www.amcham.hr

Američka gospodarska komora u Hrvatskoj | American Chamber of Commerce in Croatia

Zagreb, srpanj 2026.

Uređenje kaznene odgovornosti umjetne inteligencije

Sadržaj

Uvod

Umjetna inteligencija (AI) postaje ključna tehnologija za povećanje produktivnosti, konkurentnosti i inovacijskog kapaciteta gospodarstva. Njezina primjena već danas transformira poslovne procese, potiče razvoj novih proizvoda i usluga te stvara prilike za gospodarski rast.

Istovremeno, razvoj i primjena AI sustava otvaraju nova pitanja sigurnosti, odgovornosti i upravljanja rizicima, osobito u situacijama kada uporaba takvih sustava može dovesti do štetnih posljedica za građane, organizacije ili društvo u cjelini.

U Hrvatskoj je kroz izmjene i dopune Kaznenog zakona u listopadu 2025. godine uvedeno novo kazneno djelo izazivanja opasnosti uporabom sustava umjetne inteligencije - Izazivanje opasnosti uporabom sustava umjetne inteligencije (čl. 215.a)

> *„Tko u razvoju, testiranju, provjeri, nadzoru, upravljanju, uporabi sustava umjetne inteligencije ili na drugi način sustavom umjetne inteligencije izazove opasnost za život ili tijelo ljudi ili za imovinu većeg opsega, a time nije počinjeno teže kazneno djelo, kaznit će se kaznom zatvora od šest mjeseci do pet godina.*"

Time su se u hrvatskom zakonodavstvu prvi put izričito adresirale potencijalne opasnosti koje mogu nastati u razvoju, testiranju, nadzoru, upravljanju ili uporabi AI sustava. Zakon pritom predviđa i strože kazne u situacijama kada takvo ponašanje dovede do teške tjelesne ozljede, velike imovinske štete ili smrti jedne ili više osoba. Iako je temeljni cilj takve regulacije zaštita života, zdravlja i imovine od potencijalno opasnih tehnoloških sustava, formulacija odredbe otvara niz pravnih pitanja vezanih uz opseg kaznene odgovornosti, zahtjev pravne sigurnosti, odnos prema postojećim kaznenim djelima te usklađenost s europskim regulatornim pristupom.

AmCham podržava uspostavu regulatornog okvira koji osigurava visoku razinu zaštite građana i društva od štetnih posljedica. Međutim, smatramo da postojeće rješenje stvara regulatornu neizvjesnost za poslovnu zajednicu koja razvija ili koristi AI sustave, što može negativno utjecati na ulaganja, razvoj inovacija i širu primjenu novih tehnologija u Hrvatskoj.

Cilj ovog dokumenta je ukazati na ključne izazove postojećeg rješenja te predložiti izmjene koje bi omogućile bolju ravnotežu između zaštite građana i stvaranja okruženja koje je poticajno za inovacije i primjenu novih tehnologija.

Nedostaci postojećeg rješenja

Preširoko definiran krug potencijalno odgovornih osoba

Jedan od ključnih izazova članka 215.a jest vrlo širok krug osoba koje mogu biti obuhvaćene kaznenom odgovornošću. Odredba obuhvaća razvoj, testiranje, provjeru, nadzor, upravljanje i uporabu AI sustava, čime potencijalno zahvaća gotovo sve sudionike u njegovu životnom ciklusu:

- programere i developere AI sustava,
- osobe koje testiraju ili validiraju modele,
- poduzeća koja implementiraju ili integriraju sustave u svoje poslovne procese,
- operatore i administratore sustava,
- krajnje korisnike.

Takvo rješenje reflektira činjenicu da je AI rezultat složenih tehnoloških i organizacijskih procesa u kojima sudjeluje više aktera. Međutim, Zakon ne precizira koje konkretne radnje u pojedinim fazama razvoja ili uporabe sustava predstavljaju osnovu za kaznenu odgovornost, što stvara neizvjesnost oko toga gdje ona zapravo počinje.

Za poslovnu zajednicu važno je da regulatorni okvir bude jasan i predvidiv. Kada granice odgovornosti nisu dovoljno precizno definirane, raste pravna nesigurnost i otežava se donošenje investicijskih i poslovnih odluka. Ako je zakonska norma formulirana vrlo široko ili neodređeno, postoji opasnost da će njezin stvarni sadržaj biti oblikovan tek kroz sudsku praksu. Iako sudovi u

praksi često razrađuju opće zakonske pojmove, kazneno pravo nastoji izbjeći situacije u kojima bi granice kažnjivosti bile prepuštene značajnoj diskreciji sudova ili tijela kaznenog progona.

Dodatni izazov proizlazi iz same prirode AI sustava. Posljedica štetnog događaja može proizaći iz kombinacije različitih čimbenika, poput dizajna algoritma, kvalitete podataka za treniranje, načina implementacije ili načina uporabe sustava. U takvim okolnostima može biti teško precizno utvrditi čija je konkretna radnja izazvala opasnost ili štetu.

Zbog svega navedenog, postavlja se pitanje ispunjava li odredba u potpunosti zahtjeve jasnoće, preciznosti i predvidivosti, koji su ključni za kaznenopravne norme. Smatramo da bi kaznena odgovornost AI-ja trebala biti povezana s konkretnim povredama regulatornih obveza, sigurnosnih standarda ili zahtjeva propisanih europskim regulatornim okvirom koji se odnosi na AI. Takav pristup osigurao bi veću pravnu sigurnost za gospodarstvo i poticaj za inovacije, uz zadržavanje učinkovite zaštite od doista opasnih postupanja.

Neprecizno definirano „izazivanje opasnosti"

Kazneno pravo zahtijeva jasno određene radnje i posljedice kako bi se osigurala pravna sigurnost i predvidivost kaznenopravne odgovornosti. Međutim, odredba kaznene odgovornosti AI-ja predviđa kažnjivost već za samo „izazivanje opasnosti" za život, tijelo ili imovinu većeg opsega.

Takvo rješenje može biti teško primjenjivo iz sljedećih razloga:

- nije uvijek jasno kada određena tehnološka pogreška predstavlja stvarnu opasnost,
- granica između tehničkog nedostatka i kaznenopravno relevantne opasnosti može biti nejasna.

Dodatni izazov predstavlja činjenica da pojam opasnosti može imati različita tumačenja. Može se odnositi na konkretnu i neposrednu opasnost, ali i na apstraktnu mogućnost nastanka štete. Budući da zakon ne precizira o kojoj je vrsti opasnosti riječ, postoji rizik da granica između dopuštenog i kažnjivog ponašanja ostane nejasna. To je posebno važno kod AI-ja, gdje su određeni rizici sastavni dio razvoja, testiranja i primjene novih tehnologija.

U praksi će stoga biti ključno kako će sudovi tumačiti pojam opasnosti i u kojim situacijama će smatrati da je dosegnut prag kaznenopravne odgovornosti, što smanjuje razinu pravne sigurnosti i predvidivosti.

Odnos prema postojećim kaznenim djelima

Mnoge situacije koje mogu nastati uporabom AI-ja već su obuhvaćene postojećim kaznenim djelima.

Primjerice, Kazneni zakon već sadrži odredbe koje se odnose na:

- dovođenje u opasnost života i imovine općeopasnom radnjom ili sredstvom (čl. 215. Kaznenog zakona),
- oštećenje tuđe stvari (čl. 235. Kaznenog zakona),
- uništenje ili oštećenje zaštitnih naprava na radu (čl. 217. Kaznenog zakona).

U tom kontekstu se uvođenje posebnog kaznenog djela vezanog uz AI može smatrati simboličkom normom koja želi naglasiti posebne rizike povezane s novim tehnologijama. AI se može promatrati kao jedno od tehničkih sredstava kojim je štetna radnja počinjena, slično kao što se u kaznenom pravu već tretiraju različiti strojevi, vozila ili informacijski sustavi.

Čak i ako ova kaznenopravna norma u praksi bude rijetko primjenjivana, njezin utjecaj može biti značajan jer povećava percepciju regulatornog rizika za poslovnu zajednicu. Upravo ta percepcija snažno utječe na investicijsku klimu i poslovno planiranje.

Poduzeća koja razvijaju ili implementiraju AI sustave su nesigurna u pogledu toga:

- koje konkretno ponašanje može dovesti do kaznene odgovornosti,
- tko u unutar organizacije može snositi odgovornost (developer, menadžer, operator),
- kako će sudovi tumačiti pojmove poput „opasnosti" ili „nehaja" u kontekstu AI-ja.

Takva neizvjesnost može potaknuti poduzeća na oprezniji pristup razvoju i primjeni novih tehnologija kako bi smanjila regulatorni rizik. Dodatnu neizvjesnost stvara činjenica da se relativno široko definirana kaznena odgovornost kombinira s vrlo ozbiljnim sankcijama, koje u slučaju najtežih posljedica uključuju i dugotrajne zatvorske kazne. Posljedično, može doći do smanjenja ulaganja u nove tehnologije, slabijeg korištenja potencijala AI-ja u hrvatskom gospodarstvu, opreznijeg uvođenja inovacija te preusmjeravanja investicija na tržišta s poticajnijim regulatornim okruženjem. To posebno pogađa startupove, mala i srednja poduzeća te istraživačke organizacije, koje su ključni nositelji inovacija.

Neusklađenost s regulatornim pristupom EU

Donošenjem Akta o umjetnoj inteligenciji (EU AI Akt), Europska unija je uspostavila sveobuhvatan regulatorni okvir koji se primarno temelji na upravljanju rizicima, transparentnosti, ljudskom nadzoru i uređivanju obveza različitih dionika u životnom ciklusu AI sustava.

Cilj takvog pristupa nije kažnjavanje same tehnologije, već sprječavanje nastanka štete kroz procjenu rizika, tehničke i organizacijske mjere, nadzor tržišta i regulatorne sankcije. Drugim riječima, naglasak je na prevenciji i upravljanju rizicima prije nego što dođe do štetnih posljedica. Kazneno pravo pritom ostaje krajnje sredstvo za najozbiljnije slučajeve.

Sličan pristup vidljiv je i u drugim europskim inicijativama kao što je Direktiva o odgovornosti za proizvode. Europska komisija pitanja odgovornosti za štetu uzrokovanu AI-jem nastoji rješavati prvenstveno kroz građanskopravne i regulatorne mehanizme, uključujući pravila o odgovornosti za proizvode i naknadi štete, umjesto stvaranja novih općih kaznenih djela povezanih s umjetnom inteligencijom. Cilj je postići ravnotežu između zaštite pojedinaca i poticanja tehnoloških inovacija.

Šira europska praksa

Komparativna praksa također pokazuje da većina država prednost daje regulatornim, građanskopravnim i administrativnim mehanizmima odgovornosti, dok se kazneno pravo uglavnom koristi za konkretne i jasno definirane zlouporabe tehnologije. Primjerice Ujedinjeno Kraljevstvo u dokumentu *„AI regulation: a pro-innovation approach*" izričito zagovara proporcionalan i proinovacijski regulatorni model te upozorava da bi krut pristup mogao usporiti usvajanje AI-ja i ugušiti inovacije. Umjesto jedinstvenog kaznenopravnog režima, UK se oslanja na sektorske regulatore, postojeće pravne okvire i postupno oblikovanje standarda[1]. Dodatno, Italija, koja je 2025. godine usvojila nacionalni zakon o umjetnoj inteligenciji, je kaznenopravne odredbe vezala uz specifične oblike zlouporabe poput nezakonitog širenja *deepfake* sadržaja, prijevara ili krađe identiteta, a ne uz općenito „izazivanje opasnosti" tijekom razvoja ili uporabe AI sustava[2].

Slično tome, Francuska[3], Njemačka[4] i Ujedinjeno Kraljevstvo[5] su kriminalizirale ili pokazali namjeru kriminalizirati neovlašteno stvaranje i distribuciju seksualiziranih *deepfakeova* - digitalno fabriciranog seksualnog sadržaja koji može, ali ne mora biti generiran uz pomoć AI-ja, kako bi zaštitile privatnost, pravo osobnosti i ljudsko dostojanstvo. Takvi oblici sadržaja sve se češće kvalificiraju kao oblik seksualnog nasilja, a europski zakonodavni razvoj ide u smjeru njihove kriminalizacije kroz nacionalne kaznene odredbe ili kroz implementaciju EU Direktive o suzbijanju nasilja nad ženama i nasilja u obitelji[6].

[1] Dostupno na: https://www.gov.uk/government/publications/ai-regulation-a-pro-innovation-approach Preuzeto 2. lipnja 2026.
[2] Dostupno na: https://www.nortonrosefulbright.com/en/knowledge/publications/9bfedfea/italy-enacts-law-no-132-2025-on-artificial-intelligence-sector-rules-and-next-steps Preuzeto: 2. lipnja 206.
[3] Dostupno na: https://www.hoganlovells.com/en/publications/france-prohibits-non-consensual-deep-fakes Preuzeto: 1. lipnja 2026.
[4] Dostupno na: https://www.gesetze-im-internet.de/stgb/__201a.html Preuzeto: 1 lipnja 2026.
[5] Dostupno na: https://www.mishcon.com/news/government-to-criminalise-the-creation-of-sexually-explicit-deepfakes Preuzeto: 3. lipnja 2026.
[6] Dostupno na: https://ceeddw.org/wp-content/uploads/2025/05/NCII_DeepFakes_ThreatsRecommendations.pdf Preuzeto: 3 lipnja 2026.

Međunarodna praksa

I izvan Europe prevladava pristup koji AI regulira prvenstveno kroz načela odgovornosti, upravljanja rizicima i tehničke standarde, a ne kroz široke kaznene zabrane.

OECD-ova načela o umjetnoj inteligenciji, ažurirana 2024. godine, naglašavaju odgovornost aktera, upravljanje rizicima i proporcionalnost prema ulozi aktera i kontekstu uporabe[7]. Slično tome, UNESCO-ova Preporuka o etici umjetne inteligencije temelji se na ljudskim pravima, transparentnosti, ljudskom nadzoru, odgovornosti i vladavini prava[8].

U Sjedinjenim Američkim Državama, barem na saveznoj razini u području opće AI regulacije, važnu referentnu točku predstavlja *NIST AI Risk Management Framework*, koji je izričito zamišljen kao dobrovoljan alat za organizacije kako bi upravljale rizicima i povećale pouzdanost AI sustava. To ponovno pokazuje međunarodnu tendenciju da se AI prvenstveno uređuje kroz standarde, procese i upravljanje rizikom, a ne kroz samostalna kaznena djela općeg tipa[9].

Južna Koreja je primjer države koja ima jedan od najstrožih režima borbe protiv *deepfakeova*. Ondje je posebno značajno da je čak i posjedovanje ili gledanje pornografskog *deepfake* sadržaja nastalog bez pristanka osobe kazneno djelo (uz kaznu zatvora ili novčanu kaznu). Zakon također uvodi obvezne minimalne kazne: najmanje jednu godinu zatvora za ucjenu korištenjem *deepfake* sadržaja te najmanje tri godine zatvora za stvaranje seksualnih *deepfakeova* s namjerom njihove distribucije. Uz to, država je obvezna pomoći žrtvama u uklanjanju *deepfake* sadržaja s interneta[10].

U tom kontekstu hrvatsko rješenje može se smatrati strožim od prevladavajućih europskih i međunarodnih trendova, koji nastoje postići ravnotežu između zaštite građana i poticanja inovacija te kazneno pravo zadržavaju kao krajnje sredstvo za najteže oblike zlouporabe. Članak 215.a od toga odstupa jer uvodi posebno kazneno djelo za izazivanje opasnosti uporabom AI sustava, uz kazne zatvora koje u slučaju smrtnog ishoda dosežu do petnaest godina. Time se umjetna inteligencija izdvaja iz općeg regulatornog pristupa EU-a i podvrgava strožem kaznenopravnom režimu.

AmCham-ove preporuke

AmCham podržava postojanje učinkovitih mehanizama zaštite od štetne i neodgovorne uporabe umjetne inteligencije. Međutim, smatramo da postoji prostor za dodatno unaprjeđenje postojećeg okvira kako bi se osigurala veća pravna sigurnost, predvidivost i usklađenost s europskim regulatornim pristupom. Posebno je važno osigurati da opseg kaznene odgovornosti bude jasno definiran i proporcionalan ozbiljnosti sankcija koje zakon predviđa. Time bi se smanjila regulatorna neizvjesnost i osiguralo okruženje koje istodobno štiti građane i potiče razvoj inovacija.

1) Uvođenje blanketne norme

Jedno od mogućih rješenja za ublažavanje navedenih nedostataka bilo bi preoblikovanje odredbe u tzv. blanketnu kaznenopravnu normu. Blanketne norme u kaznenom pravu upućuju na druge propise koji detaljnije uređuju određeno područje, čime se osigurava veća fleksibilnost i usklađenost kaznenog prava s tehničkim i regulatornim standardima. U kontekstu AI-ja takva bi norma mogla upućivati na relevantne europske i nacionalne propise, prije svega na obveze koje proizlaze iz EU AI Akta, tehničkih standarda sigurnosti sustava, obveza procjene rizika ili zahtjeva za ljudski nadzor nad visokorizičnim sustavima.

Primjerice, kaznenopravna odgovornost mogla bi biti vezana uz situacije u kojima osoba namjerno krši propisane sigurnosne obveze vezane uz razvoj ili uporabu visokorizičnih AI sustava, a takvo kršenje dovede do ozbiljne opasnosti ili štetnih posljedica za život, zdravlje ili imovinu. Time bi se

[7] Dostupno na: https://www.oecd.org/en/topics/sub-issues/ai-principles.html Preuzeto: 8. lipnja 2026.
[8] Dostupno na: https://www.unesco.org/en/artificial-intelligence/recommendation-ethics Preuzeto: 8. lipnja 2026.
[9] Dostupno na: https://www.nist.gov/itl/ai-risk-management-framework Preuzeto: 3. lipnja 2026.
[10] Dostupno na: https://ondato.com/blog/deepfake-laws Preuzeto: 3. lipnja 2026.

kazneno pravo usmjerilo na povredu konkretnih normativnih obveza, a ne na apstraktno izazivanje opasnosti.

- ***Preporuka:***
  Kroz blanketnu normu kaznenu odgovornost jasno povezati s konkretnim povredama sigurnosnih i regulatornih obveza propisanih europskim i nacionalnim zakonodavstvom koji uređuje korištenje AI sustava.

2) Preciznije definiranje opsega

AmCham smatra da je potrebno preciznije vezati kaznenu odgovornost uz određene specifične posljedice uzrokovane uporabom AI-ja. Umjesto općeg pojma „izazivanja opasnosti", predlažemo da se definira uži skup situacija u kojima dolazi do kaznene odgovornosti. Primjerice, kada je AI korišten na način koji dovodi do ozbiljnih povreda sigurnosti, manipulacije informacijama s teškim društvenim posljedicama, ugrožavanja kritične infrastrukture ili drugih oblika štete. Takav pristup već je prisutan u nekim europskim zakonodavstvima, gdje se kazneno pravo predviđa prvenstveno za konkretne zlouporabe tehnologije, poput ozbiljnih prijevara ili manipulacija identitetom (*deepfake*).

AmCham podržava odgovornu primjenu AI-ja i potrebu sankcioniranja njegovih ozbiljnih zlouporaba. Međutim, smatramo da kaznenopravni okvir mora biti dovoljno jasan, predvidiv i usklađen s europskim regulatornim pristupom kako bi istodobno štitio građane i poticao inovacije. Jasnije definiranje granica odgovornosti i njihovo povezivanje s konkretnim regulatornim obvezama doprinijelo bi stvaranju stabilnog okruženja za razvoj i primjenu umjetne inteligencije u Hrvatskoj te poticanje gospodarskog rasta.

- ***Preporuka:***
  Kaznenu odgovornost preciznije ograničiti na jasno definirane i posebno štetne oblike zlouporabe AI-ja kao što su manipulacija identitetom, ozbiljne prevare i ugrožavanje kritične infrastrukture.

3) Primjena načela proporcionalnosti i postupnosti odgovornosti

AmCham predlaže jasnije razlikovanje regulatornih, građanskopravnih i kaznenopravnih oblika odgovornosti, pri čemu bi se kazneno pravo primjenjivalo prvenstveno na najteže i namjerne oblike zlouporabe AI-ja.

Većina europskih i međunarodnih regulatornih okvira pitanja povezana s AI sustavima prvenstveno rješava kroz upravljanje rizicima, regulatorni nadzor, upravne mjere i odgovornost za štetu, dok se kazneno pravo koristi kao krajnje sredstvo za posebno opasna ili namjerna postupanja. Takav pristup omogućuje učinkovitu zaštitu građana uz veću pravnu sigurnost za organizacije koje razvijaju i koriste AI sustave.

- ***Preporuka:***
  Kazneno pravo treba primjenjivati prvenstveno na najteže i namjerne zlouporabe umjetne inteligencije, dok se ostali rizici trebaju rješavati kroz regulatorne i građanskopravne mehanizme u skladu s međunarodnom praksom.

Za dodatne informacije molimo kontaktirajte: Američka gospodarska komora u Hrvatskoj

Andrea Doko Jelušić | Izvršna direktorica

T: 01 4836 777 | E: andrea.doko@amcham.hr