Univerzitetska misao - časopis za nauku, kulturu i umjetnost [ISSN: 1451-3870]
Vol. 21, str. 164-175, 2022 god., web lokacija gde se nalazi rad:http://um.uninp.edu.rs
Tematska oblast u koju se svrstava rad: Društvene i humanističke nauke / podoblast: Pravo
Datum prijema rada: 29.06.2022. *Datum prihvatanja rada: 19.10.2022.*
UDK: 004.8:341.231.14 doi: 10.5937/univmis2221164G

Originalni naučni rad

PRIKAZ STAVOVA U POGLEDU SADRŽINE ČLANA 5 PREDLOGA UREDBE EVROPSKE UNIJE O VEŠTAČKOJ INTELIGENCIJI: IZAZOV PRONALASKA PRAVE MERE

"The potential benefits of artificial intelligence are huge, so are the dangers"

Dave Waters

Milena Galetin

Educons univerzitet, Sremska Kamenica; Univerzitet Privredna akademija u Novom Sadu, Pravni fakultet za privredu i pravosuđe u Novom Sadu, Srbija
milena.galetin@gmail.com

Jovana Škorić
Univerzitet u Novom Sadu, Filozofski fakultet, Srbija
jovana.skoric@ff.uns.ac.rs

Milan Mihajlović
Educons univerzitet, Sremska Kamenica, Srbija
milan.mihajlovic@educons.edu.rs

Apstrakt

Iako sama primena veštačke inteligencije u gotovo svim oblastima nije novina, poslednjih nekoliko godina se intenzivno radi na njenom pravnom regulisanju. Mada možemo reći da se još uvek radi o relativno početnim koracima, očigledno je da Evropska unija ulaže velike napore i sredstva kako bi imala vodeću ulogu u tom procesu. U aprilu 2021. godine je donet jedan od najznačajnijih pravnih dokumenata u ovoj oblasti - Predlog uredbe Evropske unije o veštačkoj inteligenciji. Autori se u radu bave analizom člana 5 ovog Predloga uredbe koji govori o tome u kojim slučajevima bi upotrebu veštačke inteligencije trebalo zabraniti. Uzimajući u obzir da još uvek nema dovoljno znanja i iskustva u pogledu posledica primene veštačke inteligencije, istražuju različite stavove u pogledu suženja njene primene. Činjenica da bi zakonodavstvo Republike Srbije trebalo da bude usaglašeno sa pravnom regulativom Evropske unije, a što korespondira i sa ciljevima navedenim u Strategiji za razvoj veštačke inteligencije RS za period 2020-2025. godine doprinosi i posebnom značaju ovog istraživanja.

Ključne reči: veštačka inteligencija i pravna regulativa, Predlog uredbe Evropske unije o veštačkoj inteligenciji, zabrana primene veštačke inteligencije

REVIEW OF THE STANDPOINTS REGARDING THE CONTENT OF THE ARTICLE 5 OF THE PROPOSAL FOR THE EUROPEAN UNION'S ARTIFICIAL INTELLIGENCE ACT: THE CHALLENGE OF FINDING THE BALANCE

Abstract

Although the application of artificial intelligence in almost all areas is not new, in the last few years intensive work has been done on its legal regulation. Despite the fact that only initial steps have been taken, it is obvious that the European Union is investing great efforts and resources in order to play a leading role in this process. In April 2021, one of the most important legal documents in this area was adopted – the Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts. The authors deal with the analysis of Article 5 of this Draft Regulation, which lays down the cases in which the use of artificial intelligence should be banned. Taking into account that there is still not enough knowledge and experience regarding the consequences of the use of artificial intelligence, available different attitudes are explored. The fact that the legislation of the Republic of Serbia should be harmonized with the legal regulations of the European Union, which corresponds to the goals stated in the Strategy for the Development of Artificial Intelligence in the Republic of Serbia for the period 2020-2025, also contributes to the special significance of this research.

Key words: artificial intelligence and legal regulation, artificial Intelligence Act, prohibition of AI applications

I UVOD

Poslednjih nekoliko godina se u Evropskoj uniji (EU) intenzivno radi na pravnoj regulativi koja se odnosi na primenu veštačke inteligencije i, pri tom, se ističe da se *pristup EU veštačkoj inteligenciji usredsređuje na izvrsnost i poverenje, sa ciljem da podstakne istraživačke i industrijske kapacitete i obezbedi ostvarivanje osnovnih prava*, odnosno da će ovaj *pristup obezbediti da se sva poboljšanja veštačke inteligencije zasnivaju na pravilima kojima se štiti funkcionisanje tržišta i javni sektor, kao i bezbednost ljudi i osnovna prava* (Shaping Europe's digital future, A European approach to artificial intelligence, An official website of the European Union, European Commission). Kao najznačajnije momente u ovom procesu bismo izdvojili osnivanje Ekspertske grupe za veštačku inteligenciju 2018. godine (*the High-Level Expert Group on Artificial Intelligence*) i objavljivanje Bele knjige o veštačkoj inteligenciji– Evropski pristup izuzetnosti i poverenju 2020. godine (White Paper on Artificial Intelligence A European approach to excellence and trust, Brussels, 19.2.2020 COM(2020) 65 final), te donošenje Predloga uredbe Evropske unije o veštačkoj inteligenciji, u aprilu 2021. godine (Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts COM/2021/206 final) (Predlog uredbe). Za Republiku Srbiju (RS), kao kandidata za članstvo u Evropskoj uniji, je od izuzetne važnosti da prati trendove u

EU i svoje zakonodavstvo usaglasi sa pravilima EU, što je predviđeno i u Strategiji za razvoj veštačke inteligencije RS za period 2020-2025. godine.

Predlog uredbe koji sadrži odredbe i o etičkim standardima je naišao na široko odobravanje, te se smatra da ima potencijal da postane lider u oblasti pravne regulative veštačke inteligencije na globalnom nivou, odnosno da postane tzv "*superregulator*" (Biber, 2021: 1). Naglask bi, međutim, prema jednom mišljenu, trebalo staviti na činjenicu da je intencija Evropske unije da jasno zaštiti vladavinu prava od "vladavine tehnologije" (Biber, 2021: 1). Namera je da ovaj pravni okvir sadrži harmonizovana pravila koja su i u saglasnosti sa postojećim instrumentima zaštite ljudskih prava u Evropskoj uniji i pravnom regulativom EU koja se odnosi na zaštitu podataka, zaštitu potrošača, zabranu diskriminacije, rodnu ravnopravnost (Townsend, 2021: 4). To je, između ostalog, navedeno kao poseban cilj u obrazloženju Predloga uredbe: obezbediti da se sistemi veštačke inteligencije koji se stavljaju na tržište Unije i koriste bezbedni i usaglašeni sa postojećim osnovim pravima i vrednostima Unije; obezbediti pravnu sigurnost kako bi se olakšala ulaganja i inovacije u oblasti veštačke inteligencije; poboljšanje upravljanja i efikasna primena postojeće regulative u oblasti osnovnih prava i bezbednosnih zahteva primenjivih na sisteme veštačke inteligencije; olakšavanje razvoja jedinstvenog tržišta za zakonite, bezbedne i pouzdane primene veštačke inteligencije i sprečavanje fragmentacije tržišta (Predlog uredbe, obrazloženje, 2021: 3)

U članu 3 Predloga uredbe se pod sistemom veštačke inteligencije podrazumeva softver koji je razvijen pomoću jedne ili više tehnika i pristupa navedenih u Aneksu I i koji može, za određeni skup ciljeva koji je definisan od strane čoveka, da generiše izlazne rezultate kao što su sadržaj, predviđanja, preporuke ili odluke, koji utiču na okruženja sa kojima su u interakciji. Tehnike i pristupi na koje se misli u ovom članu su:

- Pristupi mašinskog učenja, uključujući nadgledano, nenadgledano i učenje sa podrškom, koristeći široki spektar metoda uljučujući duboko učenje
- Pristupi zasnovani na logici i na znanju, uključujući reprezentaciju znanja, induktivno (logičko) programiranje, baze znanja, mehanizme za inferenciju i dedukciju, (simboličko) zaključivanje i ekspertske sisteme
- Statistički pristupi, Bajesovska procena (*Bayesian estimation*), metode istraživanja/pretraživanja i optimizacije.

Evropska komisija može usvojiti neophodne akte kako bi se izmenila lista ovih tehnika i pristupa, kako bi se ona ažurirala u skladu sa tržišnim i tehnološkim novinama.

Kreatori Predloga uredbe pokušali su da pronađu balans između primene veštačke inteligencije u svakodnevnom životu i zaštite bezbednosti i ljudskih prava putem pristupa koji se zasniva na rizicima (*risk-based aproach*), te se razlikuje primena veštačke inteligencije koja predstavlja neprihvatljiv rizik, visok rizik i nizak ili minimalan rizik. Reč je, zapravo, o horizontalnom regulatornom okviru prema kojem se kreiranje, stavljanje na tržište i primena sistema veštačke inteligencije određuje na osnovu rizika koji takvi sistemi predstavljaju za bezbednost i zdravlje ljudi i osnovna prava. Tako je primena veštačke inteligencije koja predstavlja neprihvatljiv rizik zabranjena, osim u izuzetnim slučajevima. U slučajevima kada primena veštačke

inteligencije predstavlja visok rizik, njena upotreba podleže ispunjenju određenih zahteva i obaveza i to i pre i nakon stavljane u upotrebu na tržištu Unije – ovde su u pitanju sistemi veštačke inteligencije koji predstavljaju značajan rizik za zdravlje i bezbednost, kao i osnovna prava. U Aneksu III Predloga uredbe su navedene oblasti u kojima primena veštačke inteligencije predstavlja visok rizik. To su, na primer, primena sistema veštačke inteligencije prilikom ocenjivanja učenika/studenata, procenjivanja kreditne sposobnosti, ocenjivanja prilikom zasnivanja radnog odnosa, sistemi za nadzor (sistemi za prepoznavanje lica), prilikom utvrđivanja verodostojnosti putničkih dokumenata (migracije, azil i kontrola granica), prilikom primene prava na određene činjenice (pravosuđe i demokratski procesi) (Kop, 2021). Kada primena veštačke inteligencije predstavlja ograničeni rizik, tada se zahtevaju da budu ispunjeni određeni uslovi u pogledu transparentnosti. To je, na primer, slučaj sa upotrebom *chatbot*-ova, kada je neophodno korisnicima predočiti da su u interakciji sa mašinom. Konačno, svi ostali sistemi veštačke inteligencije mogu se kreirati i koristiti u skladu sa postojećom regulativom, bez dodatnih obaveza (Durmus, 2022).

Mi se u radu bavimo pitanjem koja je to upotreba veštačke inteligencije koja sa sobom nosi neprihvatljiv rizik, te bi je trebalo zabraniti jer je u pitanju primena koja je protivna vrednostima Evropske unije.

II ANALIZA ČLANA 5 PREDLOGA UREDBE EVROPSKE UNIJE O VEŠTAČKOJ INTELIGENCIJI

Glava II Predloga Uredbe nosi naziv "Zabranjene prakse u području veštačke inteligencije" i u okviru nje se nalazi član 5 koji govori o tome kada bi primenu veštačke inteligencije trebalo zabraniti:

a) Stavljanje na tržište, stavljanje u upotrebu ili korišćenje sistema veštačke inteligencije koji primenjuje subliminalne tehnike koje su izvan čovekove svesti kako bi bitno uticali na ponašanje ljudi na način koji uzrokuje ili bi mogao prouzrokovati fizičku ili psihološku štetu tom ili nekom dugom licu

b) Stavljanje na tržište, u upotrebu ili korišćenje sistema veštačke inteligencije koji iskorišćava bilo koju ranjivost određene grupe lice zbog njihovog uzrasta, fizičkog ili mentalnog invaliditeta kako bi se bitno uticalo na ponašanje osobe iz takve grupe na način koji uzrokuje ili može da izazove fizičku ili psihološku štetu toj ili drugoj osobi

c) Stavljanje na tržište, stavljanje u upotrebu ili korišćenje sistema veštačke inteligencije od strane javnih vlasti ili u njihovo ime za evaluaciju ili klasifikaciju pouzdanosti fizičkih lica u određenom vremenskom periodu na osnovu njihovog društvenog ponašanja ili poznatih ili pretpostavljenih ličnih karakteristika ili karakteristika ličnosti, i sa društvenom ocenom koja dovodi do jednog ili oba sledeća:

(i) štetan ili nepovoljan tretman određenih fizičkih lica ili čitavih grupa u društvenim kontekstima koji nisu povezani sa kontekstima u kojima su podaci prvobitno generisani ili prikupljeni;

(ii) štetan ili nepovoljan tretman određenih fizičkih lica ili čitavih grupa koji je neopravdan ili nesrazmeran njihovom društvenom ponašanju ili njegovim posledicama.

d) korišćenje sistema za daljinsku biometrijsku identifikaciju u „realnom vremenu" na javnim mestima za potrebe krivičnog gonjenja, osim i samo u meri u kojoj je takva upotreba nužna za jedan od sledećih ciljeva:

(i) ciljane potrage za konkretnim potencijalnim žrtvama krivičnih dela, uključujući nestalu decu;

(ii) sprečavanje konkretne, ozbiljne i neposredne pretnje po život ili fizičku bezbednost fizičkih lica ili terorističkog napada

(iii) otkrivanja, lociranja, identifikacije ili krivičnog gonjenja počinioca krivičnog dela ili osumnjičenog za krivično delo iz člana 2(2) Okvirne odluke Saveta 2002/584/ JHA1 i koje je kažnjivo u državi članici kaznom zatvora ili oduzimanjem slobode čiji maksimalani period trajanja ne može biti manji od 3 godine, kako je utvrđeno pravom države članice.

2. Upotreba sistema za daljinsku biometrijsku identifikaciju u „realnom vremenu" na javnim mestima za potrebe krivičnog gonjenja za bilo koji od ciljeva navedenih u stavu 1 tačka d) uzima u obzir sledeće elemente:

(a) prirodu situacije koja dovodi do moguće upotrebe, posebno ozbiljnosti, verovatnoće i razmere štete koja bi nastala nekorišćenjem sistema;

(b) posledice korišćenja sistema za prava i slobode svih lica na koje se primenjuje, posebno ozbiljnost, verovatnoću i razmere tih posledica.

Pored toga, korišćenje sistema za daljinsku biometrijsku identifikaciju u „realnom vremenu" na javnim mestima za potrebe krivičnog gonjenja za bilo koji od ciljeva navedenih u stavu 1 tačka d) mora biti u skladu sa nužnim i srazmernim zaštitnim merama i uslovima u kojima se primenjuje, posebno u pogledu vremenskih, geografskih i ličnih ograničenja.

3. Što se tiče stava 1. tačka (d) i stava 2, svako pojedinačno korišćenje sistema za daljinsku biometrijsku identifikaciju u „realnom vremenu" na javnim mestima za potrebe krivičnog gonjenja podleže prethodnom odobrenju sudskog organa ili nezavisnog organa uprave države članice u kojoj će se koristiti, izdato na osnovu obrazloženog zahteva i u skladu sa detaljnim pravilima nacionalnog prava iz st.4. Međutim, u određenoj opravdanoj hitnoj situaciji, korišćenje sistema može se započeti bez odobrenja i ovlašćenje se može tražiti tek tokom ili nakon upotrebe.

Nadležni sudski ili upravni organ izdaje odobrenje samo ako se uveri, na osnovu objektivnih dokaza ili jasnih indikacija koje su mu predočene, da je upotreba konkretnog sistema za daljinsku biometrijsku identifikaciju u „realnom vremenu" nužna i srazmerna postizanju jedanog od ciljeva navedenih u stavu 1. tačka (d), kao što je navedeno u zahtevu. Prilikom odlučivanja o zahtevu, nadležni sudski organ ili organ uprave uzima u obzir elemente iz stava 2.

Council Framework Decision 2002/584/JHA of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States (OJ L 190, 18.7.2002, p. 1) - Okvirna odluka Saveta o Evropskom nalogu za hapšenje i postupcima predaje između država članica.

4. Država članica može odlučiti da predvidi mogućnost da u potpunosti ili delimično odobri upotrebu sistema za daljinsku biometrijsku identifikaciju u „realnom vremenu" na javnim mestima za potrebe krivičnog gonjenja u granicama i pod uslovima navedenim u stavu 1. , tačka (d) i stavu 2. i 3. Ta država članica će u svom nacionalnom pravu propisati neophodna detaljna pravila za traženje, izdavanje i izvršavanje, kao i nadzor u vezi sa odobrenjima iz stava 3. Ta pravila takođe preciziraju u pogledu kojih ciljeva navedenih u stavu 1. tačka (d), uključujući i za koja od krivičnih dela iz tačke (iii), nadležni organi mogu biti ovlašćeni da koriste te sisteme za potrebe krivičnog gonjenja. (Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts COM/2021/206 final)

Kao što se može videti, primenu sistema veštačke inteligencije koja sa sobom nosi neprihvatlji rizik jer predstavlja opasnost po život, bezbednost i ljudska prava, bismo mogli podeliti u četiri kategorije (Kop, 2021: 3). U prve dve spadaju sistemi koji primenjuju manipulativne subliminalne/podsvesne tehnike ili iskorišćavaju osetljivost određenih društvenih grupa, To znači da bi se druge manipulativne ili iskorišćavajuće prakse koje utiču na odrasle osobe, a koje bi mogle da budu olakšane primenom sistema veštačke inteligencije, mogle obuhvatiti postojećom regulativom iz oblasti zaštite podataka, zaštite potrošača i digitalnih usluga koja predviđa da su fizička lica propisno informisana i imaju slobodan izbor o tome da budu subjekti profilisanja ili drugih postupanja koja mogu uticati na njihovo ponašanje (Predlog uredbe, obrazloženje, 2021: 12, 13). Zatim, posebnu kategoriju predstavljaju sistemi veštačke inteligencije koji se koriste od strane javne vlasti (ili u njihovo ime) za društveno ocenjivanje (*social scoring*) i, konačno, sistemi za daljinsku biometrijsku identifikaciju „realnom vremenu" na javnim mestima za potrebe krivičnog gonjenja (osim u gorepomenutim, izuzetnim sluajevima, kada je dozvoljeno korišćenje). Čini se da je namera kreatora Predloga uredbe da poslednje dve kategorije svrsta u ovu grupu jer predstavljaju, pre svega, neprihvatljiv rizik za pravo na privatnost i zabranu diskriminacije, ali svakako ugrožavaju i druga ljudska prava.

U brifingu iz januara 2022. godine (BRIEFING 'EU Legislation in Progress', Artificial intelligence act, 2022) nalazimo sa više strana upućene komentare i primedbe u vezi sa ovim članom. Neki od njih su da bi zabranu upotrebe veštačke inteligencije trebalo postaviti šire, kao i da sam pristup koji se zasniva na proceni rizika ne obezbeđuje visok nivo zaštite osnovnih prava. Takođe, bilo je i inicijativa za zabranu neselektivne ili proizvoljne upotrebe biometrije na javnim mestima. *AccessNow* ističe da su odredbe člana 5 poprilično nejasne i takođe predlaže širu zabranu korišćenja veštačke inteligencije za klasifikaciju ljudi na osnovu podataka o fiziološkim karakteristikama, ponašanja ili biometrijskih podataka, za prepoznavanje emocija, i ukazuju na opasnost upotrebe u kontekstu policije, migracija, azila i granične kontrole. Zanimljiv stav je i *AlgorithmWatch* koji navode da primenu određenih pravila ne treba zasnivati na vrsti tehnologije, već na uticaju koji ona ima na pojedinca i društvo (BRIEFING 'EU Legislation in Progress', Artificial intelligence act, 2022: 8). Istaknuta je i ideja da se ustanovi procedura koja bi omogućila Komisiji da proširi listu zabranjenih sistema veštačke inteligencije, kao i da se zabrane postojeći manipulativni sistemi veštačke inteligencije (kao na primer *deepfakes*), društveno ocenjivenje i neke biometrije, čak i kada se koriste u privatne svrhe (BRIEFING 'EU Legislation in Progress', Artificial intelligence act, 2022: 9). Takođe, predlog je i da se uvede korišćenje nove definicije – podaci zasnovani na biometriji (*'biometrics-based data'*) jer je predložena "biometrijski podaci" suviše uska. Takođe, Evropski supervizor za zaštitu podataka i Evropski odbor za zaštitu podataka su pozvali na opštu zabranu upotrebe veštačke inteligencije za automatsko prepoznavanje ljudskih karakteristika na javnim mestima (BRIEFING 'EU Legislation in Progress', Artificial intelligence act, 2022: 10).

U izveštaju *Human Rights Watch* je istaknuto da se jasna zabrana veštačke inteligencije zahteva kada primena veštačke inteligencije ugrožava ljudska prava i ne postoji način kojim bi se to efikasno moglo ublažiti. Smatraju da bi trebalo zabraniti bilo koju vrstu ocenjivanja ponašanja koja neopravdano ograničava ili ima negativan uticaj na ljudska prava i ističu da ocenjvanje *pouzdanosti* tokom određenog perioda vremena nejasno i ne vide njegovu smislenu primenu. Propis bi, kako navode, trebalo da jasno ukaže na protivljenje upotrebe algoritama koji odlažu ili uskraćuju pristup bilo kojim beneficijama, a zabrana ocenjivanja bi trebalo da se odnosi i na javne vlasti i na privatne aktere. Nalaze da je malo verovatno da će postojeća lista neprihvatljivih rizika obuhvatiti svaku pretnju ljudskim pravima s obzirom da se radi o oblasti koja brzo napreduje i stalno se menja, te zbog toga smatraju da bi trebalo uspostaviti mehanizam za predlaganje i dopunjavanje liste koja se odnosi na to kada primena sistema veštačke inteligencije predstavlja neprihvatljiv rizik, a zalažu se i za učešće javnosti i civilnih društava u ovom procesu (Human Rights Watch, 2021: 25).

Ovim pitanjem se prilično detaljno bavila *BEUC The European Consumer Organisation* (BEUC The European Consumer Organisation, The Consumer Voice in Europe, 2021: 10-16), te predlažu da lista kada je zabranjeno primenjivati veštačku inteligenciju u članu 5 mora biti proširena: član 5, tačka 1. a) i b) se odnosi na to da je primena veštačke inteligencije sada zabranjena samo u slučajevima kada izaziva fizičku ili psihološku štetu, ali ne i ukoliko je u pitanju ekonomska šteta (kao primer navode korišćenje podataka pametnih brojila kako bi se utvrdila cena energije za

svakog potrošača na osnovu podataka o njihovoj potrošnji - snabdevači bi mogli da, prateći potrošnju, prilagode cenu tako da potrošači plate više, odnosno da cena električne energije bude viša kada je potrošnja visoka). Osim toga, iz ove organizacije poručuju i da bi trebalo učiniti izmene teksta u ovom delu jer se primena veštačke inteligencije isključuje samo u slučaju postojanja *namere* da se izazove fizička ili psihološka šteta, ali ne i usled *mogućeg korišćenja*, odnosno *razumno predvidive zloupotrebe* korišćenja sistema veštačke inteligencije. Takođe, smatraju da bi *subliminalno* kao kriterijum trebalo izbaciti jer je nejasno i nepotrebno, dok bi društvenu štetu, pod kojom se smatra manipulisanje na takav način da to ima uticaj na demokratiju i vladavinu prava, treblo obuhvatiti. Dalje, član 5, tačka1, b) bi trebalo da ima mnogu širi opseg, a ne samo da se odnosi na iskorišćavanje ranjivosti dece ili osoba sa fizičkim ili mentalnim invaliditetom, kao na primer u slučajevima privremene ranjivosti (tuga, stres), a koji ne spadaju u navedene grupe ili u slučaju tzv. digitalne asimetrije. Što se društvenog ocenjivanja tiče, zalažu se za potpunu zabranu primene veštačke inteligencije i to kako od strane javne vlasti, tako i od privatnih aktera i to bez obzira na kontekst u okviru koga su podaci prikupljeni (posebno ističu da se u Predlogu uredbe uopšte ne spominje društveno ocenjivanje od strane privatnih aktera – niti u članu 5, niti u delu koji se odnosi na primenu veštačke inteligencije koja predstavlja visok rizik). Dalje, autori iz ove organizacije ističu da primenu sistema za daljinsku biometrijsku identifikaciju u „realnom vremenu" na javnim mestima od strane privatnih subjekata treba zabraniti, bez izuzetka i naglašavaju da bi institucije EU trebalo da razmotre potpunu zabranu ove primene i od strane javne vlasti. To je i u skladu sa preporukama Evropskog supervizora za zaštitu podataka i Evropskog odbora za zaštitu podataka, koji se protive korišćenu veštačke inteligencije za prepoznavanje ljudskih karakteristika na javnim mestima, kao što su prepoznavanje lica, hoda, otisaka prstiju, DNK, glasa, i slično, u bilo kom kontekstu. Konačno, upotreba veštačke inteligencije za prepoznavanje emocija nije svrstana ni ovde, ni u primenu koja sa sobom nosi visok rizik, te se u ovom slučaju samo zahtevaju obaveze u pogledu transparentnosti. Međutim, stav ove organizacije, ali i preporuka Evropskog supervizora za zaštitu podataka i Evropskog odbora za zaštitu podataka, je da bi korišćenje veštačke inteligencije za prepoznavanje emocija trebalo, takođe, zabraniti, osim u tačno određenim izuzetnim slučajevima koji se odnose na zdravstvene ili istraživačke svrhe, kao i da bi trebalo zabraniti upotrebu veštačke inteligencije za koju nije dokazana naučna validnost/ili je nauka opovrgla njenu korisnost, kao i one koje su u direktnoj suprotnosti sa osnovnim vrednostima Evropske unije.

Istu preporuku je izneo i *Ada Lovelace Institute* (Ada Lovelace Institute, 2022): ukloniti "subliminalno" i proširiti primenu "ranjivosti", nezavisno od starosti ili invalidnosti i dodati "ekonomsku štetu", kao i propisivanje zabrane korišćenja biometrije za kategorizaciju/klasifikaciju i prepoznavanje emocija. Smatraju da bi član 5, tačka 1, d) trebalo da obuhvata i retrospektivnu biometrijsku identifikaciju u privatnim prostorima, *online* i od strane privatnih aktera. Predlažu uvođenje testa "pojačane proporcionalnosti" koji se ne odnosi samo na procenu rizika po ljudska prava pojedinaca, zdravlje i bezbednost, već i za nastanak društvene štete i štete po

životnu sredinu – time bi se omogućila primena bilo kog sistema veštačke inteligencije koji predstavlja neprihvatljiv rizik u izuzetnim okolnostima, a koja je uslovljena prolaskom testa. U vezi sa tim, predlažu propisivanje obaveze objavljivanja svih odluka kojima se odobrava, u izuzetnim okolnostima, stavljanje na tržište ili korišćenje sistema veštačke inteligencije čija primena predstavlja neprihvatljiv rizik.

Navešćemo još nekoliko zanimljivih primedbi i komentara u vezi sa ovim članom. Jedna od njih je da bi zabrana upotrebe sistema za daljinsku biometrijsku identifikaciju u „realnom vremenu" na javnim mestima trebalo proširiti i na sve javne aktere, a ne smo u slučaju potrebe krivičnog gonjenja (Smuha, Ahmed-Rengers, Harkens, Li, MacLaren, Piselli i Yeung, 2021: 20 i dalje, 56). Jedan autor upozorava da bi trebalo obratiti pažnju na to da sistemi za daljinsku biometrijsku identifikaciju nisu isto što i sistemi za biometrijsku kategorizaciju jer prvi služe za identifikaciju fizičkih lica na osnovu njihovih biometrijskih podataka, dok se pomoću druge fizičko lice svrstava u određene kategorije, kao što su pol, godine, etničko poreklo, seksualna ili politička orijentacija i sl. U vezi sa tim su Evropski supervizor za zaštitu podataka i Evropski odbor za zaštitu podataka pozvali na zabranu korišćenja sistema biometrijske identifikacije i kategorizacije na javnim mestima (Biber, 2021: 2,3). Ovaj autor se zalaže za zabranu još nekih upotreba sistema veštačke inteligencije, kao što su sistemi koji se koriste za graničnu kontrolu i migracije, kao i sistemi veštačke inteligencije koji se koriste za prediktivan rad policije (*predictive policing*) čija uporeba može da dovede do rasne diskriminacije/rasizma i u suprotnosti je sa pretpostavkom nevinosti (Biber, 2021: 3).

Nešto drugačiji pristup ima KEIDANREN (Japan Business Federation) (Opinions on the Proposed European Artificial Intelligence Act, 2021, AI Utilization Strategy Taskforce Committee on Digital Economy). Oni ističu da pristup zasnovan na proceni rizika koji koristi preširoke definicije zabranjenih i visokorizičnih sistema veštačke inteligencije sa sobom nosi opasnost od usporavanja inovacija u Evropskoj uniji, te smatraju da bi regulativa, kao i metode za merenje i procenu rizika trebalo da budu jasnije,. Po nijma bi se primena propisa mogla odrediti na osnovu pojedinačnih slučajeva upotrebe i nivoa rizika koji su sa njima povezani. Za razliku od prethodno navedenih mišljenja, oni smatraju da primena sistema veštačke inteligencije koji bez postojanja namere imaju subliminalni efekat (audio-vizuelni sadržaji, komercijalne poruke u marketinške svrhe), ne bi trebalo da potpada pod ovu regulativu. Što se tiče sistema za daljinsku biometrijsku identifikaciju u „realnom vremenu" za potrebe krivičnog gonjenja, smatraju da bi trebalo razjasniti da li su ovim obuhvaćeni slučajevi kada privatna kompanija šalje izveštaj nedležnim organima jer je njihov sistem veštačke inteligencije registrovao, odnosno prepoznao sumnjivu aktivnost.

III ZAKLJUČNA RAZMATRANJA

Prvo na šta bismo ukazali jeste da ovaj korak u pravnom regulisanju oblasti veštačke inteligencije ima ogroman značaj i to ne samo za države članice Evropske unije, nego i mnogo šire. Ono što se odmah primećuje je težnja zakonodavca da pomiri razvoj tehnologije i inovacija sa zaštitom ljudskih prava, izražavajući na taj način svesnost kako koristi, tako i opasnosti koju primena veštačke inteligencije nosi. Kako

je u pitanju oblast koja se brzo razvija, nije jednostavno pronaći balans prilikom regulisanja bilo kog aspekta primene veštačke inteligencije. Zbog činjenice da se ovde susreću osnovna prava, zdravlje, bezbednost, zaštita podataka o ličnosti, zaštita potrošača sa primenom savremenih tehnologija imperativ je u dobro postavljenoj fleksibilnosti ovog dokumenta (Townsend, 2021: 6).

U radu smo ukazali na različita mišljena u pogledu sadržine člana 5 Predloga uredbe, te sugestije kako bi on trebalo da glasi. Još uvek se radi o iznošenju stavova i potrazi za najboljim rešenjima. I različite države imaju različite stavove o ovom pitanju.Tako se, na primer, Nemačka zalaže za potpunu zabranu primene tehnologije za prepoznavanje lica na javnim mestima, dok neke države, kao što je Francuska smatraju da je ova upotreba opravdana u slučajevima zaštite nacionalne bezbednosti (Heikkilä, 2022).

Ujedinjene nacije su, takođe, ukazale na opasnost primene veštačke inteligencije na ljudska prava i pozvale države da uvedu moratorijum na neke sisteme veštačke inteligencije sve dok se ne ustanovi adekvatna međunarodna zaštita (UN News, 2021). I u Strategiji razvoja veštačke inteligencije u Republici Srbiji za period 2020–2025. godine je naglašen značaj bezbedne primene veštačke inteligencije: između ostalog, kao poseban cilj je navedena etična i bezbedna primena veštačke inteligencije, odnosno uvođenje preventivnih mehanizama koji će omogućiti odgovoran razvoj veštačke inteligencije i načina verifikacije da su sistemi zasnovani na mašinskom učenju u skladu sa najvišim etičkim i bezbednosnim standardima. (Strategija razvoja veštačke inteligencije u Republici Srbiji za period 2020–2025. godine: 53 i dalje).

Kao što se vidi, na svim nivoima postoji određena doza opreznosti i zabrinutosti kada je primena veštačke inteligencije u pitanju. Upravo zbog toga je postavljanje granice njene primene, odnosno utvrditi kada je njena primena zabranjena jedan od ključnih koraka u ovom procesu. Definitivno se slažemo sa stavovima da nedostatak iskustva i znanja stvara regulatorne probleme, da ne možemo znati kako će samo društvo izgledati u budućnosti (Hydén, 2022: 295-313), kao i da bi prepoznavanje problematičnih praksi trebalo da bude glavni fokus zakonodavca (Biber, 2021: 3). Pronaći pravi balans u primeni veštačke inteligencije koja omogućava korišćenje svih njenih benefita, ali na bezbedan način je izazov koji je upravo započet. Proširenje ograničenja primene veštačke inteligencije u analiziranom dokumentu svakako ima svoje opravdanje, ali ostaje da se vidi kakva će biti njegova konačna verzija.

LITERATURA

1. *A European approach to artificial intelligence*, dostupno na: https://digital-strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence.

2. Ada Lovelace Institute (2022) People, risk and the unique requirements of AI, 18 recommendations to strengthen the EU AI Act, Policy briefing, dostupno na: https://www.adalovelaceinstitute.org/policy-briefing/eu-ai-act/.

3. Biber, S. E. (2021) Machines Learning the Rule of Law: EU Proposes the World's first Artificial Intelligence Act, dostupno na: https://ssrn.com/abstract=3951908.
4. BRIEFING 'EU Legislation in Progress', Artificial intelligence act (2022), dostupno na: https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/698792/EPRS_BRI(2021)698792_EN.pdf.
5. Durmus, M. (2022) EU Artificial Intelligence Act: Risk Levels, dostupno na: https://murat-durmus.medium.com/eu-artificial-intelligence-act-risk-levels-f42b2e837df6.
6. Heikkilä, M. (2022) A quick guide to the most important AI law you've never heard of, MIT Technology Review, dostupno na: https://www.technologyreview.com/2022/05/13/1052223/guide-ai-act-europe/.
7. Hydén, H. (2022) Regulation of AI: Problems and Options u *Nordic Yearbook of Law and Informatics 2020–2021, Law in the Era of Artificial Intelligence*, Liane Colonna & Stanley Greenstein (eds), Stiftelsen Juridisk Fakultetslitteratur (SJF) and The Swedish Law and Informatics Research Institute (IRI) Law Faculty, Stockholm University.
8. KEIDANREN (Japan Business Federation) (2021) Opinions on the Proposed European Artificial Intelligence Act, AI Utilization Strategy Taskforce Committee on Digital Economy, dostupno na: https://www.keidanren.or.jp/en/policy/2021/069.html.
9. Kop, M. (2021) EU Artificial Intelligence Act: The European Approach to AI, Stanford - Vienna Transatlantic Technology Law Forum, Transatlantic Antitrust and IPR Developments, Stanford University, Issue No. 2/2021. https://www-cdn.law.stanford.edu/wp-content/uploads/2021/09/2021-09-28-EU-Artificial-Intelligence-Act-The-European-Approach-to-AI.pdf.
10. Prlja, D., Gasmi, G., Korać, V. (2021), *Veštačka inteligencija u pravnom sistemu EU*, Institut za uporedno pravo, Beograd.
11. *Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts* COM/2021/206 final.
12. Q&A: How the EU's Flawed Artificial Intelligence Regulation Endangers the Social Safety Net, Human Rights Watch (2021), dostupno na: https://www.hrw.org/sites/default/files/media_2021/11/202111hrw_eu_ai_regulation_qa_0.pdf.
13. Regulating AI to Protect the Consumer Position Paper on the AI Act, BEUC The European Consumer Organisation, The Consumer Voice in Europe (2021) (Contact: Frederico Oliveira da Silva and Kasper Drazewski), dostupno na: https://www.beuc.eu/publications/beuc-x-2021-088_regulating_ai_to_protect_the_consumer.pdf.
14. Smuha, N. A., Ahmed-Rengers, E., Harkens, A., Li, W., MacLaren, J., Piselli, R., Yeung, K. (2021) How the EU Can Achieve Legally Trustworthy AI: A Response to the European Commission's Proposal for an Artificial Intelligence Act, dostupno na: https://ssrn.com/abstract=3899991.
15. Strategija razvoja veštačke inteligencije u Republici Srbiji za period 2020–2025.
16. Townsend, B. (2021), Decoding the Proposed European Union Artificial Intelligence Act. American Society of International Law, ASIL Insights, Volume: 25 Issue: 20, dostupno na:

https://eprints.whiterose.ac.uk/178738/1/Townsend_Decoding_the_Proposed_EU_AI_Act_ASIL_Insights.pdf.
17. UN News (2021), Global perspective Human stories, Urgent action needed over artificial intelligence risks to human rights, dostupno na: https://news.un.org/en/story/2021/09/1099972.
18. *White Paper on Artificial Intelligence A European approach to excellence and trust*, Brussels, 19.2.2020 COM(2020) 65 final, dostupno na: https://ec.europa.eu/info/sites/default/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf.

RESUME

It is obvious that the European Union (EU) is investing great efforts and resources in order to play a leading role in the process of the legal regulation of artificial intelligence (AI). Many significant steps have already been taken in that regard. In April 2021, the Commission adopted the proposal for a regulation laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). The creators of this document have tried to find a balance between the application of artificial intelligence in everyday life and the protection of human rights and safety through a risk-based approach. Thus, the AI systems are divided in the following categories: AI systems presenting unacceptable risk, high risk, limited risk and minimal or no risk systems.

The authors deal with the analysis of Article 5 of the draft of the AI Act, which lays down the cases in which the use of artificial intelligence should be banned. The emphasis was on the presentation of some different opinions and suggestions regarding the content of this Article. It could be stated that finding the right balance in the application of artificial intelligence that allows the use of all its benefits, but in a safe way, is a great challenge.

This paper should contribute to better understanding of EU legislation concerning this issue, which is very important considering that the legislation of the Republic of Serbia should be harmonized with the legal regulations of the European Union. This, as well as the significance of the safe application of artificial intelligence is emphasized in the Strategy for the Development of Artificial Intelligence in the Republic of Serbia for the period 2020-2025.