UDK: 343.296:004.8(4-6EU) DOI: 10.51204/Internet_Dijalog_2410A

prof. dr Neda Zdraveva
redovna profesorka, Univerzitet „Sv. Kirilo i Metodije“
– Pravni fakultet „Justinijan Prvi“

ODGOVORNOST ZA ŠTETU PROUZROKOVANU UPOTREBOM SISTEMA VEŠTAČKE INTELIGENCIJE U PRAVU EVROPSKE UNIJE – STANJE I IZAZOVI

Rezime: *Predmet ovog rada je istraživanje pravnog uređenja veštačke inteligencije (AI) unutar Evropske unije (EU), a naročito pitanje odgovornosti. U radu se naročito analiziraju odredbe Direktive EU o odgovornosti za veštačku inteligenciju. Diskusija počinje sa obrazloženjem potrebe za regulacijom i odgovornošću u kontekstu AI sistema. Autorka dalje analizira svrhu regulacije. U drugom delu, veštačka inteligencija se analizira kroz pristup zasnovan na riziku, uzimajući u obzir etičke i pravne standarde koji su ključni za obezbeđivanje pouzdanosti AI. Takođe se istražuju karakteristike AI i nivoi rizika povezani sa njegovom primenom. Zahtevi usaglašenosti koje je uspostavila Uredba EU o veštačkoj inteligenciji su detaljno razmotreni, pružajući uvid u standarde koji se postavljaju kako bi se AI sistemi smatrali pouzdanim i bezbednim. Nakon toga, vrši se pregled pitanja vezanih za odgovornost za štetu koju uzrokuju AI sistemi. Ključni aspekti uključuju identifikaciju strana u potencijalnim slučajevima – tužioca i tuženog, prirodu štete, uzročnu vezu i ciljanu oborivu pretpostavku uzročnosti, kao i pretpostavku o nepoštovanju zahteva za usaglašenost, kao odraz sistema odgovornosti zasnovanog na krivici. Rad se završava raspravom o "otvorenim pitanjima" u vezi sa stvaranjem sveobuhvatnog režima odgovornosti za AI unutar EU i njihovim uticajem na nacionalne sisteme odgovornosti. Autorka ovde adresira izazove približavanja nacionalnih propisa o odgovornosti sa propisima EU, kao i izazove pri sprovođenju pravila.*

Ključne reči: *Veštačka inteligencija. – Regulacija veštačke inteligencije. – Pristup zasnovan na riziku. – Šteta. – Odgovornost zasnovana na krivici. – Objektivna odgovornost.*

1. UVOD

Tačka spajanja veštačke inteligencije (AI) i regulacije odgovornosti je (relativno) nova i dinamična pravna oblast. Nedavni empirijski podaci sugerišu da, za brojne korporacije, strahovi u vezi sa odgovornošću predstavljaju značajnu prepreku za integraciju AI. Konkretno, istraživanje

sprovedeno širom Evrope otkrilo je da 33% preduzeća odgovornost za potencijalnu štetu doživljava kao značajan izazov za uključivanje AI sistema u poslovanje.[1]

Ova zabrinutost je racionalna, ako se uzmu u obzir karakteristični rizici povezani sa AI tehnologijama, kao što su nepredvidivo ponašanje ili donošenje odluka koje odstupa od utvrđenih ljudskih standarda. Očekuje se da će ova pitanja biti ublažena (predlogom) Evropske komisije za Direktivu o odgovornosti za veštačku inteligenciju.[2] Zakonodavni okvir koji treba da uspostavi ova direktiva, ima dva opšta i tri specifična cilja.[3] Prvi opšti cilj je poboljšanje funkcionisanja unutrašnjeg tržišta smanjenjem postojećih prepreka i sprečavanjem pojave novih u prekograničnoj razmeni proizvoda i usluga sa AI (sa pozitivnim efektom na privredu i konkurentnost Evropskog AI sektora); drugi je da se doprinese 'ekosistemu poverenja' kako bi se promovisalo prihvatanje proizvoda i usluga sa veštačkom inteligencijom, tako što će se obezbediti da subjekti oštećeni upotrebom proizvoda i usluga sa veštačkom inteligencijom budu podjednako zaštićeni kao i lica koja su pretrpela štetu štetnim radnjama koje ne uključuju veštačku inteligenciju (Recital 7, AILD). Specifični ciljevi uključuju: povećanje pravne sigurnosti u vezi sa izloženošću riziku odgovornosti poslovnih aktivnosti koje uključuju AI; da spreči pojavu fragmentiranih pravila specifičnih za veštačku inteligenciju na unutrašnjem tržištu; da se spreči nedostatak naknade štete obezbeđivanjem istog nivoa zaštite u slučajevima koji uključuju AI.

Direktiva o prilagođavanju pravila vanugovorne građanske odgovornosti veštačkoj inteligenciji zasnovana je na čl. 114. Ugovora o funkcionisanju Evropske unije (UFEU), koji reguliše približavanje odredaba propisanih zakonom, uredbom ili administrativnih radnji u državama članicama koje imaju za cilj uspostavljanje i funkcionisanje unutrašnjeg tržišta. Direktiva usklađuje ciljane aspekte postojećih pravila o građanskoj odgovornosti država članica

---

1 Istraživanje evropskih preduzeća o upotrebi tehnologija zasnovanih na veštačkoj inteligenciji – Konačni izveštaj, Evropska komisija, Generalni direktorat za komunikacione mreže, sadržaj i tehnologiju, Kancelarija za publikacije, 2020, https://data.europa.eu/doi/10.2759/759368. Istraživanje je utvrdilo da svest o veštačkoj inteligenciji je visoka širom EU (78% ispitanika). Četiri od deset (42%) preduzeća su usvojila najmanje jednu AI tehnologiju, 25% je usvojilo najmanje dve, 18% planira da usvoji AI u naredne dve godine, 40% niti je usvojilo AI niti planira da to uradi. Tri ključne interne prepreke za usvajanje AI su poteškoće u zapošljavanju novog osoblja sa odgovarajućim veštinama (57%), troškovi usvajanja (52%) i troškovi prilagođavanja operativnih procesa (49%). Smanjenje neizvesnosti može biti od koristi, jer preduzeća smatraju da su odgovornost za potencijalne štete (33%), standardizacija podataka (33%) i regulatorne prepreke (29%) glavni spoljni izazovi za usvajanje AI.

2 Predlog direktive Evropskog parlamenta i Saveta o prilagođavanju pravila vanugovorne građanske odgovornosti veštačkoj inteligenciji (Direktiva o odgovornosti za veštačku inteligenciju), COM/2022/496 final; u daljem tekstu i AIDL.

3 Brifing, Adaptiranje pravila o odgovornosti na veštačku inteligenciju, Procena uticaja (SWD(2022) 319, SWD(2022) 320 (rezime); dostupno na https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/757810/EPRS_BRI%282024%29757810_EN.pdf

koja se primenjuju na AI sisteme, kako bi se poboljšali uslovi za funkcionisanje unutrašnjeg tržišta proizvoda i usluga sa AI.

Direktiva o odgovornosti za veštačku inteligenciju treba da se posmatra kao deo paketa napora EU da reguliše veštačku inteligenciju. Uredba EU o veštačkoj inteligenciji[4] (u daljem tekstu AIA) je usmerena na stvaranje ekosistema poverenja u AI, gde će AI sistemi koji se plasiraju na tržište Unije ili na drugi način utiču na ljude u Uniji biti orijentisani na ljude, bezbedni i u skladu sa zakonom. Cilj akta je obezbeđivanje bezbednosti AI sistema, poštovanje postojećih zakona o osnovnim pravima i vrednostima Unije i pravna sigurnost za investicije i inovacije u AI. Uredba uključuje zabranu određenih štetnih praksi AI, ograničenja i zaštitne mere za upotrebu daljinskog biometrijskog prepoznavanja u svrhe sprovođenja zakona, i metodologiju za definisanje "visoko rizičnih" AI sistema.

Činjenice su očigledne: tehnologija postoji, koristi se i infiltriraće se u sve više aspekata svakodnevnog života. To će nas primorati da preispitamo svoje poglede i na neke od osnovnih pravnih pojmova. Ključno pitanje je koliko pravni sistem koji se očekuje da će se uspostaviti novim EU pravilima o građanskopravnoj odgovornosti za štetu prouzrokovanu AI sistemima, teorijski i praktično, može da odgovori na potrebe prevencije štete i naknade štete.

Kada je u pitanju predlog pravnog okvira za odgovornost, nameće se nekoliko pitanja na koja ćemo pokušati da odgovorimo u ovom radu. Struktura rada će imati odštetno-pravni pristup tako što će se prvo izložiti šta je ili šta može da bude izvor opasnosti za prouzrokovanje štete AI sistema, a potom, koje su karakteristike odštetno-pravnog odnosa koji bi nastao (strane tog odnosa, opšti uslovi za nastanak odnosa, uključujući štetu, štetnu radnju i uzročnost, kao i osnov odgovornosti). Na osnovu analize ovih pitanja nastojimo da utvrdimo koji su (neki) izazovi koji proizlaze iz predloženog sistema regulacije za ostvarivanje cilja njegovog uspostavljanja – dosledan i visok nivo zaštite javnih interesa u pogledu zdravlja, bezbednosti i osnovnih prava.

4 Uredba Evropskog parlamenta i saveta o utvrđivanju usklađenih pravila o veštačkoj inteligenciji (Zakon o veštačkoj inteligenciji) i izmenama pojedinih zakonskih akata Unije, COM/2021/206 final; Stav Evropskog parlamenta usvojen u prvom čitanju 13. marta 2024. u cilju usvajanja Uredbe (EU) 2024/1689 Evropskog parlamenta i Saveta o utvrđivanju usklađenih pravila o veštačkoj inteligenciji i izmenama i dopunama Uredbe (EZ) br. /2008, (EU) br. 167/2013, (EU) br. 168/2013, (EU) 2018/858, (EU) 2018/1139 i (EU) 2019/2144 i direktive 2014/90/EU, (EU) 2016/797 i (EU) 2020/1828 (Akt o veštačkoj inteligenciji) i Ispravka stava Evropskog parlamenta usvojenog u prvom čitanju 13. marta 2024. s ciljem donošenja Uredbe (EU) 2024/... Evropskog parlamenta i Saveta o utvrđivanju usklađenih pravila o veštačkoj inteligenciji i o izmeni uredaba (EZ) br. 300/2008, (EU) br. 167/2013, (EU) br. 168/2013, (EU) 2018/858, (EU) 2018/1139 i (EU) 2019/2144 te Direktiva 2014/90/EU, (EU) 2016/797 i (EU) 2020/1828 (Akt o veštačkoj inteligenciji) P9_TA(2024)0138 (COM(2021)0206 – C9–0146/2021 – 2021/0106(COD)). Pri navođenju članova ove Uredbe korištena je verzija teksta po Ispravci stava Evropskog parlamenta iz 19.04.2024 dostupna na https://artificialintelligenceact.eu/the-act/

2. VEŠTAČKA INTELIGENCIJA KAO IZVOR RIZIKA

2.1. Osnovna (etička) pravila sistema veštačke inteligencije

U poslednjoj dekadi svedoci smo razvoja i upotrebe veštačke inteligencije u svakodnevnom životu i poslovanju. Uprkos brzini kojom tehnologija napreduje, nema opšteprihvaćene, jednoznačne i precizne definicije onoga što nazivamo veštačkom inteligencijom. Termin se odnosi na niz tehnologija uključujući programe računara, algoritme, procese i robote koji ne deluju isključivo na komandu ljudskog operatera, ali su sposobni za analitičke i izvršne funkcije (zasnovane na tehnikama velikih podataka ili automatizovanom učenju, poznato pod nazivom mašinsko učenje) koje su manje-više nezavisne. Metod mašinskog učenja se zasniva na obradi takozvanih podatka za obuku, uz pomoć kojih algoritam uči-prepoznaje obrasce i razvija pravila. Duboko učenje, oblik mašinskog učenja, koristi strukture tipa neuronskih mreža, zasnovane donekle na funkcionisanju ljudskog mozga, koje uče vežbanjem i povratnim informacijama. Rezultat ovog naprednog razvoja tehnologije je da kroz korišćenje algoritama, sistemi AI mogu praktično da uče sami, da postanu autonomni i da se prilagođavaju.

Uredbom o veštačkoj inteligenciji EU, takođe se pokušava definisati veštačka inteligenciju u cilju konstruisanja regulatornog okvira. AIA (čl. 3(1/1)) opisuje pojam sistema veštačke inteligencije – a ne apstraktni koncept veštačke inteligencije: 'Za svrhu(e) Uredbe[,] sistem veštačke inteligencije (AI sistem) označava mašinski-zasnovan sistem koji je dizajniran da radi sa različitim nivoima autonomije i koji može pokazati prilagodljivost nakon postavljanja, i koji, za eksplicitne ili implicitne ciljeve, zaključuje, na osnovu ulaznih podataka koje prima, kako da generiše rezultate kao što su predviđanja, sadržaj, preporuke ili odluke koje mogu uticati na fizičko ili virtuelno okruženje.' Definicija teži ka tome da bude što neutralnija.[5]

Ključno pitanje u utvrđivanju pravila o odgovornosti za štetu je kakva treba da bude veštačka inteligencija. Pravna pravila predviđena Uredbom EU o veštačkoj inteligenciji su pravila za etičku usaglašenost i primenjuju se na sve AI sisteme. U ovom smislu treba da se ima u vidu da li se ta usaglašenost može verifikovati za bilo koji AI sistem koji deluje u bilo kojoj situaciji.[6]

Veštačka inteligencija kojoj se može verovati – pouzdana AI[7] ima tri komponente, koje bi trebalo da budu ispunjene u celom životnom ciklusu celog sistem: (1) zakonitost – AI treba da bude zakonita, u skladu sa svim

5 Z.G. Balogh,. „Liability for Damage Caused by AI Entities." *Acta Universitatis Sapientiae: Legal Studies*, vol. 11, no. 2, 2022, 5–18.

6 L. Brennan, „AI Ethical Compliance Is Undecidable," *Hastings Science and Technology Law Journal 14*, no. 2, 2023, str. 315.

7 Evropska komisija, Etičke smernice za pouzdanu veštačku inteligenciju, Ekspertska grupa visokog nivoa za veštačku inteligenciju, 2019, str. 5; https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai

važećim zakonima i propisa, (2) iskazivanje etičkog ponašanja – da obezbedi poštovanje etičkih principa i vrednosti i (3) robusnost – AI bi trebalo da bude robusna, kako sa tehničke tako i sa socijalne perspektive, jer čak i iz dobre namere, sistemi veštačke inteligencije mogu prouzrokovati nenamernu štetu. Ovi osnovni principi su transponovani u sedam dodatnih posebnih zahteva za postizanje pouzdane veštačke inteligencije: (1) ljudsko delovanje i nadzor; (2) tehnička robusnost i sigurnost; (3) privatnost i upravljanje podacima; (4) transparentnost; (5) različitost, nediskriminacija i pravičnost; (6) društveno i ekološko blagostanje; (7) odgovornost. Artikulisani koncept pouzdane veštačke inteligencije zasnovan je na evropskoj doktrini o osnovnim pravima i odgovarajućem skupu etičkih principa koji su ključni u kontekstu veštačke inteligencije. Etičke smernice su razvijene u skladu sa osnovnim vrednostima utvrđene Ugovorima i Poveljom EU: (1) poštovanja ljudske autonomije, (2) sprečavanje štete, (3) pravičnost i (4) objašnjivost.

Sprečavanje štete, kao princip, označava da sistemi veštačke inteligencije ne bi trebalo da uzrokuju niti uvećavaju štetu ili na drugi način negativno utiču na ljudska bića. Ovo podrazumeva zaštitu ljudskog dostojanstva, mentalnog i fizičkog integriteta. Sistemi veštačke inteligencije i okruženja u kojima oni rade moraju biti bezbedni i sigurni. Posebna pažnja, po Smernicama, se mora obratiti na situacije u kojima sistemi veštačke inteligencije mogu da izazovu ili uvećaju štetne uticaje zbog asimetrije moći ili informacija, kao što su odnosi između poslodavaca i zaposlenika, preduzeća i potrošača ili vlade i građana.[8]

Ovi principi, kao i način uspostavljanja i funkcionisanja sistema veštačke inteligencije, svoj pravni odraz dobijaju u Uredbi o AI. Imajući u vidu da se pravila uredbe protežu i na subjekte koji su izvan Evropske unije, uticaj sistema[9] koje će se uspostaviti Uredbom je utoliko značajniji.

2.2. Rizici, zabrane i obaveze za AI sisteme

Jedan od ciljeva Uredbe je da obezbedi dosledan i visok nivo zaštite javnih interesa u pogledu zdravlja, bezbednosti i osnovnih prava. U ovom kontekstu na Uredbu se gleda kao na instrument koji treba da uspostavi zajedničke normativne standarde za sve visoko-rizične sisteme veštačke inteligencije. Ti standardi treba da budu u skladu sa Poveljom o osnovnim pravima Evropske unije (Povelja) i treba da budu nediskriminatorni i u skladu sa međunarodnim trgovinskim obavezama Unije.[10] Da bi se uveo proporcionalan i efikasan skup obavezujućih pravila za sisteme veštačke inteligencije, Uredba propisuje da treba slediti jasno definisan pristup zasnovan na riziku. Taj pristup treba da prilagodi vrstu i sadržaj takvih pravila intenzitetu i obimu rizika

8 *Ibid,* str. 12.

9 J. Williams, N. G. Kohne, M. A. Reed, J. Arlington, „New Proposed EU AI Regulation Extends beyond Europe," *RAIL: The Journal of Robotics, Artificial Intelligence & Law* 4, no. 5 /2021, 383–388.

10 Recital 1, AIA.

koje sistemi veštačke inteligencije mogu da generišu.[11] Stoga, Uredba propisuje neophodne zabrane određenih praksi veštačke inteligencije, utvrđuje zahteve za visoko-rizične sisteme veštačke inteligencije i obaveze za relevantne operatere, kao i obaveze transparentnosti za određene AI sisteme.

Uredba identifikuje četiri nivoa rizika[12] – AI sisteme koje predstavljaju neprihvatljiv rizik (zabranjene AI sisteme), visok rizik (predmet usaglašavanja sa obaveznim zahtevima), specifičan rizik (obaveze transparentnosti za one koje su u interakciji sa fizičkim licima) i ne-visok-rizik (dobrovoljno usvojeni kodeksi ponašanja). Odgovornost je preduzeća da procene Al sisteme koje dobavljaju ili uvode i utvrde u koju grupu rizika spadaju.[13]

2.2.1. Zabranjeni AI sistemi

Uredba EU o veštačkoj inteligenciji striktno zabranjuje stavljanje na tržište, stavljanje u upotrebu ili korišćenje sistema veštačke inteligencije koji potencijalno nanosi štetu pojedincima i društvu. To uključuje (Čl. 5, AIA):

1. Sistemi veštačke inteligencije koji primenjuju podsvesne tehnike. Ovo se odnosi na sisteme veštačke inteligencije koji primenjuju podsvesne tehnike izvan čovekove svesti ili namerno manipulativne ili obmanjujuće tehnike, sa ciljem ili efektom materijalnog iskrivljavanja ponašanja osobe ili grupe osoba (Čl. 5(1(a)), AIA). U literaturi se nalazi da nedostatak definicije 'podsvesnih tehnika' u Uredbi omogućava brojne forme manipulacije zasnovane na AI.[14]
2. AI sistem koji praktikuje iskorišćavanje osetljivosti. Ovo se odnosi na sisteme veštačke inteligencije koji iskorišćavaju bilo koju osetljivost fizičkog lica ili određene grupe lica zbog njihovog uzrasta, invaliditeta ili specifične socijalne ili ekonomske situacije sa ciljem da se promeni njihovo ponašanje, čime im se nanosi neka šteta (Čl. 5(1(b), AIA).
3. AI sistemi za evaluaciju ili klasifikaciju fizičkih lica ili grupa lica. Ovo se odnosi na sisteme koji tokom određenog vremenskog perioda evaluiraju ili klasifikuju fizička lica ili grupu lica na osnovu njihovog socijalnog ponašanja, ličnih osobina, sa socijalnim rezultatom koji vodi do štetnog ili nepovoljnog tretmana ovih osoba (i) u socijalnim kontekstima koji nisu povezani sa kontekstima u kojima su podaci prvobitno generisani ili prikupljeni i/ili (ii) koji je neo-

11 Recital 26, AIA.

12 Čl. 3 (1/2), AIA: „rizik" znači kombinacija verovatnosti nastanka štete i težine te štete.

13 Prema čl.u 6 (4) dobavljač koji smatra da AI sistem naveden u Prilogu III nije visoko rizičan treba da dokumentuje svoju procenu pre nego što taj sistem stavi na tržište ili ga stavi u upotrebu. Takav dobavljač će biti obavezan da se registruje u EU bazi podataka (prema obavezi iz čl.a 49(2) u vezi sa čl.om 71), a na zahtev nacionalnih nadležnih organa treba da pruži dokumentaciju o proceni.

14 Mezei K, Trager A., "The European Approach to Artificial Intelligence. Ethical and Regulatory Implications." *Acta Universitatis Sapientiae: Legal Studies*, vol. 11, no. 2, 2022, str. 25 i citirani autori (f. 21).

pravdan ili nesrazmeran njihovom socijalnom ponašanju ili njegovoj težini (Čl. 5(1(c), AIA).

4. Sistem koji omogućuje procene rizika od fizičkih lica: Odnosi se na AI sisteme za izradu procena rizika fizičkih lica u cilju procene ili predviđanja rizika od izvršenja krivičnog dela fizičkog lica, isključivo na osnovu profilisanja fizičkog lica ili procene njegovih osobina i karakteristika ličnosti (Čl. 5(1(d), AIA).
5. AI sistem za stvaranje baza podataka za prepoznavanje lica: odnosi se na AI sisteme koje kreiraju ili proširuju baze podataka za prepoznavanje lica putem neciljanog prikupljana slika lica sa interneta ili nadzornih snimaka (Čl. 5(1(e), AIA);
6. AI sistema za prepoznavanje emocija: odnosi se na one sisteme koje donose zaključke o emocijama fizičkog lica na radnom mestu ili u obrazovnim institucijama, osim kada je upotreba AI sistema namenjena za medicinske ili bezbednosne razloge (čl. 5(1(f), AIA);
7. Sistemi biometrijske kategorizacije: ovo se odnosi na sisteme koji individualno kategorišu fizička lica na osnovu njihovih biometrijskih podataka da bi se na taj način zaključivalo o njihovoj rasi, političkim mišljenjima, članstvu u sindikatu, verskoj pripadnosti ili filozofskim uverenjima, seksualnom životu ili seksualnoj orijentaciji. Pri tom ova zabrana se ne odnosi na zakonito stečene biometrijske podatke u oblasti sprovođenja zakona (čl. 5(1(h), AIA);
8. Sistemi biometrijske identifikacije na javnim prostorima: obuhvata sisteme koji u realnom vremenu iz daljine rade biometrijsku identifikaciju za potrebe sprovođenja zakona. Izuzeci postoje ako se radi o potragama za nestalim osobama; sprečavanju konkretne, značajne i neposredne pretnje po život ili fizičku bezbednost fizičkih lica ili terorističkog napada i otkrivanju, lokalizaciji, identifikaciji ili krivičnom gonjenju počinioca ili osumnjičenog za krivična dela određena uredbom.[15] U vezi sa navedenim izuzecima, propisana su ograničenja u koju svrhu oni mogu da se primene[16] i postupka koji treba da se sprovede da bi se izuzeci primenili.[17]

---

15 Aneks II, Lista krivičnih dela, koja obuhvaća dela kao: *terorizam, trgovanje ljudima, seksualno iskorištavanje dece i dečja pornografija, nezakonita trgovina opojnim drogama i psihotropnim supstancama, nezakonita trgovina oružjem, municijom i eksplozivima, ubistvo i teška telesna povreda, nedozvoljena trgovina ljudskim organima, kidnapovanje, uzimanje talaca, silovanje, kaznena dela u nadležnosti Međunarodnog krivičnog suda i dr. Prethodna verzija teksta je upućivala na krivična dela obuhvaćena pravilima Evropskog naloga za hapšenje i bila je znatno šira, a ovo skraćenje ide u prilog zaštiti osnovnih prava.*

16 Uredba (EU) 2016/679 Evropskog parlamenta i Saveta od 27. aprila 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), *SL L 119, 4.5.2016, 1–88.*

17 Pri tome, po čl. 5(2), AIA upotreba ovih sistema za potrebe sprovođenja zakona je ograničeno samo na potvrđivanje identiteta specijalno targetirane osobe, a treba da uzme u obzir prirodu situacije, uključujući ozbiljnost, verovatnoću i razmere štete ako se sistem ne koristi. Takođe, pri oceni dali se sistem treba upotrebiti, treba se razmo-

2.2.2. AI sistemi koji su dozvoljeni i zahtevi za usklađivanje

Visoko-rizični AI sistemi i oni koji predstavljaju specifičan rizik su dozvoljeni pod određenim uslovima predviđenim AI Aktom. AI sistemi koji nisu visoko rizični su predmet samoregulacije. Imajući u vidu da se pitanje odgovornosti vezuje za poštovanje obaveza za usklađivanje, u centru razmatranja ovog dela rada su zahtevi za usklađivanje koji su predviđeni za različite grupe AI sistema i različite činioce u lancu vrednosti AI sistema.

2.2.2.1. Visoko rizični AI sistemi i zahtevi za usklađivanje ovih sistema

Uredba EU o veštačkoj inteligenciji uređuje niz zahteva za visoko rizične AI sisteme. Pri tome Uredba ne daje konkretnu i jasnu definiciju šta je to visoko rizična AI, već postavlja kriterijume po kojima će se odrediti da li je jedan AI sistem visoko rizičan (Čl. 6, AIA). Visoko rizični sistemi veštačke inteligencije su oni koji mogu da ugroze zdravlje i bezbednost ili osnovna prava fizičkih lica. Oni nisu zabranjeni, ali podložni su usklađivanju sa obaveznim zahtevima određenim u Uredbi.

Postoje dve kategorije visoko rizičnih AI sistema. Prva obuhvata AI sisteme namenjenim da se koriste kao bezbednosna komponenta proizvoda koji podležu *ex ante* proceni usklađenosti treće strane (Čl. 6 (1), AIA). Ovi sistemi veštačke inteligencije podižu rizik zbog posebnih karakteristika sektora u kojima se nalaze i načina na koji se koriste. Druga kategorija uključuje druge samostalne AI sisteme sa uglavnom fundamentalnom implikacijom prava koja su eksplicitno navedena u Aneksu III (Čl. 6(2) i Aneks III, AIA). Ovim se potvrđuje da, bez obzira na određeni sektor, „može takođe biti izuzetnih slučajeva u kojima, zbog rizika koji je u pitanju, upotreba AI sistema za određene namene se smatra visoko rizičnom kao takva".[18]

Uredba nameće niz obaveznih zahteva za visoko rizične Al sisteme, kroz prizmu krivice[19] (Čl. 8 (1), AIA) i povezanih obaveza dobavljača[20] i su-

---

triti uticaj sistema na prava i slobode svih uključenih pojedinaca, posebno ozbiljnost, verovatnoću i razmere ovih posledica. Upotreba ovih sistema treba da bude u skladu sa neophodnim i proporcionalnim zaštitnim merama i uslovima, posebno u pogledu vremenskih, geografskih i ličnih ograničenja. Svako pojedinačno korišćenje ovih sistema za sprovođenje zakona treba da podleže prethodnom odobrenju sudskog ili nezavisnog administrativnog organa države (čl.ice) u kojoj će se koristiti. Ovo ovlašćenje je zasnovano na obrazloženom zahtevu i skladu sa nacionalnim pravom. U hitnim situacijama, sistem se može koristiti bez prethodnog odobrenja, ali se autorizacija mora tražiti tokom ili nakon upotrebe.

18 Evropska komisija, Javne konsultacije o Beloj knjizi veštačke inteligencije: Finalni izveštaj, novembar 2020, dostupno na adresi: https://ec.europa.eu/digital-single-market/en/news/white-paper-artificial-intelligence-public-consultation-towards-european-approach-excellence.; 18.

19 C. Wendehorst, „Strict Liability for AI and Other Emerging Technologies," *Journal of European Tort Law*, vol. 11, no. 2, 2020, 156–157.

20 Čl. 3(1/3), AIA: 'dobavljač' označava fizičko ili pravno lice, javni organ, agenciju ili drugo telo koje razvija AI sistem ili model opšte namene ili koje je razvilo AI sistem ili model

bjekata koji uvodi sistem,[21] kao i drugih ključnih učesnika u lancu Al. Pri usklađivanju sa tim zahtevima (čl. 8 (2), AIA) moraju se uzeti u obzir namena visokorizičnog AI sistema i sistema upravljanja rizicima. Zahtevi koje se odnose na sve visokorizične AI sisteme uključuju:

- Uspostavljanje, implementaciju, dokumentovanje i održavanje sistema upravljanja rizicima za životni ciklus AI visokog rizika (čl. 9, AIA);
- Ispunjavanje kriterijuma za kvalitet podataka za trening, validiranje i testiranje (čl. 10, AIA);
- Izradu tehničke dokumentacije na način opredeljen direktivom pre nego što je Al sistem stavljen na tržište ili je stavljen u upotrebu i njeno ažuriranje (čl. 11, AIA);
- Omogućavanje Al sistemima da automatski beleže događaje (dnevnici) koji moraju biti u skladu sa određenim standardima (čl. 12, AIA);
- Obezbeđivanje transparentnosti u projektovanju i razvoju AI sistema tako da korisnici mogu da tumače rezultate AI sistema (čl. 13, AIA);
- Dizajn i razvoj Al sistema tako što će se omogućiti nadzor od strane fizičkih lica koji treba da bude u svrhu prevencije ili minimalizovanja rizika po zdravlje, bezbednost ili po osnovna prava (čl. 14, AIA);
- Postizanje prikladnog nivoa tačnosti, robusnosti i sajber bezbednosti i njegovo konzistentno održavanje tokom životnog ciklusa sistema (čl. 15, AIA).

Pored ovih zahteva koje se odnose na sve visoko rizične AI sisteme, za dobavljače postoji obaveza da obezbede (čl. 16, AIA):

- sistem za upravljanje kvalitetom (čl. 17, AIA);
- tehničku dokumentaciju (čl. 18, AIA);
- dokumentovanje automatski beleženih događaja, kad je to pod njihovom kontrolom (čl. 20, AIA);
- procena usklađenosti sistema koji je stavljen na tržište ili je stavljen u upotrebu (čl. 43, AIA) i korekcije kada AI sistem nije usklađen, korekcije u slučaju neusklađenosti i obaveštavanje nadležnih organa države gde je AI sistem stavljen na tržište ili u upotrebu o neusklađenosti i korektivnim merama (čl. 20, AIA) i na zahtev nadležnih organa demonstracija usklađenosti (čl. 16 (1/k), AIA);
- sastavljanje deklaracije o usklađenosti (čl. 47, AIA) i postavljanje CE oznake kako bi se naznačila usklađenost sa zahtevima Uredbe (čl. 48, AIA);

---

opšte namene i stavlja ga na tržište ili stavlja AI sistem u upotrebu pod svojim imenom ili zaštitnim znakom, bez obzira da li se za to plaća ili je besplatno.

21 Čl. 3(1/4), AIA: 'subjekt koji uvodi sistem' [eng. deployer] označava fizičko ili pravno lice, javni organ, agencija ili drugo telo koje koristi AI sistem pod svojom nadležnošću, osim ako se AI sistem koristi u okviru lične neprofesionalne aktivnosti.

- registracija u EU bazu podataka (čl. 49(1) u vezi sa čl.om 71, AIA);
- usaglašenost AI sistem sa zahtevima za pristupačnost[22],
- naznačavanje ovlašćenog predstavnika[23] dobavljača koji je iz ne-EU zemlje a lansira visoko rizičan AI sistem u EU (čl. 22, AIA).

Obaveza uvoznika[24] je da osiguraju da AI sistem ispunjava sve zahteve za usklađivanje (Čl. 23, AIA). Ovo uključuje proveru da li je sistem prošao neophodne procene, da ima ispravnu dokumentaciju, da je označen CE simbolom i da je dobavljač naznačio ovlašćenu osobu. Ako uvoznik posumnja da sistem ne ispunjava propise ili ima lažnu dokumentaciju, ne sme da ga stavi u promet dok ne bude u skladu sa propisima. Uvoznici takođe moraju da navedu svoje kontakt podatke na sistemu ili na njegovom pakovanju, da obezbede da se skladišti i transportuje bezbedno i da čuvaju evidenciju o sertifikaciji i uputstvima 10 godina. Oni takođe moraju da sarađuju sa vlastima onda kada je potrebno.

Posebne obaveze postoje za distributere[25], koji moraju osigurati, pre svega, da su dobavljač i uvoznik ispunili svoje obaveze u pogledu usklađenosti. Ako distributer veruje da sistem veštačke inteligencije ne ispunjava ove standarde, ne može ga staviti u promet dok to ne učini. Takođe treba da obezbede da sistem veštačke inteligencije ostane usklađen tokom skladištenja ili transporta. Ako se utvrdi da prodati AI sistem nije usklađen, distributer ga mora ispraviti, povući ili opozvati. Oni takođe moraju da sarađuju sa vlastima i da pruže sve tražene informacije o sistemu veštačke inteligencije (Čl. 23, AIA).

Subjekti koji uvode visoko rizičan AI sistem imaju niz obaveza (Čl. 26, AIA). Oni moraju preduzeti tehničke i organizacione mere kako bi obezbedili upotrebu tog sistema u skladu sa uputstvima i obezbediti kompetentan ljudski nadzor. Dalje, ovi subjekti moraju obezbediti da ulazni podaci budu odgovarajući, da prate rad sistema i da obaveste dobavljače ako se pojave rizici ili incidenti, osim za osetljive podatke iz oblasti sprovođenja zakona. Evidencije se moraju čuvati najmanje šest meseci, a zaposleni moraju biti obavešteni o upotrebi AI sistema. Javne vlasti, kada uvode visoko rizične AI sisteme, moraju poštovati obaveze registracije, a visoko rizični AI sistemi koji se koriste

22 Zahtevi koji proizlaze iz Direktive (EU) 2016/2102 Evropskog parlamenta i Saveta od 26. oktobra 2016. o pristupačnosti veb stranica i mobilnih aplikacija organa javnog sektora (tekst od značaja za EGP), *SL L 327, 2.12.2016, str. 1–15* i Direktive (EU) 2019/882 Evropskog parlamenta i Saveta od 17. aprila 2019. o zahtevima pristupačnosti za proizvode i usluge, PE/81/2018/REV/1, *SL L 151,* 7.6.2019, 70–115.

23 Čl. 3(1/5), AIA: „ovlašćeni predstavnik" znači fizičko ili pravno lice koje se nalazi ili je osnovano u Uniji koje je primilo i prihvatilo pismen ovlašćenje od dobavljača AI sistema ili modela AI opšte namene da, respektivno, obavlja i sprovodi u njegovo ime obaveze i procedure utvrđene ovom Uredbom.

24 Čl. 3(1/6), AIA: „uvoznik" znači fizičko ili pravno lice koje se nalazi ili ima sedište u Uniji koje stavlja na tržište sistem veštačke inteligencije koji nosi naziv ili žig fizičkog ili pravnog lica sa sedištem u trećoj zemlji.

25 Čl. 3 (1/7), AIA: 'distributer' znači fizičko ili pravno lice u lancu snabdevanja, a koje nije dobavljač ili uvoznik, a koje pravi AI sistem dostupnim na EU tržištu.

u istragama zahtevaju sudsku autorizaciju. Subjekti koji uvode visoko rizičan AI sistem takođe moraju obavestiti pojedince koji su podložni donošenju odluka pomoću AI i sarađivati sa nadležnim vlastima. Posebne obaveze koje imaju javni organi i pružaoci javnih usluga pri uvođenju AI sistema jeste sprovođenje ocene uticaja visoko rizičnog AI sistema na osnovna ljudska prava (Čl. 27, AIA).

Uredba uspostavlja pravila u odnose lica u lancu vrednosti AI. Tako, svaki distributer, uvoznik, korisnik ili druga treća strana će se smatrati dobavljačem visoko rizičnog AI sistema i imati obaveze kao dobavljač (Čl. 16 i članovi na koje upućuje, AIA) ako: (a) stave svoje ime ili zaštitni znak na postojeći visoko rizični AI sistem, bez obzira na ugovorne odnose; (b) izvrše značajne izmene na postojećem visoko rizičnom AI sistemu, održavajući njegov visoko rizični status[26]; ili (c) promene predviđene svrhe AI sistema, uključujući i AI opšte namene, tako da postane visoko rizični sistem.

2.2.2.2. AI sistemi koji imaju specifičan rizik i dodatni zahtevi za usklađivanje

Uredba proširuje generalne obaveze transparentnosti i pored obaveza koje se odnose na AI sisteme visokog rizika, na određene specifične AI sisteme, za koje su postavljeni dodatni zahtevi za transparentnost i odgovornost, naročito u pogledu interakcije sa fizičkim licima, kao i u postupanju sa veštački generisanim ili manipulativnim sadržajem (čl. 50, AIA). Uredba zahteva od dobavljača odnosno subjekta koji uvodi AI sistem da informacije pruža na jasan, razumljiv i pristupačan način najkasnije prilikom prve interakcije ili objavljivanja.

1. AI sistemi namenjeni za direktnu interakciju sa fizičkim licima. Dobavljači moraju osigurati da ovi sistemi budu dizajnirani i razvijeni tako da obaveste osobe da komuniciraju sa AI sistemom, osim ako je to očigledno.[27]
2. AI sistemi, uključujući AI sisteme opšte namene, koji generišu sintetički audio, sliku, video ili tekstualni sadržaj. Subjekti koji uvode ove sisteme moraju osigurati da rezultati AI sistema budu označeni u formatu čitljivom mašinama i da se može detektovati da su veštački generisani ili manipulisani.[28]

26 Kako je definisano u čl. 6, AIA.

27 Ova obaveza se ne odnosi na AI sisteme ovlašćene zakonom za otkrivanje, sprečavanje, istraživanje ili gonjenje krivičnih dela, pod uslovom da se primenjuju odgovarajuće mere za zaštitu prava i sloboda trećih lica, osim ako ti sistemi nisu dostupni javnosti za prijavu krivičnog dela.

28 Uredba dalje opredeljuje da subjekti moraju osigurati da njihova tehnička rešenja budu efikasna, interoperabilna, robusna i pouzdana koliko je to tehnički izvodljivo, uzimajući u obzir specifičnosti i ograničenja različitih vrsta sadržaja, troškove implementacije i opšte priznati stanje tehnike, kako može biti odraženo u relevantnim tehničkim standardima. Ova obaveza se ne odnosi na AI sisteme koji vrše pomoćnu funkciju standardnog uređivanja ili ne menjaju značajno unete podatke ili semantiku istih, ili su ovlašćeni zakonom za otkrivanje, sprečavanje, istraživanje ili gonjenje krivičnih dela.

3. AI sistem za prepoznavanje emocija ili sistem za biometrijsku kategorizaciju. Subjekti koji uvode ovakav sistem moraju obavestiti fizička lica izložena tom sistemu o radu sistema, i moraju obrađivati lične podatke u skladu sa pravilima EU za zaštitu ličnih podataka.[29]
4. AI sistem koji generiše ili manipuliše slikovnim, audio ili video sadržajem koji predstavlja dublje laži ("deep fake"). Subjekti koji uvode ovakav sistem moraju otkriti da je sadržaj veštački generisan ili manipulisan.[30]

2.2.2.3. AI sistemi koji su nisu visoko rizični i njihova samoregulacija

Tekst predloga uredbe je pretrpeo terminološke promene u pogledu naziva AI sistema koji ne spadaju u grupu visoko rizičnog sistema ili specifičnog sistema. U osnovnom predlogu Komisije je korišćen termin „ne-visoko rizični" AI sistemi [eng. *not-high-risk* ili *non-high-risk*], dok u redakciji usvojenog teksta koristi termin „sistemi koji nisu visoko-rizični" [eng. *AI systems other than high-risk AI systems*]. AIA ne definiše koji su ovo sistemi, pa implicitno proizlazi da u ovu kategoriju ulaze svi sistemi koji isključuju visok rizik.

Posebne obaveze u pogledu ovih sistema ne postoje. Dobavljači, odnosno subjekti koji uvode AI i njihovi predstavnici, će biti podsticani da uspostave kodeks ponašanja za sisteme veštačke inteligencije. Očekuje se da ovi kodeksi promovišu dobrovoljno pridržavanje određenih standarda, uzimajući u obzir tehnička rešenja i najbolje prakse u industriji, podstiču upotrebu veštačke inteligencije na način koji minimalizuje uticaj na životnu sredinu, promovišu AI pismenost, obezbeđuju inkluzivnost i raznolikost i sprečavaju negativne uticaje na osetljive grupe.

2.2.3. Pristup zasnovan na riziku i njegove (moguće) implikacije

Kako je navedeno u Memorandumu sa obrazloženjem, predlog uredbe je rezultat ekstenzivnih analiza uticaja legislative i konsultacija sa zainteresovanim stranama. Zainteresovane strane su uglavnom tražile usku, jasnu i preciznu definiciju AI i istakle važnost definisanja pojmova „rizik", „visok rizik", „nizak rizik", „daljinsku biometrijsku identifikaciju" i „štetu".

---

29 Ova obaveza se ne odnosi na AI sisteme koji su dozvoljeni pravilima za otkrivanje, sprečavanje ili istraživanje krivičnih dela, uz odgovarajuće mere zaštite prava i sloboda trećih lica, i u skladu sa zakonodavstvom Unije.

30 Pri ovome, kada sadržaj čini očigledno umetničko, kreativno, satirično, fikcionalno ili analogno delo ili program, obaveza transparentnost ograničena je na otkrivanja postojanja takvog generisanog ili manipulisanog sadržaja na odgovarajući način koji ne ometa prikazivanje ili uživanje u delu. Što se tiče generiranja ili manipuliranja tekstom koji je objavljen u svrhu informisanja javnosti o pitanjima od javnog interesa, subjekti koji uvode sistem moraju otkriti da je tekst veštački generisan ili manipulisan. Ova obaveza kada je AI-generisani sadržaj podvrgnut procesu ljudske recenzije ili uređivačke kontrole i kada fizičko ili pravno lice ima uređivačku odgovornost za objavljivanje sadržaja.

Većina ispitanika se eksplicitno zalagala za pristup zasnovan na riziku, i to se smatralo boljom opcijom od opšte regulacije svih AI sistema. Prema Memorandumu, vrste rizika i pretnji treba da se zasnivaju na sektorskom pristupu i u zavisnosti od konkretnog slučaja, a pri kalkulaciji rizika potrebno je imati u vidu uticaj na prava i bezbednost.

Ipak postavlja se (veliko) pitanje koliko je Uredba odgovorila na ove zahteve. Naime, redakcija ne sadrži eksplicitnu definiciju šta će se za svrhu Uredbe smatrati rizikom, već daje kriterijume kada je jedan sistem visoko rizičan, odnosno daje listu koji se AI sistemi smatraju visko rizičnim. AI Akt zahteva uspostavljanje mehanizma za upravljanje rizikom (Čl. 9). Ipak, nisu date jasne naznake šta znači upravljanje rizikom u pogledu sistema AI, već (samo) navodi od čega se sastoji sistem upravljanja rizikom i koje mere treba da se preduzmu za smanjenje rizika.[31] Pri tome, treba se imati u vidu da se Uredba odnosi na ekstremne rizike – neprihvatljive ili visoke rizike s jedne strane, i ne-visoko rizični, s druge strane. Obaveza transparentnosti koja se odnosi na određene sisteme veštačke inteligencije u izvesnoj meri može da nadoknadi ovaj nedostatak. Ipak, ona se odnosi na neke specifične rizike koji nisu obuhvaćeni potencijalnim rizicima izazvanim AI sistemima koji su označeni kao ne-visoko rizični, što ne znači da kod njih rizik uopšte ne postoji[32].

Kako je pitanje rizika ključno u pogledu odgovornosti za štetu prouzrokovanu upotrebom AI sistema, ovi nedostaci Uredbe imaju svoj odraz i u regulisanju građanskopravne odgovornosti za štetu prouzrokovanu upotrebom AI sistema.

3. AI SISTEMI I ODGOVORNOST ZA ŠTETU

Zasnovanost na podacima, osetljivost, otvorenost, samoučenje i autonomija, nepredvidljivost, složenost, kao glavne karakteristike AI[33], dovode u pitanje tradicionalne pojmove odgovornosti za štetu. Karakteristike, kao što su zasnovanost na podacima, osetljivost i otvorenost, utiču najviše na pitanje šta je predmet zaštite kod odgovornosti za štetu, jer se tradicionalno shvatanje štete – nepovoljan rezultat štetne radnje po lica i/ili imovinu – dovodi u korelaciju sa drugim kategorijama zaštićenih interesa, kao što su privatnost, poverljive informacije, bezbednost i sl. Dalje, kad god AI sistemi imaju sposobnost samoučenja, oni razvijaju sposobnost tumačenja, učenja novih ponašanja i izvršavanja radnji bez ili sa ograničenom ljud-

31 Schuett J. Risk Management in the Artificial Intelligence Act. *European Journal of Risk Regulation*. Objavljeno online 2023:1–19. doi:10.1017/err.2023.1

32 Vidi De Cooman, J. „Humpty Dumpty and High-Risk AI Systems: The Ratione Materiae Dimension of the Proposal for an EU Artificial Intelligence Act", *Market and Competition Law Review*, vol. 6, no. 1, April 2022, 49–88.

33 Radni dokument Evropske komisije o odgovornosti za nove digitalne tehnologije koji prati dokument Saopštenje Komisije Evropskom parlamentu, Evropskom savetu, Savetu, Evropskom ekonomskom i socijalnom komitetu i Komitetu regiona „Veštačka inteligencija za Evropu", COM(2018) 237 final.

skom intervencijom.[34] Tako AI postaje autonoman sistem, što zauzvrat čini njegovo ponašanje nepredvidivim. Sistemi veštačke inteligencije koji imaju ove karakteristike pretenduju da budu netransparentni u svom funkcionisanju, zbog prirode „crne kutije" koju razvijaju.[35] Pored toga, sistemi veštačke inteligencije mogu predstavljati visok stepen složenosti kad god postoji međuzavisnost između različitih komponenti i slojeva. Dodatni izazov je pitanje (ne)pristrasnosti AI sistema koji su programirani pomoću skupa algoritama i 'uče' proučavajući podatke kako bi identifikovali obrasce. Iz tih razloga, oni su podložni pristrasnostima svojstvenim algoritmima kojima se koriste, ali i podacima koji ih 'hrane'.[36] Ovo povećava raznovrsnost uključenih subjekata i usložnjava razumevanje potencijalno štetnih procesa. Postizanje poverenja u AI sisteme je cilj različitih interesnih grupa u sektorima tehnologije i ekonomije, koji razvijaju osnovna načela dizajniranja, razvoja i korišćenja veštačke inteligencije.[37]

Kad je reč o odgovornost za štetu, na nivou Evropske unije, izuzev par ekspertskih predloga za harmonizaciju odštetnog prava[38], ne postoji jedinstveni i zajednički pristup uređenja ove oblasti. Pitanje je da li je i koliko je to uopšte i moguće.[39] Trenutno, pravila o odgovornosti za štetu u EU pravu su razvrstana po različitim segmentima: odgovornost za proizvode prema Direktivi 85/374/EZ[40] koja je u procesu revizije,[41] upravo zbog potrebe usaglašavanja sa novim tendencijama u razvoju veštačke inteligencije[42], odgovorno-

34 S. Guida, „New Machine Behavior's Evolutionary Approaches between AI Learning, Control and Ethics Promoting Cooperative Human-Machine Intelligence." *European Journal of Privacy Law & Technologies (EJPLT),* vol. 2022, no. 1, 2022, 315–335.

35 S.J. Shackelford et al. „Should We Trust a Black Box to Safeguard Human Rights?: A Comparative Analysis of AI Governance." *UCLA Journal of International Law and Foreign Affairs*, vol. 26, no. 1, Fall/Winter 2022, str. 35–88.

36 R. Yu, G.S. Ali., „What's inside the Black Box: AI Challenges for Lawyers and Researchers." *Legal Information Management,* vol. 19, no. 1, 2019, 2–13.

37 F. Rossi, "Building Trust in Artificial Intelligence." *Journal of International Affairs*, vol. 72, no. 1, 2018, str.. 127–34.

38 Bussani, M., Infantino, M., Harmonization of Tort Law in Europe. In: Backhaus, J. (eds) Encyclopedia of Law and Economics. Springer, New York, NY, 2014; R. Zimmermann, Principles of European contract law and principles of European tort law: comparison and points of contact, at: H. Koziol, B. Steininger (eds), European Tort Law Yearbook 2002. Springer, Wien, 2003, 2–31.

39 S. Banakas, ""European Tort Law: Is it Possible", *European Review of Private Law*, Issue 3, 2010, str. 363–375

40 Direktiva Saveta 85/374/EEZ od 25. jula 1985. o usklađivanju zakona, propisa i administrativnih odredbi država čl.ica koje se odnose na odgovornost za neispravne proizvode *SL L 210, 7.8.1985, str. 29–33*, dopunjena sa Direktivom 1999/34/EC Evropskog parlamenta i Saveta od 10. maja 1999. o dopuni Direktive Saveta 85/374/EEC o usklađivanju zakona, propisa i administrativnih odredbi država čl.ica koje se odnose na odgovornost za neispravne proizvode, *SL L 141,* 4.6.1999, 20–21.

41 Predlog Direktive Evropskog parlamenta i saveta o odgovornosti za neispravne proizvode, COM/2022/495 final.

42 T.S. Cabral, „Liability and Artificial Intelligence in the EU: Assessing the Adequacy of the Current Product Liability Directive." *Maastricht Journal of European and Comparative Law*, vol. 27, 5 / 2020, 615–635.

sti za povredu prava zaštite ličnih podataka[43] i odgovornost za povrede prava konkurencije.[44]

Kao rezultat toga, u ovom trenutku, pitanje odgovornosti za štete nastale tokom korišćenja sistema veštačke inteligencije je pitanje nacionalnog zakonodavstva kojim se reguliše vanugovorna odgovornost za prouzokovanje štete.

Bez obzira na različitost pravnih tradicija i kultura u Evropi i Evropskoj uniji, pa i sistema odgovornosti za štetu,[45] nacionalni odštetno-pravni sistemi temelje se na odgovornosti zasnovanoj na krivici. Specifičnosti se ogledaju u posebnim pravilima, koja menjaju određene premise (posebno u raspodeli tereta dokazivanja), ali se jasno prepoznaje odgovornost bez obzira na krivicu (objektivna odgovornost ili odgovornost zasnovana na riziku). Većina režima odgovornosti takođe obuhvata pojam odgovornosti za druge, a koja zauzvrat može biti zasnovana na krivici ili riziku, u zavisnosti od konkretne države.[46]

Evropska komisija kao predlagač AILD nalazi da su postojeća nacionalna pravila o odgovornosti, posebno ona zasnovana na krivici, nedovoljna za rešavanje sporova za naknadu štete od proizvoda i usluga omogućenih upotrebom AI.[47] Razlog, kako navodi EK, a i Evropski parlament[48], jeste taj što prema tradicionalnim pravilima subjektivne odgovornosti, oštećena strana mora da dokaže postojanje skrivenog činjenja ili propuštanja kao uzrok štete. Kako ovo zna da bude dugotrajan i skup proces, a zbog specifičnosti tehnologija još složeniji, ovo može da deluje tako da obeshrabri oštećene strane da zahtevaju odgovornost zbog pretrpljene štete. S druge strane, ako se upuste u takve sporove, odgovor nacionalnih sudova može da bude prilagođavanje primene postojećih pravila na *ad hoc* osnovi što može da dovede do pravne nesigurnost. Posmatrano s tržišnog aspekta, rešenje svakako može da utiče na prekogranično poslovanje preduzeća.

Cilj intervencije EU jeste da se stvaranjem jedinstvenog sistema onemogući fragmentacija pravila i da se dalje razvija unutrašnje tržište. Direktiva je usmerena na uspostavljanje uniformnih pravila u pogledu određenih aspekata vanugovorne građanske odgovornosti, koja proizlazi iz AI. Direktiva

---

43 Čl. 82, Uredba (EU) 2016/679 Evropskog parlamenta i Saveta od 27. aprila 2016. o zaštiti fizičkih lica u vezi sa obradom ličnih podataka i o slobodnom kretanju takvih podataka i stavljanju van snage Direktive 95/46/EC (Opšta uredba o zaštiti podataka), *SL L 119,* 4.5.2016, 1–88.

44 Direktiva 2014/104/EU Evropskog parlamenta i Saveta od 26. novembra 2014. o određenim pravilima koja regulišu tužbe za naknadu štete prema nacionalnom zakonu zbog kršenja odredbi zakona o konkurenciji država čl.ica i Evropske unije, *SL L 349,* 5.12.2014, 1–19.

45 K. Oliphant, „Cultures of Tort Law in Europe", *Journal of European Tort Law*, vol. 3, no. 2, 2012, 147–157.

46 E. Karner, B.A. Koch, Civil Liability for Artificial Intelligence – A Comparative Overview of Current Tort Laws in Europe; in: Geistfeld M.A. et all(eds), *Civil Liability for Artificial Intelligence and Software,* De Gruyte, 2023, 23 – 26.

47 Memorandum objašnjenja, AILD.

48 Rezolucija Evropskog parlamenta (EP) od 3. maja 2022. godine o veštačkoj inteligenciji u digitalnom dobu (2020/2014(INL)), tač. 144–146.

se opredeljuje za pragmatičan pristup u rešavanju pitanja odgovornosti, sa naznakom da će se dalje razmatrati primena ovih pravila i prilagođavati potrebama koje proizlaze iz brzog razvoja tehnologija.

Set ovih modernih pravila dalje ćemo analizirati kroz tradicionalnu strukturu obligacionih odnosa koje nastaju zbog prouzrokovanje štete.

3.1. Definicija odnosa

AILD ne daje specifičnu definiciju odnosa koji bi nastao, ali posredno definiše odnos preko zahteva/tužbe za naknadu štete. Tako 'zahtev za obeštećenje' znači građanskopravni vanugovorni zahtev za naknadu štete zasnovane na grešci prouzrokovanoj delovanjem sistema veštačke inteligencije ili neuspehom takvog sistema da proizvede rezultat gde je takav rezultat trebalo da bude proizveden. (Čl. 2(1/5)), AILD).

3.2. Strane

Direktiva posredno definiše strane odštetnopravnog odnosa preko definicije stranaka u postupku za naknadu štete prouzrokovanu AI sistemima. Tako, oštećeni odnosno „podnosilac zahteva" podrazumeva lice koje podnosi zahtev za naknadu štete, koje je povređeno rezultatom AI sistema ili neuspehom takvog sistema da proizvede rezultat tamo gde je takav rezultat trebalo da bude proizveden (Čl. 2(1/6(a)), AILD).[49] Prema definiciji, kao oštećeni se može javiti i fizičko i pravno lice, ali treba imati u vidu da određena prava u postupku, a kako ćemo razmotriti dalje u tekstu, imaju samo fizičke osobe.

Štetnik odnosno „tuženi" podrazumeva lice protiv kojeg se podnosi zahtev za naknadu štete (čl. 2(1/8), AILD). Direktivom se ne daje direktna definicija koje lice u lancu od dobavljača do subjekta koji uvodi sistem AI,[50] može da bude tuženo. Direktivom su određeni mehanizmi kojima se oštećenom omogućava da identifikuje potencijalno odgovorna lica. Iz odredbi o pristupu dokazima proizlazi da štetnik može da bude dobavljač sistema veštačke inteligencije, lice koja je podložno obavezama dobavljača u određenim situacijama i pod određenim uslovima kako je uređeno u AIA, može da bude distributer, uvoznik, subjekt koji uvodi sistem ili treće lice.

3.3. Šteta

AILD ne sadrži definiciju štete. Kako se navodi u Memorandumu objašnjenja, predlog obuhvata nacionalne tužbe za odgovornost za štetu, koje su uglavnom zasnovane na krivici, bilo kog lica, u pogledu naknade bilo koje

49 Isto tako, „podnosilac zahteva [.. za naknadu štete, zab. autora]" znači i lice koje je nasledio ili je subrogirano u pravo oštećenog lica na osnovu zakona ili ugovora (Čl. 2(1/6(a)), AILD); ili deluje u ime jednog ili više oštećenih lica, u skladu sa pravom Unije ili nacionalnim pravom (Čl. 2(1/6(c)), AILD). Kako AILD uređuje pitanje pristupa do informacija i dokaza od suprotstavljene strane, definiše se i „potencijalni podnosilac zahteva" tako da označava fizičko ili pravno lice koje razmatra, ali još nije podnelo zahtev/tužbu za naknadu štete (Čl. 2(1/7)), AILD).

50 Vidi detaljnije u tački 2.2.2.1 ovog rada.

štete i bilo kojeg oštećenog. Iz definicije „dužnost pažnje"(čl. 2(1/9), AILD) posredno se može zaključiti da se Direktiva odnosi na zaštitu svih pravnih interesa priznatih na nacionalnom nivou ili na nivou prava Unije, uključujući život, fizički integritet, imovinu i zaštitu osnovnih prava.

3.4. Štetna radnja

Iz Memoranduma objašnjenja i Recitala direktive se posredno može zaključiti koja se radnja smatra štetnom, u smislu nastanka odštetnog zahteva. Tako, direktiva se odnosi na odgovornost za štetu koja je prouzrokovana rezultatom ili neuspehom da se proizvede rezultat od strane sistema veštačke inteligencije kroz krivicu osobe, na primer dobavljača ili subjekta koji uvodi sistem, kako je određeno AI Aktom. Postavljena na ovaj način štetna radnja je izjednačena sa krivicom, što će biti razrađeno dalje u tekstu. Dodatno, pravilima Direktive koja se odnose na pretpostavku kauzaliteta posebno su određene radnje koje će se smatrati nepoštovanjem standarda „dužne pažnje", kako je dalje u tekstu objašnjeno. Direktivom nisu obuhvaćeni odštetni zahtevi u slučajevima prouzrokovanja štete ljudskom procenom praćenom ljudskom činidbom ili propustom, dok je sistem veštačke inteligencije samo pružio informacije ili savete koji su uzeti u obzir od strane relevantnog ljudskog aktera (Recital 15, 22, AILD).

3.5. Uzročna veza

Pitanje kauzaliteta je jedno od najspecifičnijih pitanja ove direktive. Tradicionalno shvatanje uzročnosti bi podrazumevalo da oštećeni mora da dokaže da je šteta neposredni rezultat delovanja ili propusta AI sistema. To znači da mora postojati jasna veza između ponašanja AI sistema i štete koja je nastala. Sa druge strane AIDL, polazeći od potrebe da se olakša položaj oštećene strane, uspostavlja sistem „ciljane oborive pretpostavke kauzaliteta". Pretpostavka kauzaliteta se uspostavlja onda kada se može smatrati verovatnim da se krivicom štetnika uticalo na rezultat ili nedostatak rezultata datog AI sistema, a što će se vrednovati prema okolnostima svakog konkretnog slučaja.[51] Svakako, oštećeni mora da dokaže da je do štete došlo, kakva je šteta i u kom obimu. Tako, u skladu sa AIDL (Čl. 4(1)), a u svrhu primene pravila o odgovornosti za naknadu štete, nacionalni sudovi će pretpostaviti uzročnu vezu između krivice tuženog i rezultata dobijenog upotrebom sistema veštačke inteligencije ili neuspehom AI sistema za proizvodnju rezultata, gde su kumulativno ispunjeni sledeći uslovi:

(a) oštećeni je dokazao ili je sud pretpostavio na način određen direktivom, krivicu tuženog, ili lica za čije postupke odgovara tuženi, a koja se sastoji u nepoštovanju standarda dužne pažnje,[52] propisane

51 S. Wojtczak, P. Księżak, „Causation in Civil Law and the Problems of Transparency in AI", *European Review of Private Law*, vol. 29/4, 561–582.

52 Čl. 2(1/9), AILD: "dužnost pažnje" označava zahtevani standard ponašanja, postavljen nacionalnim ili pravom Unije, kako bi se izbegla šteta pravnim interesima priznatim na

pravom Unije ili nacionalnim pravom direktno usmerenim ka zaštiti od nastale štete;

(b) može se smatrati razumno verovatnim, na osnovu okolnosti slučaja, da je krivica uticala na rezultat proizveden od strane AI sistema ili na neuspeh AI sistema da proizvede rezultat;

(c) oštećeni je dokazao da je rezultat proizveden od strane AI sistema ili neuspeh AI sistema da proizvede rezultat prouzrokovao štetu.

Ovo generalno pravilo pretpostavke uzročnosti je dalje precizirano. Prema pravilima Direktive o pretpostavci kauzaliteta, u slučaju krivice koja se sastoji u nepoštovanju dužnosti pažnje, pravi se razlika u zavisnosti od kategorije rizika AI sistema (visko rizični ili ne-visoko rizični sistem), te se određuje koje će se lice u nizu od proizvođača do subjekta koji uvodi sistem javiti kao štetnik – tužena strana. Zbog ovih posebnih pravila, koja na različiti način tretiraju različite vrste AI sistema i različite subjekte, sistem kauzaliteta uspostavljen direktivom se naziva ciljana pretpostavljena uzročnost.

U slučaju potraživanja naknade štete od dobavljača sistema veštačke inteligencije visokog rizika koji je podložan zahtevima AI Akta ili osobe koja podleže obavezama dobavljača u skladu sa AI Aktom, uslov „krivice tuženog" (Čl. 4 (1/a), AILD) biće ispunjen samo ako je tužilac dokazao da tuženi-štetnik nije ispunio obaveze usklađivanja, koje za njega proizlaze iz AI Akta[53]. Pri tom se imaju u vidu preduzeti koraci u sistemu upravljanja rizikom i rezultati sistema u skladu sa AI Aktom[54] i to kada AI sistem (čl. 4(2), AILD): (a) koristi tehnike koje uključuju trening modele na osnovu podatka koji ne ispunjavaju kriterijume za kvalitet; ili (b) nije ni dizajniran niti razvijen na način da zadovoljava zahteve transparentnosti ili (c) ne omogućava ljudski nadzor ili (d) ne postiže, u skladu sa svojim ciljem, adekvatni nivo tačnosti, robusnosti i sajber bezbednosti; ili (e) nisu preduzete potrebne korektivne mere da se postigne usklađenost sistema ili da se sistem povuče ili opozove sa tržišta.

Kada je reč o odgovornosti subjekta koji je uveo sistem veštačke inteligencije visokog rizika (čl. 4(3), AILD), smatra se da neusklađenost postoji kada (a) nije postupao u saglasnosti sa obavezom da koristi ili nadzire sistem AI u skladu sa uputstvima za korišćenje ili je suspendovao ili prekinuo korišćenje; ili (b) izložio je AI sistem podacima koji nisu relevantni za cilj sistema. Ipak, kauzalitet se neće pretpostavljati (čl. 4(4), AIDL) kada tužilac ukaže na to da se može pristupiti u dovoljnoj meri dokazima i ekspertizi da tužilac dokaže uzročnu vezu.

U slučaju AI sistema bez visokog rizika, čl. 4(5) se uspostavlja uslov za primenu pretpostavke uzročnosti – da sud utvrdi da je podnosiocu zahteva

---

nacionalnom ili nivou prava Unije, uključujući život, fizički integritet, imovinu i zaštitu osnovnih prava.

53 AIA, Glava III, Sekcija 2 (Zahtevi za visoko rizične AI sisteme; čl. 8 –15, AIA) i Sekcija 3 (Obaveze dobavljača i subjekta koji uvode visoko rizične AI sisteme i drugih lica; čl. 16 – 27).

54 Čl. 9 i čl. 16(a), AIA.

prekomerno teško da dokaže uzročnu vezu. Pri tome, stepen poteškoće će se procenjivati u svetlu karakteristika određenih sistema veštačke inteligencije, kao što su autonomija i netransparentnost, koji u praksi dovode to toga da je objašnjenje unutrašnjeg funkcionisanja AI sistema veoma teško. Nesumnjivo je da to negativno utiče na sposobnost podnosioca zahteva da dokaže uzročnu vezu između krivice štetnika i rezultata AI.

Štetnik može u svim slučajevima da obara ovu pretpostavku.

3.6. Osnov odgovornosti

Odgovornost za štetu prouzrokovanu AI sistemima je subjektivna odgovornost – odgovornost po osnovu krivice koja se sastoji od nepoštovanja obaveze dužne pažnje prema zakonu Unije ili nacionalnom pravu. Direktiva definiše dužnost pažnje (Čl. 3(1/9), AILD) kao zahtevani standard ponašanja, utvrđen nacionalnim pravom ili pravom Unije, kako bi se izbegla šteta po pravne interese priznate na nacionalnom nivou ili nivou prava Unije, uključujući život, fizički integritet, imovinu i zaštitu osnovnih prava. Zahtevani standard ponašanja je poštovanje svih pravila za usklađivanje AI sistema sa obavezama koje za relevantna lica u lancu vrednosti AI uređuje Uredba EU o veštačkoj inteligenciji. Pri tom, ako štetnik ispuni obaveze za otkrivanje dokaza na zahtev oštećenog, na način i pod uslovima određenim AILD (čl. 3(1–4)) krivica se treba dokazivati, dok će sud pretpostaviti postojanje krivice-nepažnje.

Ovako postavljen sistem odnosno osnov odgovornosti biće predmet preispitivanja od strane Komisije, nakon isteka 5 godina od roka za transponovanje direktive, koji iznosi dve godine od dana stupanja na snagu direktive, kako bi se ocenilo da li ovaj zakonodavni pristup omogućava postizanje ciljeva direktive.

U fazi izrade predloga, Evropska komisija je imala u vidu tri moguća rešenja: 1) subjektivna odgovornost, 2) objektivna odgovornost i 3) fazni pristup koji znači da će se u prvoj fazi odgovornost uspostaviti kao subjektivna odgovornost, a u drugoj fazi bi se ponovo cenila potreba za harmonizaciju pravila objektivne odgovornosti u slučaju upotrebe veštačke inteligencije sa ličnim rizičnim profilom, sa ili bez obaveznog osiguranja od odgovornosti.

4. UMESTO ZAKLJUČKA: DISKUSIJA O IZAZOVIMA ZA ODŠTETNO PRAVO

U pravnoj praksi postoji anegdota da kada pravnici ne znaju kako da nešto definišu, onda to nazivaju *sui generis.* Autorka ovog rada je ubeđena da (skoro) nikad nije postojalo bolje opravdanje za korišćenje ovog naziva nego što je to slučaj sa režimom odgovornosti za štetu prouzrokovanu veštačkom inteligencijom uspostavljenim (ili koji se očekuje da se uspostavi) novim pravilima Evropske unije za veštačku inteligenciju.

Odgovornost za štetu prouzrokovanu veštačkom inteligencijom je *sui generis* sa svim izazovima koji iz te posebnosti proizlaze, iz sledećih razloga:

1. Zakonodavac Evropske unije nastoji da reši sistemsko pitanje posebnog slučaja odgovornosti za štetu intervencijom koja je, zbog specifičnosti kompetencija koje EU ima, parcijalna. Naime, nesporna je (podeljena) nadležnost EU da kreira pravni okvir koji će minimalizovati (sve) prepreke za poslovanje na zajedničkom tržištu. Osnov predmetne intervencije je čl. 114 UFEU koji omogućuje donošenje propisa koji imaju za cilj uspostavljanje i funkcionisanje unutrašnjeg tržišta. Sva istraživanja, procene i analize koje prethode izradi nacrta Direktive o građanskopravnoj odgovornosti za štetu prouzrokovanu upotrebom AI sistema ukazuju na to da nedostatak pravila na nivou EU, koja se odnose na veštačku inteligenciju i odgovornost za štetu od veštačke inteligencije, predstavlja opasnost da se pojave smetnje na unutrašnjem tržištu. Ali, sistemsko uređenje odgovornosti za štetu nije u nadležnosti EU (i pitanje je da li će ikad biti). Iz tih razloga EU se odlučila da prvo uredi opšta pitanja veštačke inteligencije, a nakon toga i odgovornost za štetu koja proizlazi iz nje. Ipak, po pitanju odgovornosti mora da se fokusira samo na štetu koja proizlazi iz dozvoljenih sistema veštačke inteligencije koji predstavljaju visok rizik. Pitanja za odgovornost za štetu koja bi bila rezultat upotrebe nedozvoljene veštačke inteligencije ili veštačke inteligencije koja nije visok rizik ostaju izvan normativne pažnje na nivou EU. Činjenica da su određene prakse zabranjene, ne znači da ih neće biti. Očekivanja da će zainteresovane strane samostalno urediti sisteme AI koji nisu visoko rizični mogu ostati neostvarena. I jedno i drugo eventualno može dovesti do nastanka štete. U ovim slučajevima primenjivala bi se (raznolika) nacionalna pravila, što može (ponovo) dovesti do fragmentacije pravnog okvira i pravne nesigurnosti lica koja su pretrpela štetu. Nije prestrogo reći da ovo može da dovede u pitanje ostvarivanje ciljeva intervencije.
2. Evropska unija je uspela da ponudi (tehnološki) neutralnu definiciju sistema veštačke inteligencije. Podjednako uspešno i detaljno uređuje zahteve za usklađenost AI sistema sa (očekivanjima) standardima koje treba da omoguće bezbednost i poverenje da ti sistemi neće povrediti fundamentalna prava. Ali, nedostaju bitne eksplicitne definicije različitih formi rizika (neprihvatljiv rizik, visok rizik i rizik koji nije visok (poslednji termin kao izveden negativan pojam visokog rizika, koji sam po sebi ne znači da rizika nema)), štete i drugih pojmova koji su bitni za utvrđivanje odgovornosti. Time, se otvara mogućnost (relativno slobodne) interpretacije nacionalnih sudova u svetlu nacionalnih pravila, što ponovo, po našem mišljenju, može dovesti u pitanje ujednačenost u primeni pravila i konzistentnost sistema odgovornosti za štetu od (visoko rizičnih) AI sistema. Ako je svrha direktive da [.. se omogući poboljšanje funkcionisanja

unutrašnjeg tržišta] tako što će se uspostaviti jedinstveni zahtevi za određene aspekte vanugovorne građanske odgovornosti za štetu nastalu uključivanjem sistema veštačke inteligencije, autorki nije jasno zašto ovo nije izraženo i u nazivu direktive koja svojom ambicioznošću upućuje na sveobuhvatniji predmet uređenja.

3. AILD uvodi pretpostavku uzročnosti kod subjektivne odgovornosti štetnika što je atipično za odgovornost po osnovu krivice, ali je tipično za objektivnu odgovornost – odgovornost po osnovu rizika. Ukoliko bi se na odgovornost za štetu prouzrokovanu (visoko rizičnim) AI sistemom primenjivala pravila objektivne odgovornosti ovako pretpostavljeni kauzalitet bi bio logičan. Razlog uvođenja je taj što zakonodavac smatra da u ovom trenutku razvoja AI podaci koji su relevantni za dokazivanje uzročnosti između rezultata AI sistema ili nedostatka rezultata AI sistema i štete kod visoko rizičnih AI sistema nisu lako dostupni, niti je dovoljno razvijena ekspertiza. Ipak, daje mogućnost da se kauzalitet dokazuje, ako se pokaže da su dokazi i ekspertiza dostupni. Ovakva pozicija u principu znači da će se sistem odgovornosti za štetu u pogledu tereta dokazivanja uzročnosti izjednačiti sa tradicionalnim sistemima. Procena dostupnosti dokaza i ekspertize je na nacionalnim sudovima i, naravno, ponovo se može dogoditi divergentna praksa. Istovremeno, kod AI sistema bez visokog rizika pravilo je da se kauzalitet dokazuje, a izuzetno, kada je pristup dokazima otežan može se pretpostavljati. Različiti pristup je razumljiv i proizlazi iz stepena složenosti AI sistema, ali u isto vreme može ugroziti dostizanje visoko postavljenih ciljeva direktive.
4. Na kraju, ali ne manje značajno, najavljena je promena novog sistema odgovornosti. Procena uticaja je ukazala da je sistem objektivne odgovornosti za štetu prouzrokovanu veštačkom inteligencijom, bez obzira da li zajedno sa obaveznim osiguranjem ili ne, više se preferira nego sistem subjektivne odgovornosti sa pretpostavljenim kauzalitetom. Ipak, predlog uzima u obzir da u nacionalnim sistemima postoje (značajne) razlike kada je reč o objektivnoj odgovornosti, koje mogu uticati na širu javnost i dovesti u opasnost važna prava, kao što su pravo na život, zdravlje i imovinu. Iz ovih razloga uspostavlja se sistem praćenja primene Direktive, koji treba da omogući dovoljno podataka da bi se ceo sistem revidirao i da bi se uvele nove mere, kao što je uvođenje režima objektivne odgovornosti i/ili obaveznog osiguranja. Za pravnika koji svet vidi kroz prizmu Zakona o obligacionim odnosima SFRJ iz 1978. godine, a koji je sa malo intervencija par decenija kasnije postao nacionalni zakon u zemljama naslednicama federativne republike, jedini rezultat jednačine u koju ulaze rizik, opasnost i odgovornost je objektivna odgovornost za štetu. U ovim sistemima kod objektivne odgovornosti pretpostavlja se uzročnost, a kod subjektivne odgovornosti pretpostavlja

se nepažnja kao stepen krivice. Pravila EU uređuju odgovornost za štetu prouzrokovanu AI sistemima kao subjektivnu odgovornost sa pretpostavljenim kauzalitetom. Stoga, formulisanje pravnih pravila koja bi imala za cilj usaglašavanje ovih nacionalnih zakonodavstva sa pravom EU će biti teško, a primena tih pravila u praksi još teža. To će jedino biti moguće ako se na odgovornost za štetu od veštačke inteligencije gleda kao *sui generis* sistem odgovornosti. Idealno, taj sistem bi se uveo i posebnim zakonom, bez intervencija u zakonima o obligacionim odnosima kako zbog specifičnosti predmetne materije i nomotehničkog pristupa, tako i zbog očekivanja da se ovaj sistem (relativno) uskoro promeni.

LITERATURA:

Balogh Z.G., „Liability for Damage Caused by AI Entities", *Acta Universitatis Sapientiae: Legal Studies*, vol. 11, no. 2, 2022.

Banakas S., "'European Tort Law: Is it Possible", *European Review of Private Law*, Issue 3, 2010.

Brennan L., „AI Ethical Compliance Is Undecidable," *Hastings Science and Technology Law Journal 14*, no. 2, 2023.

Bussani M, Infantino M., Harmonization of Tort Law in Europe. In: J. Backhaus, (eds) *Encyclopedia of Law and Economics*. Springer, New York, NY, 2014.

Cabral T.S., „Liability and Artificial Intelligence in the EU: Assessing the Adequacy of the Current Product Liability Directive." Maastricht Journal of European and Comparative Law, vol. 27, no. 5 /2020.

De Cooman J., „Humpty Dumpty and High-Risk AI Systems: The Ratione Materiae Dimension of the Proposal for an EU Artificial Intelligence Act.", *Market and Competition Law Review*, vol. 6, no. 1 / 2022.

Guida S, „New Machine Behavior's Evolutionary Approaches between AI Learning, Control and Ethics Promoting Cooperative Human-Machine Intelligence." European Journal of Privacy Law & Technologies (EJPLT), vol. 2022, no. 1/2022.

Karner E., Koch B.A., Civil Liability for Artificial Intelligence – A Comparative Overview of Current Tort Laws in Europe; in: Geistfeld M.A. et all(eds), *Civil Liability for Artificial Intelligence and Software,* De Gruyte, 2023.

Kohne G., Reed M. A., Arlington J., „New Proposed EU AI Regulation Extends beyond Europe," RAIL: The Journal of Robotics, *Artificial Intelligence & Law,* vol. 4, no. 5, 2021.

Mezei K., Trager A., "The European Approach to Artificial Intelligence. Ethical and Regulatory Implications." *Acta Universitatis Sapientiae: Legal Studies*, vol. 11, no. 2, 2022.

Oliphant K., „Cultures of Tort Law in Europe", *Journal of European Tort Law*, vol. 3, no. 2, 2012.

Rossi F., "Building Trust in Artificial Intelligence." *Journal of International Affairs*, vol. 72, no. 1, 2018.

Schuett J., „Risk Management in the Artificial Intelligence Act", *European Journal of Risk Regulation*. Dostupno onlajn. doi:10.1017/err.2023.1

Shackelford J.S. et al. „Should We Trust a Black Box to Safeguard Human Rights?: A Comparative Analysis of AI Governance." UCLA Journal of International Law and Foreign Affairs, vol. 26, no. 1, 2022.

Wendehorst C., „Strict Liability for AI and Other Emerging Technologies," *Journal of European Tort Law*, vol. 11, no. 2/2020.

Williams J, Kohne N. G., Reed M. A., Arlington J., „New Proposed EU AI Regulation Extends beyond Europe", *RAIL: The Journal of Robotics, Artificial Intelligence & Law* vol. 4, no. 5, 2021.

Wojtczak S, Księżak P., „Causation in Civil Law and the Problems of Transparency in AI", European Review of Private Law, vol. 29, 4.

Yu R., Ali G.S.., „What's inside the Black Box: AI Challenges for Lawyers and Researchers." *Legal Information Management,* vol. 19, no. 1, 2019.

Zimmermann R., „Principles of European contract law and principles of European tort law: comparison and points of contact", in: H. Koziol, B. Steininger (eds), *European Tort Law Yearbook* 2002. Springer, Wien, 2003.

Prof. Dr. Neda Zdraveva
Full Professor, Ss. Cyril and Methodius University
– Iustinianus Primus Law Faculty

LIABILITY FOR DAMAGE CAUSED BY AI SYSTEMS IN THE EU LAW – STATUS AND CHALLENGES

Abstract: *The purpose of this article is to explore the regulation of AI and the associated liability within the European Union (EU). It focuses on the legislative approach of the EU, particularly examining the AI Liability Directive. The discussion begins by outlining the necessity for regulation and liability in the context of AI systems. Further, the author analyses the regulatory purpose and the legislative approach. In the second part, AI is analysed through a risk-based approach, considering both ethical and legal standards essential for ensuring the trustworthiness of AI. The characteristics of AI and the levels of risk associated with its deployment are also explored. The compliance requirements established by the AI Act of the EU are scrutinized, offering insights into the standards set for AI systems to be deemed reliable and safe. This is followed by a review of the issues surrounding liability for damage caused by AI systems. Key aspects include identifying the parties involved in potential cases—claimant and defendant—the nature of the damage, the causal link, and the targeted rebuttable presumption of causality as well as the presumption of non-compliance with the conformity requirements as a reflection of the fault-based liability system.*

The article concludes by discussing the perceived 'open issues' in creating a comprehensive liability regime for AI within the EU and their effect on the national liability systems. It addresses the challenges of approximating national liability laws with EU law, as well as the implementation and enforcement of the rules.

Keywords: *Artificial intelligence. Regulation of artificial intelligence. – Risk-based approach. – Damage. – Fault-based liability. – Strict liability.*