# *NOVE OPASNOSTI OD UMJETNE INTELIGENCIJE U ZAŠTITI OSOBNIH PODATAKA*

*NEW THREATS FROM ARTIFICIAL INTELLIGENCE IN THE PROTECTION OF PERSONAL DATA*

**Doc. dr. sc. Marko Horvat, v. pred.**


## SAŽETAK

*Pojam umjetne inteligencije danas je vrlo često korišten bez cjelovite spoznaje na što se zapravo odnosi. U ljudskoj je prirodi da nas plaši nepoznato. Zbog napretka i široke primjene računalnih sustava umjetne inteligencije razumljivo je da postoji opravdana zabrinutost zbog potencijalnih opasnosti koje proizlaze iz povreda prava na pristup osobnim podacima, tj. u čuvanju privatnosti. Stoga je potrebno jasno odrediti nove potencijalne opasnosti koje proizlaze iz neetičnog korištenja umjetne inteligencije u prikupljanju i obradi osobnih podataka. Također, nužno je predložiti mjere kako bi se takve opasnosti svele na najmanju moguću mjeru. Od posebne pažnje su inteligentni sustavi koje se koriste za mjerenje emocionalnih stanja, ponašanja, stavova i mišljenja, odnosno prikupljanje podataka u svrhu profiliranja osoba. U radu su navedene mogućnosti današnjih tehnologija u ovim područjima, karakteristični primjeri primjene, te koraci koji je potrebno poduzeti kako bi se smanjila mogućnost zlouporabe osobnih podataka.*

## ABSTRACT

*Artificial intelligence as a term is nowadays commonly used without the complete understanding of what it actually refers to. Due to the advancement and widespread use of artificial intelligence computer systems, it is understandable that concerns exist about the potential dangers arising from violations of the right of access to personal data, i.e. in the protection of privacy. New potential hazards arising from the unethical use of artificial intelligence in collecting and processing of personal data must be clearly identified. Further, it is necessary to propose measures to minimize these hazards. Of particular note are intelligent systems used to estimate emotional states, behaviors, attitudes and opinions, that is, aggregation of data for the purpose of customer profiling. The paper outlines the capabilities of current technologies in these fields, gives typical application examples, and suggests steps for reduction of the possibility for personal data misuse.*


## 1. UVOD

Makar je pojam umjetna inteligencija (engl. *artificial intelligence*, AI) danas iznimno korišten u javnoj komunikaciji često se zaboravlja da ne postoji opće prihvaćena definicija inteligencije kao niti umjetne inteligencije. Očiti problem je u izrazitoj interdisciplinarnoj širini samog područja kao i o brojnim mogućnostima primjene umjetne inteligencije. U ovom trenutku najčešće asocijacije povezane s umjetnom inteligencijom su samoupravljiva vozila, autonomne letjelice, humanoidni roboti, ili apstraktni računalni sustavi koji prikupljaju goleme količine nestrukturiranih podataka, nadziru, pa čak upravljaju osobnim životima. Zbog visoke tehnološke složenosti takvih sustava često je u društvu njihova namjena nejasna ili se čini inheretno zlonamjernom (npr. praćenje kretanja ili analiza ponašanja).

U praksi umjetna inteligencija je grana računalnih znanosti koja se bavi automatizacijom inteligentnog ponašanja, a želi objasniti i emulirati inteligentno ponašanje u smislu računalnih procesa. Možemo dodatno reći da umjetna inteligencija predstavlja niz tehnologija koje se koriste za obavljanje funkcija koje zahtijevaju inteligenciju ljudi, odnosno proučava kako učiniti da računala rade stvari u kojima su, trenutno, ljudi bolji.

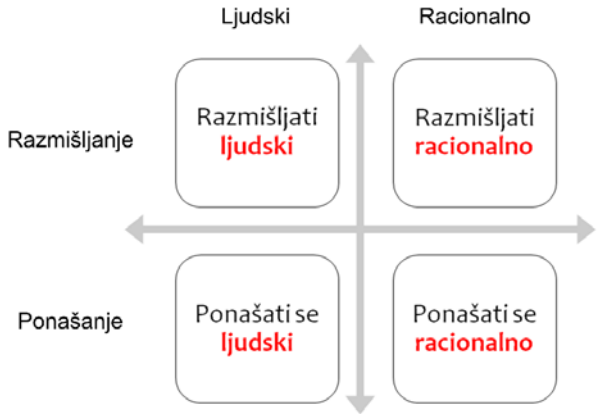
Analizirajući relevantne znanstvene izvore možemo utvrditi da je do sada objavljeno nekoliko desetaka različitih definicija pojma inteligencije. Neke od njih su većim ili manjim dijelom međusobno kontradiktorne. Pa tako najčešće definicije inteligencije koje možemo pronaći u literaturi su [1]:

(1) *Svojstvo uspješnog snalaženja jedinke u novim situacijama* (R. Pinter)
(2) *Opća sposobnost razmišljanja prilikom rješavanja problema* (Lewis Terman)

Najviše zastupljene definicije umjetna inteligencije su:

(3) *Znanstvena disciplina koja se bavi izgradnjom računalnih sustava čije se ponašanje može tumačiti kao inteligentno* (John McCarthy, 1956.)
(4) *Znanost o tome kako postići da strojevi izvode zadatke koji bi, kada bi ih radio čovjek, trebali inteligenciju* (Marvin Minsky, 1961.)

S obzirom na kompleksnost problema definirana je sistematizacija, ili podjela, definicija umjetne inteligencije kao što je prikazano na sljedećoj slici. Na jednak način podijeljeni su i sustavi, odnosno postupci i algoritmi, umjetne inteligencije s obzirom na njihovu primjenu.




*Slika 1. Podjela definicija umjetne inteligencije s obzirom na namjenu.*

Kao što se može vidjeti na slici definicije umjetne inteligencije podijeljene su u četiri načelne kategorije ili grupe s obzirom na njihovu namjenu ili svrhu:

1. Umjetna inteligencija kojoj je namjena razvoj sustava koji razmišljaju ljudski
2. Umjetna inteligencija kojoj je namjena razvoj sustava koji razmišljaju racionalno
3. Umjetna inteligencija kojoj je namjena razvoj sustava koji se ponašaju ljudski
4. Umjetna inteligencija kojoj je namjena razvoj sustava koji se ponašaju racionalno

Danas se razvijaju sustavi koji slijede sve četiri kategorije definicija umjetne inteligencije, ali najveći prioritet iz posve praktičnih razloga usmjeren je prema razvoju i izradi inteligentnih strojeva, odnosno nastojanju da se razvije i za dobrobit društva iskoristiti inteligentno ponašanje strojeva.

## 2. AKTUALNI VODEĆI STAVOVI O OPASNOSTIMA KORIŠTENJA UMJETNE INTELIGENCIJE

U posljednje vrijeme moguće je primijetiti povećanu zabrinutost mogućnih opasnosti zbog korištenja umjetne inteligencije. Ovakve stavove iznose zakonodavci, znanstvene institucije i vodeći tehnološki inovatori. Primjerice, jedan od vodećih poduzetnika i inovatora današnjice Elon Musk, nedavno je ustvrdio da bi razvoj umjetne inteligencije trebao bi biti bolje reguliran, čak i u njegovoj vlastitoj tvrtki Tesla koja proizvodi automobile sa automatskim upravljanjem [2].

S tim u svezi neki svjetski mediji izvijestili su sljedeće [3]:

*Tesla CEO Elon Musk wants to see all artificial intelligence better regulated, even at his own company.*

*Musk has a history of expressing serious concerns about the negative potential of AI. He tweeted in 2014 that it could be "more dangerous than nukes," and told an audience at an MIT Aeronautics and Astronautics symposium that year that AI was "our biggest existential threat," and humanity needs to be extremely careful.*

*Musk has been floating the idea for some kind of government oversight of AI for a while… "we ought to have a government committee that starts off with insight, gaining insight. Spends a year or two gaining insight about AI or other technologies that are maybe dangerous, but especially AI." The committee would then come up with regulations to ensure the safest uses of AI, he said. Musk added at the time that he did not think such a committee would actually happen.*

Ideja o nužnosti formiranja državnog, pa i međudržavnog, tijela koje će nadzirati primjenu tehnologija umjetne inteligencije nije nova. Štoviše, prisutni su i pozivi na oprez i zabranu korištenja tehnologija za prepoznavanje emocija. U tom smislu Institut za istraživanje umjetne inteligencije „AI Now" predlaže potpunu zabranu tehnologija za prepoznavanje emocija dok se u ovo područje ne uvede čvrsta zakonska regulativa [4]. Razlozi za to su, kako navode:

1) Nedovoljna znanstvena utemeljenost estimacije emocija pomoću računala
2) Primjena takve tehnologije može povećati nejednakosti, posebice temeljene na rasi i spolu

Prijedlozi Instituta utemeljeni su na nedavno objavljenim rezultatima istraživanja [5]. Tijekom spomenutog istraživanja sustavno je pregledana objavljena znanstvena literatura iz područja estimacije emocija. Istraživanje je bilo vrlo opsežno i trajalo je dvije godine, a naručila ga je međunarodna Udruga za psihološke znanosti. U istraživanju temeljito je analizirano više od tisuću znanstvenih radova o detekciji i estimaciji emocija [5]. Posebice je posvećena pažnja na postupke prepoznavanja emocija iz facijalnih ekspresija koje su povezane s određenim emocijama. Nedvosmislen zaključak ovog istraživanja jest da nije utemeljena pretpostavka da izrazi lica pouzdano odgovaraju emocijama ispitanika [6]. Postupci procjene emocionalnih stanja pomoću računala u praksi općenito nisu pouzdani i ne mogu pružiti dovoljno točne i precizne rezultate unutar heterogenih grupa ispitanika. Najučinkovitiji su kod personaliziranih pobuda, ali to nije uvijek primjenjivo.

Tehnologije estimacije emocija pomoću računala danas se već redovito koriste za procjenu podnositelja zahtjeva za posao i osoba osumnjičenih za zločine, u sklopu policijskih istraga, a ispituju se i za daljnje primjene, primjerice u računalnim igrama poput VR kaciga za procjenu emocija sudionika. Najčešće se koriste sustavi za prepoznavanje facijalnih ekspresija jer te tehnologije nemaju velike tehničke zahtjeve, najviše su dostupne, a istodobno brzo daju rezultate, pa čak i u stvarnom vremenu. Upravo ove tehnologije su najviše kritizirane u gore spomenutom istraživanju.

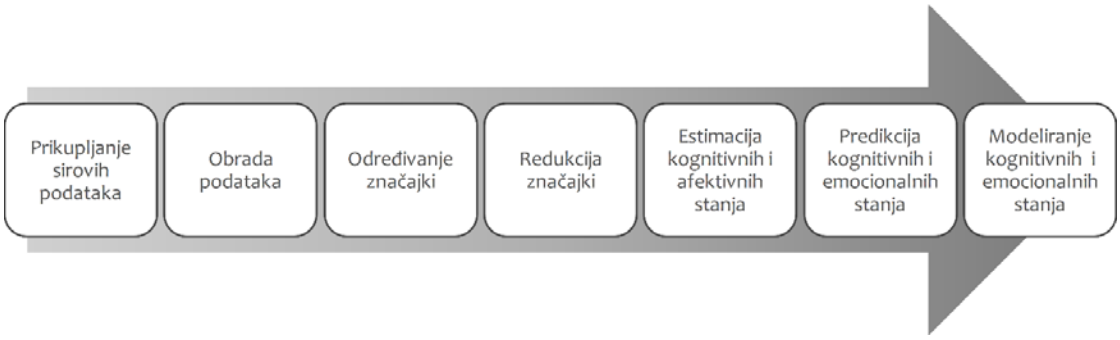
Novi elementi digitalne strategije Europske komisije objavljeni su 18. veljače 2020 [7]. U toj strategiji planirana je stroga regulacija umjetne inteligencije koju se smatra tehnologijom visokog rizika. Europa treba postati lider u pouzdanoj umjetnoj inteligenciji (engl. *trustworthy AI*), razlikujući se od slobodnijeg pristupa tim tehnologijama od Sjedinjenih Država i Kine. Komisija će izraditi nove zakone - uključujući zabranu AI sustava „crne kutije“ koje ljudi ne mogu protumačiti - za upravljanje visokorizičnim uporabama tehnologije: zdravstvenom zaštitom, transportom i kaznenim pravom. Nepristrani skupovi podataka potrebni su za izradu sustava visokog rizika kako bi oni mogli pravilno funkcionirati i osigurati poštivanja temeljnih prava, posebno nediskriminacije. Komisija također planira ponuditi novi certifikat „pouzdan AI“. Ako se za tako certificirane sustave kasnije ustanovi da su prekršili pravila oni se mogu suočiti s novčanim kaznama. Naposljetku, komisija navodi da će "pokrenuti široku europsku raspravu" o sustavima prepoznavanja lica, obliku AI koji može biometrijski identificirati ljude u maskama bez njihovog pristanka.

Također, važno je napomenuti da će prema nekim ekonomskim predviđanjima prepoznavanje emocija do 2023. god. postati komercijalna djelatnost od 23 milijarde dolara.

## 3. PREPOZNAVANJA EMOCIONALNIH STANJA KORIŠTENJEM POSTUPAKA UMJETNE INTELIGENCIJE

Strogo gledajući, cilj estimatora emocionalnih stanja je estimirati, odnosno procijeniti, na temelju fizioloških značajki (engl. *features*), ispitanikovo emocionalno stanje tijekom seanse, gdje je seansa definirana kao niz multimedijskih stimulacija različitog emocionalnog sadržaja i semantike tijekom kojih se prikupljaju fiziološki signali [8]. Tijekom seanse ispitanik se pobuđuje različitim stimulacijama te se kroz različite kognitivne i emocionalne procese unutar ispitanikovog mozga i tijela mijenja njegovo emocionalno stanje. Promjene u ispitanikovom emocionalnom stanju mogu se vidjeti u promjenama njegove fiziologije, izraza lica i u glasu [8]. Različitim akvizicijskim uređajima estimator emocionalnih stanja prikuplja različite fiziološke signale, poput EKG-a, EEG-a, vodljivosti kože, respiracije, temperature kože, EMG-a, itd., te korištenjem metoda dubinske analize računalno procjenjuje ispitanikovo emocionalno stanje [8, 9].

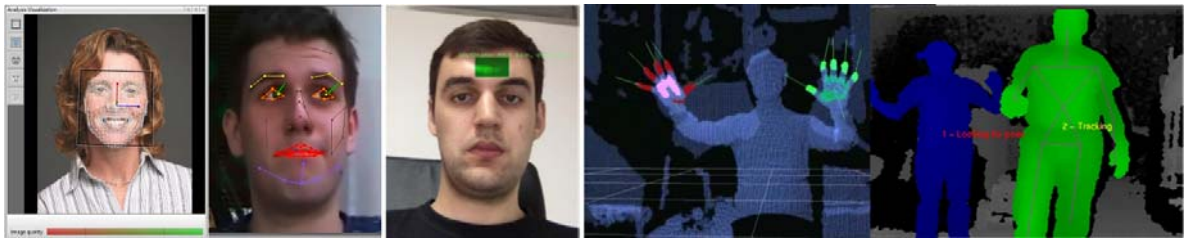
Kao što je prikazano na slici 2 postupak procjene emocija započinje s prikupljanjem sirovih podataka iz multimodalnih izvora korištenjem različitih senzora koje je potrebno obraditi. Svrha koraka obrade podataka je napraviti potrebne transformacije kako bi kasniji koraci bili uspješni. Prvenstveno to je otkloniti šum i nadomjestiti podatke koji nedostaju. Nakon toga slijedi određivanje značajki koje smanjuju kompleksnost velike količine podataka i svodi ih na nekoliko desetaka ili stotina numeričkih vrijednosti. Jednostavno rečeno, značajke opisuju model. Nakon koraka određivanja značajki slijedi odabir značajki. Ovi postupci koriste se kako bi se smanjila dimenzionalnost ulaznog skupa podataka i tako poboljšala učinkovitost postupaka strojnog učenja za izgradnju modela. Nakon odabira značajki koje nose maksimalnu informacijsku vrijednost pristupa se estimaciji, potom predikciji, a iz svega na kraju se dobiva jedinstveni model kognitivnih i afektivnih stanja [9].




*Slika 2. Tijek općenitog postupak estimacije emocija [8, 9].*

Izvori podataka za procjenu emocionalnih stanja mogu biti brojni (neki primjeri u Slika 3).

- izrazi lica, infracrvena (termalna) slika lica,
- smjer i dinamika pogleda,
- temperatura kože, elektrodermalne aktivnosti kože (vodljivost, galvanski odziv - GSR, …),
- srčani ritam i varijabilnost srčanog ritma, EKG,
- električna aktivnost mozga (EEG, evocirani potencijali, …),
- položaj i pokreti tijela,
- govorni signal (akustičke i lingvističke značajke) [10],
- pokreti miša i uporaba tipkovnice.



*Slika 3. Primjer nekih senzora koji se koriste za estimaciju emocionalnih stanja i ponašanja.*

Zbog smanjene nametljivosti i jednostavnijeg korištenja preporuča se uporaba beskontaktnih senzora umjesto kontaktnih. Procjena srčanog ritma može se i vršiti vidnim senzorima, tj. kamerom [11], bez potrebne korištenja kontaktnih senzora i na udaljenosti od nekoliko metara, a uz određena ograničenja moguće je i pametnim satovima i telefonima [12]. Tradicionalni termin za sve oblike ovakvih mjerenja je biometrija (engl. *biometrics*), ali može se koristiti i termin psihofiziologija (engl. *psychophysiology*) koji obuhvaća psihološke fenomene kao temelje fizioloških aktivnosti. Upravo ove manifestacije, odnosno aktivnosti, bilježe senzori.

## 4. ZAŠTITA OSOBNIH PODATAKA U KONTEKSTU PRIMJENE UMJETNE INTELIGENCIJE

Zaštita osobnih podataka, u užem smislu, je čvrsto određena hrvatskim i međunarodnim pravnim okvirom i pripadnim pravnim aktima.

Osobni podaci su svi podaci koji se odnose na pojedinca čiji je identitet utvrđen ili se može utvrditi („ispitanik“) [13]. Pravo na zaštitu osobnih podataka smatra se temeljnim ljudskim pravom.

*„Svatko ima pravo na zaštitu osobnih podataka koji se na njega ili nju odnose“*

Članak 8. Povelje Europske unije o temeljnim pravima (2016/C 202/02).

I također:

*„Svatko ima pravo na zaštitu svojih osobnih podataka“*

Članak 16. Ugovora o funkcioniranju Europske unije (2016/C 202/01).

Također, zaštita osobnih podataka utvrđena je s više pravnih akata [14]:

- Člankom 37. Ustava Republike Hrvatske (NN 85/10 – pročišćeni tekst) kojim se svakom jamči sigurnost i tajnost osobnih podataka, koji se bez privole ispitanika mogu prikupljati, obrađivati i koristiti samo uz uvjete određene zakonom, dok se zabranjuje uporaba osobnih podataka suprotna utvrđenoj svrsi njihova prikupljanja.
- Uredbom (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).
- Zakonom o provedbi Opće uredbe o zaštiti podataka (NN 42/18)
- Zakonom o zaštiti fizičkih osoba u vezi s obradom i razmjenom osobnih podataka u svrhe sprječavanja, istraživanja, otkrivanja ili progona kaznenih djela ili izvršavanja kaznenih sankcija (NN 68/18)

Pravo na pristup osobnim podacima je dio prava svakog ispitanika. Sukladno propisima kojima je utvrđena zaštita osobnih podataka, ispitanik ima pravo dobiti pisanu obavijesti od voditelja obrade obrađuju li se osobni podaci koji se na njega odnose, a ako se obrađuju pristup slijedećim informacijama [14]:

- svrha i pravni temelj obrade osobnih podataka;
- kategorijama osobnih podataka, ako ih ima;
- primateljima osobnih podataka;
- razdoblju pohrane;
- pravu na ispravak i brisanje;
- ograničenju prava pristupa i informacija koje se stavljaju na raspolaganje ili daju ispitaniku sukladno Zakonu o zaštiti fizičkih osoba u vezi s obradom i razmjenom osobnih podataka u svrhe sprječavanja, istraživanja, otkrivanja ili progona kaznenih djela ili izvršavanja kaznenih sankcija;
- izvoru podataka;
- pravu na podnošenje prigovora, odnosno pritužbe nacionalnom nadzornom tijelu.

Svatko tko smatra da mu je povrijeđeno neko pravo zajamčeno Općom uredbom o zaštiti podataka i Zakonom o provedbi Opće uredbe o zaštiti podataka može podnijeti zahtjev za utvrđivanje povrede prava Agenciji za zaštitu osobnih podataka.

Vrlo važno je pogledati definiciju postupka obrade osobnih podataka. Osobito je potrebno obratiti pozornost na završne odredbe koje određuju što predstavljaju „obrade osobnih podataka visokih rizika“ [15]:

„Obrada osobnih podataka obuhvaća radnje poput prikupljanja, bilježenja, čuvanja, uvida, otkrivanja, prenošenja ili uništavanja podataka. Tako primjerice možemo navesti da će Opća uredba o zaštiti podataka obuhvatiti obradu podataka zaposlenika, potrošača i klijenata, građana od strane državne administracije, pacijenata, učenika, studenata, članova udruga, korisnika društvenih mreža i svaku drugu obradu osobnih podataka koja nije u okviru gore navedenih iznimki. Također, novim

ili jačim pravilima bit će obuhvaćene one djelatnosti koje se bave obradom osobnih podataka visokog rizika za koje će biti potrebno provesti procjenu učinka. To su obrade koje se odnose na sustavnu i opsežnu procjenu osobnih aspekata pojedinaca automatiziranim putem, opsežnu obradu posebnih kategorija podataka ili podataka o kaznenim osudama ili kažnjivim djelima te sustavno praćenje javno dostupnog područja u velikoj mjeri“.

Zaključujemo da postupci estimacije emocionalnih stanja, ponašanja i kognicija zapravo predstavljaju obrade osobnih podataka visokih rizika. Pogotovo primjena estimacije emocija iz facijalnih ekspresija je jedna takva tehnologija umjetne inteligencija koja koristi osobne podatke, pokazala je nezadovoljavajuće rezultate, a vrlo često se primjenjuje u praksi.

Pri tome potrebno je voditi računa o pojedinim pravim građana, odnosno ispitanika. Ta lista je opsežna [15]:

- „transparentnost (12 - 14): pružanje informacija prilikom prikupljanja osobnih podatak kada voditelj obrade mora među ostalim informacijama obavijestiti ispitanika i o svojem identitetu i kontakt podacima, svrhama obrade i pravnoj osnovi za obradu podataka, primateljima, iznošenju u treće zemlje, razdoblju pohrane, mogućnosti povlačenja privole, itd.;
- pristup podacima (15): dobiti od voditelja obrade potvrdu obrađuju li se osobni podaci koji se odnose na njega te ako se takvi osobni podaci obrađuju, pristup osobnim podacima i informacije, među ostalim, o obrađenim osobnim podacima, o svrsi obrade, roku pohrane, iznošenju u treće zemlje itd.;
- pravo na ispravak (16): ispitanik ima pravo zahtijevati ispravak netočnih osobnih podataka koji se na njega odnose, a uzimajući u obzir svrhe obrade, ispitanik ima pravo dopuniti nepotpune osobne podatke, među ostalim i davanjem dodatne izjave;
- brisanje („pravo na zaborav“) (17): ispitanik ima pravo od voditelja obrade ishoditi brisanje osobnih podataka koji se na njega odnose bez nepotrebnog odgađanja te voditelj obrade ima obvezu obrisati osobne podatke bez nepotrebnog odgađanja ako, među ostalim, osobni podaci više nisu nužni u odnosu na svrhu obrade, ispitanik je povukao privolu za obradu, osobni podaci su nezakonito obrađeni itd., ovo pravo ima ograničenja pa tako na primjer političar ne može zatražiti brisanje informacija o sebi koje su dane u okviru svojega političkog djelovanja;
- pravo na ograničenje obrade (18): u pojedinim situacijama (na primjer kada je točnost podataka osporavana ili kada pravo na brisanju ispitanik želi da voditelj obrade zadrži njegove podatke) ispitanik ima pravo zahtijevati da se obrada ograniči uz iznimku pohrane i nekih drugih vrsta obrade;
- pravo na prenosivost (20): ispitanik ima pravo zaprimiti svoje osobne podatke, a koje je prethodno pružio voditelju obrade, u strukturiranom obliku te u uobičajeno upotrebljavanom i strojno čitljivom formatu te ima pravo prenijeti te podatke drugom voditelju obrade bez ometanja od strane voditelja obrade kojem su osobni podaci pruženi, ako se obrada provodi automatiziranim putem i temelji na privoli ili ugovoru;
- pravo na prigovor (21): ispitanik ima pravo uložiti prigovor na obradu osobnih podataka ako se ista temelji na zadaće od javnog interesa, na izvršavanje službenih ovlasti voditelja obrade ili na legitimne interesa voditelja obrade (uključujući i profiliranje), tada voditelj obrade ne smije više obrađivati osobne podatke ispitanika osim ako dokaže da njegovi legitimni razlozi za obradu nadilaze interese ispitanika te radi zaštite pravnih zahtjeva, također ako se ispitanik protivi obradi za potrebe izravnog marketinga, osobni podaci više se ne smiju obrađivati;
- pravo usprotiviti se donošenju automatiziranih pojedinačnih odluka (profiliranje) (22): ispitanik ima pravo da se na njega ne odnosi odluka koja se temelji isključivo na automatiziranoj obradi, uključujući izradu profila, koja proizvodi pravne učinke koji se na njega odnose ili na sličan način značajno na njega utječu, osim ako je takva odluka potrebna za sklapanje ili izvršenje ugovora između ispitanika i voditelja obrade podataka, ako je dopuštena pravom EU-a ili nacionalnim pravom koji se propisuju odgovarajuće mjere zaštite prava i sloboda te legitimnih interesa ispitanika ili temeljena na izričitoj privoli ispitanika“.

## 5. OGRANIČENJE PRISTUPA JAVNIM USLUGAMA I PRIJEDLOG RJEŠENJA

Što je javna usluga (engl. *public service*)? U svojoj definiciji svaka javna usluga obuhvaća tijela koja pružaju usluge i usluge od općeg interesa koja ta tijela pružaju. Vlasti mogu nametnuti obavezu javne usluge tijelu koje pruža tu uslugu (npr. zrakoplovne kompanije, željeznički prijevoznici, proizvođači energenata, itd.). U praksi pojam javnih usluga i koncept javnog sektora (uključujući i državnu administraciju) često se pogrešno zamjenjuju kao istoznačnice, ali ipak ova dva pojma razlikuju se po funkciji, statusu, vlasništvu i korisnicima.

U tradicionalnom razmišljanju osobni podaci nalaze se na osobnim računalima i pametnim telefonima korisnika ili sadržani njihovim mrežnim identitetima. Ali to nisu svi osobni podaci. Osobni podaci su i svi oni drugi podaci koji proizlaze iz ponašanja, stavova, razmišljanja, kognicije i emocionalnih reakcija korisnika.

Tijekom korištenja javnih usluga ove kategorije osobnih podataka svakodnevno ustupamo svojevoljno, a i besplatno. Ovaj problem se često zanemaruje ili posve negira.

Nameću se četiri važna pitanja: 1) Da li se i ti osobni podaci prikupljaju? 2) Za što se koriste? 3) Da li smo o tome, kao i kao korisnici i kao davatelji takvih osobnih podataka, obaviješteni? 4) Da li imamo mogućnost korištenja javnih servisa bez implicitnog ili eksplicitnog ustupanja naših osobnih podataka?

Stoga predlažem da se na vidljivim mjestima u prostorima gdje se vrši estimacija emocionalnih stanja nalaze standardizirane oznake koje na to upozoravaju.

Svrha nije samo informiranje već da korisnik usluge ocijeni da li mu je prihvatljiva razina obrade osobnih podataka i obuhvaćenih radnji.

Dakle, predlažem da se kao do sada ne me označavaju načini prikupljanja podatka (npr. video nadzor prostorije, snimanje razgovora, …), već je potrebno označavati primjenu prikupljenih podataka (orofiliranje, moderalianje, analiza, *customer churn analysis*, …).

Pri tome je vrlo važno omogućiti korisnicima alternativni pristup uslugama, posebice javnim servisima, makar odbiju predati svoje osobne podatke.

Mjerenje emocionalnih stanja, ponašanja, stavova i mišljenja, odnosno prikupljanje podataka u svrhu profiliranja, mora se provoditi isključivo uz privolu zaposlenika. Uzimajući u obzir prava građana, to ujedno implicira da usluga mora biti dostupna i ako privola za prikupljanje podataka ne postoji, odnosno ako korisnik nije dopustio prikupljanje osobnih podataka u svrhu profiliranja.

Davatelj usluga ne smije uskraćivati pružanje usluge korisnicima koji ne dopuste prikupljanje podataka. Drugim riječima, usluga ne smije biti metoda ucjene ili prisile. Niti jedna javna usluga, a pogotovo ne javna, ne smije biti uvjetovana

Korištenje usluga mora biti omogućeno bez obaveze prikupljanja podataka na koje korisnik ne pristaje.

## 6. ZAKLJUČAK

Prije svega važno je nedvosmisleno ustvrditi da se tehnologije za procjenu emocionalnih stanja, ponašanja, stavova i mišljenja ubrzano razvijaju i pronalaze široku primjenu u praksi. Osim primjene na korisnicima društvenih mreža, ove tehnologije danas se već redovito koriste i tijekom razgovora za posao ili u policijskim istragama. Brojni drugi oblici primjene su svakako mogući i potrebno je o njima voditi računa u budućnosti.

Tehnologije za procjenu emocionalnih stanja koje koriste postupke umjetne inteligencije su, kao što je nedvojbeno empirijski demonstrirano, nepouzdane i često daju poopćene rezultate koji se mogu pogrešno interpretirati, odnosno dovesti do krivih zaključaka. Rezultati mogu biti specifični za homogene skupine ispitanika koji su pobuđeni koristeći za njih prilagođen stimulacijski protokol. Takav protokol nužno obuhvaća modalitet pobude, semantiku (kontekst i sadržaj) pobude, vremenske aspekte (trajanje i pauze), individualnu psihologiju (s neurološkim temeljima), te eksperimentalnu okolinu. Svi ovi aspekti koji utječu na točnost rezultata u svakodnevnoj primjeni – van strogo nadziranog laboratorijskog okruženja – najčešće se zanemaruju, ili se na njih ne može učinkovito utjecati. Nedostatak personalizacije u pobudi i kasnijoj interpretaciji rezultata dovodi do odviše općenitih zaključaka koji mogu biti, a najčešće jesu, pogrešni kad se primijene na individualne ispitanike. Procijenjeno emocionalno stanje, ponašanje ili kognicija grupe u praksi nije identično procjeni za svakog pojedinca unutar te grupe. Jednostavno rečeno, izjednačavanje globalne s pojedinačnom estimacijom nužno će dovesti do pogrešne interpretacije emocionalnih reakcija, namjera, razmišljanja ili uzroka ponašanja korisnika.

Istodobno, postojeći zakonodavni okvir u vezi zaštite osobnih podataka, kako hrvatski tako i međunarodni, još uvijek ne prepoznaje potencijalne opasnosti koje primjena tehnologija umjetne inteligencije donosi u domeni prepoznavanja emocionalnih stanja, ponašanja i kognicije. Unatoč pozitivnim pomacima u ovom pogledu, povećanoj medijskoj pažnji i sve većem interesu zakonodavaca za pitanje regulacije umjetne inteligencije, ovo područje još nije regulirano na zadovoljavajući način. Potencijalne zloupotrebe izuzimanja i korištenja osobnih podataka su moguće. Štoviše, trenutačno korisnici ne samo da nisu informirani za što se njihovi osobni podaci koriste, već nisu niti svjesni da se vrši automatska estimacija njihovih emocionalnih stanja, ponašanja i kognicije, te da se tako dobiveni rezultati koriste za donašanje odluka s kojima su oni povezani. Takve odluke donose se djelomično ili u potpunosti automatizirano, a mogu se odnositi na – primjerice – odluku da li će dobiti traženi posao, ili da li će biti osumnjičeni tijekom policijskog postupanja.

Da bi se spriječilo neobjektivno i automatizirano donašanje zaključaka prvenstveno je potrebno osvijestiti moguće opasnosti koje primjena tehnologija umjetne inteligencije za procjenu emocionalnih stanja donosi. Potrebno je snažnije zakonski regulirati uporabu ovakvih tehnologija u bilo kojem obliku ili području primjene, a posebice nad javnim servisima koji moraju biti uvijek dostupni svim građanima, bez izuzetaka ili vanzakonskih ograničenja.

S tom svrhom u ovom radu predlaže se izrada standardiziranih znakova koji upozoravaju korisnike na prisutnost postupaka prikupljanja osobnih podataka o njihovu emocijama, ponašanju i kogniciji, te namjenu takvog postupka. Takvi znakovi moraju biti nedvosmisleni i lagano razumljivi, a njihovo razumijevanje neovisno o jeziku ili kulturi korisnika. To mogu biti vizualni simboli ili tekstualne poruke, ali obavezno se moraju nalaziti na lako zamjetljivom mjestu.

Također je vrlo važno korisnicima pružiti alternativu korištenja nekog servisa, posebice javnog, ukoliko korisnici ne želi dopustiti prikupljanje vlastitih osobnih podataka u svrhu estimacije vlastitih emocionalnih stanja, ponašanja i kognicije koji se koriste za donašanje automatiziranih odluka o njima. Bilo koji servis, tim više javni, ne smije biti uvjetovan snimanjem fizioloških podataka i profiliranjem korisnika. Ako se takvi postupci automatizirano primjenjuju, onda drugi način ostvarenja usluge servisa mora biti osiguran.

Naposljetku, možemo zaključiti da je važno kontinuirano voditi aktivnu stručnu i znanstvenu raspravu o svim aspektima razvoja i primjene tehnologija za procjenu emocionalnih stanja. U ovom području sigurno će se dogoditi brojni koraci naprijed, kako u pogledu senzora koji se koriste, količine i složenosti prikupljanih podataka, složenosti postupaka obrade podataka, tako i u pogledu točnosti i primjene dobivenih podataka.

### Literatura:

1 Legg, S., & Hutter, M. (2007). A collection of definitions of intelligence. Frontiers in Artificial Intelligence and applications, 157, 17.

2 Elon Musk, https://twitter.com/elonmusk/status/1229546793811226627, pristupljeno 24. veljače 2020.

3 The Verge, Elon Musk says AI development should be better regulated, even at Tesla, https://www.theverge.com/2020/2/18/21142489/elon-musk-ai-regulation-tweets-open-ai-tesla-spacex-twitter, pristupljeno 24. veljače 2020.

4 AI Now Report 2019, https://ainowinstitute.org/AI_Now_2019_Report.pdf, pristupljeno 24. veljače 2020.

5 Barrett, L. F., Adolphs, R., Marsella, S., Martinez, A. M., & Pollak, S. D. (2019). Emotional expressions reconsidered: challenges to inferring emotion from human facial movements. Psychological Science in the Public Interest, 20(1), 1-68.

6 MIT Technology Review, https://www.technologyreview.com/2019/07/26/238782/emotion-recognition-technology-artifical-intelligence-inaccurate-psychology/, pristupljeno 24. veljače 2020.

7 Shaping Europe's digital future: Commission presents strategies for data and Artificial Intelligence, EU press release, https://ec.europa.eu/commission/presscorner/detail/en/ip_20_273, 19 February 2020.

8 Ćosić, K., Popović, S., Horvat, M., Kukolja, D., Dropuljić, B., Kovač, B., & Jakovljević, M. (2013). Computer-aided psychotherapy based on multimodal elicitation, estimation and regulation of emotion. Psychiatria Danubina, 25(3), 0-346.

9 Kukolja, D., Popović, S., Horvat, M., Kovač, B., & Ćosić, K. (2014). Comparative analysis of emotion estimation methods based on physiological measurements for real-time applications. International journal of human-computer studies, 72(10-11), 717-727.

10 Lugović, S., Dunđer, I., & Horvat, M. (2016, May). Techniques and applications of emotion recognition in speech. In 2016 39th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), pp. 1278-1283.

11 Horvat, M., & Fodor, D. (2018). System for remote heart rate measurement using a consumer camera. Polytechnic and Design, 6(2), 128-134.

12 Pejak, I., Otočan, D., & Horvat, M. (2017). Application of Android Wear smartwatches with photoplethysmographic sensors in biofeedback therapy. Polytechnic and Design, 5(2), 133.

13 Europska komisija, Zaštita podataka, https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_hr, pristupljeno 24. veljače 2020.

14 Ministarstvo unutarnjih poslova Republike Hrvatske, Zaštita osobnih podataka, https://mup.gov.hr/zastita-osobnih-podataka/222, pristupljeno 24. veljače 2020.

15 Agencija za zaštitu osobnih podataka, Vodič kroz opću uredbu o zaštiti podataka, https://azop.hr/info-servis/detaljnije/vodic-kroz-opcu-uredbu-o-zastiti-podataka, pristupljeno 24. veljače 2020.

## Podaci o autoru:

**Doc. dr. sc. Marko Horvat, v. pred.**

e-mail: marko.horvat3@gmail.com

Diplomirao, magistrirao i doktorirao iz znanstvenog područja tehničke znanosti znanstveno polje računarstvo na Fakultetu elektrotehnike i računarstva Sveučilišta u Zagrebu, 1999., 2007. i 2013. godine. Trenutno je prodekan za znanost, vanjsku suradnju i nove studije, te viši predavač na Tehničkom veleučilištu u Zagrebu i naslovni docent na Sveučilištu u Zagrebu u navedenom području i polju. Sudjeluje u pripremi i provedbi niza stručna i znanstvenih projekata. Kao autor ili koautor objavio je više od 100 znanstvenih i stručnih radova, sažetaka sa skupova, poglavlja u knjigama, skripti i udžbenika, a od toga 9 izvornih znanstvenih radova u CC časopisima. Održao je niz javnih i pozvanih predavanja, kao i stručnih tečajeva. Član je stručne udruge IEEE u statusu Senior Member i Hrvatskog astronomskog društva.

Tehničko veleučilište u Zagrebu
Informatičko-računarski odjel
Vrbik 8, 1000 Zagreb, Hrvatska