Uporaba umjetne inteligencije za potrebe kaznenog potupka - izazovi i perspektive

Venus, Sven

Pravni fakultet Sveučilišta u Zagrebu

Katedra za kazneno procesno pravo

Sven Venus

UPORABA UMJETNE INTELIGENCIJE ZA POTREBE KAZNENOG POSTUPKA – IZAZOVI I PERSPEKTIVE

Diplomski rad

Mentorica: prof. dr. sc. Elizabeta Ivičević Karas

Zagreb, srpanj 2023.

IZJAVA O IZVORNOSTI

Ja, Sven Venus, pod punom moralnom, materijalnom i kaznenom odgovornošću, izjavljujem da sam isključivi autor diplomskog rada te da u radu nisu na nedozvoljeni način (bez pravilnog citiranja) korišteni dijelovi tuđih radova te da se prilikom izrade rada nisam koristio drugim izvorima do onih navedenih u radu.

Sven Venus, v.r.

SAŽETAK

Smisao ovog rada je razumjeti kako se umjetna inteligencija koristi za potrebe kaznenog postupka, počevši od prevencije kaznenih djela i otkrivanja njihovih počinitelja putem metoda kao što su prediktivni rad policije *(predictive policing)* ili prepoznavanje lica *(facial recognition)*, pa do toga kako umjetnu inteligenciju koriste suci kod donošenja presuda, posebno prilikom procjene rizika, ili kako se umjetna inteligencija koristi u zatvorima, u kojima se izvršava i mjera istražnog zatvora. Uporaba tih metoda je za početak istražena i uspoređena na europskoj i globalnoj razini, a zatim je opisano trenutno stanje i perspektive u Republici Hrvatskoj. Na kraju se iznosi sažeti osvrt na budućnost uporabe umjetne inteligencije u kaznenom pravu, prvenstveno od strane državnih vlasti, ali i od strane počinitelja kaznenih djela.

Ključne riječi: umjetna inteligencija, kazneni postupak, prediktivni rad policije, prepoznavanje lica, procjena rizika

ABSTRACT

The purpose of this paper is to understand how artificial intelligence is used for the purposes of criminal procedure, starting with crime prevention and catching perpetrators through methods such as predictive policing or facial recognition, to viewing how judges use artificial intelligence when sentencing, especially via risk-assessment, or how artificial intelligence is used in prisons, where additionally pre-trial detention is carried out. The use of these methods is first researched and examined across Europe and the rest of the world, and then is examined the current state and perspectives in the Republic of Croatia. At the end comes a brief view on the future use of artificial intelligence in criminal law, primarily from the state, but also from perpetrators.

Keywords: artificial intelligence, criminal procedure, predictive policing, facial recognition, risk-assessment

SADRŽAJ

1. UVOD

Ne postoji razumna osoba koja će uvjereno tvrditi da može nadmašiti stroj u obavljanju njegove funkcije. Nitko neće niti pomisliti da je brži od automobila ili da bolje može računati od računala. Svakome je jasno da su to naši alati, bez inteligencije, kojima se služimo. Ipak, riječ je o jednostavnim no svakako teškim i zamornim radnjama. Sve ostalo, poput kreativnosti i inteligencije su isključivo ljudske osobine, ili bismo tako barem očekivali. No, umjetna inteligencija (eng. *artificial intelligence*), i to ne kao neka znanstveno-fantastična ideja, već umjetna inteligencija kako postoji dan-danas i kako će se bez sumnje poboljšavati, već sad može skladati glazbu, naslikati pejsaže, voditi inteligentne razgovore te barem na nekoj razini, ispunjavati posao pravničke profesije.[1]

Poznato je već da je teško dati općeprihvaćenu definiciju što je to umjetna inteligencija. Još od 50-ih godina 20. st. postoji tzv. Turingov test, stvoren od strane britanskog matematičara Alana Turinga, po kojemu umjetna inteligencija prolazi test ako u komunikaciji s nekim čovjekom taj čovjek ne zaključi da zapravo razgovora s umjetnom inteligencijom, a ne drugom osobom.[2] Iz istog razdoblja dobivamo prvu definiciju Johna McCarthyja, smatranog ocem umjetne inteligencije, koji kaže da se radi o znanosti i inženjerstvu stvaranja inteligentnih strojeva.[3] Po najmodernijem shvaćanju, i razlikovanju brojnih povezanih i sličnih no ipak različitih pojmova, ono što je značajno za umjetnu inteligenciju je da može učiti, barem djelomično, kao čovjek.[4]

U samom pravu informacijske tehnologije nisu ništa novo, budući da već desetljećima razna odvjetnička društva, sudovi i državne organizacije koriste tzv. *legal expert* sustave kako bi olakšali svoj posao.[5] Ipak, takvi sustavi obavljali su većinom administrativne i rutinske zadatke, poput proučavanja i iščitavanja gomile dokumentacije. Ono što starije *legal expert* sustave razlikuje od novijih programa umjetne inteligencije je tzv. *machine learning*, tj. sposobnost da sama umjetna inteligencija "uči" iz svojih odluka i pogrešaka i na taj način se eksponencijalno

[1] The Economist, *How AI is transforming the creative industries* - https://www.economist.com/films/2021/04/07/how-ai-is-transforming-the-creative-industries (preuzeto 19.6.2023.)
[2] Custers, B., *AI in Criminal Law: An Overview of AI Applications in Substantive and Procedural Criminal Law*, Law and Artificial Intelligence, Heidelberg: Springer, 2022., str. 216.
[3] Manning, C., *Artificial Intelligence Definitions*, Stanford University - Human-Centered Artificial Intelligence, 2020., str. 1.
[4] *Ibid.*
[5] Popple, J., *A Pragmatic Legal Expert System*, Dartmouth, 1996., str. 3.

poboljšava, postaje "pametnija". Po predviđanjima Svjetskog ekonomskog foruma, među radnicima na koje će najviše utjecati umjetna inteligencija su upravo pravnici.[6] I nije teško za razumjeti zašto, budući da velik broj pravničkih zadataka je vremenski zamorno iščitavanje i analiziranje raznih zakona, uredbi i presuda. Tako je i početkom 2023. godine umjetna inteligencija GPT-4 "položila" američki pravosudni ispit.[7]

No, smisao ovoga rada nije osvrnuti se na totalnost umjetne inteligencije, a niti na umjetnu inteligenciju u pravu cjelokupno, već kako se umjetna inteligencija danas koristi i kako će se uskoro koristiti u domeni kaznenog procesnog prava, od istraživanja kaznenih djela i otkrivanja počinitelja, pa do donošenja odluka na sudovima i provođenja mjere istražnog zatvora. Pregledat ćemo kako su države Europske unije (dalje u tekstu: EU) kroz zadnjih nekoliko godina počele koristiti umjetnu inteligenciju u vlastitom kaznenom procesnom pravu, kako su institucije EU reagirale, kako neke značajne države svijeta poput Sjedinjenih Američkih Država (dalje u tekstu: SAD) i Kine koriste umjetnu inteligenciju i po čemu se razlikuju od država EU, što u kontekstu toga čini ili će činiti Hrvatska, te konačno što možemo očekivati u skoroj budućnost.

EU već godinama zauzima oprezan stav prema umjetnoj inteligenciji. U *Bijeloj knjizi o umjetnoj inteligenciji – Europski pristup izvrsnosti i izgradnji povjerenja* iz 2020. godine, Europska komisija uz sve već postojeće, no i buduće nepredvidive mogućnosti umjetne inteligencije poput utjecaja na zdravstvenu skrb ili poljoprivredu, pridaje posebnu pažnju na "niz potencijalnih rizika, kao što su netransparentno donošenje odluka, rodno uvjetovanu ili drugu vrstu diskriminacije, zadiranje u privatni život ili upotrebu u kriminalne svrhe."[8] Kao što je već ranije rečeno, iako se umjetna inteligencija koristi i van prava i unutar prava u nebrojene svrhe, u nekim od narednih poglavlja ćemo se usredotočiti na to kako su države EU te i sama EU pristupile uređenju umjetne inteligencije u grani kaznenog procesnog prava, i to najviše kod proaktivnih metoda poput tzv. tehnike prediktivnog rada policije (eng. *predictive policing*), kao i uobičajenijih reaktivnih metoda pri istraživanju kaznenih djela i pronalasku počinitelja, uz naglasak na potencijalne opasnosti diskriminacije i zadiranja u ljudska prava i temeljne slobode.

Na svjetskoj razini, situacija je naravno raznolika. Brazil se ugleda na uredbe EU, Kina se usredotočuje na uporabu umjetne inteligencije u sigurnosne svrhe, a SAD se trenutno više

[6] *The Future of Jobs Report*, Svjetski ekonomski forum, 2020., str. 136.
[7] Illinois Tech, *GPT-4 Passes the Bar Exam* - https://www.iit.edu/news/gpt-4-passes-bar-exam (preuzeto 20.6.2023.)
[8] *Bijela knjiga o umjetnoj inteligenciji – Europski pristup izvrsnosti i izgradnji povjerenja*, COM(2020), str. 1.

bavi na federalnoj razini neobvezujućim smjernicama. No, ono što je jasno je da ne postoji trenutno ujednačeno uređenje umjetne inteligencije na globalnoj razini.[9]

[9] Taylor Wessing, *AI Regulation Around the World* - https://www.taylorwessing.com/en/interface/2023/ai---are-we-getting-the-balance-between-regulation-and-innovation-right/ai-regulation-around-the-world (preuzeto 15.6.2023.)

2. PREDIKTIVNI RAD POLICIJE ("*PREDICTIVE POLICING*")

Ne postoji trenutno uvriježeni domaći prijevod pojma *"predictive policing"*. Na nekim mjestima se spominje prijevod "prediktivni rad policije"[10] koji djeluje odgovarajuće te će biti korišten nadalje u ovom radu. Navedeni pojam predstavlja algoritamsku uporabu velike količine podataka kako bi se razaznali šabloni mogućih budućih počinitelja kaznenih djela, žrtava te mjesta i vremena počinjenja.[11] Time prediktivni rad policije predstavlja u idealnom značenju preokret tipičnog shvaćanja kaznenoprocesnih radnji kao reaktivnih, tj. reagiranje na već počinjeno kazneno djelo, preobrazbom u proaktivne radnje, tj. postupanje da do kaznenog djela ne bi uopće ni došlo.

Prije nastupa moderne umjetne inteligencije na scenu, prediktivni rad policije bazirao se je kako je već rečeno na algoritamskoj uporabi velike količine podataka, tj. *Big Data,* a i prije toga običnim ljudskim radom predviđanja budućih kaznenih djela. U algoritamskom smislu to znači da policijske uprave pohranjuju brojne podatke poput učestalih mjesta i vremena počinjenja kaznenih djela, dosjee okrivljenika, kaznene prijave te dodatno i registarske oznake automobila. Algoritam zatim pretražuje i obrađuje te podatke, tražeći poveznice i ključne točke, time stvarajući predviđanja o mogućim budućim kaznenim djelima. No ono što umjetna inteligencija pridonosi, kako je objašnjeno u Uvodu, je da putem *machine learning*-a se algoritam trajno i kontinuirano poboljšava, tj. "učenjem" postaje "pametniji".

2.1. U EU

Prediktivni rad policije putem uporabe umjetne inteligencije zaživio je u brojnim europskim državama kroz zadnjih nekoliko godina. Primjerice u Italiji, uporabom sustava imena Delia. Postoje i drugi talijanski sustavi kao što su RTM i X Law, koji su ostvarili ponešto slabije rezultate, no Delia trenutno pokazuje najveći potencijal te na njenom primjeru možemo shvatiti pobliže kako prediktivni rad policije djeluje.[12] Delia nakon obrade do 1.5 milijuna varijabli ocjenjuje četiri kriminološka čimbenika, a to su vrsta kaznenog djela, cilj kaznenog djela, *modus operandi* počinitelja, tj. oruđa, oružja, vozila i slično te psihofizičke osobine

[10] *Knjiga sažetaka – Big Data in Law Enforcement: from Reactive to Proactive,* MUP RH, Zagreb, 2017., str. 27.
[11] González Fuster, G., *Artificial Intelligence and Law Enforcement – Impact on Fundamental Rights,* 2020., str. 22.
[12] Cinelli, V., *Crime Prevention and Predictive Analysis: The Italian Case,* Agenformedia, 2020., str. 1.

počinitelja, tj. tetovaže, ožiljci, odjeća i ostali identifikatori.[13] Delia potom analizira specifična kaznena djela kako bi odredila ključne čimbenike učestale u ostalim sličnim djelima i povezala ih s pojedinim okrivljenikom. Zatim rezultate te prve analize koristi radi predviđanja budućih kaznenih djela.[14] Prvi rezultati bili su prilično pozitivni; Delia je u okolici Milana umanjila broj oružanih pljački u trgovinama za oko 28% u prvoj godini uporabe, a proširenjem na sam Milano i na oružane pljačke u bankama uspjeh se povećao na 37%.[15]

Naspram Italije, u Francuskoj je s nešto lošijim rezultatima 2016. godine *Gendarmerie,* francuska policija za seoska i manja gradska mjesta, osmislila sustav imena PAVED.[16] *Gendarmerie* nije objavila mnogo podataka o PAVED-u pri lansiranju programa, no poznato je da se testna faza bila usredotočila na predviđanje provala i krađe automobila u jedanaest francuskih okruga, i to onih, očekivano, s velikim brojem navedenih kaznenih djela.[17] Prema jednom istraživanju, PAVED je za 3-5% umanjio broj krađa automobila u testnim područjima, no na provale nije imao utjecaj. Istraživači postavljaju hipotezu da postoji očita korelacija između toga što se na ulicama odvijaju policijske patrole i tamo se nalaze automobili kao mete krađe, a provale se s druge strane odvijaju u zatvorenim, potencijalno udaljenijim prostorima. To može stvoriti kod počinitelja percepciju većeg rizika kod krađe automobila naspram provala.[18] Početni plan za PAVED bio je da se nakon testne faze proširi i po kriterijima pokrivenog područja i po raznovrsnosti kaznenih djela, ali prema podacima iz 2022. godine to proširenje se nije obistinilo.[19] Nažalost, iako francuski zakoni predviđaju otvorenost informacija o algoritmima za javnu uporabu, na PAVED se navedeno ne odnosi budući da se koristi u sigurnosne svrhe, što uvelike otežava vanjske analize korisnosti.[20]

U Njemačkoj najznačajniji sustav je PRECOBS, na koga ćemo se i prvenstveno osvrnuti. PRECOBS je drugačiji od ostalih njemačkih sustava prediktivnog rada policije jer je kupljen od vanjskih suradnika, a ne razvijen *in-house* tj. od strane same policije, u ovom slučaju.[21] PRECOBS djeluje na temelju tzv. *near-approach* pristupa, po ideji da kaznena djela za koje je

[13] *Ibid.* str. 2.
[14] *Ibid.*
[15] *Ibid.* str. 3.
[16] Lecorps, Y., Tissandier, G., *PAVED with Good Intentions? An Evaluation of a French Police Predictive Policing System,* 2022., str. 1.
[17] *Ibid.* str. 2.
[18] *Ibid.* str. 9.
[19] *Ibid.* str. 3.
[20] *Ibid.* str. 25.
[21] Vepřek, H. L., et. al., *Beyond Effectiveness: Legitimising Predictive Policing in Germany,* Kriminologie – Das Online-Journal, br. 3, 2020., str. 428.

PRECOBS osmišljen, slično kao francuski PAVED, za provaljivanja,[22] se ponavljaju više puta po kriteriju istog mjesta i vremena, a ne odvijaju samo jednom.[23] Dvojako je potencijalno objašnjenje iza ove ideje, a to je s jedne strane zamisao da je za žrtve kaznenih djela veća vjerojatnost da će ponovno biti žrtve naspram osoba koje nisu žrtve te, s druge strane, zamisao da počinjenje kaznenog djela obilježava mjesto kao privlačno za daljnja počinjenja drugih počinitelja.[24] Rezultati PRECOBS-a su diskutabilni i u jednu ruku nezahvalni za istraživanje, tj. paradoksalni.[25] I time dolazimo zapravo do najznačajnijeg problema pri konačnom ocjenjivanju djeluju li uopće sustavi prediktivnog rada policije u svojem zamišljenom potpunom obujmu. S jedne strane trebaju predvidjeti mjesto počinjenja kaznenog djela, a s druge strane, policija bi imajući to znanje trebala moći spriječiti počinjenje istog kaznenog djela. Kazneno djelo koje se ne dogodi je po prirodi stvari nemjerljivo; nemoguće je dokazati da se nešto nije dogodilo.[26] Kako onda možemo pouzdano znati da je upravo zahvaljujući prediktivnom radu policije spriječeno kazneno djelo, kada je to nemjerljivo? Iako je moguće izvesti zaključak o rezultatima usporedbom s kontrolnim skupinama, u stvarnom svijetu van laboratorijskih uvjeta logično je da nikada dvije usporedne grupe nisu iste i time niti rezultati nisu potpuno precizni. Dodatni navodi postoje oko činjenice da uspostava kontrolnih skupina zahtjeva samo djelomično provođenje prediktivnog rada policije, jer za kontrolnu skupinu policija bi sustave koristila samo za predviđanje, a ne i prevenciju kaznenih djela, kako bi usporedno izmjerili učinak. Budući da često, kao što vidimo s PRECOBS-om, policije sustave kupuju a ne prave same, to predstavlja trošak u vidu izmaknule koristi.[27]

Svi do sada navedeni primjeri ukazuju i na dobre i na upitne rezultate ovakve uporabe prediktivnog rada policije, ali postoje i značajni problemi, uvelike u tome kako se prikupljaju podaci koje obrađuju algoritmi te u uočenim diskriminatornim tendencijama utkanima u same sustave. Europski parlament je u jednoj rezoluciji istaknuo kako prediktivni rad policije te umjetna inteligencija općenito može imati velik utjecaj na ljudska prava i temeljne slobode te kako korištenje algoritama s malim brojem lažnih pozitivnih rezultata može u konačnici

[22] *Ibid.* str. 424.
[23] Youstin, T., et. al., *Assessing the Generalizability of the Near Repeat Phenomenon*, Criminal Justice and Behavior, br. 38, 2011., str. 1042.
[24] Haberman, C., Ratcliffe, J., *The Predictive Policing Challenges of Near Repeat Armed Street Robberies*, Policing, br. 6, 2012., str. 151
[25] Vepřek, H. L., et. al., *op.cit.* (bilj. 19), str. 425.
[26] Shapiro, A., *Predictive Policing for Reform? Indeterminacy and Intervention in Big Data Policing,* Surveillance and Society, br. 17, 2019., str. 463.
[27] *Ibid.*

uzrokovati da lažna upozorenja brojčano nadmaše točna.[28] Nadalje upozoravaju kako prediktivni rad policije može vješto analizirati šablone i korelacije, no ne može nam dati odgovor na uzročnost niti točno predvidjeti ponašanja pojedinaca. Konačno, već dvije godine je u izradi *Uredba Europskog parlamenta i Vijeća o utvrđivanju usklađenih pravila o umjetnoj inteligenciji i izmjeni određenih zakonodavnih akata unije,* tj. tzv. AI Act (dalje u tekstu: Uredba o umjetnoj inteligenciji). Riječ je o značajnoj i sveopsežnoj uredbi o umjetnoj inteligenciji u cijelosti, nalik na poznatu Opću uredbu o zaštiti podataka (GDPR), a u planu je da stupi na snagu do kraja 2023. godine. Uredba o umjetnoj inteligenciji bi podijelila sustave umjetne inteligencije u razne skupine, ovisno o riziku koji predstavljaju za sigurnost te ljudska prava i temeljne slobode, s najrizičnijom skupinom označenom kao neprihvatljivim rizikom.[29] I upravo u tu skupinu po trenutnoj verziji Uredbe o umjetnoj inteligenciji spadaju sustavi prediktivnog rada policije, što bi značilo da je do kraja godine sasvim moguće da na cijelom području EU prediktivni rad policije postane potpuno zabranjen.

U prilog tome idu istraživanja koja naglašavaju diskriminatorne posljedice korištenja prediktivnog rada policije, na primjeru Španjolske na području EU, no i u ostalim državama svijeta, o čemu će više riječi biti kasnije. U Španjolskoj, istraživači su pronašli kako *machine-learning* sustavi za procjenu rizika recidivizma, ponovnog počinjenja kaznenog djela od strane ranije osuđivane osobe, kod maloljetnih počinitelja su diskriminirali uglavnom muške počinitelje, počinitelje strance te pripadnike određenih nacionalnosti.[30]

Slični rezultati dobiveni su u Nizozemskoj. Tamo je među prvima u EU korišten prediktivni rad policije i to sustav po imenu CAS, razvijen *in-house* od strane nizozemske policije.[31] Na primjeru CAS-a možemo uočiti tzv. diskriminatorni *feedback loop,* tj. sustav gdje se izlazni čimbenici preusmjeravaju nazad kao ulazni, čime zapravo nastaje petlja koja samu sebe "hrani."[32] Najjednostavnije objašnjeno, neki policijski službenici svjesno ili nesvjesno imaju određene predrasude, često bazirane na etničkoj osnovi. Tako su jedan od glavnih izvora podataka na temelju kojih CAS donosi odluke gdje policija treba izvoditi ophodnju, podaci iz

[28] *Rezolucija Europskog parlamenta od 6. listopada 2021. o umjetnoj inteligenciji u kaznenom pravu i njezinoj primjeni od strane policije i pravosudnih tijela u kaznenim stvarima,* (2020/2016(INI)), t. M.
[29] *Prijedlog uredbe Europskog parlamenta i Vijeća o utvrđivanju usklađenih pravila o umjetnoj inteligenciji (Akt o umjetnoj inteligenciji) i izmjeni određenih zakonodavnih akata unije,* 2021/0106 (COD)
[30] Songül, T., et. al., *Why Machine Learning May Lead to Unfairness: Evidence from Risk Assessment for Juvenile Justice in Catalonia,* Canada, ICAIL, 2019., str. 1.
[31] Oosterloo, S., van Schie, G., *The Politics and Biases of the "Crime Anticipation System" of the Dutch Police,* Proceedings of the International Workshop on Bias in Information, Algorithms, and Systems, br. 2103, 2018., str. 30.
[32] *Ibid.* str. 37.

nizozemske središnje baze kaznenih podataka.[33] To znači da policija predaje CAS-u predrasudama "obojane" podatke, na temelju kojih CAS može poslati policiju u ophodnju u dijelove naselja sa znatnim brojem pripadnika etničkih manjina, gdje će policija dobiti potvrdu svojih predrasuda i napraviti novi set podataka koje će dobiti CAS, koji zatim šalje policiju u ophodnju i tako se dalje petlja održava na životu. Zato je potrebno da *input* koji ulazi u petlju nije nikako diskriminatoran, što u stvarnosti može biti iznimno teško ostvariti jer često su predrasude implicitne, te nisu jasno izrečene.[34]

Brojni dodatni navodi postoje, od strane same EU te kao što je ranije rečeno do drugih autora, upozoravajući na diskriminaciju na temelju raznih osnova, uključujući spol, rasu, nacionalnost i dr.[35]

2.2. U SVIJETU

Prediktivni rad policije našao je svoj dom prvenstveno u SAD-u. Najznačajniji sustav uopće je PredPol, čiji tvorci su *the Federal Bureau of Investigation* (tj. FBI), *the Los Angeles Police Department* (dalje u tekstu: LAPD) te *the University of California*, a korišten je više od bilo kojeg drugog takvog sustava.[36] PredPol se bazira na tehnologiji predviđanja mjesta i posljedica podrhtavanja uslijed potresa, gdje takvo mjesto bude označeno na gradskim kartama kao *hotspot*, tj. žarišna točka, s analogijom da užarena mjesta predstavljaju prisutnost kaznenih djela, a zatim slanje policije u ophodnju na ta mjesta rješenje.[37] PredPol se hvali sjajnim rezultatima, tvrdeći da korištenjem sustava razne policijske postaje su smanjile kaznena djela poput provala i pljački za 30%.[38] No, sam LAPD je, nakon dugogodišnjeg korištenja, u travnju 2020. godine prestao koristiti PredPol, navodeći nemogućnost točnog mjerenja učinkovitosti sustava.[39] Ono što je dodatno značajno, uvažavajući činjenicu da je SAD kao tzv. *melting pot* izrazito etnički heterogena država, je ogroman broj optužbi o rasnoj diskriminaciji sustava

[33] *Ibid.* str. 32.
[34] Lexology, *The perils of feedback loops in machine learning: predictive policing* - https://www.lexology.com/library/detail.aspx?g=c8fff116-2112-48dd-841c-f9d1688d722b (preuzeto 21.6.2023.)
[35] Roksandić, S., et. al., *Trustworthy Artificial Intelligence and its use by Law Enforcement Authorities: where do we stand?,* MIPRO 2022/ICTLAW, 2022., str. 1396.; Gstrein, O. J., *Ethical, legal and social challenges of Predictive Policing,* Católica Law Review, br. 3, 2019., str. 87.; Momsen, C., *Implications and Limitations of the Use of AI in Criminal Justice in Germany,* KriPoZ, br. 1, 2023., str. 9.
[36] Wong, T. A., *The Mathematics of Policing,* 2022., str. 4.
[37] *Ibid.*
[38] PredPol, *Proven Crime Reduction Results* - https://www.predpol.com/results/ (preuzeto 15.6.2023.)
[39] Los Angeles Times, *LAPD data programs need better oversight to protect public, inspector general concludes* - https://www.latimes.com/local/lanow/la-me-ln-lapd-data-20190312-story.html (preuzeto 15.6.2023.)

prediktivnog rada policije. Tako je pronađeno da, umjesto da PredPol korigira svoja predviđanja nasuprot rasnih i etničkih pristranosti, PredPol je primjerice u Oaklandu vezano za kaznena djela u svezi s drogama slao policiju u pretežno crnačke četvrti dvostruko više puta nego u pretežno bjelačke, iako je statistički među obje populacije izjednačena učestalost tih kaznenih djela.[40] No, ne možemo li očekivati da će umjetna inteligencija putem *machine-learning*-a naučiti na vlastitim greškama? Problem je i ovdje kako je ranije rečeno kod CAS-a, to što umjetna inteligencija može učiti samo na temelju podataka koji su joj dani, a ako ti sami podaci, iako nije diskriminacija izričito utkana u njih, sadrže dodatno podatke o rasi, umjetna inteligencija može "pokupiti" pristrano ponašanje.[41]

U Kini, kao autoritativno uređenoj državi, stanje je potencijalno distopijsko, uz bojazan da prediktivni rad policije neće u značajnoj mjeri smanjiti broj kaznenih djela i povećati sigurnost, već samo biti novi alat u ugnjetavanju već diskriminiranih populacija.[42] Slične, no u manjoj mjeri brige postoje i u ostalim državama, kao npr. u Indiji[43] ili Japanu.[44]

[40] O'Donell, R. M., *Challenging Racist Predictive Policing Algorithms Under the Equal Protection Clause,* New York University Law Review, br. 94:544, 2019., str. 562.
[41] *Ibid.*
[42] Sprick, D., *Predictive Policing in China: An Authoritarian Dream of Public Security,* Nordic Journal of Law and Social Research, br. 9, 2019., str. 299.
[43] Vats, A., *Building the Case for Restricted Use of Predictive Policing Tools in India,* International Review of Information Ethics, br. 32, 2022., str. 1.
[44] Hung, T-W., Yen, C-P., *On the Person-based Predictive Policing of AI,* Ethics and Information Technology, br. 23, 2021., str. 1.

3. PREPOZNAVANJE LICA ("*FACIAL RECOGNITION*")

Dodatni način kako se umjetna inteligencija koristi u kaznenom procesnom pravu je uporabom tehnologije prepoznavanja lica (eng. *facial recognition*). Riječ je o tipu biometrije, tj. identifikaciji i verifikaciji identiteta neke osobe na temelju osobina njena izgleda i/ili ponašanja.[45] Većini nas je navedena tehnologija najpoznatija njenim korištenjem za jednostavne radnje kao što je otključavanje mobitela, no u kaznenom procesnom pravu koristi se iz sigurnosnih i policijskih razloga. Radi se najviše o prepoznavanju lica u stvarnom vremenu (eng. *live facial recognition*), gdje uređaji za videonadzor kao što su sigurnosne kamere u stvarnom vremenu analiziraju lica prolaznika i uspoređuju ih s policijskim bazama podataka kako bi korisnici uređaja znali točno tko se, gdje i kada nalazi. Nije teško odmah na početku uvidjeti problematičnost uporabe ove tehnologije. Kao što vidimo i kod prediktivnog rada policije, šablona koja se počinje realizirati kod umjetne inteligencije u policijskim pitanjima je sukob sigurnosti, prevencije i pronalaženja počinitelja kaznenih djela s iznimnim zadiranjem u privatnost, potencijalnom diskriminacijom i nepouzdanosti same tehnologije.

Prepoznavanje lica u stvarnom vremenu, malo detaljnije opisano, djeluje u četiri koraka.[46] Prvi korak je detekcija, tj. sposobnost sustava da prepozna nalazi li se na slici ili videu ljudsko lice. Drugi korak je identifikacija, gdje sustav pokušava otkriti čije je to lice, usporedbom s bazama podataka ljudskih lica. Treći korak je verifikacija, gdje sustav uspoređuje dvije slike kako bi otkrio ako je na njima ista osoba. Razlika identifikacije i verifikacije je zapravo u tome što pri identifikaciji je usporedba jedne slike s mnoštvom, a kod verifikacije je riječ o usporedbi jedan-na-jedan. Konačno, četvrti, potencijalno najopasniji i najkontroverzniji korak je kategorizacija, gdje sustav analizira detalje lica kako bi otkrio osobine kao što su starost, spol, rasa, emocionalno stanje i sl.

3.1. U EU

Dodatne kontroverze na području EU su se pojavile saznanjem o ulogama privatnog sektora u uporabi prepoznavanja lica u stvarnom vremenu. Tako je otkriveno da je Clearview AI, američko društvo čija je djelatnost prepoznavanje lica te čija umjetna inteligencija

[45] Madiega, T., Mildebrath, H., *Regulating Facial Recognition in the EU,* European Parliamentary Research Service, 2021., str. 1.
[46] *Ibid.*

uspoređuje lica s milijardama indeksiranih fotografija preuzetih s interneta, imao ugovore s tisućama policijskih postaja, uključujući u Europi.[47] Tako su policijski službenici imali mogućnost predati sustavu fotografije osumnjičenika da bi ih zatim umjetna inteligencija identificirala na temelju "javno dostupnih" fotografija s interneta.[48] U Švedskoj, primjerice, agencija nadležna za zaštitu osobnih podataka pokrenula je istragu o ugovorima između Clearview AI i švedske policije, te u konačnici zbog povrede švedskog zakona o kaznenim podacima, kaznila policiju s novčanom kaznom, te joj naredila da obuči svoje službenike u korištenju osobnih podataka u skladu s njihovom zaštitom po švedskom i europskom pravu, da obavijesti sve osobe čiji su podaci bili korišteni za Clearview AI te da, u mjeri u kojoj je to moguće, obriše sve podatke prebačene na Clearview AI.[49]

Po primarnom pravu EU, kako je izloženo u Povelji Europske unije o temeljnim pravima, svi imamo pravo na poštovanje privatnog i obiteljskog života te na zaštitu osobnih podataka.[50] Najočitije moguće kršenje navedenih prava događa se jer je iznimno teško provesti davanje izričitog pristanka na obradu osobnih podataka u situacijama snimanja lica.[51] Također, postoji i već spomenuta opasnost diskriminacije, gdje prepoznavanje lica dokazano slabije prepoznaje žene od muškaraca i ne-bijele muškarce od bijelih, što dovodi do brojnih lažnih pozitivnih rezultata.[52] Time nije začuđujuće da Uredba o umjetnoj inteligenciji također rigorozno uređuje sustave prepoznavanja lica. Za razliku od sustava prediktivnog rada policije koje Uredba o umjetnoj inteligenciji stavlja, kao što je prije rečeno, u grupu neprihvatljivog rizika, sustavi prepoznavanja lica su stavljeni u narednu grupu visokog rizika. To znači da bi određeni broj sustava prepoznavanja lica bio ili zabranjen, ili bi morao biti podvrgnut značajnim regulacijama, a prepoznavanje lica u stvarnom vremenu korišteno u javnim prostorima za policijske poslove bilo bi potpuno zabranjeno, osim iznimno radi sigurnosnih razloga ako to odobri država članica i sustavi prođu sudske i administrativne provjere.[53]

[47] González Fuster, G., *op. cit.* (bilj. 11), str. 26.
[48] *Ibid.*
[49] European Data Protection Board, *Swedish DPA: Police unlawfully used facial recognition app* - https://edpb.europa.eu/news/national-news/2021/swedish-dpa-police-unlawfully-used-facial-recognition-app_en (preuzeto 14.6.2023.)
[50] *Povelja Europske unije o temeljnim pravima* (2016/C 202/02), čl. 7. i čl. 8.
[51] Madiega, T., Mildebrath, H., *op. cit.* (bilj. 45), str. 6.
[52] *Ibid.* str. 7.
[53] *Ibid.* str. 1.

3.2. U SVIJETU

U SAD-u, na tragu uporabe prediktivnog rada policije, također nije teško za predvidjeti koji su rezultati i problemi tehnologije prepoznavanja lica. Godine 2016. bilo je zabilježeno kako u SAD-u State Department (ministarstvo nadležno za vanjske poslove) vodi bazu podataka s licima od preko 117 milijuna američkih državljana, preuzetih uglavnom preko slika s vozačkih dozvola[54]. Za očekivati je da se taj broj mogao samo povećati. No, u pogledu neuspjeha tehnologije, navode se brojke po kojima je spol krivo prepoznat kod 35% lica crnih žena, naspram bijelih muškaraca koji su identificirani s 99% točnosti.[55] Dodatno, u SAD-u se trenutno provode istraživanja poboljšavanja navedene tehnologije uz pomoć umjetne inteligencije, na način da se olakša uočavanje lica u otežanim uvjetima.[56] Naravno, ne možemo očekivati da će svaki put počinitelj kaznenog djela s nepokrivenim licem izravno pogledati u nadzorni uređaj. Zato se uči umjetna inteligencija da poboljša uvjete uočavanja i prepoznavanja kada su lica snimljena u uvjetima lošeg osvjetljenja, kada je rezolucija slike niska, ili osumnjičenik nosi masku, maramu, kacigu ili sl.[57]

Slično se navedena tehnologija primjenjuje i pri prepoznavanju ne samo lica, nego i registarskih tablica na vozilima, tako da se umjetna inteligencija postepeno trenira pri prepoznavanju brojeva i slova sa snimki sve nižih i nižih rezolucija, budući da su snimke s prometnih nadzornih uređaja u pravilu niske kvalitete, primjerice zbog brzine vožnje i kvalitete samih kamera.[58] Tako bi sustav umjetne inteligencije mogao dobiti na prepoznavanje sliku iznimno niske rezolucije te i dalje biti sposoban prepoznati što se na slici nalazi, ili koji brojevi i slova pišu na registarskim tablicama.

U Japanu, Hitachi Inc. radi povećane potrebe za sigurnosti u susret ljetnih Olimpijskih igara 2020. godine najavio je sustav prepoznavanja lica koji može identificirati osobe iako im lice nije potpuno vidljivo, već je identifikacija moguća i s profila ili čak pozadine glave, a dodatno navode da je identifikacija moguća i preko odjeće i načina hoda, slično kao u SAD-u.[59]

---

[54] Fortune, *Here's How Many Adult Faces Are Scanned From Facial Recognition Databases by Cops* - https://fortune.com/2016/10/18/facial-recognition-database/ (preuzeto 15.6.2023.)
[55] Nkonde, M., *Automated Anti-Blackness: Facial Recognition in Brooklyn, New York,* Harvard Kennedy School Journal of African American Policy, br. 2019-2020., str. 32.
[56] Rigano, C., *Using Artificial Intelligence To Address Criminal Justice Needs,* NIJ Journal, br. 280, 2019., str. 39.
[57] *Ibid.*
[58] *Ibid.*
[59] Hung, T-W., Yen, C-P., *op. cit.* (bilj. 44), str. 12.

No u Engleskoj, tehnologija prepoznavanja lica je pokazala iznimno loše rezultate kada je utvrđeno 2018. godine od strane londonske policije da u testu identifikacije 104 osobe osumnjičene za počinjenja kaznenih djela sustav je pogrešno identificirao 102, tj. imao je neuspjeh od 98%.[60]

Po navedenim primjerima zapravo možemo uočiti jednu značajnu, a i zanimljivu nit vodilju koja se proteže kroz razne metode uporabe umjetne inteligencije u kaznenom procesnom pravu, a to je simultano postojanje zapanjujuće te čak i pomalo znanstveno-fantastične tehnologije, koja znatno brže i točnije djeluje nego čovjek. Ali ujedno te tehnologije su i dalje iznimno sklone greškama, a kako se može raditi o životu i smrti, ili općenito povredama ljudskih prava, pitanje je jesmo li skloni dati umjetnoj inteligenciji da donosi ili barem navodi na odluke.

[60] Santow, E., *Can Artificial Intelligence Be Trusted With Our Human Rights*?, Australian Quarterly, br. 91, 2020., str. 15.

4. ANALIZA ODREĐENIH VRSTA MATERIJALNIH DOKAZA

Neupitno je to da bez kvalitetne analize materijalnih dokaza u kriminalističkom istraživanju teško je točno otkriti identitet okrivljenika. Iako su personalni dokazi, kao što su svjedoci, i dalje ključni, materijalni dokazi pomažu kod indicijalnog dokazivanja, npr. prisutnosti okrivljenika na mjestu zločina. Analiza takvih dokaza od strane umjetne inteligencije poput dolje opisanih DNK tragova i tragova iz vatrenih oružja može predstavljati veliku pomoć istražiteljima.

4.1. TRAGOVI DNK

Jedan od tih načina kako se umjetna inteligencija može koristiti pri otkrivanju počinitelja kaznenih djela i pretraživanju dokaza je putem DNK analize.[61] Kao što je općepoznato, počinitelji kaznenih djela pri doticaju s objektima djela, okolinom, žrtvom i sl. ostavljaju ovisno o njihovoj spretnosti i vrsti djela razne biološke tragove poput krvi, dijelova kože ili kose. Sve su to tragovi koji sadrže DNK počinitelja. Analizom spornih DNK tragova i usporedbom s nespornom DNK istražitelji kaznenih djela dolaze do identiteta počinitelja, koristeći ponovno brojne baze podataka. Za navedeno je lakše umjetnoj inteligenciji da obavi pretragu i usporedbu nego što je to čovjeku.[62]

Ono čemu umjetna inteligencija najviše pridonosi je rješavanje problema tzv. dekonvolucije, tj. razdvajanja DNK različitih počinitelja istog kaznenog djela i odvajanje od DNK koji je slučajno dio uzorka, a nebitan je za rješavanje djela.[63] U SAD-u trenutno postoje razna istraživanja koja bi koristila *machine-learning* metode dekonvolucije, budući da je riječ o velikom broju zamršenih podataka, prezamršenih za analizu od strane čovjeka, a vrlo prikladnih za umjetnu inteligenciju.[64]

[61] Rigano, C., *op. cit.* (bilj. 56), str. 41.
[62] Wankhade, T. D., et. al., *Artificial Intelligence in Forensic Medicine and Toxicology: The Future of Forensic Medicine*, Cureus, br. 14, 2022., str. 1768.
[63] Rigano, C., *op. cit.* (bilj. 56), str. 41.
[64] *Ibid.*

4.2. TRAGOVI VATRENOG ORUŽJA

U SAD-u, slično kao u slučaju DNK analize, trenutno se razvijaju programi umjetne inteligencije koji mogu olakšati istragu kod kaznenih djela u kojima je korišteno vatreno oružje. Ne radi se o obradi samih oružja ili ispaljenog zrna, već o zvuku pucnjave.[65] Snimljeni zvukovi pucnjave na pametnim mobitelima ili nadzornim uređajima bi se analizirali, uzimajući u obzir ideju da zvuk pucnjave ovisi o vrsti vatrenog oružja, kalibru, geometriji mjesta događaja, i naravno uređaju kojim je snimljen zvuk.[66] Umjetna inteligencija bi zatim mogla otkriti zvuk pucnjave s neke audio snimke, odrediti vremenski raspon između više ispaljenih zrna, odrediti broj korištenih vatrenih oružja, odrediti koje ispaljeno zrno pripada kojem oružju i sl.[67]

[65] *Ibid.* str. 7.
[66] *Ibid.*
[67] *Ibid.*

5. ISTRAŽIVANJE KIBERNETIČKIH KAZNENIH DJELA

Jedno područje na kojemu je teško i vremenski zahtjevno provoditi istrage je upravo internet. Ogromna količina podataka te brojne *darkweb* stranice mogu zahtijevati godine truda i brojne prikrivene istražitelje kako bi se pridobilo povjerenje osumnjičenika radi otkrivanja ili priznanja počinjenja kaznenih djela, jer često je riječ o zatvorenim stranicama kojima rukovode počinitelji koji nerado daju pristup novim ljudima.[68] Dodatne komplikacije mogu nastati povodom toga što, slično kao i po našem Zakonu o kaznenom postupku, i u drugim državama radi se o posebnim dokaznim radnjama koje traže sudsko odobrenje. Tako ukoliko je dokaz pribavljen policijskom zamkom (eng. *entrapment*), postoji opasnost da će biti neuporabljiv.[69] Naime, u nekim državama, primjerice u Engleskoj,[70] dokazi pribavljeni na taj način su u određenim uvjetima nezakoniti te se ne mogu koristiti tijekom suđenja.

Umjetna inteligencija se ovdje može upotrijebiti tako da djeluje na internetu kao kibernetički agent. Prisjetimo se Turingovog testa, kojeg umjetna inteligencija prolazi ako u komunikaciji s čovjekom uspije zavarati tu osobu da priča s drugim čovjekom, a ne s umjetnom inteligencijom. Primjer za navedeno je Sweetie, *chatbot*, tj. umjetno inteligentni govornik na internetu, koji je dizajniran da izgleda i komunicira kao dvanaestogodišnja djevojčica.[71] Očita ideja je da se identificiraju pedofili, što je i uspjelo jer je preko 20.000 muškaraca iz 71 države uistinu mislilo da razgovaraju s djevojčicom.[72]

Iako postoje problemi nastali s proceduralne strane, kao već spomenut problem policijske zamke ili logični zaključak da je nemoguće spolno zlostavljati umjetnu inteligenciju, u Australiji, Belgiji i Engleskoj došlo je do kaznenih presuda zahvaljujući navedenoj tehnologiji.[73] U Australiji je bila i prva od presuda, i to na temelju priznanja okrivljenika po tri točke optužnice za slanje vlastitih golih slika Sweetie-ju, za posjedovanje na računalu slika spolno zlostavljane djece te za nepridržavanje sudske mjere za seksualne prijestupnike.[74] Budući da se samo jedna od tri točke specifično tiče Sweetie-ja, možemo zaključiti da nije

[68] Custers, B., *op. cit.* (bilj. 2), str. 215.
[69] *Ibid.*
[70] Crown Prosecution Service, *Abuse of Process* - https://www.cps.gov.uk/legal-guidance/abuse-process (preuzeto 29.6.2023.)
[71] BBC, *Sweetie: 'Girl' chatbot targets thousands of paedophiles* - https://www.bbc.com/news/av/technology-42461065 (preuzeto 16.6.2023.)
[72] Custers, B., *op. cit.* (bilj. 2), str. 216.
[73] *Ibid.*
[74] BBC, *Webcam sex with fake girl Sweetie leads to sentence* - https://www.bbc.com/news/technology-29688996 (preuzeto 29.6.2023.)

nužno da okrivljenik "zlostavlja" sam Sweetie, već korištenje Sweetie-ja može poslužiti kao povod za daljnje istrage kojima budu otkrivena druga kaznena djela ili prekršaji.

6. UPORABA UMJETNE INTELIGENCIJE NA SUDOVIMA

6.1. OPĆENITO

Do sada analizirana područja ticala su se uporabe umjetne inteligencije pri prevenciji kaznenih djela te otkrivanju počinitelja već počinjenih kaznenih djela. Slijedi pregled kako se umjetna inteligencija koristi ne toliko od strane policije i drugih istraživačkih službi, već samih sudova općenito te specifično u kaznenom postupku. Ideja iza uporabe umjetne inteligencije u sudovima je da se smanji arbitrarnost suca i poveća objektivnost, tj. smanji prevelika moć suca koja je po nekima prekomjerna.[75] Također postoje benefiti poput racionalizacije dodjeljivanja predmeta sucima, pa sve do toga da umjetna inteligencija donese odluku umjesto suca, no očiti problem koji iz svega navedenog proizlazi je moguć udar na neovisnost sudstva kao grane vlasti te samih sudaca.[76] Posebno ćemo se osvrnuti na korištenje umjetne inteligencije radi tzv. "procjene rizika" (eng. "*risk-assessment*"), kako u EU, tako u svijetu.

Na području EU, za razliku od kako ćemo kasnije vidjeti ostalih država svijeta, posebice SAD-a i Kine, ne postoji još toliko raširena uporaba umjetne inteligencije u kaznenim postupcima, već se više koristi u građanskim sporovima, posebice pri alternativnim metodama rješavanja sporova poput arbitraže.[77] Zato ćemo u ovom dijelu, sagledavajući cjelokupno sudstvo, ispitati kako umjetna inteligencija može utjecati na sudačku neovisnost, kao vanjsku dimenziju gdje je sudstvo odvojeno i van utjecaja ostalih grana vlasti, tako i na unutarnju nepristranost, koja podrazumijeva da sudac nije naklonjen niti jednoj od stranaka. Sve navedeno bitan je dio primarnog prava EU.[78]

Mogući primjeri kako umjetna inteligencija može utjecati na sudstvo su neizravni pritisak savjeta umjetne inteligencije kod donošenja odluke, smanjivanje sudačke plaće radi racionalizacije uporabom sustava umjetne inteligencije, što može povećati korupciju te iz istih razloga smanjivanje financiranja sudstva, pa do pitanja tko uopće stvara i u konačnici upravlja algoritmima koje suci koriste.[79] Dodatni problem vezan je za konkretnu uporabu umjetne inteligencije. Hoće li ih sami suci koristiti, za što moraju biti informatički obučeni, hoće li

[75] González Fuster, G., *op. cit.* (bilj. 11), str. 27.
[76] Gentile, G., *AI in the Courtroom and Judicial Independence: An EU Perspective*, EUIdeas, 2022., str. 1.
[77] González Fuster, G., *op. cit.* (bilj. 11), str. 28.
[78] *Povelja Europske unije o temeljnim pravima* (2016/C 202/02), čl. 47.
[79] Gentile, G., *op. cit.* (bilj. 76), str. 2.

postojati dedicirani tehničari koji koriste umjetnu inteligenciju ili neka mješavina ovih mogućnosti?[80]

Iz svih tih i drugih razloga je na području Vijeća Europe CEPEJ—Odbor Vijeća Europe za učinkovitost pravosuđa, donio krajem 2018. godine *Europsku povelju o korištenju umjetne inteligencije u pravosuđu,* u kojoj je izloženo pet temeljnih načela za korištenje umjetne inteligencije.[81] Prvo načelo tiče se poštivanja temeljnih prava, po kojemu uporaba umjetne inteligencije mora biti u skladu s temeljnim ljudskim pravima i slobodama kako ih priznaju države članice Vijeća Europe. Drugo načelo tiče se zabrane diskriminacije, po kojemu uporaba umjetne inteligencije ne smije dovesti do diskriminacije nikoga niti se takve sustave smije razvijati. Treće načelo tiče se kvalitete i sigurnosti, po kojemu obrađivanje procesnih podataka od strane umjetne inteligencije mora biti odrađeno na multidisciplinarni način u sigurnom tehnološkom okruženju. Četvrto načelo tiče se transparentnosti, nepristranosti i pravednosti, po kojemu obrada podataka od strane umjetne inteligencije mora biti razumljiva i dostupna te otvorena za vanjske provjere. I zadnje, tj. peto načelo tiče se konačne vladavine korisnika, po kojemu informirani korisnik je taj koji treba donositi konačnu odluku.[82]

Kako će se uporaba umjetne inteligencije u europskim sudovima dalje razvijati ovisi naravno o državama članicama, tijelima EU i Vijeća Europe, sudovima i samim proizvođačima umjetne inteligencije, no ono što znamo je da Uredba o umjetnoj inteligenciji uporabu umjetne inteligencije pri administraciji pravosuđa i demokratskih procesa stavlja u kategoriju visokog rizika,[83] isto kao tehnologiju prepoznavanja lica.

6.2. PROCJENA RIZIKA ("*RISK-ASSESSMENT*") U UREDBI O UMJETNOJ INTELIGENCIJI

Općenito govoreći, procjena rizika je korištenje umjetne inteligencije čija namjena je da na temelju raznih podataka, poput okrivljenikovih odgovora na određena pitanja ili podataka iz dosjea, procjeni kolika je vjerojatnost ili rizik da će okrivljenik, ako je oslobođen, ponovno

[80] *Ibid.* str. 3.
[81] CEPEJ - *European Ethical Charter on the use of Artificial Intelligence in Judicial Systems and Their Environment,* 2018.
[82] *Ibid.*
[83] *op. cit.* (bilj. 29)

počiniti kazneno djelo.[84] Trenutno, sudovi niti jedne države članice EU, niti Vijeća Europe, ne koriste tehnologiju procjene rizika, iako su zabilježeni pilot-programi u Engleskoj i Francuskoj.[85]

Uredba o umjetnoj inteligenciji uređuje i tehnologiju procjene rizika. Tako Uredba o umjetnoj inteligenciji navodi da među visokorizične sustave treba uvrstiti i one "namijenjene tijelima kaznenog progona za pojedinačne procjene rizika, poligrafe i slične alate ili za utvrđivanje emocionalnog stanja pojedinca… za predviđanje počinjenja ili ponavljanja stvarnog ili potencijalnog kaznenog djela na temelju izrade profila pojedinaca ili procjenu osobina ličnosti i karakteristika ili prijašnjeg kriminalnog ponašanja pojedinaca ili skupina, za izradu profila tijekom otkrivanja, istrage ili progona kaznenih djela, kao i za analitiku kaznenih djela koja se odnosi na pojedince."[86] Navedeno se očito odnosi na, između ostalog, tehnologiju procjene rizika. Uredba o umjetnoj inteligenciji nadalje propisuje, referirajući se na popis sadržan u Prilogu III. uz Uredbu,[87] koji uključuje i tehnologiju procjene rizika, da te tehnologije moraju ispunjavati zahtjeve iz Uredbe.[88] Ti zahtjevi tiču se uspostavljanja, održavanja i primjenjivanja sustava upravljanja rizicima, vođenja dokumentacije o istome, te njegova redovitog ažuriranja.[89] Također je propisano da je za umjetne inteligencije visokog rizika potrebno da imaju funkciju automatskog bilježenja događaja, što zapravo osigurava sljedivost,[90] te da njihov rad mora biti dovoljno transparentan da korisnici mogu tumačiti i informirano koristiti umjetnu inteligenciju.[91] Dodatno, potreban je ljudski nadzor nad sustavima[92] te odgovarajuća razina točnosti, otpornosti i kibersigurnosti.[93] Svime nabrojanim nastoji se da visokorizični sustavi kao što je procjena rizika budu uvelike ograničeni.

Budući da je prepoznavanje lica također u istoj kategoriji, analogno se navedeno uređenje primjenjuje i na tu tehnologiju, za razliku od tehnologija prepoznavanja lica u stvarnom

---

[84] American Bar Association, *Artificial Intelligence: Benefits and Unknown Risks* - https://www.americanbar.org/groups/judicial/publications/judges_journal/2021/winter/artificial-intelligence-benefits-and-unknown-risks/ (preuzeto 16.6.2023.)
[85] Chelioudakis, E., *Risk assessment tools in criminal justice: is there a need for such tools in Europe and would their use comply with European data protection law?,* ANU JOLT, br. 1, 2020., str. 73.
[86] *op. cit.* (bilj. 29), t. 38.
[87] *Annexes to the Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts*, COM(2021)
[88] *op. cit.* (bilj. 29), čl. 8.
[89] *Ibid*. čl. 9.
[90] *Ibid.* čl. 12.
[91] *Ibid.* čl. 13.
[92] *Ibid.* čl. 14.
[93] *Ibid.* čl. 15.

vremenu i prediktivnog rada policije koje bi bile zabranjene, čime je zapravo Uredbom o umjetnoj inteligenciji pokriveno područje uporabe umjetne inteligencije od strane tijela kaznenog progona.

6.3. PROCJENA RIZIKA ("*RISK-ASSESSMENT*") U SVIJETU

Procjena rizika u ostalim državama koristi se uvelike u SAD-u, gdje ga američki suci koriste kako bi si olakšali donošenje presuda, a navedena tehnologija u uporabi je u skoro svim saveznim državama SAD-a.[94] Najznačajniji primjer tehnologije procjene rizika je COMPAS. COMPAS se koristi u više stadija, uključujući prethodni postupak, u vezi određivanja jamčevine, suđenje, u vezi s donošenjem presude, povodom uvjetne osude, u zatvorima, a i povodom uvjetnog puštanja iz zatvora. COMPAS djeluje na temelju dva modela rizika, i to *General Recidivism Risk*, tj. opći rizik recidivizma te *Violent Recidivism Risk*, tj. rizik nasilnog recidivizma.[95] U tim modelima postoji skala od četrdeset i tri točke, od kojih se ne moraju sve koristiti, a svaka točka ima ljestvicu od jedan do deset, gdje jedan do četiri predstavlja nisku ocjenu naspram okrivljenika iz iste skupine, pet do sedam predstavlja srednju, a osam do deset visoku ocjenu.[96] Neke od točaka su primjerice povijest nasilja, ovisnost o opojnim sredstvima, neuspjeh socijalizacije, društvena izolacija, kriminalitet u obitelji, financijski problemi, "kriminološka osobnost" i dr.[97] Kroz svoju povijest COMPAS je primijenjen na više od milijun američkih okrivljenika.[98]

Nakon prijašnjih podnaslova, vjerojatno neće biti preveliko iznenađenje otkriće da COMPAS ne djeluje baš kako je osmišljen te da postoje brojni problemi diskriminacije. Jedno istraživanje zaključilo je da je COMPAS crne okrivljenike naspram bijelih ocjenjivao s dvostruko većim rizikom recidivizma.[99] Također je zaključeno da od svih okrivljenika za koje je COMPAS predvidio da će počiniti nasilno kazneno djelo, samo njih 20% je tako i učinilo.[100] No, ova istraživanja nisu ostala bez odgovora. Tako je i Equivant, bivši Northpointe, vlasnik

---

[94] Epic.org, *AI in the Criminal Justice System* - https://epic.org/issues/ai/ai-in-the-criminal-justice-system/ (preuzeto 16.6.2023.)
[95] *Practitioner's Guide to COMPAS Core*, Northpointe Inc., 2015., str. 1.
[96] *Ibid.* str. 8
[97] *Ibid.* str. 24.
[98] Dressel, J., Farid, H., *The Accuracy, Fairness, and Limits of Predicting Recidivism*, Science Advances, br. 4, 2018., str. 1.
[99] González Fuster, G., *op. cit.* (bilj. 11), str. 28.
[100] Flores, A. W., et. al., *False Positives, False Negatives, and False Analyses: A Rejoinder to "Machine Bias: There's Software Used Across the Country to Predict Future Criminals. And it's Biased Against Blacks."*, Federal Probation, br. 80, 2016., str. 43.

COMPAS-a, negirao zaključke istraživanja, a i pridružili su im se i neki drugi istraživači, navodeći da ne negiraju postojanje rasne diskriminacije, niti potiču korištenje procjene rizika, već smatraju da postoje problemi u metodologiji kojom su prijašnji istraživači došli do svojih zaključaka.[101] Istraživanje koje je uslijedilo nakon navedenih zaključilo je pomalo kompromisno da COMPAS bolje predviđa od pojedinaca koji nemaju znanja iz kaznenog prava i znanosti, no lošije od skupina pojedinaca koji imaju; COMPAS je imao točnost od 65%, a skupina 67%.[102]

Tako je primjerice 2013. godine američki državljanin Eric Loomis bio uhvaćen kako vozi automobil koji je bio korišten tijekom pucnjave, nakon čega je bio uhapšen i optužen po pet točaka te se izjasnio krivim za dvije najlakše, a to su bježanje od prometnog policajca i korištenje vozila bez suglasnosti vlasnika. Sudac je u njegovom slučaju pri odmjeravanju kazne koristio upravo COMPAS.[103] COMPAS je ocijenio da postoji visok rizik da će Loomis ponovno počiniti neko kazneno djelo te ga je sudac osudio na zatvorsku kaznu u trajanju šest godina.[104] Potom se Loomis žalio Vrhovnom sudu savezne države Wisconsin, navodeći da mu je, zbog toga što se presuda temelji na algoritmu čije unutarnje djelovanje je tajno i ne može biti ispitano, povrijeđeno pravo na pravično suđenje.[105] Vrhovni sud savezne države Wisconsin je u konačnici odbio žalbu, navodeći kako mu nije povrijeđeno pravo na pravično suđenje te da bi sudac i bez korištenja COMPAS-a donio istu odluku, no ipak su postavili zahtjev da suci moraju obrazložiti kako koriste COMPAS.[106] Slijedom toga Loomis se žalio saveznom Vrhovnom sudu, koji je odbacio žalbu.[107]

Još jedan značajan slučaj u SAD-u ticao se SAVRY-ja, sustava nalik COMPAS-u koji se koristi kod osuđivanja maloljetnika. SAVRY je odredio kako je jedan maloljetnik, kojem je obećana uvjetna osuda u zamjenu za izjašnjavanje krivim, i dalje u visokom riziku za recidivizam te treba biti osuđen kaznom zatvora.[108] Branitelji maloljetnika usprotivili su se

[101] *Ibid.* str. 38.
[102] Dressel, J., Farid, H., *op. cit.* (bilj. 98), str. 1.
[103] LexisNexis, *State v. Loomis* - https://www.lexisnexis.com/community/casebrief/p/casebrief-state-v-loomis (preuzeto 17.6.2023.)
[104] The Atlantic, *A Popular Algorithm Is No Better at Predicting Crimes Than Random People* - https://www.theatlantic.com/technology/archive/2018/01/equivant-compas-algorithm/550646/ (preuzeto 17.6.2023.)
[105] *Regulating Artificial Intelligence for Use in Criminal Justice Systems in the EU - Policy Paper*, FairTrials, str. 27.
[106] González Fuster, G., *op. cit.* (bilj. 11), str. 28.
[107] Reiling, A. D., *Courts and Artificial Intelligence*, International Journal for Court Administration, br. 11, 2020., str. 6.
[108] González Fuster, G., *op. cit.* (bilj. 11), str. 28.

takvoj procjeni te su na kraju uvjerili suca, koji je odlučio da se u tom pojedinom slučaju SAVRY ne smije koristiti.[109]

U Kini, Vrhovni sud izdao je 2022. godine zahtjev da svi kineski sudovi moraju do 2025. godine uvesti umjetnu inteligenciju, smatrajući da će to poboljšati učinkovitost i sigurnost. Ipak, i dalje Vrhovni sud ističe da umjetna inteligencija ne smije zamijeniti suce kod donošenja presuda, već im smije samo olakšati posao. Dodatno Vrhovni sud traži da do 2030. godine umjetna inteligencija na sudovima bude dovoljno razvijena i poboljšana da može biti korištena tijekom cijelog sudskog postupka.[110] Također, Kineske vlasti objavile su krajem 2021. godine da su s idejom da rasterete rad državnih odvjetnika razvile "umjetno inteligentnog državnog odvjetnika" koji može s 97% točnosti na temelju glasovnog opisivanja slučaja podnijeti tužbu, i to za osam čestih kaznenih djela kao što su obijesna vožnja, klađenje ili prijevara.[111]

U Engleskoj nalik COMPAS-u u uporabi je HART, no više se koristi od strane policije nego suda, generirajući procjenu rizika recidivizma kako bi policija lakše donijela odluku o zadržavanju osumnjičenika u pritvoru.[112] Kontroverza s HART-om nastala je kada se saznalo da sustav koristi tzv. *consumer segmentation* podatke dobivene od privatnih društava; to su podaci koji razdijele korisnike u brojne kategorije na temelju zajedničkih osobina, kao što su dob, spol ili interesi.[113]

[109] *Ibid.*
[110] China Daily, *Chinese courts must implement AI system by 2025* - https://www.chinadaily.com.cn/a/202212/09/WS6392fa3ba31057c47eba3a3f.html (preuzeto 17.6.2023.)
[111] South China Morning Post, *Chinese scientists develop AI 'prosecutor' that can press its own charges* - https://www.scmp.com/news/china/science/article/3160997/chinese-scientists-develop-ai-prosecutor-can-press-its-own (preuzeto 17.6.2023.)
[112] González Fuster, G., *op. cit.* (bilj. 11), str. 28.
[113] Segment, *Customer Segmentation* - https://segment.com/growth-center/customer-segmentation/ (preuzeto 17.6.2023.)

7. IZVRŠAVANJE MJERE ISTRAŽNOG ZATVORA

U zatvorima umjetna inteligencija još nije široko raširena, ali postoje brojni načini kako se isprobava i razvija te kako bi mogla uskoro djelovati.[114] Premda se provedena istraživanja uglavnom odnose za izvršavanje zatvorskih kazni, moguće je povući određene paralele s izvršavanjem istražnog zatvora, budući da je riječ o mjeri koja se izvršava u penalnim ustanovama i čije izvršenje je uvelike uređeno penitencijarnopravnim propisima. Po jednom je istraživanju ispitana dvadeset i jedna zatvorska uprava (trinaest europskih, jedna australska, dvije azijske te pet sjevernoameričkih) o tome koriste li trenutno umjetnu inteligenciju ili je namjeravaju početi koristiti te na koji način.[115] Po rezultatima istraživanja umjetna inteligencija se u zatvorima najviše koristi iz sigurnosnih razloga, a najsuvremeniji primjer toga je u Kini, koja koristi tip tehnologije prepoznavanja lica da prati zatvorenike van i unutar ćelija, analizirajući pokrete i stvarajući dnevni izvještaj o ponašanju svakog zatvorenika, u konačnici upozoravajući ako je otkriveno sumnjivo ponašanje.[116] Mogući primjer navedenog ponašanja je da ako se zatvorenik pokušava ozlijediti, umjetna inteligencija može to uočiti i odmah obavijestiti čuvare. Na sličan način djeluju i narukvice nalik *fitness* uređajima koje su zatvorenici dužni nositi. Ti uređaji prate životne znakove i lokaciju zatvorenika, također upozoravajući ako se zatvorenik ozlijedi. Zaključak istraživanja je da većina ispitanih trenutno ne koriste umjetnu inteligenciju, no namjeravaju u bližoj budućnosti, ali još bez preciznih planova.[117]

I dalje najraširenija uporaba umjetne inteligencije u zatvorima je, kao i na sudovima, tehnologija procjene rizika. Jedina zapravo značajna razlika je što u ovom slučaju umjetna inteligencija ne daje procjenu rizika na temelju koje sudac donosi osuđujuću presudu, već procjenu rizika na temelju koje upravitelji zatvora odlučuju kako najbolje rehabilitirati zatvorenika ili općenito odrediti njegov smještaj unutar zatvora, primjerice u Finskoj.[118]

Jedan od ostalih načina je uporaba umjetne inteligencije za nadziranje razgovora zatvorenika. Po jednom izvještaju iz 2019. godine nenadzirani razgovori zatvorenika prema van

[114] Redden, J., et. al., *Artificial Intelligence Applications in Corrections,* U.S. Department of Justice, National Institute of Justice, Office of Justice Programs, 2020., str. 4.
[115] Puolakka, P., Van De Steene, S., *Artificial Intelligence in Prisons in 2030: An Exploration on the Future of AI in Prisons,* Advancing Corrections Journal, br. 11, 2021., str. 131.
[116] *Ibid.*
[117] *Ibid.* str. 135.
[118] *Ibid.* str. 132.

su jedno od vodećih sigurnosnih prijetnji, posebice jer nadziranje svakog telefonskog razgovora od strane djelatnika zatvora predstavlja vremenski vrlo zahtjevan posao.[119] Umjetna inteligencija ovdje može olakšati posao tako što nadzire razgovore, "slušajući" za određene riječi ili fraze koje je naučena da prepoznaje kao opasne.[120] Još jedan značajan problem u zatvorima je kontrabanda, tj. zabranjeno unošenje ili iznošenje stvari u i van zatvora, primjerice oružja ili droge. Umjetna inteligencija ovdje djeluje tako da analizira slikovne ili video sadržaje i pretražuje ih za predmete koje je programirana da uočava, analogno licima ili pokretima kod tehnologije prepoznavanja lica.[121] Konačno, umjetna inteligencija se može koristiti kako bi olakšala organizaciju u zatvorima, bilo kod najučinkovitijeg razmještaja zatvorenika, bilo kod olakšavanja papirologije, ili kod organiziranja rasporeda za posjete u zatvorima.[122] No kao i kod svih ranije navedenih metoda, potrebno je naravno uvjeriti se da zatvorski sustavi umjetne inteligencije u stvarnosti djeluju tj. će djelovati kako su zamišljeni, i po točnosti i po nepostojanju diskriminacije.

[119] Russo, J., et. al., *Countering Threats to Correctional Institution Security: Identifying Innovation Needs to Address Current and Emerging Concerns*, RAND Corporation, 2019., str. 1.
[120] Redden, J., et. al., *op. cit.* (bilj. 114), str. 4.
[121] *Ibid.*
[122] *Ibid.* str. 5.

8. TENDENCIJE UPORABE UMJETNE INTELIGENCIJE ZA POTREBE KAZNENOG POSTUPKA U REPUBLICI HRVATSKOJ

Vjerojatno nije iznenađujuće da u Hrvatskoj umjetna inteligencija još nije toliko raširena kao u nekima od ranije spomenutih zemljama EU i svijeta. Hrvatska je znatno manja država, koja zasigurno nije tehnološki predvodnik kao SAD ili Kina, no ujedno je i među najsigurnijim državama svijeta te nema neke od problema s kojima se susreću ostale države.[123]

Na općoj razini, Hrvatsku kao državu članicu EU obvezuju sve uredbe pa tako i Uredba o umjetnoj inteligenciji kad stupi na snagu, no iako u nacionalnom pravu još ne postoji slično uređenje, postoje razmatranja koja se osvrću na pitanje tehnologija umjetne inteligencije. Tako je u travnju 2023. godine Odbor za pravosuđe Hrvatskog sabora donio jedno mišljenje o Uredbi o umjetnoj inteligenciji, tj. točnije mišljenje kojim je podržao stajalište Republike Hrvatske o Uredbi o umjetnoj inteligenciji u pogledu izvanugovorne odgovornosti.[124] Mjesec dana kasnije u Saboru zaprimljen je prijedlog o donošenju Rezolucije o umjetnoj inteligenciji.[125] Prijedlog započinje s uvažavanjem relevantnih rezolucija, smjernica, prijedloga, izvještaja i istraživanja donesenih na EU i svjetskoj razini, te nastavlja s prijedlogom svim nadležnim institucijama u Hrvatskoj da uvaže iznesena stajališta o umjetnoj inteligenciji po etičkim, pravnim i sigurnosnim pitanjima.[126] Posebno zanimljiva je t. 20. Prijedloga u kojoj je iznesen stav o "zabrani upotrebe sustava umjetne inteligencije radi ozbiljnih opasnosti od narušavanja temeljnih ljudskih prava, financijskih gubitaka, te nemogućnosti pravednog utvrđivanja odgovornosti za odluke, postupke i događaje, za: 1. prediktivnu primjenu u sustavima za regulaciju javnog reda i mira, prvenstveno u policijskim i pravosudnim poslovima, 2. odlučivanje o konačnim posljedicama, naročito u pitanjima života i smrti, osobnih sloboda, oduzimanja slobode i izdržavanja kazni, te djelatne sposobnosti, bez ljudskog nadzora i odgovornosti…".[127]

---

[123] World Population Review, *Crime Rate by Country* 2023 - https://worldpopulationreview.com/country-rankings/crime-rate-by-country (preuzeto 20.6.2023.)
[124] *Mišljenje Odbora za pravosuđe Hrvatskog sabora o Stajalištu Republike Hrvatske o Prijedlogu direktive Europskog parlamenta i Vijeća o prilagodbi pravila o izvanugovornoj građanskopravnoj odgovornosti s obzirom na umjetnu inteligenciju (Direktiva o odgovornosti za umjetnu inteligenciju COM (2022) 496),* URBROJ: 6521-9-23-02
[125] *Prijedlog Rezolucije o umjetnoj inteligenciji,* URBROJ: 65-23-02
[126] *Ibid.*
[127] *Ibid.* t. 20.

Navedene tehnologije jasno odgovaraju prediktivnom radu policije te korištenju procjene rizika kao zamjenu za suce kod donošenja kaznenih presuda. No, Hrvatski sudovi trenutno ne koriste procjene rizika, niti policija umjetnu inteligenciju u svrhu prediktivnog rada, ali značajno je to što je 2016. i 2020. godine Ministarstvo unutarnjih poslova (dalje u tekstu: MUP) kupilo tehnologiju prepoznavanja lica, i to u slučaju iz 2016. radi nadziranja granica, tj. u sigurnosne razloge, a 2020. godine iz "tajnih" razloga — javni natječaj za nabavu bio je klasificiran oznakom tajnosti "Ograničeno."[128] Iako se i dalje ne zna za koju točnu svrhu je korištena tehnologija iz kasnijeg natječaja, možemo pretpostaviti da se radi o tehnologiji prepoznavanja lica u stvarnom vremenu.

Značajno je još što je u vrijeme kasnijeg natječaja Hrvatski sabor donio Zakon o obradi biometrijskih podataka (dalje u tekstu: ZOBP), radi učinkovitog utvrđivanja identiteta i zaštite fizičkih osoba od zlouporabe njihovih osobnih podataka, kako ZOBP određuje.[129] ZOBP dalje propisuje kako nadležna tijela prikupljaju biometrijske podatke sukladno posebnim propisima i pohranjuju ih u odgovarajuće zbirke i to za obrađivanje biometrijskih podataka koji su prikupljeni, između ostalog, tijekom kriminalističkih istraživanja, bez obzira na državljanstvo.[130] Ti podaci obrađuju se npr. u svrhu otkrivanja počinitelja kaznenih djela i traganja za počiniteljima kaznenih djela tako da se uspoređuju s biometrijskim podacima prikupljenim iz drugih razloga, kao što su npr. prilikom postupka izdavanja osobnih identifikacijskih isprava ili od državljana trećih zemalja ili osoba bez državljanstva koji podnose zahtjev za izdavanje vize.[131] Time je zapravo stvorena mrežna povezanost biometrijskog identificiranja fizičkih osoba, tako da se podaci prikupljeni za jedan od ZOBP-om nabrojanih razloga koriste za identifikaciju osoba ako je to potrebno za neki od drugih razloga i obrnuto. Uz ZOBP donesen je kasnije iste godine od strane ministra nadležnog za unutarnje poslove (MUP), uz prethodnu suglasnost ministra nadležnog za poslove pravosuđa (Ministarstvo pravosuđa i uprave) i ministra nadležnog za vanjske poslove (Ministarstvo vanjskih i europskih poslova), Pravilnik o obradi biometrijskih podataka (dalje u tekstu: Pravilnik).[132] Pravilnik određuje djelovanje ABIS-a, tj. Automatiziranog sustava za biometrijsku identifikaciju, što je informacijski sustav koji bez ljudske intervencije provodi uspoređivanje biometrijskih

[128] Faktograf.hr, *Hrvatska policija skriva kako koristi tehnologiju za prepoznavanje lica* - https://faktograf.hr/2021/03/01/hrvatska-policija-skriva-kako-koristi-tehnologiju-za-prepoznavanje-lica/ (preuzeto 20.6.2023.)
[129] *Zakon o obradi biometrijskih podataka,* NN 127/19, čl. 1.
[130] *Ibid.* čl. 6. st. 2. t. 2.
[131] *Ibid.* čl. 8.
[132] *Pravilnik o obradi biometrijskih podataka,* NN 122/2020

podataka.[133] ABIS je zamjena za dotadašnji AFIS — Automatizirani sustav za identifikaciju otisaka prstiju, a može isto kao AFIS identificirati osobe na temelju unosa tragova papilarnih linija prstiju radi usporedbe s bazom podataka te još i isto tako identificirati osobe na temelju fotografija lica, tj. tehnologija prepoznavanja lica.[134]

Trenutno najizgledniji način korištenja tehnologije umjetne inteligencije u hrvatskom kaznenom sudskom postupku je znatno manje zapanjujući i glamurozan, no nije nimalo nevažan. Radi se o automatiziranom transkribiranju ročišta, što bi značilo da umjetna inteligencija na temelju *speech-to-text* tehnologije bi govore sudionika pretvarala u pisanu riječ.[135] Trenutni problem je što po nekim podacima tehnologija još nije savršeno točna pri uporabi za hrvatski jezik,[136] no prednost *machine-learning* tehnologije, kako je ranije navedeno, je da može učiti na svojim greškama i poboljšavati se vremenom.

[133] *Ibid.* čl. 3. st. 1.
[134] Centar za forenzična ispitivanja, istraživanja i vještačenja Ivan Vučetić, *ABIS* - https://forenzika.gov.hr/sluzbe/sluzba-daktiloskopije-i-identifikacije/abis/96 (preuzeto 20.6.2023.)
[135] Burić, Z., *Deveta novela Zakona o kaznenom postupku – moderno pravosuđe spremno za buduće izazove*?, Hrvatski ljetopis za kaznene znanosti i praksu (Zagreb), vol. 29, br. 2/2022, str. 324.
[136] *Ibid.* str. 325.

9. BUDUĆNOST UMJETNE INTELIGENCIJE U KAZNENOM PRAVU

Iako je sve do sada navedeno samo malen dio umjetne inteligencije unutar pravnih grana, koje čini sićušan dio upotrebe umjetne inteligencije općenito, postojeći sustavi će se nastaviti razvijati i novi će biti osmišljeni i stavljeni u uporabu. Izgledno je da će barem neke od obrađenih tehnologija biti zabranjene ili uvelike ograničene kroz godine, barem u EU, ali poznato je da tehnologija napreduje brže od zakona, što i dalje čini cijelu problematiku nepredvidivom i vrlo dinamičnom.

U domeni materijalnog kaznenog prava, no od velikog značaja i za sam kazneni postupak, vjerojatno će aktualno postati pitanje primjene načela krivnje na robote, tj. pomalo senzacionalistički postavljeno, može li robot biti kriv za ubojstvo? Inteligentni, samo-vozeći automobili, tzv. *self-driving cars,* nisu više nimalo znanstveno fantastična ideja nego realna tehnologije današnjice.[137] Što kada pogazi pješaka? Odgovara li vlasnik auta, ili putnik u vozilu, proizvođač, prodavatelj, ili sam auto? Primjenjivi su razni već postojeći pojmovi iz kaznenog prava, kao što su izravna odgovornost, određeni oblik posrednog počiniteljstva, zapovjedna odgovornost ili prirodno vjerojatna posljedica.[138] Na odgovor na pitanje koji oblik odgovornosti će u konačnici biti primijenjen morat ćemo pričekati.

U Kini su 2019. godine znanstvenici predložili MANN, *machine-learning* umjetnu inteligenciju koja uzima pisani opis kaznenog slučaja i na temelju toga s izvrsnim rezultatima donosi predviđanje o presudi suca, no uz još neriješene probleme vezane za odmjeravanje kazne zatvora te postojanje više okrivljenika u istom slučaju.[139] Time se otvaraju vrata za tzv. *robo-judges,* tj. umjetno inteligentne suce koji mogu u budućnosti zamijeniti ljudske, po argumentu da ako već mogu savršeno predvidjeti kako će ljudski sudac presuditi, zašto ne dati da umjetna inteligencija odmah ne donese presudu?

Ali umjetna inteligencija se neće samo razvijati za uporabu od strane države, već se koristi a i koristit će se više i više od strane samih počinitelja kaznenih djela, npr. kod počinjenja kibernetičkih kaznenih djela razvijanjem umjetno inteligentnih *malware* programa,[140] ili kod

[137] TechCrunch, *Self-driving cars are taking ages to become a reality, but they won't take forever* - https://techcrunch.com/2023/05/16/self-driving-tech-predictions/ (preuzeto 22.6.2023.)
[138] Berdica, J., Herceg Pakšić, B., U*mjetna inteligencija i odabrani aspekti kaznenoga prava - O nekim izazovima za suvremenu pravnu kulturu,* Filozofska istraživanja, br. 42/1, 2022., str. 96.
[139] *Ibid.* str. 99.
[140] *Malicious Uses and Abuses of Artificial Intelligence,* Trend Micro Research, 2020., str. 6.

oponašanja ljudi[141] kao već postojeći oblici počinjenja, ili kod sve sofisticiranije uporabe *deepfake* tehnologije[142] kao potencionalno budući oblik, koje sadrži znatno veće implikacije od samog počinjenja kibernetičkih kaznenih djela. Sve navedeno predstavljat će nove probleme za policijske službe, pogotovo uzevši u obzir da prediktivni rad policije, i da ne bude zabranjen, od male je pomoći za kaznena djela koja nemaju mjesto počinjenja izuzev samog kibernetičkog prostora interneta.

Nabrojana problematika je samo sažet prikaz raznolikih smjerova razvoja; što će zapravo biti preostaje nam da vidimo.

[141] *Ibid.* str. 19.
[142] *Ibid.* str. 53.

10. ZAKLJUČAK

Kod prikaza tehnologija umjetne inteligencije u ovom radu većina zaključaka su zapravo proizašli kao negativni. Konstantno se pojavljuje problem diskriminacije i kršenja temeljnih sloboda, zadiranje u privatnost, neučinkoviti rezultati, manjak transparentnosti te uglavnom buduća obećanja o poboljšanjima. Ali to ne bi trebalo predstavljati osudu umjetne inteligencije cjelokupno, već njenu trenutnu uporabu u kaznenom procesnom pravu. Umjetna inteligencija je na kraju samo alat kojeg ljudi koriste, te kao što je prikazano u poglavlju o prediktivnom radu policije, kada je *input* koji umjetna inteligencija dobiva barem prešutno diskriminatoran i pun predrasuda, a na temelju toga umjetna inteligencija donosi zaključke, nerazumno je očekivati savršenstvo tehnologije. Jer umjetna inteligencija zapravo, da se koristi i da bude prihvaćena, vjerojatno niti ne mora biti savršena, nego samo bolja od čovjeka. Ne očekujemo da čovjek donosi odluke bezgrješno—iako i dalje bi trebali držati službenike u kaznenom procesu po najvišem mogućem standardu—pa tako i umjetna inteligencija sigurno neće nikada biti precizna u stopostotnom obujmu a vremenom će biti sve više i više prihvaćena.

EU je na najboljem tragu zabranom ili ograničavanjem tehnologija umjetne inteligencije čiji problemi trenutno daleko nadmašuju njihovu korist. Moguće je da će u budućnosti neki od tih problema biti riješeni kao što su preciznost, no za neke vjerojatno nema nade dokle god umjetna inteligencija ne postane sama dovoljno inteligentna da može unaprijed prepoznati i shvatiti ljudske predrasude i adekvatno na njih dati svoj odgovor. Zato je značajno da danas umjetna inteligencija bude nadopuna, ili alat u ljudskim rukama, i što se tiče konačne odgovornosti i uvažavanja svih činjenica i okolnosti, uključujući one na koje umjetna inteligencija još ne može reagirati, kao što su ljudske emocije.

U Hrvatskoj, kao i u ostatku svijeta, možemo uočiti trend širenja uporabe umjetne inteligencije u kaznenom pravosuđu. Trend će zasigurno djelomično usporiti utjecajem EU zabrana, najviše za prijašnje obrađeno pitanje uporabe tehnologije prepoznavanja lica od strane hrvatske policije. Tako će navedena uporaba morati ili u cijelosti prestati, ili barem biti značajno ograničena, a za ostale metode kao što su prediktivni rad policije ili procjena rizika zbog istih EU ograničenja i zabrana postojat će sve manja inicijativa ili općenito mogućnost za uvođenje istih.

Budućnost je ovdje jednako uzbudljiva koliko je moguće zastrašujuća.

LITERATURA

KNJIGE I ČLANCI

1. Berdica, J., Herceg Pakšić, B., U*mjetna inteligencija i odabrani aspekti kaznenoga prava - O nekim izazovima za suvremenu pravnu kulturu,* Filozofska istraživanja, br. 42/1, 2022., str. 87-103.
2. Burić, Z., *Deveta novela Zakona o kaznenom postupku – moderno pravosuđe spremno za buduće izazove*?, Hrvatski ljetopis za kaznene znanosti i praksu (Zagreb), vol. 29, br. 2/2022, str. 311-342.
3. Chelioudakis, E., *Risk assessment tools in criminal justice: is there a need for such tools in Europe and would their use comply with European data protection law?,* ANU JOLT, br. 1, 2020., str. 72-96.
4. Cinelli, V., *Crime Prevention and Predictive Analysis: The Italian Case*, 2020., Agenformedia
5. Custers, B., *AI in Criminal Law: An Overview of AI Applications in Substantive and Procedural Criminal Law,* Law and Artificial Intelligence, Heidelberg: Springer, 2022., str. 205-223.
6. Dressel, J., Farid, H., *The Accuracy, Fairness, and Limits of Predicting Recidivism*, Science Advances, br. 4, 2018.
7. Flores, A. W., et. al., *False Positives, False Negatives, and False Analyses: A Rejoinder to "Machine Bias: There's Software Used Across the Country to Predict Future Criminals. And it's Biased Against Blacks.",* Federal Probation, br. 80, 2016., str. 38-46.
8. Gentile, G., *AI in the Courtroom and Judicial Independence: An EU Perspective,* EUIdeas, 2022.
9. González Fuster, G., *Artificial Intelligence and Law Enforcement – Impact on Fundamental Rights*, 2020.
10. Gstrein, O. J., *Ethical, legal and social challenges of Predictive Policing,* Católica Law Review, br. 3, 2019., str. 77-98.
11. Haberman, C., Ratcliffe, J., *The Predictive Policing Challenges of Near Repeat Armed Street Robberies*, Policing, br. 6, 2012., str. 151-166.
12. Hung, T-W., Yen, C-P., *On the Person-based Predictive Policing of AI,* Ethics and Information Technology, br. 23, 2021.

13. Lecorps, Y., Tissandier, G., *PAVED with Good Intentions? An Evaluation of a French Police Predictive Policing System*, 2022.
14. Madiega, T., Mildebrath, H., *Regulating Facial Recognition in the EU,* European Parliamentary Research Service, 2021.
15. Manning, C., *Artificial Intelligence Definitions,* Stanford University - Human-Centered Artificial Intelligence, 2020.
16. Momsen, C., *Implications and Limitations of the Use of AI in Criminal Justice in Germany,* KriPoZ, br. 1, 2023., str. 8-16.
17. Nkonde, M., *Automated Anti-Blackness: Facial Recognition in Brooklyn, New York,* Harvard Kennedy School Journal of African American Policy, br. 2019-2020., str. 30-36.
18. O'Donell, R. M., *Challenging Racist Predictive Policing Algorithms Under the Equal Protection Clause,* New York University Law Review, br. 94:544, 2019., str. 544-580.
19. Oosterloo, S., van Schie, G., *The Politics and Biases of the "Crime Anticipation System" of the Dutch Police,* Proceedings of the International Workshop on Bias in Information, Algorithms, and Systems, br. 2103, 2018., str. 30-41.
20. Popple, J., *A Pragmatic Legal Expert System*, Dartmouth, 1996.
21. Puolakka, P., Van De Steene, S., *Artificial Intelligence in Prisons in 2030: An Exploration on the Future of AI in Prisons,* Advancing Corrections Journal, br. 11, 2021., str. 128-138.
22. Redden, J., et. al., *Artificial Intelligence Applications in Corrections,* U.S. Department of Justice, National Institute of Justice, Office of Justice Programs, 2020.
23. Reiling, A. D., *Courts and Artificial Intelligence*, International Journal for Court Administration, br. 11, 2020.
24. Rigano, C., *Using Artificial Intelligence To Address Criminal Justice Needs,* NIJ Journal, br. 280, 2019., str. 37-46.
25. Roksandić, S., et. al., *Trustworthy Artificial Intelligence and its use by Law Enforcement Authorities: where do we stand?,* MIPRO 2022/ICTLAW, 2022., str. 1395-1402.
26. Russo, J., et. al., *Countering Threats to Correctional Institution Security: Identifying Innovation Needs to Address Current and Emerging Concerns*, RAND Corporation, 2019.
27. Santow, E., *Can Artificial Intelligence Be Trusted With Our Human Rights*?, Australian Quarterly, br. 91, 2020., str. 10-17.
28. Shapiro, A., *Predictive Policing for Reform? Indeterminacy and Intervention in Big Data Policing*, Surveillance and Society, br. 17, 2019., str. 456-472.
29. Songül, T., et. al., *Why Machine Learning May Lead to Unfairness: Evidence from Risk Assessment for Juvenile Justice in Catalonia*, Canada, ICAIL, 2019.

30. Sprick, D., *Predictive Policing in China: An Authoritarian Dream of Public Security,* Nordic Journal of Law and Social Research, br. 9, 2019., str. 299-324.
31. Vats, A., *Building the Case for Restricted Use of Predictive Policing Tools in India,* International Review of Information Ethics, br. 32, 2022.
32. Vepřek, H. L., et. al., *Beyond Effectiveness: Legitimising Predictive Policing in Germany,* Kriminologie – Das Online-Journal, br. 3, 2020., str. 423-443.
33. Wankhade, T. D., et. al., *Artificial Intelligence in Forensic Medicine and Toxicology: The Future of Forensic Medicine,* Cureus, br. 14, 2022., str. 1767-1776.
34. Wong, T. A., *The Mathematics of Policing,* 2022.
35. Youstin, T., et. al., *Assessing the Generalizability of the Near Repeat Phenomenon,* Criminal Justice and Behavior, br. 38, 2011., str. 1042-1063.

PRAVNI IZVORI

1. *Annexes to the Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts,* COM(2021)
2. *Bijela knjiga o umjetnoj inteligenciji – Europski pristup izvrsnosti i izgradnji povjerenja,* COM(2020)
3. *Mišljenje Odbora za pravosuđe Hrvatskog sabora o Stajalištu Republike Hrvatske o Prijedlogu direktive Europskog parlamenta i Vijeća o prilagodbi pravila o izvanugovornoj građanskopravnoj odgovornosti s obzirom na umjetnu inteligenciju (Direktiva o odgovornosti za umjetnu inteligenciju COM (2022) 496),* URBROJ: 6521-9-23-02
4. *Povelja Europske unije o temeljnim pravima* (2016/C 202/02)
5. *Pravilnik o obradi biometrijskih podataka,* NN 122/2020
6. *Prijedlog Rezolucije o umjetnoj inteligenciji,* URBROJ: 65-23-02
7. *Prijedlog uredbe Europskog parlamenta i Vijeća o utvrđivanju usklađenih pravila o umjetnoj inteligenciji (Akt o umjetnoj inteligenciji) i izmjeni određenih zakonodavnih akata unije,* 2021/0106 (COD)
8. *Rezolucija Europskog parlamenta od 6. listopada 2021. o umjetnoj inteligenciji u kaznenom pravu i njezinoj primjeni od strane policije i pravosudnih tijela u kaznenim stvarima,* (2020/2016(INI))
9. *Zakon o obradi biometrijskih podataka,* NN 127/19

IZVJEŠĆA I VODIČI

1. CEPEJ - *European Ethical Charter on the use of Artificial Intelligence in Judicial Systems and Their Environment*, 2018.
2. *Knjiga sažetaka – Big Data in Law Enforcement: from Reactive to Proactive*, MUP RH, Zagreb, 2017.
3. *Malicious Uses and Abuses of Artificial Intelligence*, Trend Micro Research, 2020.
4. *Practitioner's Guide to COMPAS Core*, Northpointe Inc., 2015.
5. *Regulating Artificial Intelligence for Use in Criminal Justice Systems in the EU - Policy Paper*, FairTrials
6. *The Future of Jobs Report*, Svjetski ekonomski forum, 2020.

MREŽNI IZVORI

1. American Bar Association, *Artificial Intelligence: Benefits and Unknown Risks* - https://www.americanbar.org/groups/judicial/publications/judges_journal/2021/winter/artificial-intelligence-benefits-and-unknown-risks/
2. BBC, *Sweetie: 'Girl' chatbot targets thousands of paedophiles* - https://www.bbc.com/news/av/technology-42461065
3. BBC, *Webcam sex with fake girl Sweetie leads to sentence* - https://www.bbc.com/news/technology-29688996
4. Centar za forenzična ispitivanja, istraživanja i vještačenja Ivan Vučetić, *ABIS* - https://forenzika.gov.hr/sluzbe/sluzba-daktiloskopije-i-identifikacije/abis/96
5. China Daily, *Chinese courts must implement AI system by 2025* - https://www.chinadaily.com.cn/a/202212/09/WS6392fa3ba31057c47eba3a3f.html
6. Crown Prosecution Service, *Abuse of Process* – https://www.cps.gov.uk/legal-guidance/abuse-process
7. Epic.org, *AI in the Criminal Justice System* - https://epic.org/issues/ai/ai-in-the-criminal-justice-system/
8. European Data Protection Board, *Swedish DPA: Police unlawfully used facial recognition app* - https://edpb.europa.eu/news/national-news/2021/swedish-dpa-police-unlawfully-used-facial-recognition-app_en
9. Faktograf.hr, *Hrvatska policija skriva kako koristi tehnologiju za prepoznavanje lica* - https://faktograf.hr/2021/03/01/hrvatska-policija-skriva-kako-koristi-tehnologiju-za-prepoznavanje-lica/

10. Fortune, *Here's How Many Adult Faces Are Scanned From Facial Recognition Databases by Cops* - https://fortune.com/2016/10/18/facial-recognition-database/
11. Illinois Tech, *GPT-4 Passes the Bar Exam* - https://www.iit.edu/news/gpt-4-passes-bar-exam
12. LexisNexis, *State v. Loomis* - https://www.lexisnexis.com/community/casebrief/p/casebrief-state-v-loomis
13. Lexology, *The perils of feedback loops in machine learning: predictive policing* - https://www.lexology.com/library/detail.aspx?g=c8fff116-2112-48dd-841c-f9d1688d722b
14. Los Angeles Times, *LAPD data programs need better oversight to protect public, inspector general concludes* - https://www.latimes.com/local/lanow/la-me-ln-lapd-data-20190312-story.html
15. PredPol,: *Proven Crime Reduction Results* - https://www.predpol.com/results/
16. Segment, *Customer Segmentation* - https://segment.com/growth-center/customer-segmentation/
17. South Chinese Morning Post, *Chinese scientists develop AI 'prosecutor' that can press its own charges* - https://www.scmp.com/news/china/science/article/3160997/chinese-scientists-develop-ai-prosecutor-can-press-its-own
18. Taylor Wessing, *AI Regulation Around the World* - https://www.taylorwessing.com/en/interface/2023/ai---are-we-getting-the-balance-between-regulation-and-innovation-right/ai-regulation-around-the-world
19. TechCrunch, *Self-driving cars are taking ages to become a reality, but they won't take forever* - https://techcrunch.com/2023/05/16/self-driving-tech-predictions/
20. The Atlantic, *A Popular Algorithm Is No Better at Predicting Crimes Than Random People* - https://www.theatlantic.com/technology/archive/2018/01/equivant-compas-algorithm/550646/
21. The Economist, *How AI is transforming the creative industries* - https://www.economist.com/films/2021/04/07/how-ai-is-transforming-the-creative-industries
22. World Population Review, *Crime Rate by Country* 2023 - https://worldpopulationreview.com/country-rankings/crime-rate-by-country