- 1 *Uglavnom se ne slažem*.

Većina ispitanika u potpunosti se slaže ili se uglavnom slaže da u potpunosti razumiju i provode obveze kao voditelj obrade prema OUZP-u, tri ispitanika niti se slažu niti se ne slažu, a jedan se uglavnom ne slaže. Iz odgovora je moguće zaključiti kako se većina ispitanika uglavnom ili u potpunosti slaže s tvrdnjom, dok je zabrinjavajuć podatak kako se trećina ispitanika ne slaže ili se uglavnom ne slaže s tvrdnjom. Vrlo je zanimljivo usporediti ove odgovore s odgovorima prvog pitanja na koje je samo jedan ispitanik odgovorio da niti se slaže niti se ne slaže s razumijevanjem i primjenom načela obrade podataka. Obveza je voditelja obrade, prema članku 24. OUZP-a, provođenje odgovarajućih tehničkih i organizacijskih mjera kako bi mogao dokazati da je obrada u skladu s OUZP-om.

7. Prepoznajemo i u radu organizacije koristimo postupke certificiranja kako bismo dokazali usklađenost sa zahtjevima EU propisa (od 1 do 5).

Odgovori:

- 4 *Uglavnom se slažem,*
- 3 *Niti se slažem niti se ne slažem,*
- 2 *Uglavnom se ne slažem,*
- 3 *Uopće se ne slažem*.

Većina se ispitanika uglavnom ili uopće ne bi složila s tvrdnjom da njihova organizacija koristi postupke certificiranja kako bi dokazala usklađenost sa zahtjevima EU propisa, tri ispitanika niti se slažu niti se ne slažu, dok ih se samo četiri uglavnom slažu. Iako se komisija zalaže za postupke certificiranja kako bi organizacije dokazale usklađenost s obvezama, u praksi samo trećina organizacija koristi postupke certifikacije. Odgovori ukazuju na nedovoljno razvijenu svijest potrebe za primjenom postupaka certifikacije kako bi se dokazala usklađenost sa zahtjevima i obavezama EU-a.

8. Sustav informacijske sigurnosti u Vašoj organizaciji u stanju je spriječiti povrede podataka i druge incidente informacijske sigurnosti (od 1 do 5).

Odgovori:

- 3 *U potpunosti se slažem*,
- 7 *Uglavnom se slažem,*
- 1 *Uglavnom se ne slažem,*
- 1 *Uopće se ne slažem*.

Većina ispitanika u potpunosti se slaže ili se uglavnom slaže da je njihova organizacija u stanju spriječiti povrede podataka i druge incidente informacijske sigurnosti, dok se dva ispitanika uglavnom ne slažu ili se uopće ne slažu. Informacijska sigurnost ključna je kako bi se spriječile povrede podataka. Iz odgovora se može zaključiti kako većina ispitanika smatra sigurnost informacijskog sustava bitnom stavkom u svojoj organizaciji, što potvrđuje shvaćanje važnosti sigurnog informacijskog sustava kao pretpostavke sigurne obrade podataka.

9. Vaša organizacija u praksi primjenjuje koncept "Privacy by design" pri razvoju novih IT rješenja (od 1 do 5).

Odgovori:

- 2 *U potpunosti se slažem*,
- 3 *Uglavnom se slažem,*
- 4 *Niti se slažem niti ne slažem,*

- 2 *Uglavnom se ne slažem,*
- 1 *Uopće se ne slažem*.

Najviše ispitanika, njih četvero, niti se slažu niti se ne slažu s tvrdnjom, dok se tri ispitanika uglavnom ne slažu ili se uopće ne slažu, a samo se pet ispitanika u potpunosti ili uglavnom slaže s tvrdnjom. Koncept „Privacy by design“ odnosi se na niz tehničkih i organizacijskih mjera kako bi se postigla cjelokupna zaštita podataka. Odgovori ispitanika ukazuju na neujednačenu primjenu koncepta „Privacy by design“ među ispitanicima, što se može tumačiti tako da većina organizacija ipak još ne poznaje primjenu koncepta „Privacy by design“. Vjerojatno je uporaba koncepta raširenija u područjima koja to više zahtijevaju poput, primjerice, sustava UI-ja koji su ograničenog ili visokog rizika.

Iz prvog dijela odgovora može se zaključiti kako velika većina organizacija razumije i primjenjuje načela obrade podataka i druge zahtjeve OUZP-a. Vođenje dokumentacije o pravima ispitanika, kao i pružanje informacija ispitaniku kako se njihovi podaci obrađuju, trebalo bi biti okosnica sigurnog i pouzdanog UI-ja. Iz odgovora se može zaključiti da većina organizacija ispunjava navedene zahtjeve, dok kod manjine organizacija preostaje prostora za ispravak nedostataka. Obuka o tehničkim aspektima zaštite podataka, provođenja obveza kao voditelja obrade i sigurnost informacijskog sustava također su ključne za razvoj UI-ja kojemu će korisnici vjerovati te je iz odgovora vidljivo da većina organizacija shvaća važnost tih mjera i održava ih na adekvatnim razinama. Nova rješenja poput postupaka certificiranja i koncepta “Privacy by design” zaživjela su tek u manjem dijelu organizacija, dok većina organizacija još razmatra uvođenje tih mjera. Iz odgovora se može vidjeti kako i same organizacije oklijevaju pri uvođenju najnovijih mjera te vjerojatno čekaju reakciju drugih organizacija na tržištu kako bi se odlučile na uvođenje tih mjera. Uzevši u obzir kako je od uvođenja OUZP-a prošlo punih pet godina, može se smatrati da su odredbe i zahtjevi OUZP-a adekvatno prihvaćeni te pravilno primijenjeni u većini organizacija.

3.2. Drugi dio ankete

1. U Vašoj organizaciji postoji kvalificirani ljudski nadzor donošenja odluka A.I. sustava koji obrađuje osobne podatke ispitanika (od 1 do 5).

Odgovori:

- 1 *U potpunosti se slažem,*
- 1 *Uglavnom se slažem,*
- 1 *Niti se slažem niti ne slažem,*
- 1 *Uglavnom se ne slažem,*
- 1 *Uopće se ne slažem*.

Od pet ispitanika svaki je odgovorio drukčije, što ukazuje na problem neujednačenosti i nedostatka ljudskog nadzora pri donošenja odluka sustava UI-ja. Ljudski nadzor odluka koje donosi sustav UI-ja smatra se ključnom pretpostavkom za ostvarenje sigurnog i pouzdanog UI-ja te, kao što je i ranije spomenuto, svaki bi ispitanik trebao imati pravo na ljudsku intervenciju kod donošenja odluka sustava UI-ja. Međutim, u organizacijama postoji manjak ljudskog nadzora odluka, što bi moglo imati vrlo negativne posljedice te bi takav trend trebalo promijeniti tako da u organizacijama postoji više ljudske intervencije kako bi odluke sustava UI-ja bile transparentne i pouzdane.

2. Vaš A.I. sustav obrađuje samo primjerene i relevantne podatke te je ograničen na ono što je nužno za ostvarivanje svrhe podataka (od 1 do 5).
Odgovori:

- 1 *U potpunosti se slažem,*
- 2 *Uglavnom se slažem,*
- 1 *Niti se slažem niti ne slažem,*
- 1 *Uglavnom se ne slažem*.

Od pet ispitanika tri su odgovorila kako se u potpunosti ili uglavnom slažu, dok su preostala dva odgovorila da niti se slažu niti se ne slažu ili se uglavnom ne slažu. Odgovori ukazuju na to da većina organizacija primjenjuje načelo smanjenja količine i svrhe. Načelo se također smatra jednim od ključnih načela zaštite podatka koja će se odnositi na sektor UI-ja. Načelo minimiziranja bitno je pravilno utvrditi kako se ne bi zaustavile inovacije europskih poduzeća, a da se istovremeno bude u skladu sa zahtjevima EU-a, kako bi bila pružena učinkovita zaštita podataka.

3. A.I. sustav koji koristite transparentno pruža informacije korisniku kako se obrađuju njegovi podaci pri strojnom učenju (od 1 do 5).
Odgovori:

- 1 *U potpunosti se slažem*,
- 2 *Uglavnom se slažem*,
- 1 *Uglavnom se ne slažem*,
- 1 *Uopće se ne slažem*.

Većina ispitanika, njih troje, odgovorilo je da se u potpunosti slažu ili se uglavnom slažu, dok se preostalih dvoje uglavnom ne slaže ili se uopće ne slaže. Ukazuju na to da neke organizacije uspijevaju s obvezom transparentnog pružanja informacija korisniku o obradi njegovih podataka, dok ipak preostaje dosta prostora za ostale organizacije na poboljšanju ispunjenja te obveze. Načelo transparentnosti također je od velike važnosti za ostvarivanje sigurnog i pouzdanog UI-ja. Zahtjevi načela transparentnosti odnose se davanje informacija korisniku o tome kako se obrađuju njegovi podaci. Može se pretpostaviti kako manjina organizacija ima poteškoće s transparentnim objašnjavanjem toga kako njihov sustav UI-ja obrađuje podatke korisnika.

4. Način obrade osobnih podataka koje koristi Vaš A.I. sustav dovodi do stvaranja pristranih obrazaca ponašanja donošenja odluka u srži A.I. sustava (od 1 do 5).
Odgovori:

- 4 *Niti se slažem niti se ne slažem*,
- 1 *Uglavnom se ne slažem*.

Većina ispitanika odgovorila je da niti se slaže niti se ne slaže s tvrdnjom, dok je jedan ispitanik odgovorio kako se uglavnom ne slaže. Odgovori ukazuju na to kako organizacije još nisu razjasnile stvara li njihov sustav UI-ja pristrane odluke. S obzirom na to da je pristranost izražena kao jedna od najvećih izazova UI-ja, dani odgovori pružaju razlog za zabrinutost. Organizacije bi trebale težiti izbjegavanju pristranosti, no to je vrlo zahtjevna obveza o kojoj će biti potrebno još istraživanja da bi ispitanici znali kako izbjeći pristranost odluka sustava UI-ja.

5. A.I. sustav koji koristite u organizaciji može osigurati pravo korisnika na brisanje i ispravak njihovih osobnih podataka (od 1 do 5).
Odgovori:

- 1 *Uglavnom se slažem*,
- 3 *Niti se slažem niti se ne slažem*,

- 1 *Uopće se ne slažem*.

Većina ispitanika niti se slaže niti se ne slaže s tvrdnjom, dok po jedan ispitanik smatra da se uglavnom slaže ili uopće ne slaže. Slično kao kod prethodnih odgovora, najviše ispitanika niti se slaže niti se ne slaže s tvrdnjom. To također ukazuje na problem nedovoljne jasnoće i kompleksnosti problema brisanja podataka u sustavu UI-ja. Načelo točnosti trebalo bi moći poštivati kako bi se izbjegla pristranost te kako bi implementacija UI-ja bila sigurna.

6. Vaš A.I. sustav primjenjuje odgovarajuće mjere poput anonimizacije i pseudonimizacije pri obradi osobnih podataka (od 1 do 5).

Odgovori:

- 2 *Uglavnom se slažem*,
- 2 *Niti se slažem niti se ne slažem*,
- 1 *Uopće se ne slažem*.

Manji dio ispitanika odgovorio je da se uglavnom slaže s tvrdnjom da njihova organizacija primjenjuje mjere poput anonimizacije i pseudonimizacije, dvoje ispitanika odgovorilo je kako niti se slaže niti se ne slaže s tvrdnjom, a samo jedan ispitanik odgovorio je kako se uopće ne slaže. Opet je vidljiva raznolikost između organizacija te manjak ujednačenosti u korištenju mjera anonimizacije i pseudonimizacije. Dok se nekolicina koristi anonimizacijom i pseduonimizacijom, ipak većina sudionika ne može tvrditi da primjenjuje navedene mjere. Mjera anonimizacije, unatoč nekim rizicima, pokazuje se vrlo učinkovitom za sigurnu obradu podataka te bi više organizacija trebalo razmisliti o njezinu uvođenju.

7. Vaša organizacija redovito provodi ispitivanje rizika Vašeg A.I. sustava (od 1 do 5).

Odgovori:

- 1 *Uglavnom se slažem*,
- 2 *Niti se slažem niti se ne slažem*,
- 2 *Uopće se ne slažem*.

Najviše odgovora podijeljeno je između *Niti se slažem niti ne slažem* i odgovora *Uopće se ne slažem*, dok se samo jedan ispitanik uglavnom slaže s tvrdnjom. Nedostatak redovitog ispitivanja rizika može ukazivati na ozbiljne propuste organizacije te manjak

svijesti o važnosti redovitog preispitivanja rizika. Iako bi ispitivanje rizika mogle smatrati bitnim dijelom sigurnosti informacijskog sustava, većina organizacija isti ne provodi, što je prilično zabrinjavajuća činjenica. Organizacije bi svakako trebale razmatrati učestalije provođenje ispitivanja rizika kako bi njihov sustav UI-ja bio izložen što manjim rizicima.

8. Vaša organizacija smatra da će usklađivanje s odredbama predloženog *Akta o umjetnoj inteligenciji* otežati poslovanje (od 1 do 5).
Odgovori:

- 2 *U potpunosti se slažem*,
- 1 *Niti se slažem niti se ne slažem*,
- 1 *Uglavnom se ne slažem*,
- 1 *Uopće se ne slažem*.

Odgovori ukazuju na podijeljenost mišljenja, što bi moglo biti posljedica nedostatka jasnoće odredbi koje donosi predloženi *Akt o umjetnoj inteligenciji*. Kako neke odredbe OUZP-a nisu u potpunosti jasne i primijenjene, moglo bi se predvidjeti da će novi *Akt o umjetnoj inteligenciji* donijeti još problema u vezi s usklađenošću obveza među organizacijama. Odgovori također potvrđuju generalni stav zabrinutosti organizacija zbog prekomjerne regulacije područja UI-ja. To se može smatrati donekle utemeljenim, iako je već navedeno da se predloženi *Akt o umjetnoj inteligenciji* može tumačiti tako da ne otežava trenutačno poslovanje organizacije niti koči njihovu inovativnost.
9. Vaš A.I. sustav prema prijedlogu *Akta o umjetnoj inteligenciji* slijedeći pristup utemeljen na riziku može se kvalificirati kao:
1) *Neprihvatljiv ili zabranjen rizik*
2) *Visokorizičan*
3) *Ograničenog rizika*
4) *Niskog ili minimalnog rizika*
Odgovori:

- 1 *Visokorizičan*,
- 3 *Niskog ili minimalnog rizika*,
- 1 *Ograničenog rizika*.

Većina ispitanika odgovorila je kako je njihov sustav UI-ja niskog ili minimalnog rizika, dok se po jedan ispitanik opredijelio za odgovor *Visokorizičan*, kao i *Ograničenog*

rizika. Iz odgovora je vidljivo kako je primjena sustava UI-ja organizacija vrlo široka te varira od niskih do visokorizičnih sustava.

Iz dobivenih odgovora ankete može se zaključiti kako organizacije doista imaju poteškoća s pojedinim zahtjevima koji se od njih očekuju prema OUZP-u, a u vezi su s razvojem sigurnog i pouzdanog UI-ja. Sukladno odgovorima prvog dijela, većina organizacija razumije i primjenjuje načela minimizacije i transparentnosti, dok su kod složenijih zahtjeva, poput izbjegavanja pristranosti i osiguravanja prava na brisanje, odgovori vrlo raznoliki, što potvrđuje problematičnost navedenih zahtjeva. Također, ni mjere ljudskog nadzora i redovitog ispitivanja rizika nisu dospjele do svake organizacije.

Nažalost, to ostavlja dosta prostora ranjivosti, potencijalnim greškama i sigurnosnim prijetnjama te bi organizacije trebale što prije uvesti navedene mjere kako bi minimalizirale potencijalnu štetu koju može napraviti njihov sustav UI-ja. Rezultati ankete također potvrđuju kako postoji dosta neizvjesnosti oko zahtjeva obrade podataka sustava UI-ja te ni same organizacije nisu u potpunosti sigurne u kojem će smjeru ići pravna regulacija te vjerojatno čekaju poteze drugih aktera kako bi vidjele hoće li se određene mjere pokazati učinkovitima, da bi zatim uskladile svoje poslovanje. Potreban je zajednički rad svih aktera kako bi implementacija UI-ja bila sigurna za primjenu i stekla povjerenje korisnika. Mnogo je još izazova o kojima ovisi uspješna implementacija UI-ja u svakodnevnom životu, s istovremenim osiguranjem zahtjeva zaštite podataka. U vezi s ograničenjima ispitivanja svakako bi trebalo spomenuti kako bi bilo potrebno provesti zasebno istraživanje za svaki od četiriju predloženih rizika ili posebno sektorski u kojemu se koristi sustav UI-ja, kako bi rezultati bili pravilniji i prilagodljivi specifičnoj skupini.

4. ZAKLJUČAK

Digitalne tehnologije, uključujući umjetnu inteligenciju, neophodne su za europsku digitalnu suverenost, sigurnost, inovacije i gospodarski razvoj te mogu znatno pridonijeti zaštiti i promicanju temeljnih prava, demokracije i vladavine prava.[73] Implementacija načela obrade podataka iz OUZP-a može se opisati prilično dobro prihvaćenom. Većina organizacija smatra kako razumije i primjenjuje načela obrade podataka, dok se manjina organizacija ipak ne može složiti da u potpunosti razumije i primjenjuje načela obrade podataka utvrđena u OUZP-u. Organizacije su većinom usklađene u potvrdim odgovorima o ispunjavanju obveze kao voditelja obrade prema OUZP-u. Drugi dio ankete potvrđuje postojanje izazova u specifičnim pitanjima obrade

[73] Predsjedništvo Vijeća Europske unije, Zaključci predsjedništva: *Povelja o temeljnim pravima u kontekstu umjetne inteligencije i digitalnih promjena*, str. 5, Bruxelles, 2020.

podataka koji u OUZP-u nisu pokriveni. Neujednačenost u odgovorima prikazuje drukčiji pristup svih strana, poneke organizacije ozbiljnije shvaćaju obveze iz OUZP-a, dok ostale nisu toliko fokusirane na pravni okvir. Mnoštvo negativnih odgovora ukazuje na to da postoje izazovi s tumačenjem OUZP-a kao okvira koji pokriva sve novonastale tehnologije poput UI-ja te postoji dosta izazova i nejasnoća u regulatornom pristupu. Kako bi se izbjegla pravna nesigurnost potrebno je učinke predloženog *Akta o umjetnoj inteligenciji* obrazložiti u komplementarnom smislu s OUZP-om. Odgovori također ukazuju na to da se pojedini izazovi više odnose na pojedine sektore. Tijela za zaštitu podataka moraju se aktivno uključiti u dijalog sa svim dionicima uključujući voditelje obrade, izvršitelje obrade i civilno društvo, kako bi se razvili odgovarajući odgovori, temeljeni na zajedničkim vrijednostima i učinkovitim tehnologijama. Dosljedna primjena načela zaštite podataka, u kombinaciji sa sposobnošću učinkovite upotrebe tehnologije UI-ja, može pridonijeti uspjehu aplikacija UI-ja stvaranjem povjerenja i sprječavanjem rizika. Relevantno zakonodavstvo kojim se ostvaruju temeljna prava može se dovesti u pitanje zbog složenosti i netransparentnosti određenih primjena UI-ja, a to zahtijeva specijalizirano stručno znanje i postupke za razumijevanje i kontrolu ishoda takvih primjena. Ljudski nadzor i transparentnost neophodni su elementi u osiguravanju toga da sustavi UI-ja budu u skladu s relevantnim zakonodavstvom.[74] Kako bi se promovirale vrijedne prakse u vezi s upotrebom UI-ja potrebno je osigurati odvijanje razvoja i implementacije UI-ja u sociotehničkom okviru uključujući tehnologije, ljudske vještine, organizacijske strukture i norme, gdje su pojedinačni interesi, a i društvena dobra, očuvani i poboljšani. Kako bi se pružila regulatorna podrška stvaranju takvog okvira, potrebno je usredotočiti se ne samo na postojeće propise već i na načela, s obzirom na to da sadašnja pravila ne pružaju odgovarajuća rješenja i upute korisnicima, organizacijama i tijelima za provedbu. Zaštita podataka na čelu je odnosa između UI-ja i zakona, jer mnoge aplikacije UI-ja uključuju masovnu obradu osobnih podataka uključujući ciljanje i personalizirani tretman pojedinaca na temelju takvih podataka. To objašnjava zašto je zaštita podataka područje zakona koje se najviše bavilo UI-jem, iako su uključena i druga područja prava, poput *Zakona o zaštiti potrošača, Zakona o zaštiti tržišnog natjecanja, Zakona o suzbijanju diskriminacije* i *Zakona o radu*. Tehnologije UI-ja ispitivat će se i ocjenjivati na temelju najnovijih znanstvenih i tehnoloških istraživanja dugi niz godina, a njihovi

[74]Ibid., str. 8.

društveni učinci razmatrat će se uzimajući u obzir niz pristupa, od sociologije do ekonomije i psihologije. Pravni aspekti analizirat će se pozivajući se na načela i pravila europskog prava, kao i na njihovu primjenu u nacionalnim kontekstima. S obzirom na sve navedeno, OUZP je ipak dobro definiran jer ostavlja prostora za nove tehnologije, pa tako i za UI. Principi i načela ostaju isti, razviti snažan i zajednički etički okvir za transparentnu obradu osobnih podataka i automatizirano donošenje odluka koje mogu usmjeravati korištenje podataka i stalnu provedbu prava Unije. Odredbe OUZP-a o preventivnim mjerama, a posebno one koje se tiču privatnosti po dizajnu i prema zadanim postavkama, ne ometaju razvoj sustava UI-ja ako su ispravno dizajnirani i implementirani, iako mogu zahtijevati dodatne troškove. Iako je moguće tvrditi da nema nekompatibilnosti između OUZP-a i UI-ja i velikih podataka, rezultati ankete pokazuju kako organizacije ipak imaju poteškoća s tumačenjem načela i odredbi na taj način. Odgovori potvrđuju potrebu zajedničkog pristupa svih aktera i dodatnog pojašnjenja smjernica gdje postoje nejasnoće, no dosljedno već utemeljenim smjernicama kako bi se očuvala prava korisnika. U različitim slučajevima, tumačenje nedefiniranih standarda OUZP-a zahtijeva balansiranje suprotstavljenih interesa između zahtjeva utvrđivanja toga jesu li određene aktivnosti obrade i usvojene mjere opravdane u odnosu na ravnotežu interesa korisnika da ne budu predmet obrade ili da budu zaštićeni dodatnim mjerama. Istina je da potpuna upotreba moći UI-ja i velikih podataka zahtijeva prikupljanje golemih količina podataka u vezi s pojedincem i njegovim društvenim odnosima te da također obradu takvih podataka u svrhe koje nisu bile u potpunosti određene u trenutku kada su prikupljeni. Međutim, postoje načini za razumijevanje i primjenu načela zaštite podataka koji su u skladu s korisnim korištenjem UI-ja i velikih podataka. Stoga će način na koji će OUZP utjecati na uspješne primjene UI-ja i velikih podataka u Europi također ovisiti o smjernicama koje će tijela za zaštitu podataka i općenito pravni sustav moći dati voditeljima obrade i subjektima podataka. To bi smanjilo troškove pravne nesigurnosti i usmjerilo tvrtke, posebno male koje uglavnom trebaju savjete, prema učinkovitim rješenjima koja su u skladu sa zaštitom podataka. Razvoj odgovarajućih politika i propisa za UI prioritet je za Europu, s obzirom na to da UI povećava mogućnosti i rizike na načine koji su od najveće društvene i pravne važnosti. Šira poenta o tome kako najbolje postupiti razvoju vrlo složene, a opet potpuno koherentne EU arhitekture “digitalnih zakona” ostaje za rješiti. U konačnici, tehnološka rješenja mogu pomoći ako se počnemo pitati ne samo što zakon može učiniti za razvoj društveno poželjne UI-je, već što i UI može učiniti za

poboljšanje relevantnosti, koherentnosti i pravodobnosti zakona.[75] Također, Europska unija treba ustrajati na putu prema pouzdanom UI-ju. Argument da je ugrožena konkurentnost poduzeća koja koriste sustave UI-ja u Europi, naspram poduzeća iz drugih blokova, treba pobliže razmatrati kako bi se uočilo da nije ispravan, stoga što ako drugi griješe u zaštiti temeljnih prava u razvoju UI-ja, to nije povod da i Europska unija ide istim putem. Trebalo bi se iskoristiti potencijal te ključne tehnologije u promicanju gospodarskog oporavka u svim sektorima u duhu europske solidarnosti, održavati i promicati temeljna prava, demokraciju i vladavinu prava te održavati visoke pravne i etičke standarde.[76] Konkretno, upotrebom umjetne inteligencije moraju se poštovati temeljna prava i slobode, ona mora biti u skladu sa zakonima o zaštiti podataka i privatnosti i njome se moraju zajamčiti djelotvorni pravni lijekovi.

LITERATURA

Knjige i članci:

Andraško, J., Mesarčík, M., Hamuľák, O.: *The regulatory intersections between artifcial intelligence, data protection and cyber security: challenges and opportunities for the EU legal framework*, Bratislava, Olomuc, 2020.

Dragičević, D., Gumzej, N., Jurić, M., Katulić, T., Lisičar, H.: *Pravna informatika i pravo informacijskih tehnologija*, NN, Zagreb, 2015.

European VCs and tech firms sign open letter warning against over-regulation of AI in draft EU laws https://techcrunch.com/2023/06/30/european-vcs-tech-firms-sign-open-letter-warning-against-over-regulation-of-ai-in-draft-eu-laws/, prema stanju na dan 14. 9. 2023.

[75] Novelli, C., Casolari, F., Hacker, P., Spedicato, G., Floridi, L.: *Generative AI in EU Law: Liability, Privacy, Intellectual Property, and Cybersecurity*, str. 22, Bologna, 2024.
[76]Ibid., str. 3.

Fathers of the Deep Learning Revolution Receive ACM A.M. Turing Award https://www.acm.org/media-center/2019/march/turing-award-2018, prema stanju na dan 15. 9. 2023.

Kahneman, D.: *Thinking: fast and slow*, Farrar, Straus and Giroux, 2011.

Katulic, T., Protrka, N.: *Information Security in Principles and Provisions of the EU Data Protection Law*. // 42nd International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO) Opatija: IEEE, 2019. pp. 1420–1426 (predavanje, međunarodna recenzija, cjeloviti rad [*in extenso]*, znanstveni)

Katulić, A., Katulić, T., Hebrang Grgić, I.: *Application of the principle of transparency in processing of European national libraries patrons' personal data*// Digital Library Perspectives, 2022.

Katulić, T.: Towards the Trustworthy AI: *Insights from the Regulations on Data Protection and Information Securit*, Medijska istraživanja, Zagreb, 2020.

King, J., Meinhardt, C.: *Rethinking Privacy in the AI Era Policy Provocations for a Data-Centric World ,* Stanford HAI, Stanford, 2024.

Kourinian, A., Brown, M.: *Conducting an AI risk assessment,* Bloomberg Law, 2024.

Kurbalija, J., Murphy, M.: *An introduction to internet governance*, DiploFoundation, Geneva, 2016.

Mazurek, G., Małagocka, K.: *Are we down to zero-one code? Perception of privacy and data protection in the context of the development of artificial intelligence*, Journal of Management Analytics, 2019.

Mcculloch, W., Pitts, W.: *A Logical Calculus of Ideas Immanent in Nervous Activity.* Bulletin of Mathematical Biophysics, 1943.

Mitrou, L.: *Data Protection, Artificial Intelligence and Cognitive Services: Is the General Data Protection Regulation (GDPR) 'Artificial Intelligence-Proof'?*, 2018.

Novelli, C., Casolari, F., Hacker, P., Spedicato, G., Floridi, L.: *Generative AI in EU Law: Liability, Privacy, Intellectual Property, and Cybersecurity,* Bologna, 2024.

Pagallo, U., Casanovas, P., Madelin, R.: *The middle-out approach: assessing models of legal governance in data protection, artificial intelligence, and the Web of Data*, The Theory and Practice of Legislation, 7:1, Routledge, 2019.

Rosenblatt, F.: *The perceptron - A perceiving and recognizing automaton*. Technical Report 85-460-1, Cornell Aeronautical Laboratory, Ithaca, New York, siječanj 1957.

Turing, A. M.: *Computing machinery and intelligence*, Mind, 1950.

Umjetna inteligencija u Hrvatskoj postaje već ozbiljan globalni biznis 16. kolovoza 2023. https://lidermedia.hr/tehno/umjetna-inteligencija-u-hrvatskoj-postaje-vec-ozbiljan-globalni-biznis-152504, prema stanju na dan 20. 9. 2023.

Vojković, G., Milenković, M., Katulić, T.: *IoT and Smart Home Data Breach Risks from the Perspective of Croatian Data Protection and Information Security Law*. // Proceedings of the ENTRENOVA -ENTerprise REsearch InNOVAtion Conference / Milković, Marin; Seljan, Sanja; Pejić Bach, Mirjana; Peković, Sanja; Perovic, Djurdjica (ur.). Rovinj: Udruga za promicanje inovacija i istraživanja u ekonomiji "IRENET", Zagreb, 2019. pp. 298-308. (https://www.bib.irb.hr/1020078) (predavanje, međunarodna recenzija, cjeloviti rad [*in extenso*], znanstveni).

We Forgot To Give Neural Networks The Ability To Forget https://www.forbes.com/sites/ashoka/2023/01/25/we-forgot-to-give-neural-networks-the-ability-to-forget/?sh=44424d816853, prema stanju na dan 27. 9. 2023.

Pravni izvori:

Direktiva (EU) 2016/680 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka od strane nadležnih tijela u svrhe sprečavanja, istrage, otkrivanja ili progona kaznenih djela ili izvršavanja kaznenih sankcija i o slobodnom kretanju takvih podataka o stavljanju izvan snage Okvirne odluke Vijeća 2008/977/PUP

EPDB, Europski odbor za zaštitu podataka: *Smjernice 4/2019 o članku 25. Tehnička i integrirana zaštita podataka*,, verzija 2.0, doneseno 20. listopada 2020.

Europska komisija, Directorate-General for Communications Networks, Content and Technology: *Etičke smjernice za pouzdanu umjetnu inteligenciju*, Publications Office, 2019.

Europska komisija: *Prijedlog Uredbe Europskog parlamenta i Vijeća o Utvrđivanju i usklađivanju pravila o umjetnoj inteligenciji (Akt o umjetnoj inteligenciji) i izmjeni određenih zakonodavnih akata Unije*, Bruxelles, 21. 4. 2021.

Povelja Europske unije o Temeljnim pravima 2010/C 83/02

Radna skupina iz članka 29: *Smjernice o transparentnosti na temelju Uredbe 2016/679*, donesene 29. studenoga 2017. kako su zadnje revidirane i donesene 11. travnja 2018.

Radna skupina za zaštitu podataka iz članka 29: *Smjernice o automatiziranom pojedinačnom donošenju odluka i izradi profila za potrebe Uredbe 2016/679*, donesene 3. listopada 2017. kako su zadnje revidirane i donesene 6. veljače 2018.

Uredba (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (Opća uredba o zaštiti podataka)

Ugovor o funkcioniranju Europske unije 2016 C 202/47

Statistička izvješća i baze podataka:

Agencija Europske unije za temeljna prava: *Getting the future right – Artificial intelligence and fundamental rights*, Beč, 2020.

High level expert group on artificial intelligence (HLEG AI): *A definition of Artificial Intelligence: main capabilities and scientific disciplines,* Bruxelles, 2018.

CEDPO AI Working Group; *Generative AI: The Data Protection Implications*, 2023.

EDPB-EDPS: *Zajedničko mišljenje 5/2021 o Prijedlogu uredbe Europskog parlamenta i Vijeća o utvrđivanju usklađenih pravila o umjetnoj inteligenciji (Akt o umjetnoj inteligenciji)*, Bruxelles, 2021.

Europska komisija: *Bijela knjiga o umjetnoj inteligenciji – Europski pristup izvrsnosti i izgradnji povjerenja*, Bruxelles, 2020.

Europski parlament: *Izvješće o umjetnoj inteligenciji u digitalnom dobu*, Bruxelles, 2020.

Predsjedništvo Vijeća Europske unije, Zaključci predsjedništva: *Povelja o temeljnim pravima u kontekstu umjetne inteligencije i digitalnih promjena*, Bruxelles, 2020.

Federal office of Information security: *Generative AI Models Opportunities and Risks for Industry and Authorities,* 2024.

Think tank: European Parliament: *The impact of the General Data Protection Regulation (GDPR) on Artificial Intelligenc*e, 2020.

Sudska praksa:

C-131/12 Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD) i Mario Costeja González