

Dr. sc. Ivan Glavić*
Ivan Vidaković**

POTENCIJALI UPORABE UMJETNE INTELIGENCIJE U RADU DRŽAVNOG ODVJETNIŠTVA KROZ PRIZMU UREDBE (EU) 2024/1689 O UMJETNOJ INTELIGENCIJI

Počinitelji kaznenih djela već dugi niz godina koriste prednosti rapidnog razvoja tehnologije, ali oni nisu jedini koji imaju taj potencijal. Tijela kaznenog progona, u prvom redu državno odvjetništvo, imaju mogućnost primjene sustava umjetne inteligencije kako bi učinkovitije ostvarivala svoju temeljnu zadaću kaznenog progona počinitelja kaznenih djela, uz svojevrsne rizike. U prvom dijelu rada daje se pregled pravnih izvora koji reguliraju uporabu sustava UI-ja koji imaju potencijal primjene u radu državnog odvjetništva te se analiziraju načela uporabe sustava umjetne inteligencije koja su im zajednička. Nadalje, analiziraju se odredbe Uredbe EU-a o umjetnoj inteligenciji, s naglaskom na sustave različite kategorije rizika. Nastavak rada daje analizu utjecaja uporabe sustava umjetne inteligencije na rad državnog odvjetništva, s naglaskom na temeljna načela Zakona o kaznenom postupku te kompatibilnost uporabe de lege lata. Posljednji je dio usmjeren na organizaciju rada i potencijal primjene UI-a kroz uočavanje dijelova organizacije rada koji imaju slabosti i gdje primjena umjetne inteligencije ima najveći potencijal, uz prijedloge de lege ferenda. Rezultati rada upućuju na to da su načela hrvatskog kaznenog postupka i ovlasti državnog odvjetništva komplementarni obvezama iz prava EU-a te postojećim inicijativama, ali da su nužne dopune pozitivnih propisa radi

* Dr. sc. Ivan Glavić, zamjenik Glavnog državnog odvjetnika Republike Hrvatske; ivan.glavic@dorh.hr; ORCID iD: <https://orcid.org/0000-0003-4055-3286>

** Ivan Vidaković, univ. mag. iur., asistent na Katedri kaznenopravnih znanosti, Sveučilište J. J. Strossmayera u Osijeku, Pravni fakultet Osijek; ivan.vidakovic@pravos.hr; ORCID iD: <https://orcid.org/0000-0002-7003-632X>

osiguranja transparentnosti i mogućnosti ocjene zakonitosti i vjerodostojnosti podataka i dokaza.

Ključne riječi: državno odvjetništvo, umjetna inteligencija, učinkovitost kaznenog progona, zakonitost dokaza, vještačenje

1. UVODNA RAZMATRANJA

Pravo, iako percipirano kao tradicionalno, izloženo je dugi niz godina tehnološkim inovacijama i implementacijama novih tehnologija. Transformativni je potencijal prava u tom smislu neograničen. Takav proces modernizacije i digitalizacije sada ima i potencijalnu novu dimenziju, a to je uključivanje umjetne inteligencije. To je prepoznato i u Nacionalnoj razvojnoj strategiji Republike Hrvatske do 2030. godine, gdje se među prvim razvojnim potrebama i potencijalima navode upravo tehnološke promjene i rastuća uloga umjetne inteligencije.¹ Jednako tako i u Strategiji digitalne Hrvatske za razdoblje do 2032. implementacija i uporaba umjetne inteligencije kroz sinergiju akademske zajednice te javnog i privatnog sektora predstavlja jednu od okosnica ostvarivanja ciljeva.² Putem Nacionalnog plana razvoja pravosudnog sustava za razdoblje od 2022. do 2027. godine naglašen je potencijal umjetne inteligencije u radu sudova i državnih odvjetništava, uz kritiku da se trenutačno koristi izrazito ograničeno.³

Takve težnje i trendovi Republike Hrvatske nisu iznimka, već su utemeljeni na primjerima i politikama drugih država, pogotovo država Europske unije koje su glede implementacije i razvoja sustava umjetne inteligencije u pravosuđu malo više odmakle. Potencijal državnog odvjetništva za takav tip transformacije nije iznimka, a uporaba umjetne inteligencije u različitim aspektima rada predstavlja jedan od temeljnih ciljeva svih ranije navedenih dokumenata. Sukladno Izvješću Glavnog državnog odvjetnika Republike Hrvatske o radu državnih odvjetništava u 2024. godini zaprimljeno je 235 785 novih predmeta, odnosno 14 615 predmeta više u odnosu na prethodnu godinu, što predstavlja povećanje od 6,6 %.⁴ Već iz takvih podataka možemo zaključiti o potencijalu

¹ Nacionalna razvojna strategija Republike Hrvatske do 2030. godine, *Narodne novine*, br. 13/2021.

² Strategija digitalne Hrvatske za razdoblje do 2032. godine, *Narodne novine*, br. 2/2023.

³ Ministarstvo pravosuđa i uprave, Nacionalni plan razvoja pravosudnog sustava za razdoblje od 2022. do 2027. godine, 2022, dostupno na: https://mpudt.gov.hr/UserDocsImages/dokumenti/Strategije,%20planovi,%20izvješća/Nacionalni%20plan%20razvoja%20pravosudnog%20sustava%20za%20razdoblje%202022_2027.pdf (11. 8. 2025).

⁴ Državno odvjetništvo Republike Hrvatske, Izvješće o radu državnih odvjetništava u 2024. godini, 2025, str. 9, dostupno na: <https://dorh.hr/sites/default/files/dokumenti/2025-04/>

uporabe sustava umjetne inteligencije, koji bi pomogao u filtriranju predmeta, selekciji i dodjeli u rad. Jednako tako, kompleksnost kriminala postaje sve veća, a spisi predmeta kompliciraniji, stoga sustavi umjetne inteligencije mogu biti od značajne pomoći u organizaciji predmeta, evaluaciji dokaza i drugih aktivnosti državnog odvjetnika. Znatno lakše globalno kretanje i migracija unose drugi segment kompleksnosti suvremenih kaznenih postupaka, a to je višejezičnost i nerazumijevanje pravne kulture i zakonskih odredaba. Umjetna inteligencija može pridonijeti premošćivanju toga jaza i osiguranju ostvarivanja pravne zaštite i pravodobnog i potpunog informiranja osoba iz trećih država.

Ipak, takva rješenja ne dolaze bez rizika. Upravo su rizici koje uporaba sustava umjetne inteligencije donosi u središtu mnogobrojnih inicijativa za pravno uređenje njihove uporabe. Razmatrajući njihov spektar, neovisno o različitosti pristupa u pokušajima regulacije, mogu se pronaći zajednička načela kojima se nastoji osigurati umanjivanje rizika. Rizici posebno dolaze do izražaja u kaznenim postupcima i postupanjima državnih odvjetništava i sudova s obzirom na narav pravnih vrijednosti koje se štite kaznenim pravom, ali i osjetljivosti kaznenog postupka za pojedince. Naime, tradicionalna i prihvaćena načela kaznenog postupka, poput načela legaliteta, slobodne ocjene dokaza, pretpostavke okrivljenikove nedužnosti, ali i druga pod izravnim su utjecajem primjene umjetne inteligencije. Izgledno je da će ona biti sve prisutnija u pravosuđu, stoga bi potonje spomenuta ravnoteža trebala biti utemeljena na zajednički prepoznatim potencijalima i rizicima kroz različite regulatorne inicijative, uvažavajući tradicionalne postavke kaznenog postupka.

2. PRISTUPI STVARANJU PRAVNOG OKVIRA ZA UPORABU UMJETNE INTELIGENCIJE

Rapidan razvoj i primjena tehnologije potaknuli su niz regulatornih inicijativa kojima se nastojao stvoriti pravni okvir za uporabu umjetne inteligencije. Mozaik takvih inicijativa jasno pokazuje različite pristupe pravnom uređenju od humanocentričnih i onih usmjerenih na ljudska prava i temeljne slobode do sektorskih te onih usmjerenih na tehničke i gospodarske aspekte.⁵ Ipak, takva

Izvješće%20o%20radu%20državnih%20odvjetništava%20za%202024.%20godinu.pdf (11. 8. 2025.).

⁵ Vidi više o različitim pristupima i regulatornim inicijativama: Viljanen, M.; Parviainen, H., AI Applications and Regulation: Mapping the Regulatory Strata, *Frontiers in Computer Science*, 2022, str. 5–10; Strojín, G., Pristupi međunarodne zajednice u regulisanju umjetne inteligencije, u: Završnik, A.; Simončić, K. (ur.), *Pravo i umjetna inteligencija: pitanja etike, prava čovjeka i društvene štete*, Dobra knjiga, Sarajevo, 2023, str. 17–29.

plejada propisa u sjecištu Vennova dijagrama ima određena načela i zahtjeve koji se mogu smatrati zajedničkim i kao takvi postavljaju temelje za specijalizirani pristup. To uključuje i temelje za pravno uređenje uporabe umjetne inteligencije u kaznenom pravosuđu, a samim time i radu državnog odvjetništva. Najvažnije izvore klasificirali su Rotenberg i Kyriakides kroz temeljnu podjelu na međunarodne i nacionalne instrumente regulacije, uz poseban naglasak na izvršne uredbe SAD-a. To uključuje: Povelju Vijeća Europe o etičkoj uporabi umjetne inteligencije u pravosuđu, Preporuke OECD-a o umjetnoj inteligenciji, Deklaraciju Ujedinjenih naroda iz Santiaga o pristupu pravosuđu u digitalno doba, Preporuku UNESCO-a o etici umjetne inteligencije, Smjernice Deklaracije iz Seoula o etici umjetne inteligencije, Okvirnu konvenciju Vijeća Europe o umjetnoj inteligenciji, ljudskim pravima, demokraciji i vladavini prava, Uredbu EU-a o umjetnoj inteligenciji, ali i neke druge izvore.⁶

Kad se razmatraju predmetni izvori, kao i niz drugih izvješća nevladinih organizacija i *think tankova*, mogu se uočiti određene zajedničke karakteristike. Prvenstveno se može zaključiti da globalne inicijative za pravno uređenje uporabe umjetne inteligencije imaju širi pristup od nacionalnih. Drugi je ključak da postoje određeni standardi i načela koji se postavljaju kao zahtjev za uporabu umjetne inteligencije neovisno o pristupu ili akterima koji su sudjelovali u njihovu kreiranju. Analizom predmetnih pristupa mogu se izdvojiti četiri načela koja su zajednička velikoj većini tih inicijativa, a čija je primjenjivost imperativ za prihvatljivu primjenu umjetne inteligencije u kaznenom pravosuđu i radu državnog odvjetništva. To su transparentnost i objašnjivost, ljudska kontrola nad odlukama, odnosno ograničenje automatiziranog odlučivanja, pravo na pravni lijek te načelo zabrane diskriminacije.⁷

2.1. Transparentnost i objašnjivost

Transparentnost kao koncept u kontekstu prava najbolje je definirana kao sposobnost sustava UI-ja da donose odluke na način koji čovjek može tumačiti

⁶ Vidi više: Rotenberg, M.; Kyriakides, E., *The AI Policy Sourcebook 2025*, Center for AI and Digital Policy, United States of America, 2025. Sličan pristup ima Schmitt, L., Mapping global AI governance: a nascent regime in a fragmented landscape, *AI Ethics*, vol. 2, 2022, str. 303–305; Cihon, P.; Maas, M. M.; Kemp, L., Fragmentation and the Future: Investigating Architectures for International AI Governance, *Global Policy*, vol. 11, br. 5, 2020, str. 546.

⁷ Sličan zaključak glede zajedničkih načela i standarda u različitim regulatornim inicijativama imali su Babnik, Simončić i Završnik, vidi više: Babnik, A.; Simončić, K.; Završnik, A., Upravljanje sistemima umjetne inteligencije: pregled regulacijskih inicijativa u svjetlu uspostavljanja efikasnog sistema globalnog upravljanja, u: Završnik, A.; Simončić, K. (ur.), *Pravo i umjetna inteligencija: pitanja etike, prava čovjeka i društvene štete*, Dobra knjiga, Sarajevo, 2023, str. 68–70.

i razumjeti, što predstavlja temelj za pravo i mogućnost da se takve odluke pregleđaju i ospore.⁸ Podrazumijeva dva bitna elementa: fizičku transparentnost, koje obuhvaća uvid u podatke, algoritme i način rada sustava, te kognitivnu transparentnost, koja postavlja zahtjev da sustav mora ljudima pružiti razumljiva objašnjenja svojih odluka.⁹ Ključan aspekt transparentnosti jest obavijest osobi da je predmetom obrade sustava umjetne inteligencije, bilo izravno bilo da je odluka državnog odvjetnika donesena na temelju uporabe sustava umjetne inteligencije.¹⁰ Sadržajno se objašnjivost i potonji vid transparentnosti preklapaju, stoga su i predmetom zajedničke analize. Takvi zahtjevi transparentnosti predlažu se i kroz mnogobrojne izvore, poput Univerzalnih smjernica za umjetnu inteligenciju (u daljnjem tekstu: Univerzalne smjernice) pod t. 1.¹¹ Oba su ta aspekta propisana i točkama 1.3. OECD-ovih načela za umjetnu inteligenciju i Smjernica G20.¹² Širi učinak načela razmatran je kroz t. 37.–41. UNESCO-ovih preporuka o etici umjetne inteligencije, uz napomenu da su transparentnost i objašnjivost nužnost za pravičnost, demokratsko društvo i režime odgovornosti u slučaju povrede temeljnih ljudskih prava i sloboda.¹³ Transparentnost je također jedno od temeljnih načela koja se navode u čl. 8. Okvirne konvencije Vijeća Europe u odnosu na specifičan kontekst i rizike kroz cjelokupni životni vijek sustava.¹⁴ Velika većina tih, ali i drugih izvora upućuje na to da osobe moraju biti obaviještene da su u interakciji, odnosno da su prema njima primijenjeni sustavi umjetne inteligencije. Također, poznavanje rada sustava kako bi se mogao procijeniti njihov rezultat jedan je od temeljnih aspekata transparentnosti, koji je nužan za njezino ostvarivanje.

Državni odvjetnici, postupajući u konkretnom predmetu, na temelju svojeg stručnog znanja, pravila logike i općeg životnog iskustva donose zaključke o

⁸ Papadouli, V., Transparency in Artificial Intelligence: A Legal Perspective, *Journal of Ethics and Legal Technologies*, vol. 4, 2022, str. 29.

⁹ *Ibid.*, str. 29–30.

¹⁰ Erdogan, I., Diving into the Iceberg: Establishing Transparency in AI for Law Enforcement, *European Papers*, vol. 9. br. 3, 2024, str. 962–965.

¹¹ The Public Voice, Universal Guidelines for Artificial Intelligence, Brussels, 2. listopada 2018., dostupno na: <https://thepublicvoice.org/AI-universal-guidelines/> (u daljnjem tekstu: Univerzalne smjernice).

¹² OECD, Recommendation of the Council on Artificial Intelligence, OECD/LEGAL/0449, 22. svibnja 2019., dostupno na: <https://legalinstruments.oecd.org/en/instruments/oecd-legal-0449> (u daljnjem tekstu: OCDE-ova načela za umjetnu inteligenciju).

¹³ UNESCO, Recommendation on the Ethics of Artificial Intelligence, Paris, 2021, dostupno na: <https://unesdoc.unesco.org/ark:/48223/pf0000380455> (u daljnjem tekstu: UNESCO-ove preporuke o etici umjetne inteligencije).

¹⁴ Council of Europe, Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law, CETS No. 225, usvojena 17. svibnja 2024., otvorena za potpis 5. rujna 2024., dostupno na: <https://www.refworld.org/legal/agreements/coeministers/2024/en/148016> (u daljnjem tekstu: Okvirna konvencija Vijeća Europe o umjetnoj inteligenciji).

nizu bitnih pitanja za okrivljenika, podrazumijeva se, u okviru Ustava, zakona te međunarodnih propisa. Postojanje osnovane sumnje i pokretanje kaznenog postupka jedno je od tih pitanja, o kojem, u skladu s načelom legaliteta, državni odvjetnik mora odlučiti na temelju niza postojećih izvora saznanja da je vjerojatnija činjenica da je osoba počinila kazneno djelo nego da nije.¹⁵ Ako bi procjenu postojanja odnosno nepostojanja osnovane sumnje utvrđivao sustav umjetne inteligencije, onda bi proces trebao biti jasan i obrazložen, odnosno element fizičke transparentnosti morao bi biti zadovoljen. Obveza objašnjivosti, a u ovom kontekstu i s njom neodvojiva transparentnost, proizlaze iz čl. 4. st. 4. Zakona o kaznenom postupku (u daljnjem tekstu: ZKP), koji jasno propisuje da sud i druga državna tijela moraju jasno obrazložiti svoje odluke. To proizlazi i iz pojedinačnih odredaba ZKP-a jer odluka o odbačaju kaznene prijave mora biti obrazložena sukladno čl. 206., kao što i rješenje o provođenju istrage sadrži kratko obrazloženje okolnosti iz kojih proizlazi osnovana sumnja.¹⁶ Jednako tako, obrazloženje koje sadrži optužnica mora sadržavati dokaze na kojima se temelji, kao i obrazloženje stanja stvari sukladno čl. 342. st. 1. t. 4. i 5. ZKP-a. Dakle, državni odvjetnik mora biti upoznat s procesom na temelju kojeg je sustav umjetne inteligencije došao do zaključka da postoji ili ne postoji osnovana sumnja kako bi ga mogao obrazložiti prilikom donošenja odluke na temelju takvih izlaznih rezultata sustava umjetne inteligencije koji bi mu dali preporuku za poduzimanje određene radnje. To je jednako tako važno i za ostvarivanja prava na učinkovitu istragu sukladno Europskoj konvenciji za zaštitu ljudski prava i temeljnih sloboda, pa i sustav nadzora nad ostvarivanjem načela legaliteta koji se ostvaruje u ustanovi supsidijarnog tužitelja.¹⁷ Stoga je nužno obavijestiti osobe koje su izravno pod utjecajem takve odluke da je ona donesena na temelju izlaznog rezultata sustava umjetne inteligencije i kako se taj rezultat formirao kako bi se proces i rezultati mogli nadzirati te kako bi se moglo ostvariti pravo na učinkovit pravni lijek u odnosu na takvu odluku.

¹⁵ Krapac, D., *Kazneno procesno pravo, Prva knjiga: Institucije, VIII. izmijenjeno i dopunjeno izdanje*, Narodne novine, Zagreb, 2020, str. 101.

¹⁶ Zakon o kaznenom postupku, *Narodne novine*, br. 152/08, 76/09, 80/11, 121/11, 91/12, 143/12, 56/13, 145/13, 152/14, 70/17, 126/19, 80/22, 36/24, 72/25 (u daljnjem tekstu: ZKP).

¹⁷ O nadzoru javnosti i uključenosti žrtve kao sastavnog elementa prava na učinkovitu istragu vidi više: Turković, K.; Viljac Herceg, F., Učinkovita istraga povreda prava zajamčenih Europskom konvencijom za zaštitu ljudskih prava, *Hrvatski ljetopis za kaznene znanosti i praksu*, vol. 26, br. 2, 2019, str. 280–281. O ulozi supsidijarnog tužitelja vidi više: Ljubanović, V.; Novokmet, A.; Tomičić, Z., *Kazneno procesno pravo – izabrana poglavlja*, Sveučilište Josipa Jurja Strossmayera u Osijeku, Pravni fakultet Osijek, 2020, str. 51–54; Krapac, D.; Lončarić, D., *Oštećenik kao tužitelj u krivičnom postupku*, Pravni fakultet u Zagrebu, Zagreb, 1985.

2.2. Zabrana automatiziranih odluka

Nameće se pitanje mora li se državni odvjetnik složiti s krajnjim rezultatom, tj. preporukom odnosno odlukom koju sustav predlaže. Analizirane inicijative nedvojbeno predlažu zabranu automatiziranih odluka kroz zagovaranje ljudskog nadzora nad automatiziranim odlučivanjem kao jedno od temeljnih načela. OECD-ova načela za umjetnu inteligenciju na više mjesta navode kao preporuku da moraju postojati mehanizmi ljudskog nadzora nad sustavima UI-ja te se to odnosi i na rizik koji može nastupiti u slučaju štete ili neželjenog ponašanja.¹⁸ Jednako tako, u UNESCO-ovim preporukama za etiku umjetne inteligencije jasno se naglašava da je logično da se ljudi oslanjaju na automatsko donošenje odluka putem sustava umjetne inteligencije zbog učinkovitosti, ali takvi sustavi nikada ne mogu zamijeniti čovjekovu konačnu ulogu.¹⁹ Okvirna konvencija Vijeća Europe povezuje transparentnost i ljudski nadzor kao obvezu da se on uspostavi u odnosu na specifičan kontekst i rizike za uporabu.²⁰ To nas dovodi do temeljnog koncepta rada sa sustavima umjetne inteligencije, a to je čovjek u petlji (engl. *human in the loop*). To je koncept koji se definira kao uključivanje osobe u donošenje pojedinačne odluke u suradnji s algoritmom. Takav model pretpostavlja da se sustavi s čovjekom u petlji uključuju kada pojedinac određuje hoće li ili kako implementirati algoritamski utemeljen zaključak. Pitanje je uloge koja je namijenjena čovjeku, a za državno odvjetništvo ključna je uloga objašnjavanja odnosno razumijevanja rezultata sustava. To je temelj i za ostvarivanje korektivne uloge. Naravno da državni odvjetnik može pogriješiti, stoga s pravom Nicholson, Crootof i Kaminski upozoravaju da samo dodavanje čovjeka nije automatsko rješenje jer može stvoriti lažan osjećaj sigurnosti, prebaciti odgovornost na ljudskog operatera i utjecaj na sam rezultat u slučaju pogrešnog rukovanja i upravljanja sustavom.²¹ Nastavno na transparentnost važno je da ljudi koji ga koriste razumiju kako funkcionira, da mogu interpretirati njegove rezultate i odlučiti ne prihvatiti algoritamsku preporuku.

Dakle, ako bi državni odvjetnik koristio sustav koji bi mu preporučio da ne podigne optužnicu ili procijenio da postoji mogućnost odbačaja kaznene prijave, on bi morao imati mogućnost ne postupiti u skladu s takvom odlukom. Ne samo to, nego bi kroz upravljanje sustavom trebao imati mogućnost definirati upite, odnosno *promptove*, te mogućnost podešavanja sustava da traži i analizira ono što je njemu relevantno za svaki individualni predmet. Time bi

¹⁸ OECD-ova načela za umjetnu inteligenciju, t. 1.2.b) i 1.4.b).

¹⁹ UNESCO-ove preporuke o etici umjetne inteligencije, t. 36.

²⁰ Okvirna konvencija Vijeća Europe o umjetnoj inteligenciji, čl. 8.

²¹ W. Nicholson, P. II.; Crootof, R.; Kaminski, M., *Humans in the Loop*, *Vanderbilt Law Review*, vol. 76, br. 2, 2023, str. 481.

se osiguralo ispunjavanje uvjeta učinkovitog ljudskog nadzora te bi se ostvarile prethodno naglašene uloge, koje onda stvaraju kvalitativnu osnovicu za izjavljivanje pravnog lijeka.

2.3. Pravo na pravni lijek

Pravo na pravni lijek kao civilizacijski standard i temeljno ljudsko pravo nije iznimka kad je u pitanju uporaba UI-ja. To više ovo se pravo ističe kao nužnost u svim relevantnim pravnim izvorima. Tako i Okvirna konvencija navodi uspostavu učinkovitog pravnog lijeka kroz cjelokupni životni ciklus sustava umjetne inteligencije, a to se nadovezuje na pitanje transparentnosti i objašnjivosti.²² OECD-ove smjernice nadovezuju se na transparentnost kao osnovni preduvjet da bi se osobe na koje je utjecao krajnji rezultat sustava mogle osporiti.²³ Isti takav pristup zastupljen je u UNESCO-ovim preporukama o etici umjetne inteligencije u t. 14. Dakle, osnovni preduvjet da bi se okrivljenik mogao žaliti, odnosno izjaviti pravni lijek jest da mora postojati obrazložena odluka koja mu za to daje osnovicu. Stoga odluka ne može biti automatizirana te osoba mora biti obaviještena da je odluka donesena na temelju rezultata sustava umjetne inteligencije i kako sustav funkcionira.

Ovdje treba naglasiti da odluke državnog odvjetnika često ne utječu samo na okrivljenika. Pitanje pravnog lijeka odnosi se i na oštećenikovo preuzimanje kaznenog progona u ulozi supsidijarnog tužitelja, koji bi u slučaju ekstenzivne primjene automatiziranog odlučivanja mogao imati naglašeniju ulogu u kontroli ostvarivanja načela legaliteta. Ako bi državni odvjetnik odustao od kaznenog progona na temelju preporuke, odnosno procjene sustava umjetne inteligencije, onda bi takav rezultat morao biti obrazložen i u uputi oštećeniku kao supsidijarnom tužitelju sukladno čl. 55. st. 1. ZKP-a kako bi mogao donijeti informiranu odluku hoće li preuzeti kazneni progon. Dakle, disruptivni element uporabe UI-ja na temelju čijeg je izlaznog rezultata odluka donesena zahtijeva određenu prilagodbu legislativnog okvira da bi se taj pravni lijek učinkovito mogao izjaviti. Primarno svaka odluka u svojem obrazloženju mora sadržavati obavijest da je upotrijebljen sustav umjetne inteligencije. Uz to, mora biti obrazložen način rada sustava na razumljiv način tako da se stvori osnovica za izjavljivanje pravnog lijeka. Istovremeno se time stvara i osnovica za odlučivanje o osnovanosti tijela koje će odlučivati povodom izjavljenog pravnog lijeka. Dakle, primjerice, ne samo za okrivljenika nego i za suca odnosno vijeće koje će u povodu žalbe okrivljenika odlučivati.

²² Okvirna konvencija Vijeća Europe o umjetnoj inteligenciji, čl. 14.

²³ OECD-ova načela za umjetnu inteligenciju, t. 1.3.iv.

2.4. Načelo zabrane diskriminacije

Razmatramo li primjenu umjetne inteligencije, posebno u sferi kaznenog prava, jedan od uočenih problema jest diskriminacija odnosno pristranost sustava.²⁴ Stoga i izvori koje ranije spominjemo upućuju na zabranu diskriminacije, poput OECD-ovih načela u t. 1.2. a), sukladno kojima svi akteri moraju poštovati princip zabrane diskriminacije i jednakosti.²⁵ Svi akteri dužni su osigurati zabranu diskriminacije sukladno čl. 10. st. 1. Okvirne konvencije Vijeća Europe kroz cjelokupni ciklus razvoja i rada sustava.²⁶ Jednako tako, UNESCO-ove preporuke u t. 28. zahtijevaju prilagodbu sustava tijekom cijelog životnog ciklusa na način da se jednako primjenjuje neovisno o rasi, spolu, podrijetlu godinama i nizu drugih atributa osiguravajući tako jednakost postupanja. Temeljno je pitanje treniranje modela, kao svojevrsna početna pozicija, jer ako modeli budu trenirani na temelju pristranih podataka, to će dovesti do diskriminatornih praksi. Istovremeno, ako su čak modeli trenirani sukladno zahtjevima kvalitete podataka iz čl. 10. st. 3. Uredbe EU-a, koji se mogu uzeti kao referentni, rezultati sustava u vidu preporuke, odluke ili predviđanja i dalje mogu biti diskriminatorni na temelju ulaznih podataka krajnjih korisnika, poput policije ili državnog odvjetništva.²⁷ To se posebno odnosi na situacije u kojima se za predviđanja koriste historijski podaci policije, kao u situacijama primjene prediktivnih sustava, bilo geografskih bilo individualnih. Takvi podaci nisu potpuno digitalizirani ili mogu biti pristrani jer, primjerice, koriste podatke policijske uprave s područja gdje imamo veću koncentraciju određenih počinitelja. U SAD-u su to četvrti i područja dominantno naseljeni afroameričkim stanovništvom, dok bi u primjeru Republike Hrvatske to mogla biti područja romskih naselja. Vidaković predlaže, na primjerima prediktivnih sustava, da se pravila o potpunosti, kvaliteti, reprezentativnosti i relevantnosti podataka prema pravilima visokorizičnih sustava trebaju koristiti i kod ulaznih podataka, a ne samo kod podataka za trening, test i validaciju.²⁸ To se odnosi na sve sustave koji koristi podatke iz ranijih postupanja policije i državnog odvjetništva jer su najčešće izvor potencijalne diskriminatorne prakse odnosno pristranosti.

²⁴ FRA, *Bias in Algorithms – Artificial Intelligence and Discrimination*, Vienna, 2022, str. 7–15.

²⁵ OECD-ova načela za umjetnu inteligenciju, t. 1.2. a).

²⁶ UNESCO-ove preporuke o etici umjetne inteligencije, t. 28.

²⁷ Okvirna konvencija vijeća Europe o umjetnoj inteligenciji, čl. 10. st. 1.

²⁸ Vidi više, Vidaković, I., *Uporaba prediktivnih sustava umjetne inteligencije namijenjenih tijelima kaznenog progona – Perspektiva Europske unije*, *Hrvatski ljetopis za kaznene znanosti i praksu*, vol. 31, br. 1, 2024, str. 114–115.

3. UREDBA EU-A O UMJETNOJ INTELIGENCIJI – POTENCIJALI I RIZICI PRIMJENE UMJETNE INTELIGENCIJE U RADU DRŽAVNOG ODVJETNIŠTVA

Regulativni pristup Uredbe Europske unije o umjetnoj inteligenciji utemeljen je na procjeni rizika te je usmjeren prema zaštiti javne sigurnosti i temeljnih ljudskih prava, zbog čega je rezultirao zabranom uporabe određenih sustava, strukturom neovisnog nadzora te strogim kriterijima za uporabu visokorizičnih sustava.²⁹ Iako se Uredba EU-a o umjetnoj inteligenciji oslanja na zaštitu temeljnih prava, temeljna je svrha uspostaviti usklađena pravila za siguran razvoj i uporabu sustava UI-ja, a ne stvarati okvir zaštite individualnih prava. To proizlazi iz činjenice da su rizici proizvodne sigurnosti tehničke i predvidive naravi, dok su rizici za temeljna prava društvenopolitički uvjetovani, složeniji i šire pravno određeni.³⁰ Razmatrajući pitanje razvoja europskog pristupa, možemo zaključiti da ima obilježje evolucijskog pristupa, koji pokazuje znatno viši stupanj razvoja i sofisticiranosti kod razumijevanja pravnog aspekta te problematike.³¹ Izdvojeno razmatranje Uredbe EU-a opravdano je iz dva razloga. Prvi proizlazi iz činjenice da je pravno uređenje u obliku uredbe, što za sve članice EU-a, pa tako i Republiku Hrvatsku, predstavlja obvezujući pravni akt koji predstavlja unifikaciju, a ne harmonizaciju. Drugi je razlog to što je to jedan od rijetkih pravnih okvira koji je usmjeren i na uporabu umjetne inteligencije u pravosudne svrhe te rad državnog odvjetništva. Takve odredbe nisu dominantne, no ipak postoji neki aspekt sektorskog pristupa koji je od velike važnosti i za rad državnog odvjetništva.³² Kad se razmotri sistematizacija sustava umjetne inteligencije, zaključak je da imamo četiri temeljne kategorije.³³ To su zabranjeni sustavi iz čl. 5. zbog neprihvatljivog rizika za temeljna prava, zdravlje i sigurnost; visokorizični sustavi čija je uporaba dopuštena uz stroge uvjete, uključujući i pravosuđe i kazneni progon; sustavi s obvezom transparentnosti, poput *chatbotova*; te jednostavni sustavi, koji ne nose značajne rizike, uz napomenu da svi subjekti moraju osigurati pismenost osoblja

²⁹ Ebers M., Truly Risk-based Regulation of Artificial Intelligence How to Implement the EU's AI Act, *European Journal of Risk Regulation*, vol. 16, br. 2, 2025, str. 689–690.

³⁰ Almada, M.; Petit, N., The EU AI Act: Between product safety and Fundamental rights, *SSRN Electronic Journal*, 2022, str. 17–18; *Ibid.*

³¹ Rotenberg, Kyriakades, *op. cit.* (bilj. 6), str. 4–5.

³² Uredba (EU) 2024/1689 Europskog parlamenta i Vijeća od 13. lipnja 2024. o utvrđivanju usklađenih pravila o umjetnoj inteligenciji i o izmjeni 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 umjetnoj inteligenciji) (u daljnjem tekstu: Uredba EU-a o umjetnoj inteligenciji), Preambula t. 59.

³³ Schwartmann, R.; Köhler, M., Risk-based approach, u: Schwartmann, R.; Keber, T. O.; Zenner, K. (ur.), *AI Act, A practical Guide*, C. F. Müller, 2025, str. 47.

u uporabi UI-ja. Ipak, u predmetnoj klasifikaciji postoje oni sustavi koji su po svojoj naravi relevantniji za rad državnog odvjetništva. Dakle, predmetom analize bit će sustavi s posebnim obvezama transparentnosti i neki visokorizični sustavi s obzirom na to da u Europi, ali i globalno, postoje primjeri njihove primjene u radu državnog odvjetništva.

3.1. Jednostavni sustavi umjetne inteligencije

U današnjem prekograničnom i višejezičnom kaznenom postupku sve se više koriste alati UI-ja za strojno prevođenje kako bi se ubrzala i olakšala obrada dokumenata. Jedan od službenih alata EU-a jest *eTranslation*, platforma Europske komisije integrirana u infrastrukturu *CEF Digital*, kojom pravosudne institucije u državama članicama mogu prevesti službene dokumente, poput europskih uhidbenih i istražnih naloga. Sa sigurnosne strane koristi se zatvorena mreža i evidencijsko pohranjivanje prijevoda na način siguran za obradu osjetljivog kaznenog materijala. Khalil i Way primijetili su da, iako *eTranslation* dosljedno prepoznaje pravne termine i strukture, sustav ponekad propušta nijanse specifične za pojedini pravni kontekst, što zahtijeva naknadnu stručnu lekturu i prilagodbu prije službene primjene u sudskim i upravnim postupcima.³⁴

Slično se u praksi koristi i *DeepL Pro*, komercijalni neuronski prevoditeljski sustav. Empirijska istraživanja kvalitete strojnog prevođenja u pravnoj domeni pokazuju određene nedostatke trenutačnih sustava UI-ja. Primjerice Giampieri u svojoj analizi platforme *DeepL* za prevođenje talijanskih pravnih tekstova na engleski prepoznaje kao ključne probleme koji nisu gramatičke naravi. Problematici su prijevodi pravnih formulacija i nepodudarnost s tradicionalnim pravničkim izražavanjem, odnosno pisanjem.³⁵ Komplementarno, Briva-Iglesias, Camargo i Dogru u svojoj usporedbi sustava *GPT-4*, *Vicuna* i *Google Translate* na četiri jezična para u pravnoj domeni otkrivaju zanimljivu diskrepanciju između automatskih metrika evaluacije i ljudske procjene. Iako *Google Translate* nadmašuje velike jezične model (LLM) u standardnim metrikama, profesionalni prevoditelji ocjenjuju *GPT-4* usporedivim ili boljim u kontekstualnoj adekvatnosti i dosljednosti terminologije, što je posebno važno

³⁴ Vidi više: Khalil, M.; Way, A., Multidimensional assessment of the eTranslation output for English to German and French translating EU legal texts, u: Martins, A. et al. (ur.), *Proceedings of the 22nd Annual Conference of the European Association for Machine Translation*, Portugal, 2018, str. 383–392.

³⁵ Giampieri, P., Is Machine Translation Reliable in the Legal Field? A Corpus-Based Critical Comparative Analysis for Teaching ESP at Tertiary Level, *Journal of English for Specific Purposes at Tertiary Level*, vol. 11, br. 1, 2023, str. 131–132.

za pravne prijevode.³⁶ Đurđević i Ivičević Karas u svojem pregledu primjene umjetne inteligencije u hrvatskom kaznenom postupku posebno ističu uvođenje obveznog tonskog snimanja rasprava te automatsko transkribiranje njihova sadržaja sukladno čl. 409.a st. 2. ZKP-a.³⁷ Autorice napominju da su prilikom rasprava najčešće korišteni alati UI-ja u početku nudili točnost transkripcije u rasponu od 70 % do 80 % za hrvatski jezik, što implicira potrebu za naknadnom provjerom i korekcijom svakog segmenta transkripta uz pomoć vremenski indeksiranih audiosnimaka.³⁸

Potencijal je ovih alata izrazito velik s obzirom na mogućnost prilagodbe kako za rad suda i državnog odvjetništva tako i, recimo, rad policije u kontaktu s osobama iz trećih zemalja prilikom uručivanja pouke o pravima i drugim sličnim situacijama. U tim slučajevima rizik bi bio nešto veći, ali jednako tako ubrzalo bi se postupanje, a potencijalno bi se i poboljšao položaj okrivljenika, koji bi lakše i brže mogao ostvariti pravnu pomoć i razumjeti pravnu situaciju na jeziku koji mu je najbliži.

3.2. Sustavi s obvezom transparentnosti

Za razliku od jednostavnih sustava, riječ je o sustavima za koje se smatra da predstavljaju umjereni rizik za prava pojedinca, zdravlje i sigurnost te su sukladno tome i nametnute obveze transparentnosti. Takva obveza za dobavljače podrazumijeva da, ako je sustav kreiran za izravnu komunikaciju s fizičkim osobama, one moraju biti obaviještene o činjenici da komuniciraju sa sustavom umjetne inteligencije, osim ako je to očito sa stajališta razmjerno dobro informirane, pronicljive i oprezne fizičke osobe, uzimajući u obzir okolnosti i kontekst upotrebe.³⁹

Primjeri su virtualni asistenti, odnosno *chatbotovi*, poput sustava EVVA, koji se primjenjuje u SAD-u, i *chatbota Sophia*. EVVA (*Enhanced Virtual Victim Assistant*) *chatbot* je razvijen u suradnji policije i istraživačkog instituta *RTI International*, testiran u gradu Greensboro u saveznoj državi Sjeverna Karolina.⁴⁰ Namjena je komunikacija sa žrtvama kaznenih djela, i to kon-

³⁶ Vidi više: Briva-Iglesias, V.; Camargo, J.; Dogru, G., Large language models „ad referendum“: How good are they at machine translation in the legal domain?, *Monografías de Traducción e Interpretación*, br. 16, 2024, str. 75–107.

³⁷ Đurđević, Z.; Ivičević Karas, E., Uporaba umjetne inteligencije u hrvatskom kaznenom postupku: postojeće stanje i perspektive, *Hrvatski ljetopis za kaznene znanosti i praksu*, vol. 30, br. 2, 2023, str. 231–232.

³⁸ *Ibid.*, str. 233.

³⁹ Uredba EU-a o umjetnoj inteligenciji, čl. 50. st. 1.

⁴⁰ Stratta, P., Greensboro Police Implement Chatbot Technology for Burglary Victims, 30. kolovoza 2022., dostupno na: <https://abc45.com/news/local/greensboro-police-implement-chatbot-technology-burglary-victims> (7. 8. 2025.).

kretno kaznenih djela koja bi odgovarala našem zakonskom opisu teške krađe iz čl. 229. st. 1. t. 1. sa svrhom pružanja podrške i pravovremene informacije nakon što prijave kazneno djelo. Riječ je o automatskom razgovornom agentu koji pruža informacije o tome kako zatražiti kopiju policijskog izvještaja, kako doći do kontaktnih podataka odjela ili istražitelja, kako podnijeti zahtjev za osiguranje, na koje načine osigurati dom nakon provale te koje su vrste usluga podrške dostupne u zajednici.⁴¹ Cilj je poboljšati komunikaciju sa žrtvama i njihovo zadovoljstvo postupkom, a istodobno rasteretiti istražitelje rutinskih upita. Sve dok *chatbot* samo daje informacije, bez autonomnog odlučivanja koje bi utjecalo na prava građana, možemo ga kategorizirati kao sustav s obvezom transparentnosti.

Slično vrijedi i za *Sophiu*, *chatbot* neprofitne udruge *Spring ACT* u Švicarskoj, koji anonimno savjetuje žrtve obiteljskog nasilja i pomaže im prikupiti dokaze zlostavljanja te potražiti pomoć. *Sophia* je pokrenuta 10. prosinca 2021. kao prvi globalni *chatbot* namijenjen isključivo žrtvama obiteljskog nasilja.⁴² Sustav funkcionira 24 sata na dan sedam dana u tjednu, dostupan je na više od 25 jezika i do danas je ostvario više od 42 000 interakcija s korisnicima iz 172 zemlje. Ključna dimenzija *chatbota Sophia* očituje se u njegovu modelu prikupljanja, procjene i učenja (engl. *Gather, Assess, Learn – GAL*).⁴³ Funkcija prikupljanja omogućuje žrtvama sigurno prikupljanje i pohranjivanje dokaza nasilja. Dokumenti, fotografije i glasovne poruke pohranjuju se u digitalni sef sustava na švicarskim poslužiteljima uz korištenje tehnologije kompatibilne s protokolom Amazon S3 s najstrožim standardima zaštite podataka. Faza procjene pruža pravne informacije o pravima žrtava, objašnjava policijske postupke i savjetuje o kontaktu s pravnim stručnjacima. Komponenta učenja educira korisnike o dostupnim pravnim sredstvima i lokalnim resursima podrške.

Chatbotovi u pravosuđu koji služe komunikaciji, bilo za podršku žrtvama i svjedocima bilo za informiranje građana, nisu visoko rizični jer ne obavljaju funkcije odlučivanja. Ipak, zanimljivo bi bilo razmatrati njihovu klasifikaciju ako bi davali informacije o oštećenikovu preuzimanju kaznenog progona na temelju kojih bi oštećenik odustao od preuzimanja kaznenog progona upravo uslijed takvih informacija.⁴⁴

⁴¹ Langton, L. et al., *Using AI to Enhance Victim Response*, *Police Chief Online*, 31. srpnja 2024., dostupno na: <https://www.policechiefmagazine.org/using-ai-victim-response/> (7. 8. 2025.).

⁴² Sundaraj Kuhn, S., *Spring ATC, Sophia: A Beacon of Hope on International Human Rights Day, 2023*, dostupno na: <https://springact.org/2023/12/21/international-human-rights-day/> (7. 8. 2025.).

⁴³ SOLVE, <https://solve.mit.edu/solutions/60260> (7. 8. 2025.).

⁴⁴ Možemo zamisliti situaciju u kojoj bi *chatbot* više puta upozoravao oštećenika kao supsidijarnog tužitelja na odredbu čl. 149. st. 2. ZKP-a prilikom informiranja o preuzimanju kaznenog progona. Opetovano upozoravanje na obvezu snošenja troškova postupka u slučaju

3.3. Sustavi visokog rizika

Visokorizični sustavi, kako ih definira čl. 6. i Prilog III. Uredbe EU-a o umjetnoj inteligenciji, obuhvaćaju sve alate UI-ja koji se koriste za evaluaciju pouzdanosti dokaza, predviđanje kriminalnog ponašanja, procjenu recidiva, prepoznavanje emocija ili detekciju obmane. Takvi sustavi izravno utječu na tijek kaznenog postupka, a pogrešna procjena može imati ozbiljne posljedice, od neopravdanog oduzimanja slobode do odustajanja od kaznenog progona, odnosno njegova pokretanja. Stoga su za takve sustave Uredbom propisane stroge obveze.⁴⁵ Oni moraju imati uspostavljen sustav upravljanja rizicima koji identificira moguće štetne učinke na prava pojedinca i predviđa načine njihova ublažavanja. Podaci za treniranje, testiranje i validaciju moraju biti kvalitetni, reprezentativni i nepristrani kako bi se izbjeglo ponavljanje postojećih diskriminatorskih obrazaca. Potrebno je voditi opsežnu tehničku dokumentaciju koja opisuje rad sustava, korištene algoritme i podatke, kao i rezultate provjera. Svaki izlaz mora biti evidentiran tako da se naknadno može rekonstruirati kako je umjetna inteligencija došla do određenog zaključka. Ključna je i transparentnost prema korisnicima, tužitelji i istražitelji moraju znati kako čitati rezultate, koja su njihova ograničenja i u kojim ih situacijama treba dodatno provjeriti. Ljudski nadzor ostaje obavezan, a sustav mora biti robustan, točan i siguran od manipulacija.

3.3.1. Evaluacija dokaza tijekom istrage ili progona kaznenih djela

Cjelokupni postupak kaznenog progona počiva na otkrivanju i evaluaciji otkrivenog. Načelo legaliteta nedvojbeno nalaže državnom odvjetniku da je dužan pokrenuti kazneni progon kada postoji osnovana sumnja da je određena osoba počinila kazneno djelo za koje se kazneni progon provodi po službenoj dužnosti, a nema zakonskih smetnji za poduzimanje tog progona.⁴⁶ Što konstituira stupanj sumnje koji je dostatan za pokretanje kaznenog progona, procjenjuje državni odvjetnik. To je nesporna tradicionalna djelatnost, ali novi, disruptivni elementi poput UI-ja mogu utjecati na nju. To su sustavi umjetne inteligencije koji mogu vršiti analize i procjene dokaza koje bi mogle upozoriti na određene korelacije koje nisu lako uočljive. Jednako tako, takvi sustavi na temelju analize ranijih predmeta mogu donijeti zaključak može li određeni

preuzimanja kaznenog progona koji bi završio oslobađajućom presudom, presudom kojom se optužba odbija ili rješenjem o obustavi postupka moglo bi imati učinak odvratanja od ostvarivanja prava preuzimanja kaznenog progona.

⁴⁵ Uredba EU-a o umjetnoj inteligenciji, čl. 8.–15.

⁴⁶ ZKP, čl. 2. st. 2.

krug indicija odnosno spoznaja činiti dostatan stupanj sumnje za pokretanje kaznenog progona. Jednako tako, o toj državnoodvjetničkoj ocjeni ovisi odluka o odustanku od kaznenog progona ili podizanju optužnice. Temeljna se pitanja nadovezuju na već ranije objašnjena načela, a to je u prvom redu kako ti sustavi dolaze do zaključka, odnosno kako formiraju rezultat u vidu preporuke ili čak odluke, koliko je to jasno i objašnjeno ljudima koji sustav koriste te koliko su oni na koje takve odluke utječu upoznati s time, odnosno jesu li dovoljno da mogu učinkovito izjaviti pravni lijek.

Primjena takvih sustava nije samo teoretska. Sustav *VeriPol* razvijen je u Španjolskoj kao algoritamski alat namijenjen otkrivanju lažnih prijava kaznenih djela inkriminiranih u čl. 457. španjolskog Kaznenog zakona. Temelji se na metodama obrade prirodnog jezika i modelu *Ridge Logistic Regression*, a svrha mu je analiza sadržaja pisanih prijava radi procjene vjerojatnosti da su one lažne.⁴⁷ Operativno, nakon što građanin podnese prijavu, policijski je službenik unosi u informacijski sustav SIDENPOL. Istražitelj zatim odlučuje hoće li je uputiti u obradu kroz *VeriPol*, koji analizira opis događaja i vraća procjenu vjerojatnosti lažnosti u rasponu od 0 do 1, pri čemu se vrijednosti bliže 1 interpretiraju kao veća vjerojatnost da je prijava lažna. Rezultat nije obvezujući, već služi kao pomoćno sredstvo u radu državnog odvjetništva i policije.⁴⁸

U početnim testiranjima kreatori sustava navode da je točnost modela u tim testovima dosegla 90–92 %, a u kasnijim evaluacijama i 96 %, uz stopu pogrešnih pozitivnih rezultata (engl. *false positives*) od oko 9 %.⁴⁹ Unatoč početnim optimističnim pokazateljima, primjena u praksi otkrila je niz metodoloških i operativnih ograničenja. Model je treniran na svega približno 1100 prijava iz jedne godine, što ga čini ograničeno reprezentativnim u odnosu na ukupni broj prijava koje se godišnje zaprimaju.⁵⁰ Jezične i kulturne razlike među regijama nisu bile uzete u obzir, a dodatni izvor pristranosti predstavlja činjenica da sustav analizira tekst koji sastavlja policijski službenik na temelju izjave prijavitelja, a ne neposredne riječi samog prijavitelja. Time se u analizu ugrađuje i standardizirani stil pisanja policajaca, koji može nesvjesno varirati između slučajeva za koje se kasnije pokaže da su lažni i onih koji su istiniti.⁵¹

⁴⁷ Quijano-Sánchez, L. et al., Applying automatic text-based detection of deceptive language to police reports: Extracting behavioral patterns from a multi-step classification model to understand how we lie to the police, *Knowledge-Based Systems*, vol. 149, 2018, str. 157–158.

⁴⁸ Martínez Garay, L. et al., *Three Predictive Policing Approaches in Spain: VioGén, RisCanvi and VeriPol. Assessment from a Human Rights Perspective*, Universitat de València, 2022, str. 125, dostupno na: <https://ai-watch.github.io/AI-watch-T6-X/service/90122.html> (8. 8. 2025.).

⁴⁹ Quijano-Sánchez, et al., *op. cit.* (bilj. 47), str. 163–164.

⁵⁰ *Ibid.*

⁵¹ Martínez Garay, L. et al., *op. cit.* (bilj. 48), str. 123.

Pravna priroda rezultata također je jasno određena, zaključci *VeriPola* nemaju dokaznu vrijednost u kaznenom postupku te se ne mogu koristiti kao samostalna osnova za pokretanje kaznenog progona zbog kaznenog djela lažnog prijavljivanja.⁵² Oni služe isključivo kao interni indikator za odlučivanje hoće li se nastaviti istraga i na koji način. Ne postoji formalni protokol koji bi propisivao kada i kako se sustav mora koristiti, a odluka o njegovu uključivanju prepuštena je diskreciji istražitelja.⁵³

Case Explorer jest sustav UI-ja razvijen za potrebe Ureda krunskog tužiteljstva u Ujedinjenom Kraljevstvu u suradnji s *NTT Data UK&I* i *Microsoft* namijenjen ubrzanju i unapređenju pregleda kaznenih spisa u složenim predmetima.⁵⁴ Temelji se na naprednoj obradi prirodnog jezika, koja omogućuje semantičku analizu velikih količina nestrukturiranog teksta iz policijskih izvješća, iskaza svjedoka, forenzičkih nalaza i drugih dokaznih materijala. Sustav automatski sažima dokumente, ističe ključne činjenice, osobe, događaje i dokaze, povezuje informacije unutar predmeta te prepoznaje obrasce u dokazima, čime tužiteljima daje brzi i strukturirani pregled ključnih elemenata slučaja. Dakle, primjenjuje se primarno u fazi kada tužitelj odlučuje o podizanju optužnice i tijekom pripreme suđenja, osobito u predmetima s velikim brojem dokumenata, poput financijskih istraga, organiziranog kriminala i slično. Interna ispitivanja i pilotni projekti pokazuju da slične funkcionalnosti UI-ja, primjerice *Microsoft Copilot*, mogu uštedjeti tisuće radnih sati godišnje i znatno smanjiti administrativno opterećenje tužitelja i pravnih službenika.⁵⁵ *Case Explorer* trebao bi se koristiti isključivo kao pomoćni alat, svi sažeci generirani uz pomoć UI-ja podliježu ljudskoj provjeri i konačna odluka uvijek ostaje na tužitelju.

Ipak, na ovom mjestu treba upozoriti na potencijalne probleme uporabe takvih sustava u svrhe kaznenog progona. Takvi sustavi u sumiranju mogu previdjeti određene informacije koje mogu direktno utjecati na odluku državnog

⁵² Maqueda, A. *et al.*, Spanish National Police Halts Veripol, Its Flagship AI To Detect False Reports, Algorithm Watch, 2025, dostupno na: <https://algorithmwatch.org/en/spanish-police-halts-veripol/> (7. 8. 2025.).

⁵³ Martínez Garay, L. *et al.*, *op. cit.* (bilj. 48), str. 125.

⁵⁴ Chaturvedi, S., *A force for good: How AI and GenAI are reshaping our world, Explore real-world examples that show how organizations and industries around the globe are using AI and GenAI to rapidly change for the better*, 2025, dostupno na: <https://services.global.ntt/en-us/insights/blog/a-force-for-good-how-ai-and-genai-are-reshaping-our-world#:~:text=spending%20significantly%20less%20time%20on,streamlined%20engineering%20workflows%20and%20delivered> (8. 8. 2025.).

⁵⁵ UK Parliament, Crown Prosecution Service: Artificial Intelligence, Question for Attorney General, UIN 26406, tabled on 27 January 2025, dostupno na: <https://questions-statements.parliament.uk/written-questions/detail/2025-01-27/26406?ref=machine.news#:~:text=A%20pilot%20of%20Microsoft%20Copilot,presentations%2C%20and%20analysing%20excel%20data> (7. 8. 2025.).

odvjetnika. Sumiranjem činjenica slučaja sustavi bi mogli favorizirati činjenice koje idu u prilog krivnji nasuprot nedužnosti, što bi moglo biti suprotno obvezi iz čl. 9. ZKP-a st. 1. i 2. ZKP-a. Stoga će za primjenu takvih sustava biti nužna edukacija, odnosno razvoj pismenosti u skladu s čl. 4. Uredbe EU-a o umjetnoj inteligenciji jer pogrešna interpretacija rezultata koji potencijalno u budućnosti mogu imati i preporuku kako postupiti u predmetu ima značajne posljedice za okrivljenika. U tim slučajevima moguće su i korelacije koje nisu bile vidljive ili jasne državnom odvjetniku, stoga će i objašnjivost biti ključna. Kvaliteta ulaznih podataka ovisit će o kvaliteti spisa predmeta, ali to bi moglo imati pozitivan učinak glede uniformnosti postupanja na razini cjelokupnog teritorija djelovanja državnog odvjetništva.

3.3.2. Poligrafi i slični alati

Drugi segment evaluacije dokaza može se odnositi na provjeru istinitosti iskaza svjedoka ili okrivljenika. Prepoznavanje emocija može biti od značajne važnosti, kao i uočavanje nepodudarnosti. Iako je riječ o tradicionalnoj djelatnosti državnog odvjetnika, policije i istražitelja, s vremenom su se razvili alati koji mogu detektirati određene emocije kod osobe čiji se iskaz može koristiti kao dokaz u kaznenom postupku. Primarno je pitanje u koju skupinu visokorizičnih sustava svrstati te sustave UI-ja. Izvorno bi s obzirom na svoje karakteristike trebali biti svrstani u kategoriju poligrafa i sličnih alata iz Annexa III, t. 6.b).⁵⁶ Ipak, smatramo da je, ako se sustav koristi za procjenu vjerodostojnosti iskaza svjedoka, okrivljenika ili vještaka, riječ o evaluaciji dokaza s obzirom na to da su to, sukladno odredbama hrvatskog Zakona o kaznenom postupku, dokazi u užem smislu riječi.⁵⁷ Jednako tako, takvi sustavi mogu se smatrati sustavima za prepoznavanje emocija iz točke 1.c) Annexa III, što bi bila druga kategorija, ali konačni rezultat ostaje isti. Njihova uporaba od strane državnog odvjetništva, neovisno o tome u koju kategoriju spadaju, rezultira jednakom primjernom strogih kriterija koje visokorizični sustavi moraju ispuniti.

Ti su sustavi fokusirani prvenstveno na fiziološke i bihevioralne pokazatelje, a ne na lingvističku analizu iskaza. Među njima posebno mjesto zauzima *Computer Voice Stress Analyzer*, tehnologija koja mjeri mikrotremore u glasu ispitanika, za koje se tvrdi da su fiziološka reakcija na stres izazvan laganjem. Test se može provoditi uživo ili analizom snimljenog govora, a softver potom

⁵⁶ Takav zaključak temelji na razmatranjima budućnosti poligrafa u kombinaciji s umjetnom inteligencijom i tehnologijom prepoznavanja lica od strane Tomičića, vidi više: Tomičić, Z., Poligrafsko ispitivanje – drugačiji pogled i nove perspektive, *Zbornik radova Pravne fakulteta u Splitu*, god. 60, 1/2023, str. 169–171.

⁵⁷ Krapac, *op. cit.* (bilj. 15), str. 436.

daje procjenu vjerojatnosti neiskrenosti. Iako proizvođači navode da se sustav oslanja na objektivne bihevioralne pokazatelje, neovisne forenzičke i kriminološke studije pokazuju da ne postoji dosljedna znanstvena potvrda pouzdanosti takvih metoda niti da one sustavno nadmašuju slučajno pogađanje.⁵⁸ Sudska praksa stoga takve rezultate tretira analogno poligrafu kao nepouzdanu i neprimjenjivu kao dokaz u kaznenom postupku. Čak i kada su ispitanici nakon testa davali priznanja, sudovi inzistiraju na jasno odvojenim izjavama, nezavisnim od same evaluacije uz pomoć UI-ja.⁵⁹

Drugi je primjer *EyeDetect*, komercijalni sustav koji koristi infracrvene kamere za mjerenje pokreta očiju, dilatacije zjenica i obrazaca pogleda tijekom odgovaranja na pitanja. Temelji se na pretpostavci da laganje izaziva povećano kognitivno opterećenje, koje se odražava u parametrima okulomotorike. Proizvođač *Converus* navodi laboratorijsku točnost od oko 85 %, no neovisna evaluacija naglašava da pouzdanost te metode u forenzičkim uvjetima nije potvrđena te da rezultati mogu varirati ovisno o vrsti pitanja, iskustvu ispitanika i kontekstu ispitivanja.⁶⁰ Kritičari ističu da se *EyeDetect* suočava s istim problemima kao i druge tehnologije detekcije laži: nepoznata stopa pogreške u realnim uvjetima, manjak općeprihvaćenosti i ograničena transparentnost algoritama, zbog čega se njegova dokazna uporaba trenutačno ne preporučuje u dokazne, već isključivo istražne svrhe.⁶¹

Potencijal i rizike primjene tih sustava treba shvatiti ozbiljno. Najčešća se kritika odnosi na neprihvatljivost rezultata kao dokaza, ali to treba staviti u perspektivu različitih stadija kaznenog postupka. Novokmet, Tomičić i Vidaković već su naglasili da rezultati takvih sustava ne bi trebali biti korišteni u stadijima kaznenog postupka u kojima se primjenjuje pravilo *in dubio pro reo*.⁶² Ipak,

⁵⁸ Vrij, A.; Fisher, R. P., Unraveling the Misconception About Deception and Nervous Behavior, *Frontiers in Psychology*, vol. 11, 2020, str. 1–8.

⁵⁹ Vidi više: McCall, B., Voice Stress Analysis: Is „Some Evidence“ Sufficient Grounds for Making Legal Determinations?, *Barry Law Review*, vol. 29, br. 1, 2024, str. 32–69; *People v. Salgado*, No. G028368, 2003 WL 21311241 (Cal. Ct. App. June 9, 2003), *United States v. Ricketts*, 141 F. App'x 93 (4th Cir. 2005), *State v. Schiefelbein*, 230 S.W.3d 88 (Tenn. Crim. App. 2007); *People v. Springsted*, 2016 COA 188 (Colo. App. 2016).

⁶⁰ Sve naznake učinkovite uporabe te tehnologije pokazale su se isključivo u kontroliranim i eksperimentalnim uvjetima, dok se uzima rezerva primjene u stvarnim uvjetima istraživanja i dokazivanja. Tako i Ghosh, M. M.; Mahajan, P. B.; Ramesh, P. P., Detection of Deception through Eye Detect System (EDS), *International Journal of Indian Psychology*, vol. 11, br. 2, str. 355–366.

⁶¹ Burgoon, J.; Pete Blair, J.; Qin, T.; Nunamaker, J., Detecting Deception through Linguistic Analysis, *Intelligence and Security Informatics*, 2003, str. 91–101.

⁶² Novokmet, A.; Tomičić, Z.; Vidaković, I., Facial Recognition Technology in EU Criminal Justice – Human Rights Implications and Challenges, *EU and Comparative Law Issues and Challenges Series (ECLIC)*, vol. 7, str. 562–564. Isto tako Tomičić, *loc. cit.* (bilj. 56).

postoji potencijal primjene u istraživačkom radu državnog odvjetništva, gdje bi se mogla procjenjivati pouzdanost iskaza osoba, na temelju koje bi se mogle donositi i druge odluke, kako o odustanku od kaznenog progona tako i one o nastavku. Jednako tako, uz druge indicije i spoznaje rezultati tih sustava mogli bi biti značajni za poduzimanje nekih drugih dokaznih radnji, poput pretrage, te bi mogli rezultirati i podizanjem optužnice, pa u konačnici i osudom. Rizik je takvih sustava to što su pseudoznanstveni, no kao pomoćno sredstvo mogu poslužiti državnom odvjetniku za opravdanje poduzimanja pojedinih dokaznih radnji te druge relevantne odluke o kaznenom progону.

3.4. Zabranjene prakse u području umjetne inteligencije

Za neke se sustave pretpostavlja da njihova uporaba predstavlja neprihvatljiv rizik temeljnim pravima i vrijednostima Unije, stoga su sukladno čl. 5. Uredbe EU-a o umjetnoj inteligenciji zabranjeni. Ipak, za određene sustave predviđene su iznimke, odnosno strogo i usko definirani kriterij kada bi njihova uporaba mogla biti dopuštena. Jedni su od njih prediktivni sustavi, odnosno sustavi koji procjenjuju ili predviđaju rizik da će osoba počiniti kazneno djelo isključivo na temelju izrade profila ili njihovih osobina i obilježja ličnosti; ta se zabrana ne primjenjuje na sustave UI-ja koji se upotrebljavaju za potporu ljudskoj procjeni uključenosti osobe u kriminalnu aktivnost, koja se već temelji na objektivnim i provjerljivim činjenicama izravno povezanim s kriminalnom aktivnošću.⁶³

Quatrocchio tumači tu iznimku na način da se ta mogućnost odnosi na druge sustave, nakon što se ustanovi povezanost osobe s konkretnim kriminalnim aktivnostima.⁶⁴ Time se anulira mogućnost primjene prediktivnih sustava za individualno profiliranje u skladu s njihovom inherentnom prirodom, a to je da na temelju historijskih podataka, koji su pretežito podaci za izradu profila, osobina i ličnosti, predvide da će osoba biti počinitelj kaznenog djela prije negoli je djelo uopće počinjeno. Quatrocchio naglašava da se to odnosi na sve aktuarijske alate s obzirom na podatke koje oni obrađuju kako bi došli do izlaznog rezultata.⁶⁵ Na istom su tragu Voigt i Hullen, koji navode, tumačeći odredbe Uredbe, da predviđanje sustava da će određena osoba opljačkati banku koje je rezultat osobnih podataka, poput prisutnosti na nastavi, mjesta prebivališta, prijašnjih kazneni djela i slično nije dopušteno. Ako bi pak sustav pratio bankovne račune i transakcije za prepoznavanje sumnjivih transakcija, njegova bi uporaba bila dopuštena, poput sustava za usporedbu otisaka prstiju na konkret-

⁶³ Uredba EU-a o umjetnoj inteligenciji, čl. 5. st. 1. toč. d).

⁶⁴ Quatrocchio, S., *Criminal law enforcement through AI*, u: Barfield, W. H.; Pagallo, U. (ur.), *Research Handbook on the Law of Artificial Intelligence*, 2025, str. 361–363.

⁶⁵ *Ibid.*

nom mjestu počinjenja kaznenog djela kao sustava koji pružaju potporu ranijoj procjeni učinjenoj na temelju objektivnih i provjerljivih činjenica.⁶⁶

Teorijski inverzija bi bila moguća na način da se prediktivni sustavi koriste nakon uspostavljanja sumnje da je određena osoba počinila konkretno kazneno djelo, kao svojevrsna *ex post* provjera ranijih spoznaja utemeljenih na objektivnim i provjerljivim činjenicama. Time se nameće pitanje svrhe takvih sustava jer je priroda njihova rezultata predikcija, a ne validacija, odnosno anulira se brzina obrade podataka i mogućnost planiranja preventivnih aktivnosti. Na jedan termin posebno treba obratiti pozornost, a to je pojam *isključivo*, jer bi se mogli dodati drugi elementi za stvaranje predikcije, koji ne bi imali stvarnog učinka na rezultat, a sve kako bi se zaobišla zabrana uporabe sustava. Kako bi se osigurala učinkovitost takve odredbe, Komisija je u svojim smjernicama koje pojašnjavaju te odredbe naglasila da svi ti drugi elementi moraju biti stvarni, bitni i smisleni kako bi mogli opravdati zaključak da se zabrana ne primjenjuje.⁶⁷ Potrebno je naglasiti da ta zabrana eksplicitno ne obuhvaća geografske prediktivne sustave, kao i sustave za predviđanje žrtava kaznenih djela.

Sustavi za daljinsku biometrijsku identifikaciju u stvarnom vremenu izrazito su intruzivni i mogu ozbiljno utjecati na privatnost velikog dijela stanovništva, stvarajući osjećaj stalnog nadzora i odvrćajući od ostvarivanja temeljnih prava, poput slobode okupljanja. Njihove tehničke netočnosti mogu dovesti do pristranih i diskriminatorskih rezultata, osobito prema skupinama definiranim dobi, etničkom pripadnošću, rasom, spolom ili invaliditetom. Budući da djeluju trenutačno i bez mogućnosti naknadne provjere ili ispravka, ti sustavi nose posebno visoke rizike za prava i slobode osoba u kontekstu kaznenog progona.⁶⁸ Europski zakonodavci to su prepoznali normirajući zabranu uporabe biometrijskog prepoznavanja u stvarnom vremenu uz iznimne mogućnosti. Kad se analiziraju odredbe čl. 5. st. 1. t. h(1–3), nameće se pitanje radi li se o usko definiranim iznimkama ili je pak riječ o potencijalnu ekspanzivne uporabe tih sustava kao visokorizičnih.⁶⁹

To pitanje najviše nameće točka h(3) predmetnog članka širokim postavljanjem jednog od dopuštenih ciljeva za uporabu takvih sustava u stvarnom vremenu; to znači za potrebe lociranja ili identifikacije osobe osumnjičene za počinjenje

⁶⁶ Voigt, P.; Hullen, N., *The EU AI Act: Answers to Frequently Asked Questions*, Springer, 2024, str. 42–43.

⁶⁷ Europska komisija, Komunikacija komisije C(2025) 5025 final, Smjernice Komisije o zabranjenim praksama u području umjetne inteligencije uspostavljenima Uredbom (EU) 2024/1689 (Akt o umjetnoj inteligenciji).

⁶⁸ Uredba EU-a o umjetnoj inteligenciji, recital 32.

⁶⁹ Barkane, I.; Buka, L., Prohibited AI surveillance practices in the Artificial Intelligence Act: promises and pitfalls in protecting fundamental rights, u: Galis, V.; Gundhus, H. O. I.; Vradis, A. (ur.) *Critical Perspectives on Predictive Policing*, Elgar, 2025, str. 119.

kaznenog djela u svrhu vođenja kaznene istrage ili progona ili izvršenja kaznene sankcije za kaznena djela iz Priloga II. za koja je u dotičnoj državi članici zaprijećena kazna zatvora ili oduzimanja slobode u maksimalnom trajanju od najmanje četiri godine. S obzirom na to da je riječ o većem broju kaznenih djela, teško se može reći da je riječ o usko definiranim iznimkama. Tome u prilog ide i test proporcionalnosti iz st. 2(a) i razmatranje posljedica iz st. 2(b), koji su načelno propisani te namijenjeni za procjenu *in concreto*. Ipak, ravnoteži u ovoj raspravi pridonose procesne pretpostavke koje moraju biti ispunjene: obvezna procjena učinka na temeljna prava, registracija, prethodno sudsko (ili upravno) odobrenje, hitne iznimke pod strogom kontrolom, obvezno brisanje podataka i nadzor tržišnih te nadzornih tijela. Osim toga, takvi sustavi smiju se koristiti samo ako država članica izričito propiše tu mogućnost u nacionalnom pravu, pa ih države mogu u potpunosti zabraniti.⁷⁰ Novokmet, Tomičić i Vidaković detaljno su analizirali utjecaj biometrijske identifikacije u stvarnom vremenu na presumpciju nedužnosti, pravilo *in dubio pro reo* i druga prava okrivljenika,⁷¹ stoga će u nastavku rada predmetom analize biti pitanje biometrijske identifikacije kroz prizmu pitanja zakonitosti dokaza, kao i relevantnosti dokaza i podataka.

4. UMJETNA INTELIGENCIJA U KONTEKSTU ZAKONITOSTI DOKAZA

Pravo na zaštitu od umjetne inteligencije kao ljudsko pravo *sui generis* ne postoji, ali njezina zlouporaba može predstavljati tehnološko sredstvo za ostvarenje povrede nekog drugog zaštićenog dobra. U kontekstu zakonitosti dokaza najčešće su povrede prava obrane ili prava na zaštitu privatnog i obiteljskog života, ali u obzir dolazi i povreda osobne slobode. Naime, primijeni li se sustav umjetne inteligencije tako da se subliminalnim, manipulativnim ili obmanjujućim tehnikama ili iskorištavanjem ljudskih slabosti utječe na iskrivljavanje ponašanja okrivljenika, svjedoka ili drugog sudionika u postupku i njihovu sposobnost da donesu informiranu odluku, takva psihička prisila u smislu hrvatskih kaznenoprocenih normi predstavljat će sredstvo slično sili, a iznuđeni dokaz po sili zakona bit će nezakonit.⁷² Na neka pitanja povezana sa zaštitom ljudskih prava, koja su naposljetku ugrađena u Uredbu EU-a o umjetnoj inteligenciji, već je prije odgovorila praksa Europskog suda za ljudska prava, primjerice protivnost daljinske biometrije za identifikaciju u stvarnom vremenu u svrhu kaznenog progona, čak i radi li se o javnom mjestu, očekivanju snimane

⁷⁰ *Ibid.*

⁷¹ Novokmet; Tomičić; Vidaković, *op. cit.* (bilj. 62), str. 550–564.

⁷² ZKP, čl. 6. st. 2. i 3. u svezi s čl. 10. st. 2. t. 3.

osobe da će njezina privatnost biti zaštićena, s posljedicom miješanja u pravo na privatni i obiteljski život u smislu čl. 8. Europske konvencije za zaštitu ljudskih prava i temeljnih sloboda.⁷³ Za ocjenu zakonitosti dokaza nije presudno radi li se formalno o zabranjenoj praksi prema Uredbi EU-a o umjetnoj inteligenciji,⁷⁴ uporabi visokorizičnog ili drugog sustava umjetne inteligencije, budući da se svaki potencijalno može zloupotrijebiti u nezakonite svrhe.

Jednako tako, ne postoji i *sui generis* dokaz umjetnom inteligencijom. Podaci za treniranje, validaciju i testiranje modela, ulazni podaci i generirane izlazne vrijednosti umjetne inteligencije, kao što su predviđanja, sadržaj, preporuke ili odluke,⁷⁵ neovisno o istinitosti zapisa, imaju vrijednost za pravne odnose te predstavljaju dokaz ispravom, a ovisno o obliku u kojem su pohranjeni i dokaz snimkom ili elektronički (digitalni) dokaz. Dok će nezakonitost podataka za treniranje, validaciju i testiranje ili ulaznih podataka u pravilu imati za posljedicu nezakonitost generiranih izlaznih vrijednosti, zakonitost ulaznih podataka može se cijiniti *eo ipso* te u tom kontekstu ovisi o svrsi koja je postojala u trenutku njihova prikupljanja. Navedeno je uočljivo radi li se o biometrijskoj obradi u sustavu umjetne inteligencije. Snima li se javni događaj u svrhu daljinske identifikacije sudionika u stvarnom vremenu kako bi se protiv lociranih i utvrđenih počinitelja kaznenih djela poduzeo kazneni progon, a da za to nisu ostvareni posebni uvjeti,⁷⁶ nezakonit dokaz predstavlja sama snimka zajedno s izlaznim vrijednostima. Međutim, upotrijebi li se u daljinskom biometrijskom sustavu umjetne inteligencije inače zakonito pribavljena fotografija ili audio-videozapis osobe, ali protivno uvjetima za korištenje visokorizičnih sustava,⁷⁷ sama snimka i dalje će opstati kao zakonit dokaz podoban za naknadno vještačenje.

Premda se može činiti kako nema potrebe za zasebnim normiranjem umjetne inteligencije kroz odredbe Zakona o kaznenom postupku povezane sa zakonitošću dokaza, zakonodavne intervencije nužne su u dva pravca – rješavanje pitanja neposredno primjenjive pravne stečevine Europske unije kao izvora prava, pri čemu područje umjetne inteligencije, uz prekogranično pribavljanje dokaza od pružatelja *online*-usluga,⁷⁸ predstavlja proboj u normiranju zajedničkih pravila za prikupljanje podataka i dokaza u svrhu kaznenog progona, te rješavanje odnosa umjetne inteligencije i dokazne radnje vještačenja.

⁷³ Europski sud za ljudska prava, *Glukhin protiv Rusije*, 2023.

⁷⁴ Uredba EU-a o umjetnoj inteligenciji, poglavlje II, čl. 3. st. 1. t. a) i b).

⁷⁵ Uredba EU-a o umjetnoj inteligenciji, čl. 3. st. 1., 30.–33.

⁷⁶ Uredba EU-a o umjetnoj inteligenciji, čl. 5. st. 1. toč. h) i st. 2., 3. i 5.

⁷⁷ Uredba EU-a o umjetnoj inteligenciji, čl. 26. st. 10.

⁷⁸ Uredba (EU) 2023/1543 Europskog parlamenta i Vijeća od 12. srpnja 2023. o europskim nalozima za dostavljanje i europskim nalozima za čuvanje elektroničkih dokaza u kaznenim postupcima i za izvršenje kazni zatvora nakon kaznenog postupka, *Službeni list Europske unije*, br. L 191/118 od 28. srpnja 2023.

4.1. Uredba EU-a o umjetnoj inteligenciji kao izvor prava Europske unije

Protekom više od desetljeća nakon pristupanja Europskoj uniji ZKP je tek djelomično prilagođen njezinoj pravnoj stečevini budući da su naknadnim izmjenama i dopunama njime prenesene direktive i okvirne odluke kaznenoprocne naravi, ali nije prilagođen uredbama kao neposredno primjenjivom *acquis communautaire*. Premda državnoodvjetničke radnje formalno proizlaze iz Ustava Republike Hrvatske, pravne stečevine Europske unije, zakona i drugih izvora prava,⁷⁹ njima prikupljeni dokazi nezakoniti su u smislu čl. 10. st. 2. t. 2. Zakona o kaznenom postupku samo ako su nastali povredom Ustavom, zakonom ili međunarodnim pravom zajamčenih prava obrane, prava na ugled ili čast te prava na nepovredivost osobnog i obiteljskog života, što ujedno predstavlja odstupanje od ustavne podjele izvora prava u kojoj se pravo Europske unije izdvaja kao zasebna kategorija.⁸⁰ Navedeno osobito dolazi do izražaja kod Uredbom EU-a o umjetnoj inteligenciji propisanih zabranjenih sustava ili ograničenja uporabe povezanih sa zaštitom privatnosti, iako bi se nedostatak nejasnoće kaznenoprocne norme u budućoj pravosudnoj praksi mogao otклонiti primjenom analogije u korist okrivljenika.

Ozbiljniji problem odnosa nacionalnog i prava Europske unije predstavlja okolnost da su dokazi pribavljeni povredom odredaba kaznenog postupka, sukladno čl. 10. st. 3. Zakona o kaznenom postupku, nezakoniti samo ako su izričito predviđeni tim zakonom, usprkos tendenciji da se provedba uredbama, ali i prenošenje u pravni sustav pojedinih direktiva, ostvaruje posebnim zakonima čak i kada uređuju pitanja zaštite ljudskih prava pri prikupljanju podatka i dokaza za potrebe kaznenog postupka.⁸¹ Kako je smisao *ex lege* nezakonitih dokaza korištenje diskrecijske ovlasti zakonodavca da odluči hoće li zbog povrede određenog temeljnog prava zajamčenog procesnom normom propisati

⁷⁹ Zakon o državnom odvjetništvu, *Narodne novine*, br. 67/2018, 21/2022, čl. 3. st. 2.

⁸⁰ Ustav Republike Hrvatske, *Narodne novine*, br. 56/1990, 135/1997, 8/1998, 113/2000, 124/2000, 28/2001, 41/2001, 55/2001, 76/2010, 85/2010, 5/2014, čl. 141.c.

⁸¹ Vidi Ministarstvo pravosuđa, uprave i digitalne transformacije, Savjetovanje s javnošću za Obrazac zakonodavnih aktivnosti – Zakon o provedbi uredbe (EU) 2024/1689 Europskog parlamenta i Vijeća od 13. lipnja 2024. o utvrđivanju usklađenih pravila o umjetnoj inteligenciji (Akt o umjetnoj inteligenciji), otvoreno od 18. prosinca 2024. do 2. siječnja 2025., <https://esavjetovanja.gov.hr/ECon/MainScreen?entityId=29348> (7. 9. 2025.); Ministarstvo pravosuđa, uprave i digitalne transformacije, Nacrt Prijedloga Zakona o prekograničnom prikupljanju elektroničkih dokaza u kaznenim postupcima, Zagreb, lipanj 2025.; Zakon o zaštiti fizičkih osoba u vezi s obradom i razmjenom osobnih podataka u svrhe sprječavanja, istraživanja, otkrivanja ili progona kaznenih djela ili izvršavanja kaznenih sankcija, *Narodne novine*, br. 68/2018.

ekskluzijsko pravilo,⁸² nije osnovano ograničiti je na procesne odredbe koje proizlaze iz nacionalnog prava ostavljajući izvan domašaja u toj mjeri teške povrede prava na privatni i obiteljski život da su, u interesu Europske unije, proglašene općezabranjenima na njezinu području. Navedeno se osobito odnosi na sustave za daljinsku biometrijsku identifikaciju u stvarnom vremenu, budući da ostale zabranjene prakse Uredbe EU-a o umjetnoj inteligenciji pripadaju područjima koja se ne odnose na kazneni progon ili kao primjena sili sličnog sredstva ionako po drugoj pravnoj osnovi predstavljaju *ex lege* nezakonit dokaz.

4.2. Uporaba umjetne inteligencije u vještačenju

Određujući visokorizičnima sustave umjetne inteligencije namijenjene korištenju od strane pravosudnih tijela ili u njihovo ime za pomoć u istraživanju i tumačenju činjenica i prava te primjeni prava na konkretan skup činjenica, Uredba EU-a o umjetnoj inteligenciji, prije svega, sprječava da umjetno generirane vrijednosti zamijene pravosudne odluke.⁸³ Premda njome nije izričito određeno značenje izraza „pravosudno tijelo“, praksom Suda Europske unije u odnosu na taj autonomni pojam prava Europske unije ustaljeno je stajalište kako se radi o konceptu koji ne obuhvaća samo suce ili sudove države članice već ga u širem smislu valja tumačiti na način da obuhvaća tijela koja sudjeluju u kaznenom sudovanju te uključuje i državnog odvjetnika, za razliku od ministarstava ili policije, koji su dio izvršne vlasti.⁸⁴ Neka pitanja vezana uz visokorizične sustave ipak ostaju otvorena do odgovarajućih odluka Suda Europske unije. Za područje vještačenja osobito je relevantno podrazumijevaju li se vještaci koji postupaju temeljem naloga pravosudnog tijela osobama koje djeluju u njihovo ime. Upitno je i postaju li besplatni sustavi opće namjene (npr. za pretraživanje veće količine digitalnih podataka) ili komercijalni sustavi umjetne inteligencije dostupni odvjetnicima ili vještacima koji rade i za privatne stranke (npr. specijalizirani forenzički alati) visokorizični samim time što su ih za svoje potrebe počela koristiti ili nabavila pravosudna tijela ili osobe koje djeluju u njihovo ime.

⁸² Bojanić, I.; Đurđević, Z., Dopuštenost uporabe dokaza pribavljenih kršenjem temeljnih ljudskih prava, *Hrvatski ljetopis za kazneno pravo i praksu* (Zagreb), vol. 15, broj 2, 2008, str. 999; Martinović, I.; Kos, D., Nezakoniti dokazi: teorijske i praktične dvojbe u svjetlu prakse Europskog suda za ljudska prava, *Hrvatski ljetopis za kaznene znanosti i praksu*, vol. 23, broj 2, 2016, str. 333.

⁸³ Vidi odjeljak 61. uvida Uredbe EU-a o umjetnoj inteligenciji.

⁸⁴ Sud Europske unije, C-509/18 (Glavni državni odvjetnik Litve) od 27. svibnja 2019.

U ovom trenutku presudno je to što je Uredbom EU-a o umjetnoj inteligenciji određena gornja granica prihvatljivoga u radu državnih odvjetništava i sudova prilikom istraživanja i tumačenja činjenica, koja se ne može zaobići delegiranjem djelatnosti vještacima uz snižavanje standarda da je umjetna inteligencija samo tehnička pomoć. Unatoč njezinoj načelnoj prihvatljivosti kao pomoćnog sredstva vještaku u izradi nalaza i mišljenja,⁸⁵ postojeće norme hrvatskog kaznenoprocenog prava ne nameću mu obvezu da barem naznači kakav je sustav koristio i način na koji je on korišten. Primjereni način *de lege ferenda* bila bi dopuna čl. 312. st. 1. Zakona o kaznenom postupku o prethodnim obavijestima i upozorenjima vještaku ili čl. 316. st. 1. istog Zakona o sadržaju vještačenja.

Razlozi za zakonodavne intervencije radi osiguranja transparentnosti dokaza vještačenjem uz pomoć umjetne inteligencije višestruki su. Njezina prikrivena uporaba ne pruža dostatno jamstvo državnom odvjetniku i sudu da će konačni rezultat vještačenja koje nalože biti prihvatljiv kao dokaz. Pojave li se osnove sumnje u točnost danog mišljenja, sukladno čl. 318. Zakona o kaznenom postupku obveza je tijela koja vode postupak otkloniti nedostatke ponovnim ispitivanjem ili određivanjem novog vještaka. Međutim, upitno je hoće li biti u mogućnosti ispuniti tu svoju funkciju ne mogu li utvrditi stvarnog „autora“ sadržaja nalaza i mišljenja zato što ih pritom ometa svojstvo sustava umjetne inteligencije da generirani izlazni rezultati oponašaju ljudsku djelatnost. Nezakonitost dokaza može biti i posljedica korištenja umjetne inteligencije već u pripremnoj fazi, čak i kada je vještak naknadnim korištenjem znanstvenih metoda provjerio točnost iznesenih činjenica. Upotrijebi li vještak biometrijski sustav u kojem su, protivno čl. 5. st. 1. t. e) Uredbe EU-a o umjetnoj inteligenciji, baze podataka za prepoznavanje lica stvorene ili proširene neciljanim prikupljanjem fotografija lica s interneta ili snimaka zatvorenog televizijskog sustava (engl. *Closed-Circuit Television*, CCTV), odnosno videonadzora, povreda prava na privatni i obiteljski život ne može konvalidirati tako da se utvrđeni zapis predstavi kao javno dostupan podatak o identitetu okrivljenika i obavi vizualna usporedba s materijalom u spisu. Dodatno, upotrijebi li vještak umjetnu inteligenciju makar i kao pomoćno sredstvo za utvrđivanje činjenica koje su osnova njegove struke (npr. klasifikacija uobičajenih ozljeda na lake, teške i osobito teške kod sudskomedicinskog ili utvrđivanje individualnih značajki rukopisa kod grafološkog vještačenja), upitno je posjeduje li potrebno stručno znanje u području za koje mu je dan nalog. Iz pozicije prava obrane, prema stajalištu Europskog suda za ljudska prava, već sama nemogućnost otkrivanja tehničkih detalja koji su osnova za nalaz i mišljenje može predstavljati ometanje okrivljenika da vještačenje ispita, s posljedicom dovođenja u pitanje

⁸⁵ Vidi u Đurđević; Ivičević Karas, *op. cit.* (bilj. 37), str. 231.

jednakosti oružja kao sastavnog dijela prava na pošteno suđenje u smislu čl. 6. Europske konvencije za zaštitu ljudskih prava i temeljnih sloboda.⁸⁶

Razloga za normiranje područja umjetne inteligencije u pravcu osiguranja transparentnosti drugih dokaza, s obzirom na načela hrvatskog kaznenog postupka, nema. Iako generirane izlazne vrijednosti predstavljaju isprave, primarno se radi o dokazima prikupljenim od okrivljenika i drugih osoba ili javno dostupnima, primjerice u slučajevima kada je umjetnom inteligencijom počinjeno kazneno djelo ili se posredstvom takva sustava odvijala komunikacija okrivljenika ili žrtve. Razna izvješća, analize, bilješke i slični zapisi državnog odvjetništva i policije o sadržaju i istinitosti nekog dokaza predstavljaju pismena bez dokazne snage, bez obzira na to jesu li nastale kao posljedica vizualnog pregleda, uporabe klasičnih forenzičkih programa ili umjetne inteligencije. Također, ispis izlaznih vrijednosti sustava umjetne inteligencije koji su upotrijebili policija ili državno odvjetništvo nije podoban biti dokaz ispravom s obzirom na to da se pravo okrivljenika iz čl. 64. st. 1. t. 10. Zakona o kaznenom postupku da ispita „suokrivljenike, svjedoke i vještake“ tumači na način da obuhvaća i isprave.⁸⁷ Posljedično, radi njegova ostvarenja ne samo što bi okrivljenik morao imati pristup svim izlaznim vrijednostima već i samim podacima za treniranje, validaciju i testiranje, kao i stvarnu mogućnost njihova osporavanja, što je nezamislivo ako bi na njegova pitanja odgovarao taj isti sustav umjetne inteligencije. Realno je stoga kako će jedini normirani dokaz sa svojstvom pomoći državnom odvjetništvu i sudu u istraživanju i tumačenju činjenica ostati čl. 309. Zakona o kaznenom postupku o određivanju dokaza vještačenjem treba li za utvrđivanje ili ocjenu neke važne činjenice pribaviti nalaz i mišljenje od osobe koja raspolaže potrebnim stručnim znanjem ili vještinom.

5. POMOĆ UMJETNE INTELIGENCIJE U OCJENI RELEVANTNIH OKOLNOSTI

Kako je i naglašeno od strane Venecijanske komisije, temeljna je zadaća državnog odvjetnika poduprijeti materijalno i procesno pravo, pri čemu ima dvostruku odgovornost podržavanja optužbe i istovremenog osiguravanja da slabi slučajevi ili oni koji se temelje na nezakonito prikupljenim dokazima ne dođu do suda. Pritom okolnost da će isto tijelo u stadiju rasprave u konačnici ocijeniti sve dokaze ne oslobađa državnog odvjetnika obveze da procijeni

⁸⁶ Europski sud za ljudska prava, *Kartoyev i drugi protiv Rusije* (2021), br. 9418/13.

⁸⁷ Mrčela, M., *Konfrontacijsko pravo u novijim odlukama Vrhovnoga suda Republike Hrvatske, Novine u kaznenom zakonodavstvu 2025. – zbornik radova*, Vrhovni sud Republike Hrvatske – Pravosudna akademija, Rovinj, 2025, str. 1.

kvalitetu dokaza koje će mu predočiti.⁸⁸ Kazneni progon kao temeljna ovlast i glavna dužnost državnog odvjetnika prema čl. 38. st. 1. Zakona o kaznenom postupku podrazumijeva sve radnje koje državno odvjetništvo poduzima pojavi li se sumnja na počinjenje kaznenog djela, a sastavni je dio tog procesa i donošenje odluke o njegovu nepoduzimanju ili neodržavanju nije li navedena pretpostavka utvrđena ili potvrđena. Umjetnom inteligencijom može se, kao i vještačenjem, pojedinom dokazu, primjerice u području biometrije i grafologije, pridružiti određeni stupanj vjerojatnosti postojanja pravno relevantne činjenice. U tom smislu ona može imati svojstvo pomoćnog sredstva u ocjeni materijala, a naposljetku i dovesti do zaključka o potrebi daljnjeg prikupljanja podataka i dokaza radi razjašnjenja činjenica. Međutim, neprihvatljiva je bilo kakva „pomoć“ kako bi državni odvjetnik utvrdio što je u konkretnom predmetu osnovana sumnja kao sastavni dio načela legaliteta i s pravom se ističe da je ocjena tog i drugih dokaznih standarda u kaznenom postupku ljudska aktivnost koja se ne može zamijeniti matematičkim izračunima.⁸⁹

Daljnja karakteristika strukture hrvatskog kaznenog postupka, presudna za razumijevanje zašto državni odvjetnik ima šire mogućnosti uporabe umjetne inteligencije od suda, okolnost je da se pravo obrane na jednakost oružja ne ostvaruje u istražnoj fazi, već omogućavanjem okrivljeniku da na raspravi ispita dokaze koji ga terete.⁹⁰ Paradoksalno, ali upravo zbog redukcije prava obrane u stadiju u kojem kazneni postupak vodi državni odvjetnik podaci na kojima temelji odluku o kaznenom progonu sve do eventualnog podizanja optužnice ne moraju imati svojstvo dokaza. Navedeno ne mora nužno dovesti do nepovoljnijeg položaja okrivljenika. Dapače, pružaju li izlazne vrijednosti umjetne inteligencije obrazložene zaključke čija se pouzdanost može ocijeniti, ona je podobna za provjeru dostavljenih podataka i dokaza koji terete okrivljenika. Navedeno posebno dolazi do izražaja postoje li nedosljednosti u sadržaju kaznene prijave koje upućuju na to da bi se moglo raditi o nevjerođostojnom materijalu, uključujući i *deepfake*, kako je definiran čl. 3. st. 60. Uredbe EU-a o umjetnoj inteligenciji. S obzirom na to da trenutna struktura hrvatskog kaznenog postupka priječi državnom odvjetniku da već tijekom izvida odredi dokaz vještačenjem (osim u slučaju opasnosti od odgode ili dokaznih radnji

⁸⁸ Venice Commission, CDL-AD(2019)006, Georgia – Opinion on the concept of the legislative amendments to the Criminal procedure code concerning the relationship between the prosecution and the investigators, March 16, 2019.

⁸⁹ Vidi opširnije u: Karas, Ž., Sudska praksa o policijskom postupanju: osnove sumnje i osnovana sumnja; zatvoreni krug indicija, *Policijska i sigurnost*, vol. 20, br. 2/2011, str. 620; Mrčela, M.; Delost, D., Dokazni standardi u kaznenom postupku, *Policijska i sigurnost*, vol. 28, br. 4/2019, str. 432.

⁹⁰ O jednakosti oružja i konfrontacijskom načelu vidi odluke Vrhovnog suda Republike Hrvatske br. I Kž 17/2020-4 od 22. siječnja 2020., Visokog kaznenog suda Republike Hrvatske br. I Kž-418/2021-4 od 5. siječnja 2022., Kž-rz-15/2023-4 od 3. svibnja 2023.

prema nepoznatom počinitelju⁹¹), primjenom umjetne inteligencije može se spriječiti da kazneni postupak bezrazložno prijeđe u stadij istrage samo zato što je to jedini način da državni odvjetnik ocijeni dokaz u čiju pouzdanost već u samom početku ima razloga sumnjati.

5.1. Relevantnost podataka i dokaza

Prvu normu Zakona o kaznenom postupku o ovlasti ocjenjivanja podataka i dokaza, kronološki prema načinu postupanja državnog odvjetnika, predstavlja čl. 206. st. 1. o obvezi ispitivanja i provjere kaznene prijave u informacijskom sustavu. Razrada u Poslovníku državnog odvjetništva⁹² upućuje na dužnost provjere vjerodostojnosti navoda anonimnog podnositelja uvidom u javno dostupne podatke i evidencije državnih tijela i pravnih osoba s kojima je povezan informacijski sustav državnog odvjetništva (CTS). Iako to nije izričito navedeno s obzirom na to da se prijave policije i drugih poznatih osoba *prima facie* smatraju autentičnima, na istovjetan način postupit će se i pojave li se dvojbe oko njihova sadržaja. Daljnje Poslovníkom propisane provjere odnose se na utvrđivanje povezanosti zaprimljene prijave s predmetima ranije unesenima u informacijski sustav. Trenutačno se ne može govoriti o primjeni sustava umjetne inteligencije, već o pronalaženju podudarnosti zadanim naredbama za obradu podataka klasičnog računalnog programa s ograničenim skupom indeksnih vrijednosti (podaci o okrivljeniku i drugim sudionicima, vrsta predmeta i pismena, uneseni opisi i sl.). Postojeća ograničenja informacijskog sustava uključuju prepreke pronalaženju u već postojećim predmetima podataka o istovjetnom događaju, sadržaju podneska, dokaza koji se namjeravaju pribaviti i slično. Nije riječ samo o teškoćama u utvrđivanju međusobne povezanosti kaznenih predmeta, jer se i u spisima građansko-upravnog odjela nalaze podaci potencijalno relevantni za utvrđivanje raspolaganja protupravnom imovinskom korišću, njezin pronalazak i osiguranje oduzimanja. Osim toga, sustav umjetne inteligencije koji bi unaprijed neciljano procjenjivao vjerodostojnost kaznenih prijava i priloženih im dokaza također ne bi bio protivan ovlastima državnog odvjetnika, u smislu pomoći u učinkovitijem redosljedu poduzimanja državnoodvjetničkih radnji. Dodatno, u informatički sustav ugrađene su i funkcionalnosti koje se odnose na državnoodvjetničku upravu i ne smatraju se visokorizičnim djelatnostima u smislu Uredbe EU-a o umjetnoj inteligenciji. Unapređenja u tom pravcu moguća su pri unošenju indeksnih vrijednosti u sustav, statističkoj obradi predmeta za potrebe sačinjavanja izvješća, normiranju

⁹¹ ZKP, čl. 212. st. 4. i čl. 214.

⁹² *Narodne novine*, br. 128/2019, čl. 117., čl. 119., čl. 188., čl. 233.

težine spisa radi osiguranja ravnomjerne dodjele predmeta, ujednačavanju državnoodvjetničke prakse uoče li se bitno različita postupanja u približno jednakim situacijama. Sva naprijed navedena tehnička pomoć načelno je u skladu s odredbama Uredbe EU-a o umjetnoj inteligenciji jer bi se podaci za treniranje, validaciju i testiranje crpili iz već postojećih u informatičkom sustavu državnog odvjetništva, način njihove uporabe bio bi kompatibilan ovlastima državnog odvjetnika, pristup sustavu imali bi dužnosnici i službenici zaduženi predmetima. Pritom bi okrivljenici, oštećenici i druge osobe legitimni interes provjere postupanja državnog odvjetnika ostvarivali uvidom u spise u kojima su pronađene relevantne podudarnosti i upotrijebljene u radu.

Ne odbaci li kaznenu prijavu nakon inicijalnih provjera, državni odvjetnik može, sukladno čl. 222. st. 3. Zakona o kaznenom postupku, radi razjašnjenja pojedinih tehničkih ili drugih stručnih pitanja koja se postavljaju u svezi s pribavljenim dokazima ili pri poduzimanju dokaznih radnji, zatražiti od odgovarajuće stručne ustanove ili stručne osobe da mu o tim pitanjima da potrebna objašnjenja o kojima će sastaviti zapisnik. Ne pokrene li nakon dobivenih objašnjenja kazneni postupak, ili odustane li od njega, obrazloženo rješenje dostavit će oštećeniku s poukom o pravu na uvid u spis i na preuzimanje kaznenog progona. S druge strane, prihvati li objašnjenja i ocijeni li da upućuju na osnovanu sumnju na počinjenje kaznenog djela, takav sadržaj može koristiti pri obrazlaganju osnovane sumnje u rješenju o provođenju istrage, ali kako on nema svojstvo dokaza, mora ga se naknadno poduprijeti vještačenjem. Sama okolnost da je netko pružio stručnu pomoć tijekom izvida, a naknadno je radi razjašnjenja istih relevantnih činjenica tijekom istrage imenovan vještakom, prema sudskoj praksi ne čini njegov nalaz i mišljenje nezakonitim dokazom.⁹³ Zapisnik s danim objašnjenjima stručne osobe ne podliježe obvezi izdvajanja iz spisa prilikom podizanja optužnice (čl. 86. st. 3. Zakona o kaznenom postupku) upravo kako bi se osigurala provjerljivost postupanja državnog odvjetnika. Može se zaključiti, s obzir na to da je pružanje tehničke pomoći bez dokazne snage ionako ugrađeno u postojeće ovlasti državnog odvjetnika, kako bi bilo nužno u svrhu omogućavanja da se to ostvari i uporabom umjetne inteligencije dopuniti čl. 222. Zakona o kaznenom postupku. Radi osiguranja da okrivljenik i sud mogu ocijeniti utjecaj upotrijebljene tehnologije na zakonitost i vjerodostojnost dokaza, valjalo bi propisati i obvezu da se generirane izlazne vrijednosti moraju uložiti u spis zajedno s podacima o sustavu umjetne inteligencije koji je upotrijebljen.

Pozitivne odredbe čl. 186. st. 1. i 2. Zakona o kaznenom postupku i čl. 6. st. 1. i 2. u svezi s čl. 1. Zakona o zaštiti fizičkih osoba u vezi s obradom i razmjenom osobnih podataka u svrhe sprječavanja, istraživanja, otkrivanja ili

⁹³ Vidi opširnije u Visoki kazneni sud Republike Hrvatske, I Kž-220/2024-4 od 17. rujna 2024.

progona kaznenih djela ili izvršavanja kaznenih sankcija već priječe policiju i državno odvjetništvo da stvaraju baze podataka za treniranje, validaciju i testiranje sustava umjetne inteligencije obradom audiovizualnih zapisa, rukopisa, sadržaja izjava i drugih osobnih podataka okrivljenika i drugih sudionika u postupku, protivno svrsi u koju su izvorno prikupljeni. Stoga je predvidivo da je budućnost korištenja umjetne inteligencije u radu državnog odvjetništva naganje policiji da provjeri materijal u spisu putem raspoloživih komercijalnih sustava, pretežito u području digitalne forenzike (biometrija, prepoznavanje *deepfake* i drugog sadržaja generiranog umjetnom inteligencijom, utvrđivanje relevantnog materijala u velikoj količini privremeno oduzetih podataka).

5.2. Primjena prava

Pomoć umjetne inteligencije u tumačenju prava državni odvjetnik u pravilu ostvaruje kroz javno dostupne tražilice objavljenih propisa ili sudskih odluka. Dodatni potencijal umjetne inteligencije u primjeni prava leži u izvršavanju obveze brisanja i posebne zaštite prikupljenih osobnih podataka, za čiju obradu više ne postoji pravna osnova ili je svrha obrade u međuvremenu prestala. Navedeno uključuje uklanjanje s forenzičke kopije sadržaja koji se ne može upotrijebiti kao dokaz u postupku, a izuzet je zajedno s ostalim pravno relevantnim podacima prilikom pretrage računalnog sustava i opreme.⁹⁴ Upotrijebi li se pritom i tehnika pseudonimizacije, kojom se osobni podaci više ne mogu pripisati pojedinoj osobi bez dodatnih informacija koje se drže odvojeno od pročišćenog sadržaja,⁹⁵ moguće je ostvariti ravnotežu između zaštite privatnosti i potrebe da se ne ometa pravo okrivljenika i drugih sudionika na uvid u spis. Uostalom, na to da se ne radi o dalekoj budućnosti upućuje to što je već u uporabi sustav koji koristi napredne tehnologije obrade prirodnog jezika i strojnog učenja kako bi se anonimizirale javno dostupne sudske odluke.⁹⁶

Umjetna inteligencija podobna je za stvaranje standardiziranih predložaka iz anonimiziranih podataka informatičkog sustava državnog odvjetništva, čak i u pravcu preporuka činjeničnih opisa prilagođenih okolnostima konkretnog slučaja. Navedeno, uostalom, nije u suprotnosti s ranijim tendencijama državnog odvjetništva. Kada je 2011., povodom početka opće primjene Zakona o kaznenom postupku, izdan priručnik s više od 300 obrazaca za rad u kaznenim

⁹⁴ Vidi opširnije u: Glavić, I., Aktualna problematika dokazne radnje pretrage računalnog sustava, *Novine u kaznenom zakonodavstvu 2025. – zbornik radova*, Vrhovni sud Republike Hrvatske – Pravosudna akademija, Rovinj, 2025, str. 142–143.

⁹⁵ Definiciju vidi u čl. 4. st. 5. Opće uredbe o zaštiti podataka.

⁹⁶ Vrhovni sud Republike Hrvatske, Tražilica sudskih odluka ANON, <https://www.vsrh.hr/trazilica-sudskih-odluka-anon.aspx> (14. 9. 2025.).

predmetima, popraćen je napomenom kako mu je namjena da u tehničkom smislu pomogne u svakodnevnom radu, ali i istodobnom ogradom da se više znanje stječe svakodnevnim radom, nastavkom stalnog i stručnog usavršavanja, praćenjem sudske prakse te stručnim i teorijskim raspravama.⁹⁷

6. ZAKLJUČNA RAZMATRANJA

Ključno je, posebno za visokorizične sustave, da tijela kaznenog progona te druga relevantna tijela ne bi smjela koristiti alate UI-ja tako da postanu čimbenik nejednakosti ili isključenosti. Ne bi se trebao zanemariti utjecaj korištenja alata UI-ja na prava osumnjičenika na obranu, osobito s obzirom na poteškoću u dobivanju smislenih informacija o funkcioniranju tih sustava i posljedičnu poteškoću u osporavanju njihovih rezultata na sudu, osobito za fizičke osobe pod istragom. Time bi se značajno osigurala prevlast tendencije učinkovitosti kaznenog postupka prema ostvarivanju potpunih prava obrane. Dakle, da bi se osigurala uravnotežena uporaba sustava umjetne inteligencije, bit će nužna fizička i kognitivna transparentnost kao osnovica za donošenje obrazložene odluke državnog odvjetnika kako ona ne bi bila automatizirana te kako bi sadržavala kvalitetu i osnovicu za izjavljivanje pravnog lijeka. Sustavi čiji je izlazni rezultat određena procjena, odluka ili preporuka na temelju vjerojatnosti trebali bi imati indikatore kvalitete i rizika, ali ne i same preporuke u vidu konačne odluke, kao naprimjer da se odbaci kaznena prijava ili podigne optužnica. Time se, između ostalog, stvara i kvalitetna spoznajna osnovica za izjavljivanje pravnog lijeka. Kad se razmotre odredbe Zakona o kaznenom postupku, zaključak je da legislativne inovativnosti u vidu osiguranja pravnih lijekova nisu nužne s obzirom na to da je postojećim pravnim okvirom zajamčeno pravo na pravni lijek, samo će učinkovitost izjavljenog pravnog lijeka ovisiti o kvalitetnom ostvarivanju transparentnosti i ljudskog nadzora.

Kaznenoprocесne norme u pogledu umjetne inteligencije ne mogu ostati tehnološki neutralne. Razlozi su dvojaki. Kako i proizlazi iz Uredbe EU-a o umjetnoj inteligenciji, ona je prije svega sustav podataka za treniranje, testiranje i validaciju, ulaznih podataka i generiranih izlaznih vrijednosti, te se problematika odnosa prema temeljnim ljudskim pravima te s tim povezanog ostvarivanja provjere zakonitosti i vjerodostojnosti proteže na sve integralne dijelove, bez obzira na to radi li se o provjeri samog postupanja državnog odvjetnika ili o umjetnoj inteligenciji kao dokazu ispravom. S druge strane, zbog svojstva da izlazne vrijednosti umjetne inteligencije oponašaju ljudsku aktiv-

⁹⁷ Državno odvjetništvo Republike Hrvatske: Objavljeno drugo izdanje Priručnika za rad državnih odvjetnika, priopćenje od 24. kolovoza 2011., <https://dorh.hr/hr/priopcenja/drzavno-odvjetnistvo-republike-hrvatske-objavljeno-drugo-izdanje-prirucnika-za-rad> (14. 9. 2025.).

nost, ne postoji li obveza deklariranja o načinu na koji je korištena kao pomoć pri utvrđivanju činjenica ostalim sudionicima u postupku, okrivljenik i oštećenik neće biti u mogućnosti slobodno disponirati svojim procesnim pravima, a pravosudno tijelo različito od osobe koja je koristila umjetnu inteligenciju obaviti svoju dužnost provjere činjenica na kojima temelji odluku.

Ne počne li se državni odvjetnik baviti umjetnom inteligencijom, umjetna će se inteligencija baviti njime i iluzorno je očekivati da se kontinuirano povećanje količine podataka u informatičkom sustavu, rast broja kaznenih prijava i dokaza generiranih umjetnom inteligencijom može riješiti pukim vizualnim opažanjem ili uporabom konvencionalne tehnologije. Navedeno se podjednako odnosi na način unutarnje organizacije rada u državnom odvjetništvu i postupanje u konkretnim predmetima. Unatoč opravdanoj zabrinutosti oko točnosti izlaznih vrijednosti, umjetna inteligencija već na sadašnjem stupnju razvoja načelno nije manje pouzdana od alternativa kao što su čitanje i pamćenje svog materijala u opsežnom spisu, ručno brisanje i zaštita osobnih podataka u digitalnom obliku, procjena sadržaja snimki golim okom ili utvrđivanje istinitosti iskaza dokaznom radnjom suočenja. U takvim okolnostima središnje pitanje postaje ostvarivanje najbolje ravnoteže između uporabe umjetne inteligencije u svrhu otkrivanja i progona počinitelja kaznenih djela te legitimnih prava sudionika u postupku. Uredbom EU-a o umjetnoj inteligenciji, u vrijeme kada je njezina široka primjena bila izgledna, ali istodobno nije bilo izgledno postizanje globalnog konsenzusa o pitanjima zadiranja u temeljna ljudska prava i načina ostvarenja njihove zaštite, postavljena je granica između dopuštenog i zabranjenog, kao i dodatni zahtjevi za visokorizične, ali dopuštene sustave u svim državama članicama.

LITERATURA

1. Almada, M.; Petit, N., The EU AI Act: Between product safety and Fundamental rights, *SSRN Electronic Journal*, 2023, str. 1–26.
2. Babnik, A.; Simončić, K.; Završnik, A., Upravljanje sistemima umjetne inteligencije: pregled regulacijskih inicijativa u svjetlu uspostavljanja efikasnog sistema globalnog upravljanja, u: Završnik, A.; Simončić, K. (ur.), *Pravo i umjetna inteligencija: pitanja etike, prava čovjeka i društvene štete*, Dobra knjiga, Sarajevo, 2023, str. 31–93.
3. Barkane, I.; Buka, L., Prohibited AI surveillance practices in the Artificial Intelligence Act: promises and pitfalls in protecting fundamental rights, u: Galis, V.; Gundhus, H. O. I.; Vradis, A. (ur.) *Critical Perspectives on Predictive Policing*, Elgar, 2025.
4. Bojanić, I.; Đurđević, Z., Dopuštenost uporabe dokaza pribavljenih kršenjem temeljnih ljudskih prava, *Hrvatski ljetopis za kazneno pravo i praksu (Zagreb)*, vol. 15, broj 2/2008, str. 973–1003.
5. Briva-Iglesias, V.; Camargo, J.; Dogru, G., Large language models „ad referendum“: How good are they at machine translation in the legal domain?, *Monografías de Traducción e Interpretación*, br. 16, 2024, str. 75–107.

6. Burgoon, J.; Pete Blair, J.; Qin, T.; Nunamaker, J., Detecting Deception through Linguistic Analysis, *Intelligence and Security Informatics*, 2003, str. 91–101.
7. Cihon, P.; Maas, M. M.; Kemp, L., Fragmentation and the Future: Investigating Architectures for International AI Governance, *Global Policy*, vol. 11, br. 5, 2020, str. 545–556.
8. Crotoft, R.; Kaminski, M.; Price II, W. N., Humans in the Loop, *Vanderbilt Law Review*, vol. 76, br. 2, 2023, str. 429–510.
9. Đurđević, Z.; Ivičević Karas, E., Uporaba umjetne inteligencije u hrvatskom kaznenom postupku: postojeće stanje i perspektive, *Hrvatski ljetopis za kaznene znanosti i praksu*, vol. 30, br. 2, 2023, str. 227–242.
10. Ebers, M., Truly Risk-based Regulation of Artificial Intelligence How to Implement the EU's AI Act, *European Journal of Risk Regulation*, vol. 16, br. 2, 2025, str. 684–703.
11. Erdogan, I., Diving into the Iceberg: Establishing Transparency in AI for Law Enforcement, *European Papers*, vol. 9, br. 3, 2024, str. 956–977.
12. Ghosh, M. M.; Mahajan, P. B.; Ramesh, P. P., Detection of Deception through Eye Detect System (EDS), *International Journal of Indian Psychology*, vol. 11, br. 2, 2023, str. 355–366.
13. Giampieri, P., Is Machine Translation Reliable in the Legal Field? A Corpus-Based Critical Comparative Analysis for Teaching ESP at Tertiary Level, *Journal of English for Specific Purposes at Tertiary Level*, vol. 11, br. 1, 2023, str. 119–137.
14. Glavić, I., Aktualna problematika dokazne radnje pretrage računalnog sustava, *Novine u kaznenom zakonodavstvu 2025. – zbornik radova*, Vrhovni sud Republike Hrvatske – Pravosudna akademija, Rovinj, 2025, str. 135–145.
15. Karas, Ž., Sudska praksa o policijskom postupanju: osnove sumnje i osnovana sumnja; zatvoreni krug indicija, *Policija i sigurnost*, vol. 20, br. 2/2011, str. 617–624.
16. Khalil, M.; Way, A., Multidimensional assessment of the eTranslation output for English to German and French translating EU legal texts, u: Martins, A. et al. (ur.) *Proceedings of the 22nd Annual Conference of the European Association for Machine Translation*, Portugal, 2018, str. 383–392.
17. Krapac, D., *Kazneno procesno pravo, Prva knjiga: Institucije*, VIII. izmijenjeno i dopunjeno izdanje, Narodne novine, Zagreb, 2020.
18. Krapac, D.; Lončarić, D., *Oštećenik kao tužitelj u krivičnom postupku*, Pravni fakultet u Zagrebu, Zagreb 1985.
19. Ljubanović, V.; Novokmet, A.; Tomičić, Z., *Kazneno procesno pravo – izabrana poglavlja*, Sveučilište Josipa Jurja Strossmayera u Osijeku, Pravni fakultet Osijek, 2020.
20. Martinović, I.; Kos, D., Nezakoniti dokazi: teorijske i praktične dvojbe u svjetlu prakse Europskog suda za ljudska prava, *Hrvatski ljetopis za kaznene znanosti i praksu*, vol. 23, br. 2, 2016, str. 311–338.
21. McCall, B., Voice Stress Analysis: Is „Some Evidence“ Sufficient Grounds for Making Legal Determinations?, *Barry Law Review*, vol. 29, br. 1, 2024, str. 32–69.
22. Mrčela, M., Konfrontacijsko pravo u novijim odlukama Vrhovnoga suda Republike Hrvatske, *Novine u kaznenom zakonodavstvu 2025. – zbornik radova*, Vrhovni sud Republike Hrvatske – Pravosudna akademija, Rovinj, 2025, str. 1–7.
23. Mrčela, M.; Delost, D., Dokazni standardi u kaznenom postupku, *Policija i sigurnost*, vol. 28, br. 4, 2019, str. 417–435.
24. Novokmet, A.; Tomičić, Z.; Vidaković, I., Facial Recognition Technology in Eu Criminal Justice – Human Rights Implications and Challenges, *EU and Comparative Law Issues and Challenges Series (ECLIC)*, vol. 7, str. 525–570.
25. Papadoulis, V., Transparency in Artificial Intelligence: A Legal Perspective, *Journal of Ethics and Legal Technologies*, vol. 4, 2022, str. 25–40.

26. Quijano-Sánchez, L.; Liberatore, F.; Camacho-Collados, J.; Camacho-Collados, M., Applying automatic text-based detection of deceptive language to police reports: Extracting behavioral patterns from a multi-step classification model to understand how we lie to the police, *Knowledge-Based Systems*, vol. 149, str. 155–168.
27. Rotenberg, M., Kyriakides, E., *The AI Policy Sourcebook 2025*, Center for AI and Digital Policy, United States of America, 2025.
28. Schmitt, L., Mapping global AI governance: a nascent regime in a fragmented landscape, *AI Ethics*, vol. 2, 2022, str. 303–314.
29. Schwartzmann, R.; Keber, T. O.; Zenner, K. (ur.), *AI Act, A practical Guide*, C. F. Müller, 2025.
30. Strojín, G., Pristupi međunarodne zajednice u regulisanju umjetne inteligencije, u: Završnik, A.; Simončić, K. (ur.), *Pravo i umjetna inteligencija: pitanja etike, prava čovjeka i društvene štete*, Dobra knjiga, Sarajevo, 2023, str. 17–31.
31. Tomičić, Z., Poligrafsko ispitivanje – drugačiji pogled i nove perspektive, *Zbornik radova Pravnog fakulteta u Splitu*, god. 60, br. 1, 2023, str. 145–174.
32. Turković, K.; Viljac Herceg, F., Učinkovita istraga povreda prava zajamčenih Europskom konvencijom za zaštitu ljudskih prava, *Hrvatski ljetopis za kaznene znanosti i praksu*, vol. 26, br. 2, 2019, str. 265–290.
33. Viljanen, M.; Parviainen, H., AI Applications and Regulation: Mapping the Regulatory Strata, *Frontiers in Computer Science*, 2022, str. 1–11.
34. Vrij, A.; Fisher R. P., Unraveling the Misconception About Deception and Nervous Behavior, *Frontiers in Psychology*, vol. 11, 2020, str. 1–8.
35. Quattrocchio, S., Criminal law enforcement through AI, u: Barfield, W. H.; Pagallo, U. (ur.) *Research Handbook on the Law of Artificial Intelligence*, 2025.
36. Voigt, P.; Hullén, N., *The EU AI Act: Answers to Frequently Asked Questions*, Springer, 2024.

Summary

Ivan Glavić, PhD*

Ivan Vidaković**

POTENTIALS FOR THE APPLICATION OF ARTIFICIAL INTELLIGENCE IN THE WORK OF THE STATE ATTORNEY'S OFFICE THROUGH THE LENS OF REGULATION (EU) 2024/1689 ON ARTIFICIAL INTELLIGENCE

For many years, perpetrators of criminal offences have taken advantage of the rapid development of technology, culminating in the widespread application and presence of artificial intelligence. However, they are not the only ones who can benefit from AI systems. Law enforcement authorities, primarily the State Attorney's Office, also have the potential to apply such systems to more effectively fulfil their core task of prosecuting offenders. While advantages include the speed of processing large volumes of data, as well as improved accuracy and adaptability to specific objectives, the use of AI in criminal prosecution also carries certain risks, which may ultimately lead to violations of fundamental human rights and freedoms. The first part of the paper provides an overview of the legal sources regulating the use of AI systems that may be applied in the work of the State Attorney's Office. By analysing these sources, the paper identifies the principles of AI use that they share, which simultaneously represent an imperative for the application of AI in the work of the State Attorney's Office. At the same time, the regulation of AI is examined through the provisions of the EU Artificial Intelligence Act, with particular emphasis on high-risk and prohibited systems and the conditions for their use. The next part of the paper analyses the application of AI systems to the work of the State Attorney's Office, with particular emphasis on the fundamental principles of the Criminal Procedure Act and the compatibility of such use *de lege lata*. The final part of the paper focuses on the question of work organisation and the potential application of AI by identifying those segments of organisational functioning that have the most weaknesses and where AI has the greatest potential, including some *de lege ferenda* proposals. The paper thus presents a balanced discussion of the potential for the application of AI, taking into account all the advantages it may bring for the efficiency of criminal prosecution, while at the same time weighing all the risks such use may pose for defendants and for the fairness of proceedings as a whole. The findings indicate that the principles of Croatian criminal procedure and the powers of the State Attorney's Office are complementary to the obligations arising from EU law and from comparative practice aimed at improving the efficiency of criminal prosecution through AI. However, amendments to the positive legal framework are necessary to ensure transparency of actions and the related ability to assess the lawfulness and reliability of the data and evidence on which the decision to prosecute is based.

Keywords: State Attorney's Office, artificial intelligence, efficiency of criminal prosecution, lawfulness of evidence, expert testimony

* Ivan Glavić, PhD, Deputy State Attorney General; ivan.glavic@dorh.hr; ORCID iD: <https://orcid.org/0000-0003-4055-3286>.

** Ivan Vidaković, Teaching Assistant, Chair of Criminal Law Sciences, Josip Juraj Strossmayer University of Osijek, Faculty of Law Osijek; ivan.vidakovic@pravos.hr; ORCID iD: <https://orcid.org/0000-0002-7003-632X>.