

Upravljanje krivičnopravnim rizicima upotrebe veštačke inteligencije: okvir Saveta Evrope i Republike Srbije, uz osvrt na pravo Evropske unije

ZORAN T. HARDI, nezavisni istraživač, Bad Doberan, Nemačka
ORCID: 0009-0006-1137-8895

Pregledni rad
UDC: 343.21:004.8(497.11)
DOI: 10.5937/TEHNIKA2603301H

Primena sistema veštačke inteligencije sve više utiče na način funkcionisanja savremenih organizacija i institucija, što otvara pitanje upravljanja rizicima koji mogu nastati usled njihove upotrebe. Poseban izazov predstavlja upravljanje pravnim i krivičnopravnim rizicima koji nastaju kada se sistemi veštačke inteligencije koriste u aktivnostima koje mogu dovesti do povrede pravno zaštićenih dobara. Cilj ovog rada jeste analiza krivičnopravnog okvira odgovornosti za posledice upotrebe veštačke inteligencije u Republici Srbiji, uz poseban osvrt na instrumente Saveta Evrope i relevantne elemente prava Evropske unije. Rad posebno ispituje način na koji se postojeći instituti krivičnog prava mogu primeniti u situacijama kada se veštačka inteligencija koristi kao sredstvo izvršenja krivičnih dela ili kao deo složenog lanca odlučivanja koji dovodi do zabranjene posledice. U radu se primenjuju normativna i komparativna metoda, uz analizu relevantnih institucionalnih i pravnih izvora. Posebna pažnja posvećena je Studiji izvodljivosti CDPC-a o veštačkoj inteligenciji i krivičnom pravu, Okvirnoj konvenciji Saveta Evrope iz 2024. godine i načinu na koji se savremeni teorijski modeli pripisivanja odgovornosti, kao što su Hallevyjevi modeli i doktrina dozvoljenog rizika, mogu primeniti u srpskom pravnom sistemu. Rezultati analize ukazuju na to da efikasno upravljanje krivičnopravnim rizicima upotrebe veštačke inteligencije zahteva jasno definisane normativne standarde, odgovarajuće mehanizme nadzora i odgovornost organizacija koje razvijaju ili koriste ove sisteme, te da Republika Srbija može da se osloni na instrumente Saveta Evrope kao relevantan okvir za dalji razvoj domaćeg pravnog okvira.

Ključne reči: veštačka inteligencija, upravljanje rizicima, krivičnopravna odgovornost, krivičnopravni okvir, Savet Evrope, Republika Srbija

1. UVOD

Razvoj i sve šira primena veštačke inteligencije predstavljaju jedno od ključnih obeležja savremene tehnološke stvarnosti. Sistemi zasnovani na veštačkoj inteligenciji danas se koriste u velikom broju organizacija, javnih institucija i privrednih subjekata, pri čemu njihova primena može imati značajne pravne i društvene posledice. Zbog toga upravljanje rizicima koji nastaju usled upotrebe ovih sistema postaje važan segment savremenog menadžmenta.

Upotreba veštačke inteligencije može doneti brojne koristi u pogledu efikasnosti i automatizacije procesa, ali istovremeno može stvoriti i određene rizike,

naročito u situacijama u kojima se ovi sistemi koriste na način koji može dovesti do povrede pravno zaštićenih dobara. U takvim slučajevima posebno se postavlja pitanje krivičnopravne odgovornosti i načina na koji pravni sistem reaguje na zloupotrebu savremenih tehnologija.

Na nivou Evropske unije razvijen je regulatorni pristup koji se zasniva na proceni rizika i koji nastoji da unapred definiše standarde primene sistema veštačke inteligencije. Pored regulatornih instrumenata, poseban značaj za krivičnopravnu problematiku ima rad Saveta Evrope, koji je razvio instrumente usmerene na prilagođavanje krivičnopravnih kategorija izazovima koje postavljaju autonomni sistemi. Nasuprot tome, u Republici Srbiji upotreba veštačke inteligencije u krivičnopravnom kontekstu sagledava se pre svega kroz primenu opštih instituta krivičnog prava. Osnovno istraživačko pitanje rada jeste da li postojeći krivičnopravni okvir Republike Srbije, uz oslonac na standarde Saveta Evrope i relevantni regulatorni okvir

Adresa autora: Zoran Hardi, nezavisni istraživač,
Bad Doberan, Nemačka
e-mail: hardizoran@t-online.de
Rad primljen: 15.03.2026.
Rad prihvaćen: 12.06.2026.

Evropske unije, pruža dovoljan osnov za upravljanje krivičnopravnim rizicima upotrebe sistema veštačke inteligencije. Polazna pretpostavka rada jeste da opšti instituti krivičnog prava Republike Srbije omogućavaju pripisivanje odgovornosti za štetne posledice upotrebe AI sistema, ali da odsustvo posebnih *ex ante* standarda otežava procenu dužne pažnje, nehata, uzročnosti i organizacionih propusta.

Za razliku od regulatornih analiza koje AI Act posmatraju kao centralni izvor pravila o veštačkoj inteligenciji, ovaj rad polazi od toga da se krivičnopravna odgovornost za posledice upotrebe AI sistema mora prvenstveno analizirati kroz institute krivičnog prava, standarde dužne pažnje, uzročnosti, nehata i organizacionog nadzora, dok se AI Act razmatra samo kao posredni izvor standarda relevantnih za procenu rizika.

U tom cilju, rad analizira relevantne normative instrumente i teorijske modele pripisivanja odgovornosti, te razmatra u kojoj meri postojeći krivičnopravni okvir - u instrumentima Saveta Evrope, relevantnom regulatornom okviru Evropske unije i pravnom sistemu Republike Srbije - pruža adekvatne odgovore na izazove koje donosi upotreba AI sistema.

2. POJAM VEŠTAČKE INTELIGENCIJE I UPRAVLJANJE RIZICIMA NJENE UPOTREBE

U savremenim regulatornim i institucionalnim dokumentima veštačka inteligencija definiše se funkcionalno, sa naglaskom na sposobnost sistema da generiše predviđanja, sadržaj, preporuke ili odluke koje utiču na fizičko ili virtuelno okruženje [1]. U tom smislu, pravni značaj veštačke inteligencije ne proizilazi iz ideje autonomnog tehničkog subjekta, već iz činjenice da njena primena može proizvesti posledice relevantne za pravno zaštićena dobra.

Za potrebe upravljanja rizicima, od posebnog značaja su određene karakteristike sistema veštačke inteligencije. Među njima se posebno izdvajaju sposobnost automatizovanog odlučivanja, obrada velikih količina podataka, određen stepen autonomije u funkcionisanju i ograničena predvidivost pojedinih ishoda. Ove karakteristike ne menjaju osnovna načela pravne odgovornosti, ali utiču na procenu načina upotrebe sistema, obaveza nadzora i stepena pažnje koji se zahteva od subjekata koji ih razvijaju ili primenjuju, naročito u oblastima u kojima primena AI sistema može uticati na ostvarivanje osnovnih prava [2].

Sa stanovišta menadžmenta, upotreba veštačke inteligencije zahteva sistematsko upravljanje rizicima. To podrazumeva identifikovanje mogućih štetnih posledica, procenu verovatnoće njihovog nastupanja, određivanje kontrolnih mehanizama i uspostavljanje odgovornosti u okviru organizacije. Upravljanje rizicima upotrebe veštačke inteligencije nije ograničeno

na tehničku bezbednost sistema, već obuhvata i pravne, organizacione i reputacione rizike.

Poseban značaj ima činjenica da sistemi veštačke inteligencije mogu biti upotrebljeni u oblastima koje su neposredno povezane sa zaštitom osnovnih prava, bezbednošću i zakonitošću postupanja. Zbog toga upravljanje njihovom upotrebom mora uključiti ne samo tehnički nadzor, već i jasna pravila odgovornosti, dokumentovanje odluka i kontrolu načina primene u konkretnim procesima [3].

3. VEŠTAČKA INTELIGENCIJA KAO IZVOR PRAVNIH I KRIVIČNOPRAVNIH RIZIKA

U krivičnopravnom smislu, veštačka inteligencija ne može biti subjekt odgovornosti, već se može posmatrati kao sredstvo kojim ljudski subjekti ostvaruju određene radnje. Kao i druga tehnička sredstva, sistemi veštačke inteligencije mogu biti korišćeni radi olakšavanja, ubrzavanja ili prikrivanja izvršenja protivpravnih radnji. Njihova tehnička složenost ne menja osnovno pravilo da se krivična odgovornost vezuje za fizička lica, a pod uslovima posebnog zakona i za pravna lica [3, 12].

Savremena teorija krivičnog prava suočava se sa ozbiljnim izazovima kada primenjuje klasične koncepte *actus reus* i *mens rea* na situacije u kojima je šteta prouzrokovana autonomnim sistemima. *Actus reus*, koji podrazumeva voljnu radnju ili propuštanje, teško je pripisati sistemu koji samostalno donosi odluke na osnovu obučениh modela, a ne neposredne ljudske direktive. *Mens rea*, odnosno krivična namera, znanje o okolnostima dela, bezobzirnost ili nehat, još je problematičnija kategorija, budući da AI sistemi ne poseduju svest niti subjektivnu nameru u pravnom smislu [6]. U savremenoj literaturi se kao odgovor na ove izazove predlažu dva osnovna pristupa: primena doktrine dozvoljenog rizika, koja omogućava procenu odgovornosti na osnovu standardizovanih obaveza nadzora, i uvođenje posebnih krivičnih dela ugrožavanja koja bi bila primenljiva na situacije u kojima upotreba AI sistema stvara opasnost po zaštićena dobra [11]. Jedan od uticajnih teorijskih pristupa ovom problemu razvio je Gabriel Hallevy, koji predlaže tri modela pripisivanja odgovornosti, razvijena pre svega u monografiji *When Robots Kill: Artificial Intelligence under Criminal Law* (2013) i pratećim radovima [7]: model izvršenja putem drugog lica (*perpetration-by-another*), u kome lice koristi AI sistem kao „oruđe” za izvršenje dela; model prirodne i verovatne posledice (*natural and probable consequence*), zasnovan na doktrini saučesničke odgovornosti iz anglosaksonskog krivičnog prava — prema kojoj je saučesnik odgovoran za predvidive posledice krivičnog dela koje je pomogao — a koju Hallevy adaptira na AI kontekst: korisnik je odgovoran kada je primena AI

sistema bila predvidivi uzrok zabranjene posledice, iako učinilac nije neposredno izvršio radnju dela; i model neposredne odgovornosti (direct liability), koji polazi od pretpostavke da sistem ispoljava funkcionalnu autonomiju dovoljnu da mu se pripiše radnja, ali koji je u akademskoj literaturi uglavnom ocenjen kao pozitivnopravno neprimenjiv u savremenim uslovima, jer aktuelni AI sistemi ne dosežu stepen autonomije koji bi opravdao pripisivanje krivične radnje samom sistemu [7]. Od praktičnog značaja za krivičnopravnu analizu stoga ostaju pre svega prva dva modela [6, 11].

Pravni, a naročito krivičnopravni rizici, nastaju u situacijama u kojima se sistemi veštačke inteligencije koriste za automatizovanu obradu podataka, profilisanje, nadzor, generisanje obmanjujućih sadržaja ili donošenje odluka koje mogu proizvesti štetne posledice po prava pojedinaca. U takvim slučajevima relevantno je pitanje da li je postojala dužna pažnja u razvoju, primeni i nadzoru nad sistemom, kao i da li je korisnik mogao i morao predvideti mogućnost nastupanja zabranjene posledice. U literaturi se sve više ističe i pristup koji *actus reus* tumači funkcionalno, a ne mehanički; relevantna „radnja” ne mora biti trenutni čin sistema, već ukupnost odluka koje su omogućile štetan ishod: izbor podataka za obuku, definisanje parametara rizika, testiranje i nadgledanje sistema [8].

Kod procene umišljaja i nehata poseban značaj ima odnos ljudskog subjekta prema mogućim posledicama upotrebe sistema. Automatizacija pojedinih faza rada ne isključuje odgovornost ukoliko je lice bilo svesno načina funkcionisanja sistema i mogućnosti da njegova upotreba dovede do protivpravne posledice. Takođe, ograničena predvidivost pojedinih ishoda ne isključuje nehat kada je lice bilo dužno i moglo da predvidi tipične rizike povezane sa upotrebom sistema [3]. U tom kontekstu posebno je relevantan doktrinarni koncept dozvoljenog rizika i odgovornosti za organizacione propuste. Iako Krivični zakonik Republike Srbije ne uređuje dozvoljeni rizik kao poseban opšti institut pod tim nazivom, procena dopuštenosti rizika može biti relevantna pri oceni protivpravnosti, krivice, nehata i dužne pažnje u konkretnom slučaju. Ovaj pristup je u akademskoj literaturi analiziran u analogiji sa regulatornom praksom u avioindustriji i farmaceutskom sektoru, gde se odgovornost ne procenjuje prema izolovanom događaju, već prema celokupnom sistemu upravljanja i preventivnih protokola [6]. Sa stanovišta upravljanja rizicima, posebno je važno pitanje ljudskog nadzora. Ukoliko organizacija ne uspostavi odgovarajuće mehanizme kontrole, procedure provere i raspodelu odgovornosti, povećava se rizik od nastupanja štetnih posledica, ali i od otežanog utvrđivanja odgovornosti u konkretnom slučaju. Zbog toga upravljanje upotrebom veštačke inteligencije mora biti povezano sa organizacionom strukturom, internim pravi-

lima i dokumentovanjem procesa odlučivanja. Savet Evrope u okviru Komiteta za krivičnopravna pitanja (CDPC) prepoznaje ovu problematiku i razvija instrumente koji bi usmerili nacionalne zakonodavce ka odgovarajućim mehanizmima krivičnopravne zaštite u kontekstu upotrebe AI sistema [3].

4. PRAVNI OKVIR EVROPSKE UNIJE I SAVETA EVROPE

Na nivou Evropske unije i Saveta Evrope razvijen je višeslojan normativni okvir koji se tiče upotrebe veštačke inteligencije. Za potrebe ovog rada ključno je razlikovati instrumente prema njihovoj svrsi. AI Act (Uredba EU 2024/1689) regulatorni je instrument koji klasifikuje AI sisteme prema nivou rizika i propisuje obaveze za subjekte koji ih razvijaju, stavljaju na tržište ili koriste, sa primarnim fokusom na tržišnu regulaciju i bezbednost [1]. Sam po sebi ne uvodi krivičnopravnu odgovornost, ali posredno utiče na krivičnopravnu procenu utoliko što definiše standarde dužne pažnje čije kršenje može biti relevantno za ocenu protivpravnosti i krivice u nacionalnim krivičnopravnim sistemima.

Neposredno relevantan za krivičnopravnu analizu jeste rad Komiteta za krivičnopravna pitanja Saveta Evrope (CDPC), koji je 2020. godine objavio Studiju izvodljivosti o veštačkoj inteligenciji i krivičnom pravu [3]. Ovaj dokument polazi od toga da postojeće krivičnopravne kategorije (umišljaj, nehat, uzročnost i propuštanje dužnog nadzora) mogu biti primenjene i na situacije koje uključuju AI sisteme, ali naglašava da je za to neophodno razviti specifične standarde koji uzimaju u obzir tehničke osobenosti ovih sistema: autonomnost, nepredvidivost pojedinih ishoda i složenost lanca odlučivanja. CDPC posebno ističe značaj uspostavljanja obaveza dokumentovanja i ljudskog nadzora kao preduslova za smislenu krivičnopravnu procenu.

Na nivou građanskog prava, važan korak ka sveobuhvatnom uređenju odgovornosti za štetu prouzrokovanu AI sistemima predstavlja nova Direktiva o odgovornosti za neispravne proizvode Evropske unije (Direktiva EU 2024/2853), doneta 23. oktobra 2024, objavljena u Službenom listu EU 18. novembra 2024. i stupila na snagu 8. decembra 2024. godine [9]. Ova Direktiva eksplicitno proširuje pojam „proizvoda” tako da obuhvati softver, što je relevantno i za AI sisteme zasnovane na softveru, uvodi olakšice u teretu dokazivanja za oštećene u složenim tehnološkim sporovima i predviđa obavezu otkrivanja relevantnih dokaza i dokumentacije. Iako se i ova direktiva bavi građanskom, a ne krivičnom odgovornošću, standardi dužne pažnje koje ona uspostavlja - naročito u pogledu bezbednosti softvera i AI sistema tokom njihovog životnog ciklusa, uz obavezu država članica da direk-

tivu transponuju do 9. decembra 2026. godine - mogu posredno uticati na krivičnopravnu procenu u nacionalnim sistemima, na sličan način na koji regulatorna neusklađenost u avioindustriji ili farmaceutskom sektoru može biti relevantna za utvrđivanje organizacionih propusta u krivičnom postupku.

Najznačajniji opšti međunarodnopravni instrument Saveta Evrope relevantan za procenu zakonitosti upotrebe AI sistema jeste Okvirna konvencija Saveta Evrope o veštačkoj inteligenciji i ljudskim pravima, demokratiji i vladavini prava, otvorena za potpisivanje 5. septembra 2024. godine [10]. Reč je o prvom međunarodnom pravno obavezujućem ugovoru koji direktno povezuje upotrebu AI sistema sa poštovanjem standarda vladavine prava i zaštite ljudskih prava. Za razliku od AI Act-a, ovaj instrument nije ograničen na tržišnu regulaciju, već postavlja normativne zahteve koji mogu biti relevantni za procenu zakonitosti upotrebe AI sistema u kontekstu krivičnopravne zaštite. Konvencija je otvorena i za potpisivanje od strane država koje nisu članice EU. Republika Srbija, kao članica Saveta Evrope, bila je uključena u rad Komiteta za veštačku inteligenciju (CAI), koji je pored država članica Saveta Evrope uključivao i države posmatračice i predstavnike međunarodnih organizacija [14]. Međutim, prema dostupnom stanju u registru Saveta Evrope, Republika Srbija nije navedena kao potpisnica Konvencije [15]. S tim u vezi, Konvencija za Srbiju nema neposredno obavezujuću pravnu snagu. Njen normativni sadržaj - naročito zahtevi u pogledu ljudskog nadzora, transparentnosti i odgovornosti - relevantan je kao neobavezujući referentni okvir za dalji razvoj domaćeg zakonodavstva.

5. PRAVNI OKVIR REPUBLIKE SRBIJE

U Republici Srbiji ne postoji poseban zakon koji bi sveobuhvatno uređivao upotrebu veštačke inteligencije u pravnom i krivičnopravnom kontekstu. Zbog toga se pitanja odgovornosti za posledice njene upotrebe sagledavaju prvenstveno kroz postojeće institute Krivičnog zakonika Republike Srbije i druge opšte propise [4], a kada je reč o pravnim licima — kroz Zakon o odgovornosti pravnih lica za krivična dela (*Sl. glasnik RS*, br. 97/2008) [12]. Takav pristup znači da se veštačka inteligencija posmatra kao savremeno tehničko sredstvo, dok odgovornost ostaje vezana za fizička i pravna lica.

Važeći normativni okvir omogućava primenu instituta umišljaja i nehata i u slučajevima kada je krivično delo izvršeno uz pomoć sistema veštačke inteligencije. Institut umišljaja uređen je čl. 25 KZ RS, koji razlikuje direktni umišljaj (učinilac je bio svestan svog dela i hteo njegovo izvršenje) i eventualni umišljaj (učinilac je bio svestan da usled njegovog činjenja ili nečinjenja može nastupiti zabranjena

posledica, pa je na to pristao), dok je nehat definisan čl. 26 KZ RS kao svesni nehat (učinilac je bio svestan mogućnosti nastupanja posledice, ali je olako smatrao da do nje neće doći) i nesvesni nehat (učinilac nije bio svestan mogućnosti nastupanja zabranjene posledice, iako je bio dužan i mogao biti svestan). U kontekstu upotrebe AI sistema, posebno je relevantno pitanje svesnog nehata - kada je lice bilo svesno mogućnosti nastupanja zabranjene posledice usled upotrebe sistema, ali je olako smatralo da do nje neće doći. Međutim, odsustvo posebnih pravila o razvoju, nadzoru i upotrebi ovih sistema dovodi do određenih ograničenja. Prvo, domaći pravni okvir ima pretežno reaktivan karakter u odnosu na upotrebu AI sistema, budući da ne predviđa posebna krivična dela ugrožavanja ni ex ante standarde ponašanja prilagođene specifičnostima ovih tehnologija, te interveniše pre svega tek nakon nastupanja štetne posledice kroz opšte institute krivičnog prava. Drugo, ne postoje unapred definisani standardi ponašanja koji bi olakšali procenu dužne pažnje i organizacionih propusta.

Sa stanovišta menadžmenta, posebno je važno pitanje odgovornosti organizacija koje razvijaju ili koriste sisteme veštačke inteligencije. Kada ne postoje precizni standardi usklađenosti, unutrašnje kontrole i raspodele odgovornosti, povećava se pravna neizvesnost u vezi sa procenom organizacionih propusta. To je naročito značajno u slučajevima kada su u razvoj i primenu sistema uključeni različiti subjekti, kao što su proizvođači, korisnici, rukovodioci i druga odgovorna lica.

Strategijski dokumenti Republike Srbije prepoznaju značaj razvoja veštačke inteligencije za društvo i privredu. Strategija razvoja veštačke inteligencije u Republici Srbiji za period 2020–2025. i Strategija razvoja veštačke inteligencije u Republici Srbiji za period od 2025. do 2030. godine predstavljaju važne planske dokumente, ali nemaju karakter neposredno obavezujućih normi u oblasti krivičnog prava [5, 13]. Zbog toga postojeći okvir omogućava sankcionisanje zloupotreba, ali ne obezbeđuje isti stepen normativne razrađenosti i pravne sigurnosti koji pružaju instrumenti Saveta Evrope relevantni za krivičnopravnu procenu upotrebe sistema veštačke inteligencije.

6. KOMPARATIVNA ANALIZA OKVIRA SAVETA EVROPE, EVROPSKE UNIJE I REPUBLIKE SRBIJE

Komparativna analiza u ovom radu usmerena je na krivičnopravne instrumente i mehanizme koji u razmatranim okvirima uređuju odgovornost za posledice upotrebe veštačke inteligencije. AI Act se u tom kontekstu posmatra kao regulatorni okvir koji posredno utiče na krivičnopravnu procenu, pre svega kroz utvrđivanje standarda dužne pažnje, ali sam po sebi

nije krivičnopравни instrument i ne može biti neposredna osnova krivičnopravne odgovornosti. Relevantna osnova za poređenje su, nasuprot tome, opšti instituti krivičnog prava, instrumenti Saveta Evrope usmereni na krivičnopravnu problematiku AI, i Okvirna konvencija o veštačkoj inteligenciji iz 2024. godine [3, 10].

Na nivou krivičnopравnih instrumenata, razmatrani okviri polaze od istog načela: veštačka inteligencija nije i ne može biti subjekt krivične odgovornosti. Odgovornost ostaje vezana za fizička i pravna lica koja odlučuju o razvoju, primeni i nadzoru AI sistema [3, 4]. U tom pogledu nema suštinske razlike između pristupa Saveta Evrope, budući da izveštaj CDPC-a iz 2020. godine polazi od mogućnosti primene postojećih krivičnopравnih kategorija uz neophodne prilagodbe, i srpskog Krivičnog zakonika, koji pruža normativni okvir za primenu umišljaja i nehata u situacijama koje uključuju upotrebu AI sistema, uz napomenu da se krivična odgovornost pravnih lica ne uređuje Krivičnim zakonikom, već posebnim Zakonom o odgovornosti pravnih lica za krivična dela (*Sl. glasnik RS*, br. 97/2008) [12].

Međutim, između evropskog i srpskog okvira postoji značajna razlika u pogledu ex ante (unapred postavljenih) standarda koji usmeravaju tumačenje krivičnopравnih kategorija u kontekstu AI. Na nivou Saveta Evrope, Okvirna konvencija iz 2024. godine i CDPC instrumenti postavljaju konkretne zahteve u pogledu ljudskog nadzora, transparentnosti i dokumentovanja, koji se mogu koristiti kao normativni parametar pri proceni dužne pažnje, nehata i krivice u konkretnom slučaju [3, 10].

Pravo Evropske unije, pre svega kroz AI Act, dodatno doprinosi definisanju standarda upravljanja rizicima, ali posredno, jer AI Act nije krivičnopравни instrument [1]. U srpskom pravnom sistemu takvi posebni standardi ne postoje, što otežava krivično-pravnu procenu u složenim slučajevima koji uključuju autonomne sisteme i veći broj aktera [4].

Posebno je ilustrativna razlika u pristupu pitanju umišljaja i nehata. U teorijskom okviru koji je razvio Hallevey, kao i u savremenim raspravama o actus reus i mens rea u AI kontekstu, ključno pitanje je da li je subjekt bio dužan i mogao da predvidi tipične rizike sistema koji je koristio [7, 8].

Tamo gde postoje jasni ex ante standardi, kao što su zahtevi CDPC-a ili Okvirne konvencije, ta procena je znatno lakša jer postoji normativni standard koji definiše šta se smatra pažljivim postupanjem. U odsustvu takvih standarda, kakva je situacija u Republici Srbiji, sudovi su upućeni na opšte standarde profesionalne pažnje, što nužno uvodi veću pravnu neizvesnost.

Sa stanovišta upravljanja rizicima u organizacijama, ova razlika ima praktične posledice. Organizacije koje posluju u jurisdikcijama sa jasnim ex ante standardima mogu strukturirati interne procedure usklađenosti prema definisanim normama i na taj način smanjiti ne samo regulatorni, već i krivičnopравни rizik. U odsustvu takvih standarda, kao što je slučaj u Srbiji, organizacioni propusti u razvoju ili primeni AI sistema teže je ex post (naknadno) utvrditi i pripisati konkretnim odgovornim licima, što može imati dvojak efekat: otežano krivično gonjenje, ali i nedovoljnu preventivnu funkciju krivičnog prava.

Zajednička tačka razmatranih okvira ostaje načelo da krivičnopravna odgovornost za posledice upotrebe veštačke inteligencije pripada subjektima koji su donosili ključne odluke u procesu razvoja, primene i nadzora sistema, odnosno fizičkim i, kada su ispunjeni zakonski uslovi, pravnim licima. Razlika nije u tom temeljnom principu, već u tome koliko je pravni sistem opremljen normativnim standardima koji taj princip operacionalizuju u konkretnim slučajevima koji uključuju autonomne, složene i teško predvidive AI sisteme.

7. ZAKLJUČAK

Analiza krivičnopравnog okvira upotrebe veštačke inteligencije pokazuje da razvoj savremenih digitalnih tehnologija stvara nove izazove u oblasti upravljanja rizicima i krivičnopравne odgovornosti. Sistemi veštačke inteligencije mogu značajno unaprediti efikasnost i automatizaciju brojnih procesa, ali njihova primena istovremeno može dovesti do pojave novih pravnih i organizacionih rizika, naročito kada se koriste na način koji može prouzrokovati povredu pravno zaštićenih dobara.

Sprovedena analiza pokazuje da razmatrani okviri Saveta Evrope, Evropske unije i Republike Srbije raspolazu normativnom osnovom za utvrđivanje krivičnopравne odgovornosti u slučajevima upotrebe veštačke inteligencije, ali se bitno razlikuju u stepenu razrađenosti tih osnova. Zajednički temelj jeste načelo da veštačka inteligencija ne može biti subjekt krivične odgovornosti.

Na tom principu počivaju instrumenti Saveta Evrope, pre svega Studija izvodljivosti CDPC-a iz 2020. i Okvirna konvencija iz 2024. godine, kao i srpski Krivični zakonik [3, 4, 10]. Ključna razlika, međutim, leži u stepenu normativne razrađenosti: na evropskom nivou postoje posebni standardi koji operacionalizuju pravne kategorije relevantne za AI kontekst, dok srpski pravni sistem još uvek ne raspolaže odgovarajućim posebnim normama.

Sa stanovišta savremenog menadžmenta tehnologije, upravljanje krivičnopравnim rizicima upotrebe veštačke inteligencije zahteva uspostavljanje jasnih

organizacionih procedura, sistema nadzora i raspodele odgovornosti. Dalji razvoj normativnog okvira u Republici Srbiji, oslanjajući se na instrumente Saveta Evrope relevantne za krivičnopravnu procenu upotrebe sistema veštačke inteligencije, može doprineti efikasnijem upravljanju tim rizicima i boljoj usklađenosti između tehnološkog razvoja i krivičnopravne zaštite društvenih vrednosti.

LITERATURA

- [1] European Union. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence. *Official Journal of the European Union*, OJ L 2024/1689, 12.7.2024, 2024.
- [2] European Union Agency for Fundamental Rights. *Getting the future right – Artificial intelligence and fundamental rights*. Luxembourg: Publications Office of the European Union, 2020.
- [3] European Committee on Crime Problems (CDPC), Council of Europe. *Feasibility Study on a Future Council of Europe Instrument on Artificial Intelligence and Criminal Law*. CDPC(2020)3Rev. Strasbourg, 4 September 2020.
- [4] Republika Srbija. Krivični zakonik Republike Srbije. *Službeni glasnik Republike Srbije*, br. 85/2005, 88/2005 – ispr., 107/2005 – ispr., 72/2009, 111/2009, 121/2012, 104/2013, 108/2014, 94/2016, 35/2019 i 94/2024.
- [5] Republika Srbija. Strategija razvoja veštačke inteligencije u Republici Srbiji za period 2020–2025. *Službeni glasnik Republike Srbije*, br. 96/2019. Beograd, 2019.
- [6] Lagioia, F, Sartor, G. AI Systems Under Criminal Law: a Legal Analysis and a Regulatory Perspective. *Philosophy & Technology*, 33(3), pp. 433–465. <https://doi.org/10.1007/s13347-019-00362-x>, 2020.
- [7] Hallevy, G. When Robots Kill: Artificial Intelligence under Criminal Law. Boston: Northeastern University Press, Videti takođe: Hallevy, G. The Basic Models of Criminal Liability of AI Systems and Outer Circles. SSRN Working Paper, 2019. Available at: <https://ssrn.com/abstract=3402527>, 2013.
- [8] Hashmi, M. A. I, Butt, M. F, Jawad, M, Sultan, S. Criminal Liability in the Age of Autonomous Systems: Rethinking Mens Rea and Actus Reus. *The Critical Review of Social Sciences Studies*, 3(3), pp. 290–303. <https://doi.org/10.59075/szb-tkr93>, 2025.
- [9] European Union. Directive (EU) 2024/2853 of the European Parliament and of the Council of 23 October 2024 on liability for defective products and repealing Council Directive 85/374/EEC. *Official Journal of the European Union*, OJ L 2024/2853, 18.11.2024.
- [10] Council of Europe. *Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law*. CETS No. 225. Vilnius, 5 September 2024.
- [11] Sachoulidou, A. AI Systems and Criminal Liability. A Call for Action. *Oslo Law Review*, Vol. 11, Iss. 1, pp. 1–10. <https://doi.org/10.18261/olr.11.1.3>, 2024.
- [12] Republika Srbija. Zakon o odgovornosti pravnih lica za krivična dela. *Službeni glasnik Republike Srbije*, br. 97/2008.
- [13] Republika Srbija. Strategija razvoja veštačke inteligencije u Republici Srbiji za period od 2025. do 2030. godine. *Službeni glasnik Republike Srbije*, br. 5/2025.
- [14] Council of Europe. Committee on Artificial Intelligence (CAI), official website: composition, meetings and participant lists. Strasbourg: Council of Europe.
- [15] Council of Europe. The Framework Convention on Artificial Intelligence: Signatures and Ratifications. Strasbourg: Council of Europe.

SUMMARY

MANAGING CRIMINAL-LAW RISKS IN THE USE OF ARTIFICIAL INTELLIGENCE: THE FRAMEWORK OF THE COUNCIL OF EUROPE AND THE REPUBLIC OF SERBIA, WITH REFERENCE TO EUROPEAN UNION LAW

The increasing use of artificial intelligence systems raises important questions regarding criminal liability and the management of legal risks associated with their application. A particular challenge is determining how existing criminal law concepts apply when AI systems are used in ways that may result in harm to legally protected interests, and whether current normative frameworks are adequately equipped to address such situations. The aim of this paper is to analyse the criminal law framework relevant to liability for the use of artificial intelligence in the Republic of Serbia, with particular emphasis on Council of Europe instruments and a supplementary overview of relevant European Union law. The paper examines the ways in which existing criminal law concepts can be applied in situations where artificial intelligence is used as a means of committing criminal offences or as part of a complex chain of decision-making leading to a prohibited consequence. The research is based on normative and comparative methods and includes an analysis of relevant institutional and legal sources, including the CDPC Feasibility Study on Artificial Intelligence and Criminal Law (2020) and the Council of Europe Framework Convention on Artificial Intelligence (2024). The analysis shows that the comparison must be grounded primarily in criminal-law instruments rather than in regulatory frameworks with different purposes. At the level of the Council of Europe, and with supplementary reference to relevant European Union regulatory law, the examined instruments provide standards concerning human oversight, transparency and accountability that may serve as normative parameters for assessing due diligence, negligence and culpability in concrete cases. In the Republic of Serbia, the absence of such specific standards creates greater legal uncertainty in complex cases involving autonomous systems and multiple actors in the chain of responsibility. All examined frameworks share the foundational principle that artificial intelligence cannot be a subject of criminal liability; responsibility remains with the human actors and, where the statutory conditions are met, legal persons involved in decisions about the development, deployment and supervision of AI systems. The results indicate that the effective management of criminal-law risks associated with the use of artificial intelligence requires well-defined normative standards, organisational control mechanisms and explicit responsibilities of entities involved in the development and use of such systems. The further development of Serbia's normative framework, drawing on Council of Europe instruments relevant to the criminal-law assessment of artificial intelligence, can contribute to more effective risk management and better alignment between technological development and criminal-law protection of social values.

Key Words: artificial intelligence, risk management, criminal liability, criminal law framework, Council of Europe, Republic of Serbia