

Ivan Vidaković*

UPORABA PREDIKTIVNIH SUSTAVA UMJETNE INTELIGENCIJE NAMIJENJENIH TIJELIMA KAZNENOG PROGONA – PERSPEKTIVA EUROPSKE UNIJE**

Umjetna inteligencija postala je sastavni dio svakodnevice, a kazneno pravo u širem smislu nije ostalo imuno na procese osuvremenjivanja. Implementacijom sustava umjetne inteligencije u tradicionalne djelatnosti, procese te stadije, posebno kroz prediktivne sustave, koji predviđaju buduća kaznena djela, lokacije, počinitelje i žrtve, policijsko djelovanje pomaknuto je s reaktivnog na preventivno. Ipak, učinkovitost i brzina obrade velike količine podataka imaju svoje rizike, a oni se najviše ogledaju u kvaliteti podataka, transparentnosti i točnosti. Jedan od ozbiljnijih pokušaja kontrole i minimiziranja takvih rizika jest regulacija umjetne inteligencije od strane Europske unije putem Uredbe EU-a o umjetnoj inteligenciji.

Uvodno se u radu analizira fragmentiranost pristupa regulaciji uporabe umjetne inteligencije, iznosi definicija prediktivnih sustava te navode kategorije tih sustava s obzirom na njihovu svrhu. Razmatranjem prediktivnih sustava s obzirom na njihovu svrhu analiziraju se konkretne implikacije njihove uporabe za temeljna ljudska prava i slobode. Nastavno se analiziraju dosadašnje prakse na primjerima konkretnih sustava i država kako bi se odredile reakcije pravnih sustava na njihovu uporabu putem relevantnih sudskih odluka. Na posljetku se razmatranjem regulacije uporabe umjetne inteligencije od strane Europske unije nastoji utvrditi mogu li prediktivni sustavi ispuniti striktno kriterije visokorizičnih sustava konačno prihvaćene

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

** Ovaj je rad financirao Pravni fakultet Osijek Sveučilišta Josipa Jurja Strossmayera u Osijeku internim projektom Umjetna inteligencija i kazneno pravo (IP-PRAVOS-18).

kompromisnim rješenjem s iznimnom mogućnosti uporabe kao visokorizičnih sustava.

Ključne riječi: kvaliteta podataka, prediktivni sustavi, pristup temeljen na riziku, transparentnost, Uredba EU-a o umjetnoj inteligenciji, visokorizični sustavi umjetne inteligencije

1. UVODNA RAZMATRANJA

Sveopći i rapidan razvoj tehnologije izvršio je nepovratni utjecaj na sve sfere društva. Vrhunac je tehnološkog razvoja umjetna inteligencija (dalje: UI), a njezina prisutnost u svakodnevnoj uporabi prolazila je nezapaženo do prije nekoliko godina. Razvoj tehnologije omogućio je policiji da preventivnu djelatnost poboljša uporabom različitih sustava UI-ja putem brže i preciznije obrade znatno veće količine podataka u nastojanju da predvidi područje počinjenja kaznenog djela, počinitelje, ali i žrtve.¹ U skladu s predmetnim tehnološkim razvojem policija već dugi niz godina usmjerava svoje djelovanje na prevenciju, za razliku od tradicionalnog reaktivnog djelovanja na već počinjena kaznena djela.² Ono što je zajedničko samostalnoj ljudskoj procjeni i misaonom procesu procjene potpomognutom ili u potpunosti zamijenjenom sustavima UI-ja jest rezultat, a to je procjena određenog stupnja vjerojatnosti da će određena osoba biti počinitelj kaznenog djela u budućnosti, da će kaznena djela biti više činjena na određenom području, odnosno da će određena osoba biti žrtva kaznenog djela u budućnosti.³ Neovisno o tome je li rezultat izražen u postotku ili na drugi način, takva procjena ima stvarne posljedice za pojedince odnosno grupe ljudi, njihova temeljna ljudska prava i slobode; može rezultirati povećanom preventivnom aktivnosti policije i socijalne službe na određenom području, etničkim odnosno rasnim profiliranjem, ali jednako tako i konkretnim radnjama uhićenja, pretrage i drugih invazivnih mjera policije usmjerenih na pojedince.⁴

¹ Ferguson, A. G., Policing Predictive Policing, *Washington University Law Review*, vol. 94, br. 5, 2017, str. 1113–1114.

² Jones, T., Governing Security: Pluralization, Privatization, and Polarization in Crime Control and Policing, u: Maguire, M., Morgan, R., Reiner, R. (ur.), *The Oxford Handbook of Criminology, Fifth Edition*, Oxford University Press, 2013, str. 744–757.

³ Kaufmann, M.; Egbert, S.; Lesse, M., Predictive Policing and the Politics of Patterns, *The British Journal of Criminology*, vol. 59, br. 3, 2019, str. 674–676.

⁴ Sandhu, A.; Fussey, P., The ‘uberization of policing’? How police negotiate and operationalise predictive policing technology, *Policing and Society: Policing and Technology*, vol. 31, br. 1, 2021, str. 69–71.

Utjecaj tehnologije na prediktivnu aktivnost policije samo će se povećavati, a time i rizici utjecaja na svakodnevni život, temeljna ljudska prava i slobode pojedinaca, i to sve na temelju probabilističkih rezultata.⁵ Primarni je problem usporeno i teško usklađivanje regulacije zbog neslaganja glede kategorizacije sustava kao visokorizičnih i zabranjenih, ali i pitanja definicije.⁶ Stoga se u prvom poglavlju rada nastoje dati temeljna terminološka određenja i definicije prediktivnih sustava. Fragmentirani pristup pravnoj regulaciji uzrokuje potrebu za analizom primjene pojedinih prediktivnih sustava i reakcija pojedinih pravnih sustava, ponajprije u obliku sudskih odluka. Stoga se u drugom poglavlju analiziraju konkretni prediktivni sustavi UI-a i judikatura nacionalnih sudova kao reakcija na realne implikacije u kaznenom postupku. U posljednjem poglavlju rada razmatra se nova perspektiva kroz konačno usvojen prijedloga Uredbe (EU) 2024/1689 Europskog parlamenta i Vijeća od 13. lipnja 2024. o utvrđivanju usklađenih pravila o umjetnoj inteligenciji i o izmjeni uredba (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) (dalje: Uredba EU-a o umjetnoj inteligenciji).⁷

Razmatranjem pojedinih najproblematičnijih sustava kroz prizmu imanen-tnih obilježja prediktivnih sustava procjenjuje se mogućnost ispunjavanja zahtjeva visokorizičnih sustava te se razmatra ispravnost prihvaćenog prijedloga regulacije prediktivnih sustava. Primjena pojedinih prediktivnih sustava, ali i reakcija sudbene vlasti na nju, upozorile su na mnogobrojne probleme, odnosno kritičke točke buduće regulacije. Kao kritične točke regulacije razmatraju se određeni kriteriji, odnosno načela, koja visokorizični sustavi moraju zadovoljiti, a to su kvaliteta podataka, transparentnost i točnost.

⁵ Egbert, S.; Leese, M., *Criminal Futures: Predictive Policing and Everyday Police Work*, Routledge Studies in Policing and Society, Taylor & Francis, 2021, str. 20–21.

⁶ Picotti, L., General Report, in: Picotti, L., Panattoni, B. (ur.), *Traditional Criminal Law Categories and AI: Crisis or Palingenesis?*, International Colloquium Section I, Siracusa, *International Review of Penal Law*, vol. 94, br. 1, 2023, str. 12–16. Za detaljniji uvid u fragmentiranost definiranja i klasificiranja također vidi: Nikolinakos, N. Th., *EU Policy and Legal Framework for Artificial Intelligence, Robotics and Related Technologies – The AI Act*, Springer, 2023, str. 353–369; Sheikh, H.; Prins, C.; Schrijvers, E., *Mission AI, The New System Technology*, Springer, 2023, str. 15–20.

⁷ O popisu zakonodavstava Unije za usklađivanje vidi više: Prilog I. odjeljak A. Uredba (EU) 2024/1689 Europskog parlamenta i Vijeća od 13. lipnja 2024. o utvrđivanju usklađenih pravila o umjetnoj inteligenciji i o izmjeni uredba (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), u kojem se navodi 19 pravnih izvora čije je usklađivanje nužno.

2. PREDIKTIVNI SUSTAVI U KAZNENOM POSTUPKU – TERMINOLOŠKA ODREĐENJA I OPĆA OBILJEŽJA

Iako je riječ o sveprisutnom pojmu, definiranje UI-ja nije jednostavno. Prvi je problem definiranja ukupnost tehnologija koje su obuhvaćene tim pojmom, a riječ je o jako velikom broju različitih tehnologija, ali i njihove primjene.⁸ Kada je riječ o kaznenom postupku pravne praznine, mogu biti izrazito problematične s obzirom na narav prava koja se štiti u kaznenim postupcima i posljedice koje iz njihovih nepoštivanja mogu proizaći.⁹ Naime, u ovom trenutku ne postoji centralno tijelo koje bi na globalnoj razini reguliralo UI i njegovu uporabu, već postoji više različitih međunarodnih i regionalnih organizacija koje to nastoje napraviti bez koordinacije s drugima ili uz minimalnu suradnju.¹⁰ Ipak, unifikaciji i harmonizaciji najviše pridonosi definicija UI-ja Europske unije, koja je relevantna i za hrvatski kazneni postupak. Prihvaćenom definicijom sustav UI-ja definiran je kao strojni sustav dizajniran za rad s promjenjivim razinama autonomije, koji nakon uvođenja može pokazati prilagodljivost te koji, za eksplicitne ili implicitne ciljeve, iz ulaznih vrijednosti koje prima zaključuje kako generirati izlazne vrijednosti kao što su predviđanja, sadržaj, preporuke ili odluke, koji mogu utjecati na fizička ili virtualna okruženja.¹¹ Prihvaćeni prijedlog definicije Uredbe EU-a o umjetnoj inteligenciji, kao i definicija UI-ja Okvirne konvencije Vijeća Europe o umjetnoj inteligenciji, usklađene su s definicijom OECD-a.¹² Zajednička obilježja vidljiva su upravo u prepoznavanju različitih vrsta autonomije, prepoznavanju sustava UI-ja kao strojnih sustava, a i ciljevi koji se njima ostvaruju više-manje su identični u sve tri definicije.

Uz pitanja definicije temeljno je pitanje pristupa regulaciji. Kako bi se uveo proporcionalan i djelotvoran skup obvezujućih pravila za sustave UI-ja, treba slijediti jasno definiran pristup temeljen na riziku. Vrsta i sadržaj tih pravila u tom bi pristupu trebali biti primjereni intenzitetu i opsegu rizika koje mogu stvoriti sustavi UI-ja. Stoga je potrebno zabraniti određene neprihvatljive prak-

⁸ 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.

⁹ Krapac, D., *Kazneno procesno pravo, Prva knjiga: Institucije, VIII. Izmijenjeno i dopunjeno izdanje*, Narodne novine, 2020, str. 6–14.

¹⁰ Za detaljni pregled fragmentiranosti pravnog uređenja umjetne inteligencije vidi: Cihon; Maas; Kemp, *op. cit.* (bilj. 6); Schmitt, L., Mapping global AI governance: a nascent regime in a fragmented landscape, *AI Ethics*, vol. 2, 2022, str. 303–305.

¹¹ Uredba EU-a o umjetnoj inteligenciji, čl. 3, st. 3, toč. 1.

¹² Explanatory Report to the Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy, and the Rule of Law, Council of Europe Treaty Series No. 225, str. 6, toč. 23.–25., dostupno na: <https://rm.coe.int/1680afae67> (29. 09. 2024.); OECD, Recommendation of the Council on Artificial Intelligence, OECD/LEGAL/0449, Amended on 08/11/2023, dostupno na: OECD legal instruments, <https://legalinstruments.oecd.org/en/instruments/oecd-legal-0449#dates> (15. 11. 2023.).

se u području UI-ja te utvrditi zahtjeve za visokorizične sustave UI-ja i obveze za relevantne operatore te obveze u pogledu transparentnosti za određene sustave UI-ja. Takav pristup temelji se na ideji proporcionalne regulacije – usmjeren je na postizanje ravnoteže između smanjenja rizika koji proizlaze iz upotrebe sustava UI-ja s jedne strane te inovacija i koristi koje sustavi UI-ja donose s druge strane.¹³ Iako Ebers ističe da je pristup temeljen na riziku najbolji pristup reguliranju uporabe umjetne inteligencije, napominje da takav pristup od strane EU-a nije u potpunosti u skladu s izvornom koncepcijom regulacije temeljene na riziku. Kritika pristupa EU-a proizlazi iz oslanjanja na unaprijed definirane i zatvorene kategorije rizika reguliranja sustava UI-ja, bez empirijskog utemeljenja, rigidne podjele koja nije u stanju pratiti brz razvoj tehnologije UI-ja te ovlasti Europske komisije da ažurira popis visokorizičnih sustava jer takvi procesi mogu biti podložni političkim, a ne empirijskim utjecajima. Umjesto toga zagovara se dinamičniji pristup, koji bi omogućio procjenu rizika u specifičnom kontekstu, a ne oslanjanje na statične kategorije.¹⁴ Takav regulatorni pristup rezultirao je člankom 5. Uredbe EU-a o umjetnoj inteligenciji, kojim se zabranjuje uporaba određenih sustava umjetne inteligencije, između ostalih i sustava UI-ja za procjene rizika u pogledu fizičkih osoba s ciljem predviđanja rizika da će osoba počiniti kazneno djelo isključivo na temelju profila fizičke osobe ili procjene njezinih osobina i obilježja ličnosti. Zabrana se ne primjenjuje na sustave UI-ja koji služe kao podrška ljudskoj procjeni uključenosti osobe u kriminalnu aktivnost pod uvjetom da se procjena temelji na objektivnim i provjerljivim činjenicama, izravno povezanim s kriminalnom aktivnošću. Jednako tako, člankom 6. stavkom 2. Uredbe EU-a o umjetnoj inteligenciji i Prilogom III. točkom 6. regulirana je uporaba sustava namijenjenih kaznenom progonu kao visokorizičnih, dakle onih čija je uporaba dopuštena uz ispunjavanje striktnih uvjeta, a to su: (i) sustavi UI-ja koji procjenjuju rizik da osoba postane žrtva kaznenog djela pružajući tijelima kaznenog progona alate za preventivne mjere, (ii) sustavi UI-ja poput poligrafa ili sličnih alata za podršku kaznenim tijelima, (iii) sustavi UI-ja koji evaluiraju pouzdanost dokaza tijekom istraga ili progona, (iv) sustavi UI-ja koji procjenjuju rizik da osoba počinii ili ponovi kazneno djelo koristeći analize prošlog kriminalnog ponašanja i izradu profila fizičkih osoba, (v) sustavi UI-ja koji se koriste za izradu profila osoba tijekom istraga ili progona kaznenih djela te tako omogućuju predviđanje budućeg ponašanja na temelju prethodnih podataka.

¹³ Ebers, M., *Truly Risk-Based Regulation of Artificial Intelligence – How to Implement the EU's AI Act*, dostupno na: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4870387 (08. 10. 2024.), str. 7. Vidi više Novokmet, A; Tomićić, Z.; Vinković, Z., Pretrial risk assessment instruments in the US criminal justice system – what lessons can be learned for the European Union, *International Journal of Law and Information Technology*, vol. 30, br. 1, 2022, str. 12–15.

¹⁴ Ebers, *op. cit.* (bilj. 13), str. 11–21.

Prihvaćeni model kaznenog pravosuđa pod utjecajem UI-ja i novih tehnologija započeo je transformaciju iz tradicionalnog modela, u kojem je dominirao promišljen i individualiziran pristup, prema perspektivnom, agregiranom modelu, koji uključuje naizgled učinkovitiji, ali neosoban i distanciran pristup.¹⁵ Postoje različiti sustavi UI-ja koji se koriste u kaznenom postupku.¹⁶ Jedni su od njih i prediktivni sustavi, koje je najjednostavnije definirati kao sustave UI-ja koji na temelju unesenih podataka daju rezultat u obliku predviđanja vjerojatnosti da će u budućnosti biti počinjeno kazneno djelo.¹⁷ Putem procesa prediktivne analize predviđaju se u pravilu četiri kategorije: (i) tko će vjerojatno biti počinitelj, (ii) profil ili identitet počinitelja, (iii) tko je potencijalna žrtva, (iv) potencijalno mjesto i vrijeme počinjenja kaznenog djela.¹⁸ Takvi sustavi temelje se na UI-ju kao programu, odnosno sustavu za provođenje prediktivne analize, i ulaznim podacima, koji predstavljaju temelj za takvu analizu. S obzirom na činjenicu da svaka od prethodno navedenih kategorija ima specifične pravne implikacije te prednosti i nedostatke, oni će biti predmetom obrade u nastavku.

2.1. Sustavi predviđanja kaznenih djela

Pod ovu kategoriju prediktivnih sustava podvodimo *sustave za prediktivno mapiranje*. Predmetni sustavi nastoje na temelju unesenih podataka izvršiti predviđanje i profiliranje pojedinih područja koja prepoznaju kao potencijalna područja na kojima će se učestalije činiti kaznena djela, katkad usmjerena na specifičnu vrstu kaznenih djela. Takvo predviđanje predstavlja temelj za do-

¹⁵ Karsai, K., Algorithmic Decisions within the Criminal Justice Ecosystem and their Problem Matrix, *International Review of Penal Law*, vol. 92, br. 1, 2021, str. 15.

¹⁶ Vidi više: Burić, Z.; Engelhart, M.; Novokmet, A.; Roksandić, S., Upotrebljivost rezultata masovnog nadzora komunikacije kao dokaza u hrvatskom kaznenom postupku – slučaj Sky ECC, *Hrvatski ljetopis za kaznene znanosti i praksu*, vol. 30, br. 2, 2023, str. 243–249; Đurđević, Z.; Ivičević Karas E, Uporaba umjetne inteligencije u hrvatskom kaznenom postupku, *Hrvatski ljetopis za kaznene znanosti i praksu*, vol. 30, br. 2, 2023, str. 227–229.

¹⁷ Cf. Wilson, D., Algorithmic patrol: The future of predictive policing, u: Završnik, A. (ur.), *Big data, crime and social control*, Routledge Frontiers of Criminal Justice, 2018, str. 109–110; Egbert, S.; Mann, M., Discrimination in Predictive Policing: The (dangerous) Myth of Impartiality and the Need for STS Analysis, u: Završnik, A.; Badalić, V. (ur.), *Automating, Crime Prevention, Surveillance, and Military Operations*, Springer, 2021, str. 26–27; Dymitriuk, M., Legal Tech in the Law Enforcement Agencies. u: Szostek, D.; Załucki, Z., *Legal Tech*, Nomos Verlagsgesellschaft mbH & Co. KG, 2021, 255–256.

¹⁸ Heilemann, J., Click, Collect and Calculate: The Growing Importance of the Big Data in Predicting Future Criminal Behaviour, *International Review of Penal Law*, vol. 92, br. 1, 2021, str. 50; Quattrocchio, S., *Artificial Intelligence, Computational Modelling and Criminal Proceedings: A Framework for A European Legal Discussion*, Legal Studies in International European and Comparative Criminal Law, vol. 4, Springer, 2020, str. 39.

nošenje informirane odluke u obliku povećanja policijskih patrola, prisutnosti policije i generalno preventivnih aktivnosti policije.¹⁹

Razvidne su dvije prednosti korištenja UI-ja za prediktivno mapiranje. Prva prednost proizlazi iz moćnih matematičkih modela i sustava te velike količine podataka koji omogućuju bržu obradu, ali i aktivnije traženje takozvanih *žarišta kriminala*.²⁰ Van Brakel navodi konkretan primjer korištenja javno dostupnih podataka na društvenim mrežama, koji mogu biti indikativni glede počinjenja kaznenih djela u određenom području, primjerice ako postoji najava određenih događaja ili veće količine alkoholiziranih osoba.²¹ Druga je prednost omogućena prvom jer bržom obradom znatne količine podataka ostaje više prostora za planiranje preventivne djelatnosti, koja je drugi segment svake uporabe prediktivnih sustava.²² Ipak, nedostaci uporabe tih sustava mogu imati šire društvene implikacije. Unos podataka koji predstavljaju osnovu za predviđanje područja za koja se očekuje da će imati veću stopu kriminaliteta jest nereguliran. Ovisi isključivo o subjektu koji uvodi sustav, a takvi podaci mogu biti pristrani te uzrokovati etničko odnosno rasno profiliranje. Ako je određeno područje označeno kao *žarište kriminala* na temelju podataka o uhićenju, a postoji pristranost takvih podataka, tada će takvo prediktivno mapiranje rezultirati vjerojatno još većim brojem uhićenja, a onda će se opet ti podaci unositi u sustav.²³ Time se ostvaruje fenomen *samoispunjavajućeg proročanstva*.²⁴ Dakle, jedan od temeljnih problema koji proizlazi iz uporabe prediktivnih sustava ovog tipa jest kvaliteta i selekcija podataka koji se unose u taj sustav kao ulazni podaci.²⁵

Načelno je riječ o najmanje kontroverznim prediktivnim sustavima jer u odnosu na ciljeve drugih najmanje zadire u prava i slobode pojedinca. Postupanje u skladu s rezultatima općenitije je naravi te potencijalne posljedice za

¹⁹ Fair Trials, *Automating Injustice: The Use of Artificial Intelligence & Automated Decision-Making Systems in Criminal Justice in Europe*, 2021, str. 19, dostupno na: <https://www.fairtrials.org/articles/publications/automating-injustice/> (22. 8. 2023.)

²⁰ Perry, W. L., McInnis, B., Price, C. C., Smith, S. C., Hollywood, J. S., *Predictive Policing: The Role of Crime Forecasting in Law Enforcement Operations*, The RAND Corporation, Safety and Justice Program, str. 15, 2013, dostupno na: https://www.rand.org/content/dam/rand/pubs/research_reports/RR200/RR233/RAND_RR233.sum.pdf, pristupljeno (22. 8. 2023.)

²¹ Van Brakel, R., *Policing, Pre-emptive Big Data Surveillance and its (Dis)Empowering Consequences: The case of Predictive Policing*, u: vann der Sloot B.; Broeders, D.; Schrijvers, E. (ur.), *Exploring the Boundaries of Big Data*, WRR, Amsterdam University Press, 2017, str. 121.

²² Perry *et al.*, *op. cit.* (bilj. 20), str. 17–18.

²³ Van Brakel *op. cit.* (bilj. 21), str. 125.

²⁴ Söderholm, S., *Fundamental rights control when implementing predictive policing – a European perspective*, *Peking University Law Journal*, vol. 11, br. 1, 2023, str. 5.

²⁵ Kusak, M., *Quality of data sets that feed AI and big data applications for law enforcement*, *ERA Forum*, vol. 23, 2022, str. 215.

građane nisu ozbiljne kao kod drugih sustava. Za razliku od sustava za prediktivno mapiranje, puno su kontroverzniji sustavi za predviđanje počinitelja koji će biti analizirani u nastavku poglavlja.

2.2. Sustavi predviđanja počinitelja

Sustavi usmjereni na predviđanje počinitelja nastoje utvrditi pojedince ili skupine koji bi u budućnosti mogli biti počinitelji kaznenih djela.²⁶ Mnogobrojni čimbenici uzimaju se u obzir prilikom procjene potencijala počinjenja kaznenog djela, a mnogi nisu dostatni da se samo na temelju njih može zaključiti o potencijalu budućeg činjenja kaznenog djela, dok su neki sami po sebi sporni.²⁷ Predviđanja, profili i procjene rizika tih sustava upozoravaju tijela kaznenog progona, ponajprije policiju, kako postoji potencijal da će neka osoba počiniti kazneno djelo u budućnost, a takva predikcija može imati važne posljedice za pojedinca.²⁸ Činjenica je da su povijesni policijski podaci primarni izvor koji se koristi za generiranje izlaznih rezultata, odnosno predikcije, ovih sustava. Specifične kategorije podataka razlikovat će se ovisno o sustavu; podaci mogu uključivati informacije o prošlim kaznenim djelima, poput vrste kaznenog djela, vremena i mjesta počinjenja, podataka o uhićenju, prijava i poziva socijalnim i drugim relevantnim službama.²⁹ Naime, isto vrednovanje historijskih podataka koji nemaju jednaku težinu, poput kaznene prijave, uhićenja, pravomoćne presude, prijave socijalnim službama, može biti izvor nejednakog i pristranog postupanja, a posljedično tome i nepravičnosti u cjelini.³⁰

Pri tome se ne smije zanemariti da takvi sustavi ne mogu jamčiti apsolutnu točnost, a njihovo oslanjanje na povijesne podatke može perpetuirati prethodne pristranosti i nejednakosti u kaznenom pravosuđu. U kontekstu presumpcije

²⁶ Rossbach, N., Innocent until predicted guilty: How Premature Predictive Policing Can Lead to a Self-fulfilling Prophecy of Juvenile Delinquency, *Florida Law Review*, vol. 167, 2023, str. 169.

²⁷ Vidi više: Schlehahn, E.; Aichroth, P.; Mann, S.; Schreiner, R.; Shepherd, I.; Wong, B. L.W., Benefits and Pitfalls of Predictive Policing, u: *2015 European Intelligence and Security Informatics Conference, IEEE*, 2015, str. 146.

²⁸ Fair Trials, *op. cit.* (bilj. 19), str. 8.

²⁹ Richardson, R.; Schultz, J.; Crawford, K., Dirty Data, Bad Predictions: How Civil Rights Violations Impact Police Data, Predictive Policing Systems, and Justice, *New York University Law Review Online* 192, vol. 94, 2019, str. 21.

³⁰ Macnish, K.; Wright, D.; Jiya, T., Predictive Policing in 2025: A Scenario, u: Jahankhani, H., Akhgar, B., Cochrane, P., Dastbaz, M. (ur.) *Policing in the Era of AI and Smart Societies*, 2020, *Advanced Sciences and Technologies for Security Applications*, Springer, str. 201–240.

nedužnosti to stvara poseban rizik jer se algoritmi ne temelje na dokazima o konkretnim kaznenim djelima, već na vjerojatnostima i statistikama.³¹

Presumpcija nedužnosti postavlja zahtjev da se pojedinci imaju smatrati nedužnima dokle god im se, sukladno zakonu, ne dokaže krivnja.³² Međutim, algoritamske procjene sustava UI-ja često ne uzimaju u obzir je li optužba odbačena ili je osoba oslobođena, što dovodi do toga da se pojedinci profiliraju kao potencijalni počinitelji na temelju prošlih uhićenja, bez obzira na pravni ishod.³³ Taj pristup može rezultirati preventivnim djelovanjem protiv osoba koje nisu počinile nikakvo kazneno djelo, što može ugroziti njihova temeljna prava. Drugi je problem potencijal nepoštivanja standarda koje sustavi UI-ja, posebno u sferi kaznenog prava, moraju imati, a to su standardni transparentnosti, objašnjivosti, zaštite podataka, odgovornosti i mnogi drugi, koji se smatraju imperativom za implementaciju i uporabu sustava UI-ja.³⁴

Europski sud za ljudska prava (dalje: ESLJP) u presudama *Asan Rushiti protiv Austrije* i *S. i Marper protiv Ujedinjenog Kraljevstva* zaključio je da zadržavanje podataka nevinih osoba, poput biometrijskih uzoraka, predstavlja povredu prava na privatnost i presumpciju nevinosti. U slučaju *Asan Rushiti* Sud je presudio da izražavanje sumnje o nečijoj nevinosti nakon oslobađanja krši to pravo,³⁵ dok je u predmetu *S. i Marper* zaključeno da dugotrajna pohrana podataka može proširiti kategoriju bez opravdanja.³⁶ Dodatno, u predmetu *Blokhin protiv Rusije* Sud je naglasio da odluke u kaznenim postupcima moraju biti temeljene na pouzdanim i provjerljivim dokazima, što je ključno kod algoritamskih procjena.³⁷ U presudi *Saber i Boughassal protiv Španjolske* istaknuta je važnost individualizirane procjene specifičnih okolnosti svakog pojedinca, što automatizirani sustavi često ne uzimaju u obzir.³⁸ Također, u

³¹ Sachoulidou, A., Going beyond the “common suspects”: to be presumed innocent in the era of algorithms, big data and artificial intelligence, *Artificial Intelligence and Law*, 2023, str. 9-10.

³² Council of Europe, European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14, 4 November 1950, ETS 5, čl. 6.

³³ Blount, K., Applying the Presumption of Innocence to Policing with AI, 2021, *International Review of Penal Law*, vol. 92, br. 1, 2021, str. 39-40.

³⁴ Catanzariti, M., What Role for Ethics in the Law of AI, Catanzariti, M., What Role for Ethics in the Law of AI, u: Završnik, A.; Simončić, K. (ur.), *Artificial Intelligence, Social Harms and Human rights, Critical Criminological Perspectives*, Palgrave Macmillian, 2023, str. 145-148.

³⁵ Blount, *op. cit.* (bilj. 33), str. 38.

³⁶ European Court of Human rights *S. and Marper v. United Kingdom* (2008), Application No. 30562/04 i 30566/04, § 119.-125.

³⁷ European Court of Human rights *Blokhin v. Russia*, (2016), Application No. 47152/06, § 200.-202.

³⁸ European Court of Human rights *Saber and Boughassal v. Spain* (2020), Application No. 76550/13, § 61.-64.

predmetu *Sigurður Einarsson i drugi protiv Islanda* Sud je istaknuo da tužiteljstvo mora omogućiti obrani pristup *relevantnim* podacima koji su ključni za pravičan postupak, a ne nužno svim prikupljenim podacima, dakle naglašava važnost transparentnosti i osiguravanja algoritamskih sustava koji se koriste i kod prediktivnih sustava kako bi bili dostupni za analizu i osporavanje.³⁹ Te presude, iako ne spominju izravno algoritme, postavljaju čvrste standarde koji osiguravaju da tehnologije koje se koriste u pravosuđu ne smiju narušiti temeljna prava optuženika, uključujući i pravo na presumpciju nedužnosti i pravično suđenje.

Sud Europske unije u predmetu C-634/21 (dalje: *Schufa*) donio je zaključke indikativne za algoritme koji se koriste za profiliranje. Iako je pitanje postavljeno u vezi s automatiziranim donošenjem odluka, stajalište Suda može biti relevantno za prediktivne sustave. Sud je razmatrao primjenu čl. 22. GDPR-a na usluge automatiziranih odluka, a zaključci se mogu primijeniti na prediktivne sustave. Sud je naglasio da čak i pomoćni alati moraju biti podvrgnuti regulativama GDPR-a o automatiziranom odlučivanju, a pitanje transparentnosti i prava na uvid u proces jest ključno.⁴⁰ Transparentnost u prediktivnim sustavima ključna je jer pojedinci označeni kao rizični moraju imati pravo osporavati algoritamske pristranosti.⁴¹ Također je naglašeno pravo na ispravak netočnih podataka, što je ključno i u radu prediktivnih sustava.⁴² Algoritmi mogu donijeti pogrešne procjene, pa je pravo na ispravak važno za zaštitu pojedinaca. Glede primjene konkretnih nalaza Suda u ovom predmetu treba biti oprezan te buduća razmatranja nameću pitanje može li se takva odluka podvesti pod čl. 5. st. 8. Uredbe EU-a o umjetnoj inteligenciji, koji razmatra i područje primjene GDPR-a kroz prizmu članka 2. stavka 2. točke d).

Posljedice uporabe takvih sustava od strane tijela kaznenog progona najozbiljnije su, najkonkretnije i najintruzivnije te stoga ne iznenađuje što izazivaju najviše kritika i poziva na oprez. Ipak, treba istaknuti da ideja uporabe takvih sustava može biti legitimna jer je cilj smanjiti stopu kriminaliteta, spriječiti kazneno djelo prije nego što bude počinjeno te proaktivnim preventivnim djelovanjem zaštititi pojedine članove društva, ali i društvo kao cjelinu.⁴³

³⁹ European Court of Human rights *Sigurður Einarsson and Others v. Iceland* (2019) Application no. 39757/15, § 91.

⁴⁰ Court of Justice of the European Union, *C-634/21 Schufa* (2023), § 40.–50., ECLI:EU:C:2023:957.

⁴¹ Court of Justice of the European Union, *C-634/21 Schufa* (2023), § 56.–57., ECLI:EU:C:2023:957.

⁴² Court of Justice of the European Union, *C-634/21 Schufa* (2023), § 54.–55., ECLI:EU:C:2023:957.

⁴³ Meijer, A.; Wessels, M., Predictive Policing: Review of Benefits and Drawbacks, *International Journal of Public Administration*, vol. 42, br. 12, 2019, str. 1033–1035.

2.3. Sustavi predviđanja žrtve

Sustavi koji predviđaju potencijalne žrtve često se oslanjaju na rezultate sustava predviđanja područja počinjenja kaznenog djela, odnosno određivanja *kriminalnih žarišta*.⁴⁴ Preventivne radnje policije u ovom su slučaju usmjerene prema potencijalnoj žrtvi. Preciznije, može se izraditi detaljan plan kako pomoći potencijalnoj žrtvi da izbjegne ostvarivanje tog predviđanja. To podrazumijeva jaču uključenost socijalnih i drugih odgovarajućih službi na određenim područjima, čime bi se nastojala izbjeći potreba za reaktivnim djelovanjem tijela kaznenih progona.⁴⁵

Prednosti sustava za predviđanje žrtava mogu biti dvojake. Na prvom su mjestu zaštita prava i sloboda potencijalno ugroženih građana, što je jedna od temeljnih zadaća države. Jednako tako, istraživanje predviđanja žrtava pucnjava i masovnih pucnjava pokazalo je da trošak intervencija, koje bi mogle prepoloviti rizik od stradanja u pucnjava, za 500 ljudi koje je obuhvatilo istraživanje predstavlja procijenjenu uštedu ukupnih troškova viktimizacije u iznosu od 67 milijuna dolara. Procijenjeni trošak intervencija iznosio bi oko 134 400 dolara po osobi, što za države poput SAD-a, ali i druge, znači mnogo.⁴⁶ Stoga sustavni pristup razvoju takvih prediktivnih sustava, uz financijsku, ali i druge potpore država, može predstavljati smjer budućeg preventivnog djelovanja. Jačim razvojem UI-ja takav pristup postaje izgledniji.

Jedan od najvećih problema zajednički je gotovo svim prediktivnim sustavima jer zahtijeva uporabu kompleksnih metoda, koje uključuju analizu ljudskog ponašanja i interdisciplinarni pristup; drugi je problem što se većinski sustavi oslanjaju na ulazne podatke iz policijskih izvora, a takvi podaci mogu biti pristrani, posebno u određenim državama i područjima.⁴⁷ Smjernice za regulaciju i njezinu provedbu proizlaze iz uporabe konkretnih prediktivnih sustava, koji su u mnogim državama već dugi niz godina implementirani u rad tijela kaznenog progona. Neke od tih država i sustava, ali i s uporabom prediktivnih sustava povezne sudske odluke, bit će predmetom analize u narednim poglavljima.

⁴⁴ Halford, E., 'Two Sides of the Same Coin' – A Proposed Model for Delivering a Whole System Serial Crime Reduction Plan, *Policing: A Journal of Policy and Practice*, vol. 17, 2023, str. 4–6.

⁴⁵ Heller, S.; Jakubowski, B.; Jelveh, Z.; Kapustin, M., Machine Learning Can Predict Shooting Victimization Well Enough to Help Prevent It, *National Bureau of Economic Research Working Paper Series*, Working paper 30170, 2022 (posljednji put izmijenjen u rujnu 2022.), str. 2.

⁴⁶ *Ibid.*, str. 4–5.

⁴⁷ *Ibid.*, str. 2–3.

3. PREGLED UPORABE PREDIKTIVNIH SUSTAVA I SUDSKIH ODLUKA NA PRIMJERIMA IZABRANIH DRŽAVA

Prediktivni sustavi koje koriste tijela kaznenog progona dugo su u primjeni.⁴⁸ Države se razlikuju s obzirom na intenzitet primjene, broj sustava koji se primjenjuje, vrijeme kada su se počeli koristiti te pravnu regulaciju, pa i broj sudskih odluka glede primjene prediktivnih sustava. U gotovo svim kategorijama dominiraju azijske države, poput Kine i Singapura, ali zbog specifičnosti pravnih sistema i načelne nekompatibilnosti s europskom pravnom tradicijom i vrijednostima one neće biti predmet obrade.

Sjedinjenje Američke Države prva su država koja je koristila takve sustave u radu tijela kaznenog progona.⁴⁹ Jednako tako, koristile su veći broj različitih sustava dulji vremenski period te se stoga razvila pravna regulacija i sudska praksa. Neovisno o tom što se angloamerički i europsko-kontinentalni pravni krug znatno razlikuju, iskustvo korištenja najnaprednijih sustava i dugotrajnost uporabe opravdavaju izbor SAD-a za analizu prediktivnih sustava jer to iskustvo znatno utječe na oblikovanje europske perspektive. Iz povijesno-razvojne perspektive, uz austrijski kazneni sustav, njemački je sustav znatno utjecao na oblikovanje hrvatskog kaznenopravnog sustava.⁵⁰ Uz to, Njemačka, kao gospodarski i tehnološki jedna od najnaprednijih zemalja zapadne Europe, uspješno koristi različite sustave UI-ja u svrhe kaznenog postupka, pa tako i prediktivne sustave.⁵¹ Također, Nizozemska je jedna od država zapadne Europe koja najviše eksperimentira sa sustavima UI-ja, i to u svim područjima; od tehnologija za prepoznavanje lica, prediktivnih sustava do takozvanih živućih laboratorija.⁵²

⁴⁸ Boba Santos, R., Predictive Policing: Where's the evidence, u: Weisburd, D.; Braga, A. (ur.), *Police innovation: Contrasting perspectives*, 2019, str. 366–367.

⁴⁹ Mugari, I.; Obioha, E., Predictive Policing and Crime Control in The United States of America and Europe: Trends in a Decade of Research and the Future of Predictive Policing, *Social Sciences*, vol. 10, br. 234, str. 5.

⁵⁰ Ljubanović, V.; Novokmet, A.; Tomičić, Z., *Kazneno procesno pravo – izabrana poglavlja*, Sveučilište Josipa Jurja Strossmayera u Osijeku, Pravni fakultet Osijek, 2020, str. 209–211.

⁵¹ Montag, L.; Mcleod, R.; De Mets, L.; Gauld, M.; Rodger, F.; Peška M., *EDRi report: The rise and rise of biometric mass surveillance in the EU: A legal analysis of biometric mass surveillance practices in Germany, The Netherlands, and Poland*, 2019, str. 15–18; Mugari; Obioha, *op. cit.* (bilj. 49), str. 7; Deloitte, Bringamann, B.; Fach, P.; Beierschoder, M., Fueling the AI transformation Four key actions powering widespread value from AI, right now in Germany, Deloitte's State of AI in the Enterprise, 5th Edition report, German Cut, December 2022, str. 1-33, dostupno na: <https://www2.deloitte.com/de/de/pages/trends/ki-studie-2022.html> (24. 8. 2023.).

⁵² Vidi više: Scholl, C.; de Kraker, J.; The Practice of Urban Experimentation in Dutch City Labs, *Urban Planning*, vol. 6, 2021, str. 161.

Uporaba svih tih tehnologija odrazila se i na europsku perspektivu reguliranja UI-ja.⁵³ S obzirom na sve implikacije, realne i teorijske, za potrebe buduće regulacije u nastavku rada predmetom analize bit će primjena konkretnih prediktivnih sustava u SAD-u, Njemačkoj i Nizozemskoj te reakcije pravosuđa na probleme koji su se u praksi pojavili.

3.1. Prediktivni sustavi u SAD-u – primjer *PredPol*/*Geolitice*

Jedan od najpoznatijih prediktivnih sustava UI-ja koji je koristila policija pojedinih saveznih država u SAD-u jest *Geolitica*, prije poznat kao *PredPol*. Tvrtka *SoundThinking* pred kraj 2023. kupila je tvrtke proizvođače *Predpol* odnosno *Geolitice* i inkorporirala dijelove tih sustava u svoj sustav *ResourceRouter*.⁵⁴ *Predpol* je integriran u radu policije 2013. te predviđa žarišta kriminala i vremenske vrhunce počinjenja kaznenog djela koja su prikazana na karti; koristi model predviđanja koji se zove *sekvenca naknadnog potresa epidemijskog tipa*, što je analogno modelima koji se koriste za predviđanje seizmičke aktivnosti.⁵⁵ Uz njih se koriste i statističke tehnike, koje su izvorno razvijene za proučavanje prijenosa bolesti.⁵⁶ Patrolna karta vizualizira razine aktivnosti policajaca u različitim gradskim područjima tijekom različitih vremenskih okvira ističući potencijalne prekomjerne ili nedovoljno patrolirane zone. Analiza žarišnih točaka upućuje na mikropodručja koja su intenzivna za službenike, što olakšava strateška rješenja, dok izvješćivanje o misijama prikazuje fokusirane napore policajaca prema vrsti zločina pomažući angažman zajednice.⁵⁷

Studije upućuju na potrebu opreza u tumačenju podataka glede učinkovitosti prediktivnih sustava. Tako, primjerice, Meijer i Wessels na temelju podataka iz izvorne studije iz 2017. zaključuju da pokazuje učinkovitost od 6 % smanjenja kaznenih djela od implementacije sustava Domain Awareness Systema od strane policijske službe New Yorka, iako se ne mogu svi rezultati pripisati isključivo predmetnom sustavu, dok su istraživanja iz 2015. pokazala da su

⁵³ Fair Trials, *op. cit.* (bilj. 19); Montag *et al.*, *op. cit.* (bilj. 51), str. 55–100.

⁵⁴ Mehrotra, D.; Cameron, D., The Maker of ShotSpotter Is Buying the World's Most Infamous Predictive Policing Tech, <https://www.wired.com/story/soundthinking-geolitica-acquisition-predictive-policing/> (28. 12. 2023.); <https://www.soundthinking.com/law-enforcement/resource-deployment-resourcerouter/> (28. 12. 2023.).

⁵⁵ Hälterlein, J., Epistemologies of predictive policing: Mathematical social science, social physics and machine learning, *Big Data & Society*, vol. 8, br. 1, str. 5.

⁵⁶ Strikwerda, L., Predictive policing: The risks associated with risk assessment, *The Police Journal: Theory, Practice and Principles*, vol. 94, br. 3, 2021, str. 425.

⁵⁷ Geolitica, Data-Driven Community Policing, Transparency, dostupno na: <https://geolitica.com/public-safety/> (24. 8. 2023.).

ETAS sustavi doveli do smanjenja stope kaznenih djela za 7,4 %.⁵⁸ Ipak primjer sustava PILOT, primjenjivanog u saveznoj državi Louisiani, pokazuje da nema znatnog utjecaja takva sustava na smanjenje stope kriminaliteta.⁵⁹ U Chicagu je s pomoću analize *PredPol* utvrđena pozitivna korelacija između zločina povezanih s oružjem i ubojstava.⁶⁰ U Atlanti je *PredPol* doveo do smanjene stope kriminala u usporedbi s područjima bez njegove uporabe.⁶¹ Nasumična ispitivanja pokazala su prosječno smanjenje kriminala od 7,4 % na području policijske službe Los Angelesa i u policijskoj upravi grada Kenta, iako je neovisna procjena policije Kenta dala mješovite rezultate, potencijalno zbog ograničene upotrebe policajaca tijekom ispitivanja.⁶² Jedan od važnih sudskih predmeta iz područja umjetne inteligencije i kaznenog prava jest *United States v. Loomis*, u kojem je *Eric Loomis* osporavao uporabu algoritma COMPAS namijenjenog procjeni rizika ponovnog počinjenja kaznenog djela tijekom izricanja kazne tvrdeći da je povrijeđeno njegovo pravo na pravičan postupak. *Loomis* je tvrdio da algoritam koristi vlasničke metode koje su zatvorene za javnost i da sudovi nisu mogli provjeriti ili osporiti točnost procjene. Također, naglasio je da algoritam uzima u obzir spol kao faktor rizika, što je smatrao diskriminirajućim. U osnovi, njegova je argumentacija bila da se na temelju općih podataka nije mogla donijeti individualizirana kazna.⁶³ Vrhovni sud Wisconsina odbio je *Loomisove* tvrdnje zaključujući da COMPAS nije presudan faktor u donošenju odluke o izricanju kazne te da je algoritam pružao samo opće informacije o riziku recidivizma, dok je konačna presuda ostala u granicama sudske diskrecije. Sud je također ustvrdio da upotreba spola kao varijable nije narušila pravičnost postupka jer je ona pridonijela preciznijoj procjeni rizika.⁶⁴

Iako je Vrhovni sud Wisconsina dopustio korištenje COMPAS-a, ta presuda jasno upućuje na nužnost postavljanja strožih ograničenja u upotrebi takvih alata. Algoritamske procjene rizika ne smiju biti odlučujući faktor prilikom izricanja kazne, a suci moraju biti svjesni inherentnih ograničenja tih sustava,

⁵⁸ Meijer; Wessels, *op. cit.* (bilj. 43), str. 1034–1035. To su rezultati izvorne studije koju su proveli i objavili Mohler, G. *et al.*, Randomized Controlled Field Trials of Predictive Policing, *Journal of the American Statistical Association*, vol. 110, br. 512, str. 139.

⁵⁹ *Ibid.*

⁶⁰ Mugari; Obioha, *loc. cit.* (bilj. 49).

⁶¹ PredPol, Predictive Policing Blog, 2014, dostupno na: <https://blog.predpol.com/predpol-atlanta> (24. 8. 2023.).

⁶² National Institute of Justice, Program Profile: Predictive Policing Model in Los Angeles, California, Study 1, Daily Crime Volume, dostupno na: <https://crimesolutions.ojp.gov/rated-programs/780#eo> (24. 8. 2023.).

⁶³ *State v. Loomis*, *Wisconsin Supreme Court* 881 N.W.2d 749 (2016), § 7, 34.

⁶⁴ *State v. Loomis*, *Wisconsin Supreme Court Requires Warning Before Use of Algorithmic Risk Assessments in Sentencing*, COMMENT ON: 881 N.W.2d 749 (Wis. 2016), *Harvard Law Review*, vol. 150, br. 5, 2017, str. 1531–1532.

osobito u pogledu njihove pristranosti i nedostatka transparentnosti.⁶⁵ Kao i kod algoritama poput COMPAS-a, prediktivni sustavi često koriste povijesne podatke i metode koje nisu transparentne, što može dovesti do pristranosti. Takvi sustavi moraju biti dopunjeni ljudskom kontrolom kako bi se izbjegla automatizacija pristranih odluka te je važno osigurati da algoritmi ostanu pomoćni, a ne odlučujući alat u sudskom odlučivanju.

U predmetu *SAD protiv Curryja* Žalbeni sud četvrtog okruga donio je odluku o pretrazi *Billyja Curryja, Jr.*, kod kojeg je pronađeno vatreno oružje.⁶⁶ Policija ga je pretražila na temelju rezultata sustava UI-ja zbog dojava o pučnjava u njegovu stambenom naselju. Odluka Suda, s devet glasova za i šest glasova protiv, podržala je *Curryjev* zahtjev o nezakonitosti pretrage, odnosno dokaza pribavljenih pretragom, tvrdeći da je pretraga bila bez dostatnog stupnja sumnje i da nije obuhvaćena doktrinom hitnih okolnosti.⁶⁷ Predmetna sudska odluka, iako se odnosi na sustav *ShotSpotter*, koji nije klasični prediktivni sustav, upućuje na temeljne probleme uporabe prediktivnih sustava UI-ja.

Geografski alati za predviđanje kaznenih djela koriste historijske podatke o kaznenim djelima koje je zabilježila policija za predviđanje budućih trendova kriminala, ali kvaliteta tih podataka upitna je zbog premalog i pretjeranog prijavljivanja određenih kaznenih djela i lokacija, što odražava diskriminatorne policijske prakse i društvene nejednakosti. Posljedično, rezultirajuća predviđanja vjerojatno će biti iskrivljena i netočna, što može dovesti do pristranih intervencija tijela kaznenog progona. Ti prediktivni modeli mogu ovjekovječiti pristranosti unutar podataka stvarajući cikluse koji se sami osnažuju i u kojima pristrana predviđanja utječu na policijsku aktivnost, prijavu zločina i raspodjelu resursa, što u konačnici pogoršava postojeće nejednakosti i nepravedne policijske prakse.⁶⁸ Također, rezultati tog sustava konstituiraju određeni stupanj sumnje. To je izrazito važno pitanje jer o njemu ovisi mogućnost primjene mnogobrojnih pravnih odredbi; osnove su sumnje u našem kaznenom postupku niži stupanj

⁶⁵ Han-Wei, L.; Ching-Fu, L.; Yu-Jie, C., *Beyond State v Loomis: artificial intelligence, government, algorithmization and accountability*, *International Journal of Law and Information Technology*, vol. 27, br. 2, 2019, str. 131–140.

⁶⁶ O takozvanim *Terry stops* i doktrini hitnih okolnosti vidi više: McGehee, M., *Predictive Policing Technology: Fourth Amendment and Public Policy Concerns*, dostupno na: <https://uclawreview.org/2021/02/17/predictive-policing-technology-fourth-amendment-and-public-policy-concerns/> (12. 10. 2023.).

⁶⁷ *United States v. Curry*, 965 F.3d 313 (4th Cir. 2020), str. 1–7; Concurring opinion Judge Wynn, *United States v. Curry*, 965 F.3d 313 (4th Cir. 2020), str. 40–41; Dissenting opinion Judge Wilkinson, *United States v. Curry*, 965 F.3d 313 (4th Cir. 2020), str. 63–71; Johson, L. E., *Case Brief: United States v. Curry*, *The North Carolina Law Review*, vol. 99, 2021, str. 106–107.

⁶⁸ Big Brother Watch, *Big Brother Watch briefing on Algorithmic Decision-Making in the Criminal Justice System*, 2020, str. 4–7, dostupno na: <https://bigbrotherwatch.org.uk/wp-content/uploads/2020/02/Big-Brother-Watch-Briefing-on-Algorithmic-Decision-Making-in-the-Criminal-Justice-System-February-2020.pdf> (12. 10. 2023.).

i dostatne su za provođenje izvida, kao opći uvjet za uhićenje i druge radnje, dok je osnovana sumnja viši stupanj, koji se traži kao opći uvjet za određivanje istražnog zatvora, provođenje istrage i istraživanja i slično, a pojavljuje se kada postoji veća vjerojatnost da je osoba počinila kazneno djelo nego da nije.⁶⁹ Stoga je vrlo važan stav u prethodno navedenom predmetu da je riječ o prevelikoj diskrecijskoj ovlasti policije ako bi mogla izvršiti pretragu isključivo na temelju rezultata sustava za procjenu rizika, što su u svojoj suštini i prediktivni sustavi kao određene izvanredne okolnosti koje takvu pretragu opravdavaju.⁷⁰

Nametnuta pitanja iz ova dva predmeta potrebno je razmotriti i kroz prizmu Priloga II. Uredbe EU-a o umjetnoj inteligenciji stavak 8. točka a), kojim je dopuštena uporaba sustava UI-ja namijenjenih za korištenje od strane pravosudnih tijela ili u njihovo ime za pomoć pravosudnom tijelu u istraživanju i tumačenju činjenica i prava te u primjeni prava na konkretan skup činjenica, ili za upotrebu na sličan način u alternativnom rješavanju sporova. Potencijalni problem postoji na tragu zaključaka suda EU-a u predmetu *Schufa*, pogotovo kod individualiziranih rezultata sustava usmjerenih na predviđanje konkretnog potencijala da će osoba biti počinitelj kaznenog djela, da takvi sustavi preuzmu primat kod odlučivanja, a odluke suda ili drugih tijela postanu automatizirane. Ukoliko bi se ta granica prešla, takva uporaba sustava potpala bi pod zabranjene prakse člankom 5. točkom d) Uredbe EU-a o umjetnoj inteligenciji kod prediktivnih sustava jer je nesporno da samo profiliranje prethodi ljudskoj provjerljivoj procjeni.

Analizom uporabe prediktivnih sustava u Njemačkoj i Nizozemskoj bit će prikazani drugi problemi koji su se javili glede uporabe prediktivnih sustava, a koje je prepoznala i sudbena vlast u svojim odlukama.

3.2. Njemački primjer uporabe prediktivnih sustava – *RADAR-it*, *SKALA*, *hessenData*

Njemačka je jedan od europskih predvodnika uporabe UI-ja u svrhe kaznenog progona, a to proizlazi iz broja sustava koji se koriste te sudskih i administrativnih epiloga. Osim prediktivnih sustava *RADAR-ite*⁷¹ i *Sustava za analizu i predviđanje kriminala* (u daljnjem tekstu: *SKALA*),⁷² jako puno pozornosti

⁶⁹ Burić, Z.; Karas, Ž., Prilog raspravi o dvojabama vezanima uz novu definiciju osumnjičenika i radnju njegova ispitivanja, *Hrvatski ljetopis za kazneno pravo i praksu*, vol. 24, br. 2, 2017, str. 472–473.

⁷⁰ Concurring opinion Judge Wynn, *United States v. Curry*, 965 F.3d 313 (4th Cir. 2020), str. 40–41.

⁷¹ Fair Trials, *op. cit.* (bilj. 19), str. 18.

⁷² *Ibid.*, str. 21.

javnosti izazvali su sustavi za prepoznavanje lica, poput sustava *Videmo 360*.⁷³ Za razliku od SAD-a, njemačka razmatranja puno su više usmjerena na zaštitu privatnosti i pitanje obrade podataka.

Uz predmetne sustave važan je i onaj tvrtke *Palantir* pod nazivom *Gotham*, koji je usvojen u pokrajini Hesse kao *hessenDATA* i koji omogućuje automatiziranu analizu podataka unutar policijske mreže. Pristupa različitim bazama podataka, uključujući i *POLAS*, *ComVor* i *CRIME-ST*, te redovito sinkronizira podatke. *HessenDATA* analizira podatke dobivene iz izvora poput nadzora telekomunikacija, upita za pronalaženje podataka, forenzičkih ekstrakcija i policijskih teleksa.⁷⁴ Ta se platforma koristi u približno 14 000 slučajeva godišnje u *Hessenu* u različite svrhe, uključujući i izbjegavanje opasnosti i sprječavanje kaznenih djela.

U predmetu pred Saveznim ustavnim sudom Njemačke analiziraju se implikacije korištenja automatizirane obrade podataka, posebno u kontekstu strojno vođenih procjena pojedinaca. Takve procjene, posebno one koje se odnose na *prediktivni rad policije*, mogu dovesti do ozbiljnog miješanja u temeljna prava.⁷⁵ Razmatranim odredbama nedostaju posebna ograničenja upotrebe podataka i metoda analize, što potencijalno dopušta široku primjenu *prediktivnog policijskog rada* te dopušta generiranje strojnih procjena, uključujući i predviđanja potencijalne opasnosti povezane s pojedincima putem *prediktivnih policijskih metoda*. Te odredbe omogućuju stvaranje novih uvida koji utječu na privatnost pojedinaca, bez odgovarajućih propisa koji bi ublažili nametljivost prediktivnih policijskih praksi.⁷⁶

Prethodno navedena presuda ima važne pravne implikacije budući da proglašava korištenje *Palantirova* softvera za nadzor od strane policije u *Hessenu* i Hamburgu neustavnim. Predmetom je istaknuta zabrinutost zbog potencijala prediktivnog rada policije, što dovodi do pogrešaka i diskriminatornih praksi. Odluka suda utvrđuje stroge smjernice za inteligentni softver u policijskom radu naglašavajući da su automatizirane mjere zadiranja u prava pojedinaca

⁷³ Novokmet, A.; Tomićić, Z.; Vidaković, I., Facial recognition technology in EU criminal justice: Human rights implications and challenges, *EU and comparative law issues and challenges series, The digitalization and green transformation of the European Union*, vol. 7, str. 548–550.

⁷⁴ BVerfG, Judgment of the First Senate of 16 February 2023 – 1 BvR 1547/19, § 6.–11., ECLI:DE:BVerfG:2023:rs20230216.1bvr154719.

⁷⁵ BVerfG, Judgment of the First Senate of 16 February 2023 – 1 BvR 1547/19, § 96.–97., § 100., § 121., § 147., ECLI:DE:BVerfG:2023:rs20230216.1bvr154719.

⁷⁶ Federal Constitutional Court, Legislation in Hesse and Hamburg regarding automated data analysis for the prevention of criminal acts is unconstitutional, Press Release No. 18/2023 of 16 February 2023, dostupno na: <https://www.bundesverfassungsgericht.de/SharedDocs/Pressemitteilungen/EN/2023/bvg23-018.html> (27. 8. 2023.).

dopuštene samo radi zaštite bitnih pravnih interesa, poput života i slobode.⁷⁷ Istaknuto je da sustavi poput *hessenDATA-e* mogu biti korišteni samo uz poštivanje prava na informacijsko samoodređenje, a automatizirana obrada podataka mora biti usklađena s načelom proporcionalnosti i ograničenjima svrhe. Glede prediktivnog potencijala takve automatizirane obrade podataka sud je izrazio posebnu zabrinutost zbog mogućnosti da se takvi alati koriste za profiliranje pojedinaца na temelju statističkih obrazaca, bez konkretnih dokaza ili stvarnih prijetnji, jer može povezivati različite vrste podataka, čime stvaraju profesionalne profile, profile kretanja i ponašanja, koji mogu rezultirati time da pojedinci budu nepravедno označeni od strane policije. Takvi profili nisu nužno vezani uz procjenu vjerojatnosti činenja kaznenog djela. Predmetne metode mogu povećati rizik od diskriminacije, jer se sumnje često temelje na korelacijama, a ne na stvarnim činjenicama ili ponašanjima.⁷⁸ Sud je stoga postavio stroge zahtjeve za sudski nadzor i jasne kriterije za upotrebu podataka naglašavajući da se uporaba prediktivnih sustava mora temeljiti na jasnim pravnim osnovama i specifičnoj prijetnji kako bi bila ustavno opravdana.⁷⁹ Potonji zahtjev suda u skladu je s prihvaćenim rješenjem Uredbe EU-a o umjetnoj inteligenciji jer ostavlja prostor isključivo za uporabu prediktivnih sustava kao pomoćnih alata u slučaju prije već formirane ljudske procjene postojanja specifične prijetnje, koja se temelji na objektivnim i provjerljivim činjenicama, izravno povezanim s kriminalnom aktivnošću.

Također, prilagodba zakona u ovom slučaju imala je za cilj proširiti ovlasti za korištenje alata za prediktivne sustave. To je razvidno kroz izmjene hamburškog zakona koji je pokušao ograničiti opseg primjene promjenom terminologije iz *analiza podataka* u *interpretacija podataka*. Međutim, ta promjena terminologije nije učinkovito smanjila mogućnosti zlorabe podataka niti je osigurala dovoljno usku pravnu osnovu za obradu podataka.⁸⁰ Ubrzani razvoj zakona, često uz izostanak postupaka nabave, može se tumačiti kao politička odluka da se osigura brza implementacija tehnologije, bez nužnog demokratskog procesa i rasprave.⁸¹ Takva dinamika upućuje na problematičan trend u kojem se zakonski okviri prilagođavaju tehnološkim rješenjima bez odgovarajućeg razmatranja dugoročnih implikacija za građanska prava i privatnost.

⁷⁷ Maker, M., *Wired*, Germany Raises Red Flags About Palantir's Big Data Dragnet, A court has issued strict limits on how police can pull innocent bystanders into big data investigations, 2023, dostupno na: <https://www.wired.com/story/palantir-germany-gotham-dragnet/> (27. 8. 2023.).

⁷⁸ BVerfG, Judgment of the First Senate of 16 February 2023 – 1 BvR 1547/19, § 67.–71. ECLI:DE:BVerfG:2023:rs20230216.1bvr154719.

⁷⁹ BVerfG, Judgment of the First Senate of 16 February 2023 – 1 BvR 1547/19, § 67.–71., § 109.–110. ECLI:DE:BVerfG:2023:rs20230216.1bvr154719.

⁸⁰ BVerfG, Judgment of the First Senate of 16 February 2023 – 1 BvR 1547/19, § 147.–151.

⁸¹ Ulbricht, L.; Egbert, S., In Palantir we trust? Regulation of data analysis platforms in public security. *Big Data & Society*, vol. 11, nbr. 3, str. 1, 9–11.

3.3. Nizozemska perspektiva uporabe prediktivnih sustava – primjer CASA, SyRI-ja

Nizozemska je jedna od vodećih zapadnoeuropskih država glede eksperimentiranja sa sustavima UI-ja u sferi kaznenog prava, koja se izdvojila sustavima usmjerenima na individualne predikcije, poput *ProKid*, *Top400*, *Top600*. *ProKid* je *aktuarski* alat za procjenu rizika kojim se koristi policija radi procjene rizika djece i adolescenata koji su uključeni u *buduće nasilje i oštećenje odnosno uništenje imovine*, što se pokazalo posebno spornim s obzirom na ranjivost skupine koja je objekt obrade takvih sustava.⁸²

Riječ je o jednom od europskih pionira u nacionalnom prediktivnom policijskom radu uvođenjem *Sustava za predviđanje zločina* (dalje: CAS). CAS koristi prostorno-vremensku analizu za prepoznavanje žarišta kaznenih djela, predviđanje rizika od viktimizacije i raspodjelu policijskih resursa, primarno usredotočujući se na kaznena djela kao što su provale, pljačke i krađe.⁸³ *System Risk Identification* (dalje: SyRI) alat je UI-ja koji se koristi za predviđanje prijevара, što ga razlikuje od sustava predviđanja u drugim zemljama, koji se često fokusiraju na kaznena djela povezana s nasiljem.⁸⁴ Sustav SyRI u Nizozemskoj je implementiran tijekom posljednja dva desetljeća za borbu protiv prijevара u socijalnoj skrbi olakšavanjem razmjene podataka i suradnje među administrativnim tijelima. Nakon zakonskih promjena 2013. godine više administrativnih tijela dobilo je dopuštenje za korištenje SyRI-ja.⁸⁵

Općinski sud u Haagu presudio je da korištenje sustava SyRI od strane nizozemske vlade za otkrivanje prijevара, uključujući i socijalne naknade i porezne prijevара, krši pravo na poštivanje privatnog i obiteljskog života zaštićeno člankom 8. Konvencije.⁸⁶ Sud je utvrdio da trenutačno zakonodavstvo koje regulira SyRI ne uspijeva uspostaviti pravednu ravnotežu između interesa zajednice i prava pojedinaca na privatnost, posebno u svjetlu nedostatka transparentnosti i provjerljivosti u radu sustava.⁸⁷ Zaključak je da SyRI predstavlja

⁸² Fair Trials, *op. cit.* (bilj. 19), str. 8–14.

⁸³ Gstrein, O. J.; Bunnik, A.; Zwitter, A., Ethical, Legal and Social Challenges of Predictive Policing *Católica Law Review, Direito Penal*, 2019, vol. 3, br. 3, str. 84; Hardyns, W.; Rummen, A. Predictive Policing as a New Tool for Law Enforcement? Recent Developments and Challenges, *European Journal on Criminal Policy and Research*, vol. 24, 2018, str. 207–209.

⁸⁴ Mugari, Obioha, *op. cit.* (bilj. 49), str. 7.

⁸⁵ Vidi više: van Bekkum, M.; Borgesius, F. Z., Digital welfare fraud detection and the Dutch SyRI judgment, *European Journal of Social Security*, vol. 23, br. 4, str. 323–328.

⁸⁶ Rachovitsa, A.; Johann, N., The Human Rights Implications of the Use of AI in the Digital Welfare State: Lessons Learned from the Dutch SyRI Case, *Human Rights Law Review*, vol. 22, br. 2, 2022, str. 1–4.

⁸⁷ Rechtbank Den Haag, C-09-550982-HA ZA 18-388, 20. veljače 2020., § 6.95–6.112, ECLI:NL:RBDHA:2020:1878.

prekomjerno miješanje u privatnost građana jer nije dovoljno transparentan u vezi s metodologijom i algoritmima koje koristi, kao i zbog netransparentnosti u načinu povezivanja i obrade podataka.⁸⁸ Iako se sustav *SyRI* koristio za legitimnu svrhu borbe protiv prijevara, sud je ocijenio da zakonodavni okvir nije pružao dovoljno jasne i precizne smjernice o tome kako bi se trebala odvijati obrada podataka.⁸⁹ To je dovelo do nepoštivanja prava na zaštitu podataka građana. Postojala je zabrinutost da bi sustav mogao dovesti do profiliranja i diskriminacije određenih socijalnih grupa jer je ciljano koristio podatke iz određenih naselja s nižim socioekonomskim statusom.⁹⁰ Ipak, treba naglasiti da je, kao i u prethodnim slučajevima, utvrđena neusklađenost uporabe takva sustava s postojećim pravnim okvirom, ali nije apsolutno isključena njegova primjena u slučaju usklađivanja; to se posebno odnosi na transparentnost i provjerljivost u radu sustava kao generalne probleme i zahtjeve sustava UI-ja.⁹¹ U ovom slučaju nizozemska vlada donijela je odluku o povlačenju tog sustava, ali jedan je od glavnih razloga i njegova relativna neučinkovitost.⁹²

Razmatranjem primjene konkretnih sustava i argumentacije sudbene vlasti prilikom odlučivanja o pojedinim aspektima njihove primjene mogu se prepoznati kritične točke regulacije koje su sudovi istaknuli kao nekompatibilne s postojećim standardima zaštite ljudskih prava pozitivnopravnog okvira uporabe takvih sustava.

4. EUROPSKA PERSPEKTIVA PRAVNOG UREĐENJA UPORABE PREDIKTIVNIH SUSTAVA UMJETNE INTELIGENCIJE U KAZNENOM POSTUPKU – KRITIČNE TOČKE REGULACIJE

Trenutačno jedna od najvažnijih pravnih regulacija UI-ja jest ona EU-a. Proces je započeo objavljivanjem Bijele knjige Europskog parlamenta o umjetnoj inteligenciji, koja je postavila osnovu za buduće propise.⁹³ Amandmani na Uredbu EU-a o umjetnoj inteligenciji znatno su utjecali i na regulaciju prediktivnih sustava. U izvornoj verziji prijedloga Uredbe EU-a o umjetnoj intelligen-

⁸⁸ Rechtbank Den Haag, C-09-550982-HA ZA 18-388, 20. veljače 2020., § 6.95–6.100 ECLI:NL:RBDHA:2020:1878.

⁸⁹ Appelman, N.; Ò Fathaigh, R.; van Hoboken, J., Social Welfare, Risk Profiling and Fundamental Rights: The Case of SyRI in the Netherlands, *JIPITEC* Vol. 257, 2019. para 30.–31.

⁹⁰ Rechtbank Den Haag, C-09-550982-HA ZA 18-388, 20. veljače 2020., § 6.108–6.112 ECLI:NL:RBDHA:2020:1878.

⁹¹ Rachovitsa; Johann, *op. cit.* (bilj. 86), str. 12–15; van Bekkum; Borgesisu, *op. cit.* (bilj. 85), str. 337–338.

⁹² *Ibid.*, van Bekkum; Borgesisu, str. 337–338.

⁹³ Europska komisija, Bijela knjiga o umjetnoj inteligenciji COM (2020) 65 final.

ciji prediktivni sustavi bili su predviđeni kao visokorizični sustavi, što znači da je dopuštena njihova uporaba, ali morali su zadovoljiti određene uvjete predviđene Uredbom EU-a o umjetnoj inteligenciji s obzirom na njihovu namjenu i sustav upravljanja rizicima.⁹⁴ Navedeni zahtjevi visokorizičnih sustava UI-ja koji su najsporniji u odnosu na prediktivne sustave koji su u primjeni i u odnosu na ono na što je postojeća sudska praksa već upozorila jesu: (i) zahtjevi kvalitete podataka, (ii) transparentnost sustava i (iii) pouzdanost sustava. Prihvaćanjem kompromisa između izvornog regulatornog prijedloga i dijametralno suprotnih amandmana putem gramatičkog tumačenja usvojene odredbe članka 5. stavka 1. može se zaključiti da se ona jasno odnosi na prediktivne sustave za predviđanje počinitelja, dok sustavi za predviđanje žrtve, kao i sustavi za prediktivno mapiranje, nisu u fokusu ove odredbe.⁹⁵

Ipak, takvo rješenje omogućuje korištenje prediktivnih sustava usmjerenih na individualnu procjenu potencijalnih počinitelja kaznenih djela. Kako će ti sustavi koristiti podatke dostupne policiji, jasno je da će se raditi o provjerljivim činjenicama povezanim s kriminalnom aktivnošću, jer policija unosi podatke koje koristi u svojem operativnom radu. Objektivnost takvih činjenica uvijek može biti upitna neovisno o tome tko ih obrađuje. Temeljna ideja koja je razvidna iz teksta predmetne odredbe jest da bi primarno trebala ići procjena policije glede kreiranja individualnih profila potencijalnih počinitelja, i to utemeljenih na objektivnim i provjerljivim činjenicama vezanim uz kriminalnu aktivnost, pa onda provjera putem primjene sustava UI-ja, a ne obratno, da prediktivni sustavi sami kreiraju profile, a policija ih provjerava i potvrđuje na temelju dostupnih podataka. Takav pristup anulira prednosti prediktivnih sustava, poput kompleksnijeg povezivanja podataka te njihove brže i konkretnije obrade. Za prihvatljivost takva rješenja važno je obratiti pozornost na ključne točke regulacije, kao što su kvaliteta podataka, transparentnost i točnost sustava, predviđene Uredbom EU-a o umjetnoj inteligenciji.

⁹⁴ Uredba EU-a o umjetnoj inteligenciji, čl. 9.–14.

⁹⁵ European Parliament, Amendments adopted on 14 June 2023 on the proposal for a regulation of the European Parliament and of the Council on laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts, 2023, (COM(2021)206 – C9-0146/2021 – 2021/0106(COD))(1) (u daljnjem tekstu: Amandmani na Akt o umjetnoj inteligenciji), Amandman 224. O zakonodavnoj proceduri i procesu trijaloga vidi više Foster, N., *Foster on EU Law, Fourth Edition*, Oxford University Press, 2013, str. 121–123; Bertuzzi, L., AI Act: MEPs mull narrow facial recognition technology uses in exchange for other bans, dostupno na: <https://www.euractiv.com/section/artificial-intelligence/news/ai-act-meps-mull-narrow-facial-recognition-technology-uses-in-exchange-for-other-bans/> (8. 11. 2023.).

4.1. Kvaliteta podataka

Visokorizični sustavi UI-ja, koji koriste tehnike s učenjem modelâ pomoću podataka, razvijaju se na temelju skupova podataka za učenje, validaciju i testiranje koji ispunjavaju kriterije kvalitete; skupovi podataka za učenje, validaciju i testiranje relevantni su, reprezentativni, bez pogrešaka i potpuni. Glede predmetnih skupova podataka u obzir se uzimaju, u mjeri u kojoj to iziskuje namjena, karakteristike ili elementi specifični za zemljopisno, bihevioralno ili radno okruženje u kojem je predviđena uporaba visokorizičnog sustava UI-ja.⁹⁶

Prethodno navedeni podaci prvi su i nužni korak koji mora biti reguliran kod prediktivnih sustava UI-ja. Ipak, ključno je da sustavi moraju biti naučeni prepoznati različite vrijednosti ulaznih podataka te ih vrednovati na drugačiji način. Ne može isti utjecaj na konačnu predikciju počinjenja kaznenog djela imati podatak o uhićenju osobe, rješenje o provođenju istrage i pravomoćna osuđujuća presuda. Trenutačno predložena regulacija prediktivnih sustava ima propust, a to je da se zahtjevi kvalitete podataka reguliraju samo u fazi razvoja, odnosno treniranja, testiranja i validacije sustava. Problemi uporabe takvih sustava proizlaze i iz podataka s kojima radi subjekt koji uvodi sustav. To se pokazalo u prethodno obrađenim primjerima, ali i mnogim drugima, gdje je kvaliteta podataka i pristranost upitna sa stajališta ulaznih podataka nakon što se sustavi puste u rad.

Dakle, da bi se kao visokorizični sustavi mogli upotrijebiti prediktivni sustavi, nužno je regulirati i kvalitetu ulaznih podataka prilikom uporabe. Dostatno ih je regulirati na identičan način kao za podatke za učenje, validaciju i testiranje, jer se tako omogućuje cjelovit i kvalitetan rezultat. To podrazumijeva potrebu odgovarajuće prakse upravljanja podacima; takvi podaci moraju biti dovoljno relevantni, reprezentativni i bez pogrešaka te bi trebali biti potpuni s obzirom na namjenu sustava. Trebali bi imati i odgovarajuća statistička obilježja, među ostalim u odnosu na osobe ili skupine osoba za koje se visokorizični sustav UI-ja namjerava rabiti.⁹⁷ Jedan od problema kvalitete takvih podataka jest i činjenica da se kao ulazni podaci koriste i podaci o uhićenju, kontaktu s policijom, ali i drugi podaci koji nisu nužno kriminalne naravi.⁹⁸ Činjenica da je netko uhićen ne znači da je kriv jer se primjenjuje presumpcija nedužnosti, istovremeno ne znači da će kazneni postupak uopće biti pokrenut. Stoga je nužno da se sustav trenira kako bi mogao pravilno vrednovati takve podatke, a istodobno da se odredi filter gdje se takvi podaci neće unositi ili će imati manju vrijednost prilikom predviđanja budućeg činjenja kaznenog djela.⁹⁹

⁹⁶ Uredba EU-a o umjetnoj inteligenciji, čl. 9.–14.

⁹⁷ Cf. Preambula, točka 44., Uredba EU-a o umjetnoj inteligenciji.

⁹⁸ Wilson, D., *op. cit.* (bilj. 17), str. 121–123.

⁹⁹ Vidi više Dastres; R., Soori, S., Artificial Neural Network Systems, *International Journal of Imaging and Robotics (IJIR)*, vol. 21, br. 2, 2021, str. 13–16.

Nameće se nužno rješenje na dvije razine. Prva se odnosi na normativnu izmjenu, odnosno izmjenu pravne regulacije, kojom se neće samo osiguravati kvaliteta i relevantnost podataka za trening već i ulaznih podataka od strane subjekata koji unose sustav, a to su tijela kaznenog progona. Iako Direktiva LED pruža relativno dobar pravni okvir obrade takvih podataka, bilo bi svrhovito primijeniti standarde čl. 10. Uredbe EU-a o umjetnoj inteligenciji koji se odnose na podatke za trening, testiranje i validaciju te na kvalitetu ulaznih podataka.¹⁰⁰ Druga razina problema jest različito vrednovanja ulaznih podataka koje tijela kaznenog progona unose u sustav radi konačnog rezultata, odnosno predikcije.

4.2. Transparentnost

Problem transparentnosti ima više potencijalnih različitih implikacija za kazneni postupak. Transparentnost podrazumijeva da način funkcioniranja sustava, kriteriji za donošenje odluke i sve upute za korisnike sustava moraju biti jasni, precizni i previđeni. Druga su strana ovog problema rezultati i njihova uporaba u odnosu na objekt obrade. Naime, pretjerana zatvorenost i tajnovitost postupanja tijela kaznenog progona otvara prostor proizvoljnom i zlonamjernom postupanju. S druge strane, pretjerana otvorenost i otkrivanje svih informacija u najranijim fazama kaznenog postupka dovodi u pitanje mogućnost i sposobnost države za uspješnu borbu protiv različitih oblika kaznenih djela.¹⁰¹

Transparentnost je važna za ostvarivanje prava na pravično suđenje kao stožernog načela kaznenog postupka. Teško je govoriti o ostvarivanju prava na jednakost oružja i načela kontradiktornosti ako se poduzimaju određene radnje na temelju rezultata sustava čiji način funkcioniranja nije jasan, objašnjen, a k tome samo jedna strana ima prednost pri preispitivanju rezultata i utilitariziranju takvih sustava. Dakle, nužan je trening i edukacija korisnika sustava.¹⁰² Time bi se morali obuhvatiti načini funkcioniranja sustava, selekcija podataka koju će unositi krajnji korisnik, ali i kontekstualizirani pristup usklađen s pravilima struke za pravilno tumačenje, preispitivanje, a onda, sukladno tome, i poduzimanje pojedinih radnji.¹⁰³ Time se može uspješno riješiti problem objaš-

¹⁰⁰ Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, čl. 4., čl. 10.; Uredba EU-a o umjetnoj inteligenciji, čl. 10.

¹⁰¹ Novokmet; Tomičić; Vidaković, *op. cit.* (bilj. 73), str. 537.

¹⁰² Carleton, B.; Cunningham, B.; Thorkildsen, Z., *The Use of Predictive Analytics in Policing*, Arlington, VA: CAN, 2020, str. 16–17.

¹⁰³ Gültekin-Várkonyi, G., *Predictive Policing and Bias in a Nutshell: Technical and Practical Aspects of Personal Data Processing for Law Enforcement Purposes*, u: Karsai, K.; Söztür,

njivosti jer će svaka odluka na temelju rezultata prediktivnih sustava UI-ja moći biti obrazložena i jasna te, sukladno tome, i preispitana. Drugi problem transparentnosti specifičan je za prediktivne sustave jer, kada je riječ ponajprije o *individualnom profiliranju*, ali i *geografskom predviđanju*, osoba koja je objekt obrade o tome nije obaviještena. Dakle, nema obavijesti, osoba ne dobije pouku o pravima, a istovremeno rezultati obrade takvih sustava mogu utjecati na svakodnevni život građana i osoba koje su predmet obrade. Sukladno navedenom, ne postoji mogućnost osporavanja rezultata obrade ni ostvarivanja drugih prava sve do formalnog pokretanja kaznenog postupka ili poduzimanja pojedinih radnji. Sukladno postojećim razumijevanjima pojma osumnjičenika osoba koja je predmetom obrade ne može imati takav status, ali potencijalno rješenje jest u dodjeljivanju prava koja pripadaju osumnjičeniku ili čak statusa osumnjičenika, barem u slučajevima *individualnog profiliranja*.

4.3. Točnost sustava

S obzirom na narav prediktivnih sustava može se ipak očekivati da je njihova primjena imanentnija prethodnom postupku, izvidima ili primjeni izvan formalno započetog kaznenog postupka. Posljedica pitanja točnosti jest da se takvi sustavi ne bi trebali primjenjivati u stadijima kaznenog postupka gdje je princip *in dubio pro reo* primjenjiv, dakle u raspravi i donošenju presude.¹⁰⁴ Istraživanja pokazuju da sustavi za procjenu rizika nadmašuju sudsku procjenu u točnosti predviđanja; neki su od razloga smanjenje takozvane buke, koja se javlja zbog različitog razmatranja i vrednovanja pojedinih elemenata od strane sudaca i drugih tijela kaznenog progona.¹⁰⁵ Ipak, pouzdanost sustava čiji je krajnji rezultat određeni postotak vjerojatnosti uvijek je upitna. Ponajprije, preveliko oslanjanje tijela kaznenog progona na rezultate takvih sustava potencijalni je rizik za položaj okrivljenika u kaznenom postupku.¹⁰⁶ Teško je opravdati nepostupanje u skladu s izraženom vjerojatnošću policiji i državnom odvjetništvu jer je riječ o sustavima koji koriste iste podatke kao policija i

A.; Wörner, L. (ur.), *Digital Criminal Justice: A Studybook Selected Topics for Learners and Researchers*, Istanbul, 2022, str. 15–16; Ferguson, A. G., *Policing Predictive Policing*, *op. cit.* (bilj. 1), str. 1152–1153, 1156–1157, 1168, 1175–1176, 1188.

¹⁰⁴ Cf. Isti zaključak glede primjene tehnologija za prepoznavanje lica u dokazne svrhe iznesen je jer je riječ o primjeni postotaka kada se traži dokazni standard krivnje na razini izvan svake razumne sumnje. Novokmet; Tomićić; Vidaković *op. cit.* (bilj. 73), str. 550–556.

¹⁰⁵ Goel, S.; Shroff, R.; Skeem, J.; Slobogin, C., The accuracy, equity, and jurisprudence of criminal risk assessment, u: Vogl, R. (ur.), *Research Handbook on Big Data Law*, Elgar, 2021, str. 13.

¹⁰⁶ Cohen, G.; Graver, H. S., Cops, Docs, and Code: A Dialogue Between Big Data in Health Care and Predictive Policing, *UC Davis Law Review*, vol. 51, br. 437, 2017, str. 454–458.

državno odvjetništvo, a vjerojatno i veće baze podataka, te ih obrađuju brže i kompletnije. To je problematično jer je riječ o prethodnom postupku, odnosno istrazi i istraživanju, u kojem su okrivljenikova prava i slobode najmanje zaštićeni.¹⁰⁷ To se posebno odnosi na sustave koji su preuzeli modele državno-odvjetničke istrage, poput Republike Hrvatske.¹⁰⁸ Točnost sustava ovisit će o različitim parametrima, od podataka za trening do ulaznih podataka, a činjenica da postoje različiti dobavljači sustava i različiti sustavi na području jedne države ili drugih država EU-a može dovesti do različitih praksi postupanja, ali i sudskih epiloga, čime se dodatno doprinosi pravnoj nesigurnosti.¹⁰⁹

Drugo je pitanje prihvatljivosti posljedica rezultata predviđanja za okrivljenika. Naime, rezultati predviđanja neće biti stopostotni te je okrivljeniku lakše prihvatiti da se određena radnja zadiranja u njegova prava i slobode temelji na ljudskom razmišljanju, logici, iskustvu i stručnosti.¹¹⁰ Prediktivni sustavi nisu toliko moćni da mogu dati apsolutno točan rezultat niti će to ikada biti jer nije riječ o takozvanim *kristalnim kuglama*.¹¹¹ Margina pogreške koju takav sustav može imati izazvat će veću sumnju, a samim time i nevoljkost prihvatljivosti rezultata i njegovih posljedica.¹¹² Jednako tako, sukladno čl. 4. Uredbe EU-a o umjetnoj inteligenciji, dobavljači i subjekti koji uvode sustave UI-ja poduzimaju mjere kako bi na najbolji mogući način osigurali dostatnu razinu pismenosti u području umjetne inteligencije za svoje osoblje i druge osobe uključene u rad i korištenje sustava UI-ja u njihovo ime uzimajući u obzir njihovo tehničko znanje, iskustvo, obrazovanje i osposobljavanje te kontekst u kojem će se sustavi UI-ja koristiti, kao i osobe ili skupine osoba na kojima se sustavi UI-ja trebaju upotrijebiti.

Točnost će u najvećoj mjeri ovisi o prethodna dva elementa, a to su kvaliteta podataka, kako onih za trening tako i ulaznih, te trening odnosno edukacija samih krajnjih korisnika, koji će tumačiti dobivene rezultate i sukladno njima postupati.¹¹³ Međuovisnost tih elemenata za prihvatljivost prediktivnih sustava

¹⁰⁷ Ferguson, A. G., The Legal Risks of Big Data Policing, 33 *ABA Criminal Justice Magazine*, vol. 33, 2018, dostupno na: https://digitalcommons.wcl.american.edu/facsch_lawrev/1390, (18. 9. 2023.),

¹⁰⁸ Ljubanović; Novokmet; Tomičić, *op. cit.* (bilj. 50), str. 209.

¹⁰⁹ Simončić, K.; Jerele, T., Democratizing the Governance of AI: From Big Tech Monopolies to Cooperatives, u: Završnik, A.; Simončić, K. (ur.) *Artificial Intelligence, Social Harms and Human rights, Critical Criminological Perspectives*, Palgrave Macmillian, 2023, str. 241–251.

¹¹⁰ Macnish; Wright; Jiya, *op. cit.* (bilj. 30), str. 210–211.

¹¹¹ Berk, R. A., Artificial Intelligence, Predictive Policing, and Risk Assessment for Law Enforcement, *Annual Review of Criminology*, vol. 4, 2021, str. 223–224.

¹¹² Joh, E. E., The Consequences of Automating and Deskillling the Police, *UCLA Law Review*, vol. 67, br. 134, 2019, str. 159–164.

¹¹³ Hardyns; Rummens, *op. cit.* (bilj. 83), str. 205–206.

UI-ja kao visokorizičnih je razvidna. Dakle, ako osnovni skupovi podataka za trening, test i validaciju nemaju odgovarajuće propisane kvalitete, neovisno o tome koliko kvalitetni budu ulazni podaci krajnjih korisnika sustava, rezultati neće biti odgovarajući, a trening i educiranost korisnika sustava neće moći ispraviti loše rezultate sustava. Ako pak ti isti skupovi udovolje svim tim kriterijima Uredbe, ali podaci za trening nemaju te kvalitete, onda će rezultati i dalje biti neodgovarajući jer ćemo imati, primjerice, pristranost kroz povećanu reprezentativnost određene etničke skupine, onda ni trening i educiranost neće moći utjecati na takve rezultate. Jednako tako, ako bi svi skupovi podataka bili odgovarajući, bez uputa te adekvatnog educiranja i kontekstualnog tumačenja, konačne odluke koje donosi čovjek na temelju takvih rezultata bile bi automatizirane, nekritične i potencijalno vrlo često pogrešne i pristrane.¹¹⁴

5. ZAKLJUČNA RAZMATRANJA

Za prediktivne sustave ispunjenje uvjeta visokorizičnih sustava ne ovisi isključivo o napretku tehnologije ili svojevrsnoj neizvjesnosti nego i o određenim normativnim prilagodbama. Kad se razmatra pitanje kvalitete podataka kao jedno od najspornijih, nužno je regulirati ulazne podatke prilikom unosa od strane krajnjih korisnika, odnosno policije. Tehnički prijedlog može se riješiti već postojećim rješenjima različitog vrednovanja i filtracije ulaznih podataka, koja mora biti normativno uređena, a koja za sada nije predviđena Uredbom. Prevelika diskrecija kod unosa podataka može biti manipulirajuća za krajnji rezultat, a to se pokazalo problematičnim kako za prediktivne sustave tako i za mnogobrojne druge sustave UI-ja.¹¹⁵

Pitanje transparentnosti zahtijeva dvostruki pristup. Prvi se svodi na razumijevanje funkcioniranja sustava od strane onih koji ga koriste kako bi pravilno mogli tumačiti rezultate. To podrazumijeva uporabu logike, iskustva i kontekstualizaciju, a ne suhoparno praćenje rezultata kako se odluke ne bi smatrale automatiziranima. Stoga će, osim uputa, biti nužan kvalitetan trening osoba koje takve sustave koriste kako bi mogle objasniti i opravdati poduzi-

¹¹⁴ To može uključivati razumijevanje pravilne primjene tehničkih elemenata tijekom faze razvoja sustava UI-ja, mjera koje treba primijeniti tijekom njegova korištenja, prikladnih načina tumačenja izlaznih vrijednosti sustava UI-ja i, u slučaju osoba na koje utječe umjetna inteligencija, znanje potrebno za razumijevanje načina na koji će odluke donesene uz pomoć umjetne inteligencije utjecati na njih. Vidi više točke 20., 91., 165. recitala Uredbe EU-a o umjetnoj inteligenciji.

¹¹⁵ Diskrecijska ovlast policije kod korištenja sustava za biometrijsko prepoznavanje bila je problematična i u slučaju konkretne i opširne regulacije, vidi više *R (on the application of Edward Bridges) v. The Chief Constable of South Wales Police*, [2020] EWCA Civ 1058, § 55., § 65., § 91., § 94., § 121., § 124., § 130., § 152.; jednako tako vidi *supra*, str. 12.

manje određenih mjera na temelju rezultata prediktivnih sustava. Trening će morati biti osmišljen od strane proizvođača sustava glede tehnološkog aspekta uporabe, ali istovremeno i od strane pravnika i kriminalista.¹¹⁶ Zahtjevi transparentnosti propisani u članku 13. stavku 1. i 2. Uredbe EU-a o umjetnoj inteligenciji propisuju obvezu da takvi sustavi moraju biti razvijeni i dizajnirani tako da njihov rad bude transparentan kako bi subjekti koji uvode sustav mogli tumačiti izlazne podatke sustava i primjereno ih upotrebljavati, a upute moraju biti u odgovarajućem digitalnom ili drugom formatu, sa sažetim, potpunim, točnim i jasnim informacijama koje su subjektima koji uvode sustav relevantne, pristupačne i razumljive. Upravo taj oblik zahtjeva transparentnosti može biti primijenjen i na objekte obrade sustava u obliku svojevrzne pouke o pravima, odnosno kreiranim uputama o načinu funkcioniranja sustava, koje na jednak način objašnjavanju funkcioniranje sustava i generirane izlazne rezultate osobama na koje takva odluka utječe bez nužnosti pristupa izvornom kodu. Prije svega, dostavljanje jasnih i detaljnih uputa omogućilo bi subjektima obrade da shvate temeljna načela rada prediktivnih sustava. To bi uključivalo razumijevanje postupaka obrade podataka, kriterija koji su korišteni za donošenje određenih zaključaka te toga u kojoj su mjeri odluke sustava podložne varijacijama ili odstupanjima.¹¹⁷ Na taj bi način transparentne upute postale alat za razumijevanje složenih tehnoloških procesa, čime bi se omogućilo osporavanje rezultata bez nužne potrebe za uvidom u izvorni kod. Nadalje, vještaci bi na temelju dostavljenih uputa mogli provesti neovisnu procjenu rada prediktivnog sustava. Oni bi bili u mogućnosti analizirati i provjeriti točnost odluka donesenih od strane sustava umjetne inteligencije te identificirati moguće nepravilnosti, pristranosti ili tehničke greške. Jednako tako, ako bi se pak pojavila potreba za tehničkim detaljima i pristupom kodu, prije dobiveni podaci mogli bi usmjeriti obranu i vještake u najproblematičnije dijelove sustava. Konačno, transparentne upute omogućile bi da subjekti obrade u praksi ospore valjanost odluka prediktivnih sustava na temelju poznatih kriterija i metoda rada sustava. Ako su jasno definirane granice sustava, njegov način donošenja odluka i rizici od pogrešaka, obrana bi mogla pravno te uz pomoć stručnjaka upozoriti na nepravilnosti, čime bi se izbjegla potreba za pristupom izvornom kodu. Čak i da se dobije pristup kodu, pitanje je broja vještaka koji to mogu tumačiti, vremena potrebnog za tumačenje i pripremu obrane te u konačnici nerazmjernog troška i stvarnog tereta pronalaska vještaka. Stoga prethodno rješenje ovog aspekta transparentnosti može ublažiti teret obrane jer će se lakše detektirati problematično područje te će se moći usmjeriti vještačenje na određene segmente funkcioniranja sustava i olakšati ostvarivanje prava

¹¹⁶ Carleton; Cunningham; Thorkildsen, *op. cit.* (bilj. 102).

¹¹⁷ Uzevši u obzir sadržaj takvih uputa propisan člankom 13. stavkom 3. Uredbe o umjetnoj inteligenciji, dostatan je za učinkovito osporavanje odluka sustava.

obrane, uz jednostavnije razumijevanje rada sustava na istoj ili približno istoj razini na kojoj ga razumiju i korisnici sustava.

Drugi je problem nepostojanje svijesti osobe da je predmetom obrade takvih sustava. Možebitno je rješenje u redefiniranju pojma osumnjičenika, uz razmatranje toga da se status osumnjičenika dodijeli i osobi koja je predmetom takve obrade kako bi mogla biti pravovremeno upoznata s tom činjenicom, dobiti pouku o pravima te osporiti rezultate sustava.¹¹⁸ Potencijal takva rješenja može doći kroz autonomno tumačenje pojma osumnjičenika u odlukama ESLJP-a ili normativnim reguliranjem kroz direktive. Takvim pristupom ostvario bi se cilj prediktivnih sustava, a to je prevencija, dok bi se položaj osoba koje su predmetom obrade značajno poboljšao, što bi bilo u skladu s načelom pravičnog postupka. Istovremeno, ostvarivanjem prevencije ne bi se narušila učinkovitost kaznenog postupka jer bi se spriječilo počinjenje kaznenog djela te ostvarila specijalna prevencija, odnosno do kaznenog postupka ne bi ni došlo. Potencijal rješenja proizlazi iz prava zajamčenih ponajprije čl. 3., ali i drugih odredaba Direktive o 2013/48/EU o pravu na branitelja i osobama koje su predmet obrade prediktivnih sustava ako s obzirom na rezultate obrade tijela kaznenog progona odluče poduzeti pojedine radnje.¹¹⁹ Ograničavanjem predmetnih prava odnosno jamstava u odnosu na osobe na koje se djelovalo na temelju rezultata obrade prediktivnih sustava, a ne u odnosu na sve osobe koje su bile predmet obrade, osigurava se učinkovitost sustava i dostatna razina zaštite prava pojedinca te se ostavlja prostor za razvoj pravnih lijekova, odnosno osporavanje prisutnosti osobe na listi predmetnog sustava i njegovih rezultata bez preopterećenja tijela koja bi o tom odlučivala, odnosno sustav koristila. Na taj bi se način zaštitio i psihološki integritet osoba koje bi bile pretjerano opterećene obaviješću da su predmet obrade sustava koji predviđa da bi u budućnosti mogle činiti kazneno djelo. Točnost sustava također je jedna od kritičkih točaka regulacije prediktivnih sustava. Jedan od ključnih načina poboljšanja točnosti sustava jest njihov trening. Najbolji su način upravo regulatorni izolirani prostori. Korištenje regulatornih izoliranih okruženja zagovara se radi promicanja inovacija, pružanja pravne jasnoće i ubrzavanja pristupa tržištu za tvrtke, s minimiziranjem rizika za sigurnost i temeljna prava. Ti takozvani *pješčanici* nude autoritativne smjernice nadležnih tijela omo-

¹¹⁸ Ideje konceptualne disrupcije izazvane tehnologijom primjenjive su u kontekstu konceptualnog inženjerstva pojma osumnjičenika pod utjecajem disruptivnog utjecaja tehnologije. Vidi više: Löhr, G., *Conceptual disruption and 21st century technologies: A framework, Technology in Society*, vol. 74, 2023, str. 2-8.

¹¹⁹ Vidi više: Ljubanović; Novokmet; Tomićić, *op. cit.* (bilj. 50), str. 71-73; Direktiva 2013/48/EU Europskog parlamenta i Vijeća o pravu na pristup odvjetniku u kaznenom postupku i u postupku na temelju europskog uhiđenog naloga te o pravu na obavješćivanje treće strane u slučaju oduzimanja slobode i na komunikaciju s trećim osoba i konzularnim tijelima, OJ L 294.

gućujući učinkovitu usklađenost sa zakonodavstvom. Stavovi dionika, potkrijepljeni s 408 dokumenata o stajalištima i s potporom iz najmanje 12 država članica EU-a, naglašavaju značaj regulatornih izoliranih prostora kao puta za eksperimentiranje i inovacije u novim regulatornim okvirima, a različiti predstavnici industrije podržavaju njihovo uspostavljanje.¹²⁰ Takav stav zauzeo je i EU razmatrajući Amandmane na Uredbu EU-a o umjetnoj inteligenciji kojima se predlaže obveza država članica da uspostave barem jedno regulatorno izolirano okruženje za UI na nacionalnoj razini, koje mora biti operativno najkasnije do 2. kolovoza 2026. godine. Takav pristup razvoju, testiranju i validaciji doprinosi i drugim kritičnim segmentima, npr. kvaliteti podataka, transparentnosti, procjeni rizika, posebno za temeljna prava, demokraciju i vladavinu prava, zdravlje i sigurnost te okoliš, a ne samo razvoju preciznosti i točnosti sustava, te je on stoga i prihvaćen u članku 57. usvojenog teksta Uredbe EU-a o umjetnoj inteligenciji.

Narav prediktivnih sustava takva je da njihova uporaba može predstavljati ugrozu temeljnih načela kaznenog procesnog prava, ponajprije presumpcije nedužnosti. Kako bi se spriječio nastup tih posljedica, jedan je od prvih koraka razumijevanje i svijest da je riječ o sustavima koji predstavljaju pomoćni alat u radu tijela kaznenog progona. Oni poboljšavaju preventivni rad te ih je nužno percipirati kao oruđe koje potencijalno može unaprijediti i učiniti učinkovitiju njihovu tradicionalnu djelatnost. Stoga je njihova primjena moguća isključivo na način u kojem konačnu odluku, na temelju generiranih rezultata, odnosno predviđanja, poput različitih preventivnih ili potencijalno dokaznih radnji, mora donijeti čovjek koji je obučen za rad s takvim sustavima na temelju objektivnih i provjerljivih činjenica. Izgledno je da na razini trenutačnog razvoja, uz određene prilagodbe, takvi sustavi mogu ispuniti kriterije visokorizičnih sustava, no to i dalje nije jamstvo da će uporaba takvih sustava doista biti u skladu s temeljnim načelima kaznenog procesnog prava.

¹²⁰ U nizu država, a to uključuje i države EU-a poput Njemačke, Francuske i Malte, koriste se regulatorni izolirani prostori u nekom od različitih modela, vidi više: OECD, Regulatory Sandboxes in Artificial Intelligence, OECD Digital Economy Papers, No. 356, DSTI/CDEP/AIGO(2022)7/FINAL Ferrandis, 2023, str. 30–33; Ferrandis, C. M., Regulatory sandboxes can facilitate experimentation in artificial intelligence, dostupno na: <https://oecd.ai/en/wonk/sandboxes> (4. 9. 2023.); Kelly, D. D., an AI regulatory sandbox: Emerging research and pilots, dostupno na: <https://aistandardshub.org/toward-ai-sandbox> (4. 9. 2023.); Ringe, W. G., Why We Need a Regulatory Sandbox For AI, 12. svibnja 2023., dostupno na: <https://blogs.law.ox.ac.uk/oblb/blog-post/2023/05/why-we-need-regulatory-sandbox-ai> (4. 9. 2023.).

LITERATURA

1. Appelman, N.; Ò Fathaigh, R.; van Hoboken, J., Social Welfare, Risk Profiling and Fundamental Rights: The Case of SyRI in the Netherlands, *JIPITEC*, vol. 257, 2019, str. 257-271.
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. 31-89.
3. Berk, R. A., Artificial Intelligence, Predictive Policing, and Risk Assessment for Law Enforcement, *Annual Review of Criminology*, vol. 4, 2021, str. 209-237.
4. Blount, K., Applying the Presumption of Innocence to Policing with AI, *International Review of Penal Law*, vol. 92, br. 1, 2021, str. 33-48.
5. Boba Santos, R., Predictive Policing: Where's the evidence, u: Weisburd, D.; Braga, A. (ur.), *Police innovation: Contrasting perspectives*, 2019, str. 366-369.
6. Burić Z.; Karas, Ž., Prilog raspravi o dvojabama vezanima uz novu definiciju osu-mnjičenika i radnju njegova ispitivanja, *Hrvatski ljetopis za kazneno pravo i praksu*, vol. 24, br. 2, 2017, str. 443-482.
7. Burić, Z.; Engelhart, M.; Novokmet, A.; Roksandić, S., Upotrebljivost rezultata maso-vnog nadzora komunikacije kao dokaza u hrvatskom kaznenom postupku – slučaj Sky ECC, *Hrvatski ljetopis za kaznene znanosti i praksu*, vol. 30, br. 2, 2023, str. 243-274.
8. Carleton, B.; Cunningham, B.; Thorkildsen, Z., The Use of Predictive Analytics in Policing, Arlington, VA: CNA, 2020
9. Catanzariti, M., What Role for Ethics in the Law of AI, u: u: Završnik, A.; Simončić, K. (ur.), *Artificial Intelligence, Social Harms and Human rights, Critical Criminolo-gical Perspectives*, Palgrave Macmillian, 2023, str. 141-161.
10. Chamberlain, J., The Risk-Based Approach of the European Union's Proposed Arti-ficial Intelligence Regulation: Some Comments from a Tort Law Perspective", *Europe-an Journal of Risk Regulation*, vol. 14, str. 1-13.
11. Cihon, P.; Maas, M. M.; Kemp, L., Fragmentation and the Future: Investigating Ar-chitectures for International AI Governance, *Global Policy*, vol. 11, br. 5, 2020, str. 545-566.
12. Cohen, G.; Graver, H. S.; Cops, Docs, and Code: A Dialogue Between Big Data in Health Care and Predictive Policing, *UC Davis Law Review*, vol. 51, br. 437, 2017, str. 440-472.
13. Contissa, G.; Lasagni, G., When it is (also) Algorithms and AI that decide on Criminal Matters: In Search of an Effective Remedy, *European Journal of Crime, Criminal Law and Criminal Justice*, vol. 28, br. 3, 2020, str. 280-304.
14. Dastres, R.; Soori, S., Artificial Neural Network Systems, *International Journal of Imaging and Robotics*, vol. 21, br. 2, 2021, str. 13-25.
15. Đurđević, Z.; Ivičević Karas E, Uporaba umjetne inteligencije u hrvatskom kaznenom postupku, *Hrvatski ljetopis za kaznene znanosti i praksu*, vol. 30, br. 2, 2023, str. 227-242.
16. Dymitriuk, M., Legal Tech in the Law Enforcement Agencies, u: Szostek, D.; Załucki, Z. (ur.), *Legal Tech: Information technology tools in the administration of justice*, Nomos Verlagsgesellschaft mbH & Co. KG, 2021, str. 251-266.

17. Ebers, M., *Truly Risk-Based Regulation of Artificial Intelligence – How to Implement the EU's AI Act*, dostupno na: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4870387 (8. 10. 2024.).
18. Egbert, S.; Leese, M., *Criminal Futures: Predictive Policing and Everyday Police Work*, Routledge Studies in Policing and Society, Taylor & Francis, 2021.
19. Egbert, S.; Mann, M., Discrimination in Predictive Policing: The (dangerous) Myth of Impartiality and the Need for STS Analysis, u: Završnik, A., Badalič, V. (ur.), *Automating, Crime Prevention, Surveillance, and Military Operations*, Springer, 2021, str. 26–27.
20. Ferguson, A. G., Policing Predictive Policing, *Washington University Law Review*, vol. 94, br. 5, 2017, str. 1112–1187.
21. Ferguson, A. G., The Legal Risks of Big Data Policing, *ABA Criminal Justice Magazine*, vol. 33, 2018, str. 1–6, dostupno na: https://digitalcommons.wcl.american.edu/facsch_lawrev/1390 (18. 9. 2023.).
22. Foster, N., *Foster on EU Law, Fourth Edition*, Oxford University Press, 2013.
23. Goel, S.; Shroff, R.; Skeem, J.; Slobogin, C., The accuracy, equity, and jurisprudence of criminal risk assessment u: Vogl, R. (u.), *Research Handbook on Big Data Law*, Elgar, 2021, str. 9-28.
24. Gstrein, O. J.; Bunnik, A.; Zwitter, A., Ethical, Legal and Social Challenges of Predictive Policing, *Católica Law Review, Direito Penal*, vol. 3, br. 3, 2019, str. 77–98.
25. Gültekin-Várkonyi, G., Predictive Policing and Bias in a Nutshell: Technical and Practical Aspects of Personal Data Processing for Law Enforcement Purposes, u: Karsai, K.; Sözüer, A.; Wörner, L. (ur.), *Digital Criminal Justice: A Studybook Selected Topics for Learners and Researchers*, Istanbul, 2022, str. 39-59.
26. Halford, E., 'Two Sides of the Same Coin' – A Proposed Model for Delivering a Whole System Serial Crime Reduction Plan, *Policing: A Journal of Policy and Practice*, vol. 17, 2023, str. 1–14.
27. Hälterlein, J., Epistemologies of predictive policing: Mathematical social science, social physics and machine learning, *Big Data & Society*, vol. 8, br. 1, str. 5.
28. Han-Wei, L.; Ching-Fu, L.; Yu-Jie, C., Beyond *State v Loomis*: artificial intelligence, government, algorithmization and accountability, *International Journal of Law and Information Technology*, vol. 27, br. 2, 2019, str. 131–140.
29. Hardyns, W.; Rummens, A. Predictive Policing as a New Tool for Law Enforcement? Recent Developments and Challenges, *European Journal on Criminal Policy and Research* vol. 24, 2018, str. 201–218.
30. Heilemann, J., Click, Collect and Calculate: The Growing Importance of the Big Data in Predicting Future Criminal Behaviour, *International Review of Penal Law*, vol. 92, br. 1, 2021, str. 49–67.
31. Heller, S.; Jakubowski, B.; Jelveh, Z.; Kapustin, M., *Machine Learning Can Predict Shooting Victimization Well Enough to Help Prevent It*, National Bureau of Economic Research Working Paper Series, Working paper 30170 (posljednji put u izmijenjen u rujnu 2022.).
32. Joh, E. E., The Consequences of Automating and Deskillling the Police, *UCLA Law Review*, vol. 67, br. 134, 2019, str. 136–164.
33. Johson, L. E., Case Brief: United States v. Curry, *The North Carolina Law Review*, vol. 99, 2021, str. 101–108.
34. Jones, T., Governing Security: Pluralization, Privatization, and Polarization in Crime Control and Policing, u: Maguire, M.; Morgan, R.; Reiner, R. (ur.), *The Oxford Handbook of Criminology, Fifth Edition*, Oxford University Press, 2013, str. 743-768.

35. Karsai, K., Algorithmic Decisions within the Criminal Justice Ecosystem and their Problem Matrix, *International Review of Penal Law*, vol. 92, vr. 1, 2021, str. 13–33.
36. Kaufmann, M.; Egbert, S.; Lesse, M., Predictive Policing and the Politics of Patterns, *The British Journal of Criminology*, vol. 59, br. 3, 2019, str. 674–692.
37. Krapac, Davor, *Kazneno procesno pravo, Prva knjiga: Institucije*, VIII. Izmijenjeno i dopunjeno izdanje, Narodne novine, 2020.
38. Kusak, M. Quality of data sets that feed AI and big data applications for law enforcement, *ERA Forum*, vol. 23, 2022, str. 209–219.
39. Ljubanović, V.; Novokmet, A.; Tomičić, Z., *Kazneno procesno pravo – izabrana poglavlja*, Sveučilište Josipa Jurja Strossmayera u Osijeku, Pravni fakultet Osijek, 2020.
40. Löhr, G., Conceptual disruption and 21st century technologies: A framework, *Technology in Society*, vol. 74, 2023, str. 1–9.
41. Macnish, K.; Wright, D.; Jiya, T., Predictive Policing in 2025: A Scenario, u: Jahankhani, H.; Akhgar, B.; Cochrane, P.; Dastbaz, M. (ur.), *Policing in the Era of AI and Smart Societies, Advanced Sciences and Technologies for Security Applications*, Springer, 2021, str. 199–215.
42. McGehee, M., *Predictive Policing Technology: Fourth Amendment and Public Policy Concerns*, dostupno na: <https://uclawreview.org/2021/02/17/predictive-policing-technology-fourth-amendment-and-public-policy-concerns> (24. 8. 2023.).
43. Meijer, A.; Wessels, M., Predictive Policing: Review of Benefits and Drawbacks, *International Journal of Public Administration*, vol. 42, br. 12, 2019, 1031–1039.
44. Meyer P., Judicial diplomacy of the German Federal Constitutional Court: bilateral court meetings as a novel data source to assess transnational communication of constitutional courts, *Zeitschrift für Vergleichende Politikwissenschaft*, vol. 15, br. 3, 2021, str. 295–323.
45. Mohler, G. O.; Short, M.; Malinowski, S.; Johnson, M.; Tita, G., E.; Bertozzi L., A.; Jeffrey Brantingham, P.; Randomized Controlled Field Trials of Predictive Policing, *Journal of the American Statistical Association*, vol. 110, 2015, str. 1399–1411.
46. Mugari, I.; Obioha, E., Predictive Policing and Crime Control in The United States of America and Europe: Trends in a Decade of Research and the Future of Predictive Policing, *Social Sciences*, vol. 10, br. 234, str. 1–14.
47. Nikolinakos, N. Th., *EU Policy and Legal Framework for Artificial Intelligence, Robotics and Related Technologies – The AI Act*, Springer, 2023.
48. Novokmet, A.; Tomičić, Z.; Vinković, Z., Pretrial risk assessment instruments in the US criminal justice system – what lessons can be learned for the European Union, *International Journal of Law and Information Technology*, vol. 30, br. 1, 2022, str. 1–22.
49. 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, The digitalization and green transformation of the European Union*, vol. 7, str. 525–570.
50. Picotti L., General Report, u: Picotti, L.; Panattoni, B. (ur.), Traditional Criminal Law Categories and AI: Crisis or Palingenesis?, International Colloquium Section I, Siracusa, *International Review of Penal Law*, vol. 94, br. 1, 2023, str. 11–52.
51. Quattrocchio, S., *Artificial Intelligence, Computational Modelling and Criminal Proceedings: A Framework for A European Legal Discussion*, Springer, 2020.
52. Rachovitsa, A.; Johann, N., The Human Rights Implications of the Use of AI in the Digital Welfare State: Lessons Learned from the Dutch SyRI Case, *Human Rights Law Review*, vol. 22, br. 2, 2022, str. 1–15.

53. Richardson, R.; Schultz, J.; Crawford, K., Dirty Data, Bad Predictions: How Civil Rights Violations Impact Police Data, Predictive Policing Systems, and Justice, *New York University Law Review Online*, vol. 94, 2019, str. 16–55.
54. Rossbach, N., Innocent until predicted guilty: How Premature Predictive Policing Can Lead to a Self-fulfilling Prophecy of Juvenile Delinquency, *Florida Law Review*, vol. 167, 2023, str. 168–193.
55. Roth, A., The Use of Algorithms in Criminal Adjudication, u: Barfield, W. (ur.), *The Cambridge Handbook of the Law of the Algorithms*, Cambridge University Press, 2020, str. 407–431.
56. Sachoulidou, A., Going beyond the “common suspects”: to be presumed innocent in the era of algorithms, big data and artificial intelligence, *Artificial Intelligence and Law*, 2023, str. 1–54.
57. Sandhu, A.; Fussey, P., The ‘uberization of policing’? How police negotiate and operationalise predictive policing technology, *Policing and Society: Policing and Technology*, vol. 31, br. 1, 2021, str. 66–81.
58. Schlehn, E.; Aichroth, P.; Mann S.; Schreiner, R.; Shepherd, I.; Wong, B.L.W., Benefits and Pitfalls of Predictive Policing, u: *2015 European Intelligence and Security Informatics Conference, IEEE*, 2015, str. 145–148.
59. Schmitt, L., Mapping global AI governance: a nascent regime in a fragmented landscape, *AI Ethics*, vol. 2, 2022, str. 303–314.
60. Scholl, C.; de Kraker, J., The Practice of Urban Experimentation in Dutch City Labs, *Urban Planning*, vol. 6, 2021, str. 161.
61. Schuett, J., Defining the Scope of AI Regulations, *Law, Innovation and Technology*, vol. 15., br. 1, str. 60–82.
62. Sheikh, H.; Prins, C.; Schrijvers, E.; *Mission AI, The New System Technology*, Springer, 2023.
63. Simončić, K.; Jerele, T., Democratizing the Governance of AI: From Big Tech Monopolies to Cooperatives, u: Završnik, A.; Simončić, K. (ur.), *Artificial Intelligence, Social Harms and Human rights, Critical Criminological Perspectives*, Palgrave Macmillan, 2023, str. 239–269.
64. Söderholm, S., Fundamental rights control when implementing predictive policing – a European perspective, *Peking University Law Journal*, vol. 11, br. 1, 2023, str. 91–104.
65. *State v. Loomis*, Wisconsin Supreme Court Requires Warning Before Use of Algorithmic Risk Assessments in Sentencing, *Harvard Law Review*, vol. 150, br. 5, 2017, str. 1530–1537.
66. Strikwerda, L., Predictive policing: The risks associated with risk assessment, *The Police Journal: Theory, Practice and Principles*, vol. 94, br. 3, 2021, str. 422–436.
67. Ulbricht, L.; Egbert, S., In Palantir we trust? Regulation of data analysis platforms in public security, *Big Data & Society*, vol. 11, br. 3, str. 1, 9–11.
68. van Bekkum, M.; Borgesius, F. Z., Digital welfare fraud detection and the Dutch SyRI judgment, *European Journal of Social Security*, vol. 23, br. 4, 323–340.
69. van Brakel, R., Policing, Pre-emptive Big Data Surveillance and its (Dis)Empowering Consequences: The case of Predictive Policing, u: vann der Sloot B.; Broeders, D.; Schrijvers, E. (ur.), *Exploring the Boundaries of Big Data*, WRR, Amsterdam University Press, 2016, str. 117–141.
70. Wilson, D., Algorithmic patrol: the futures of predictive policing, u: Završnik, A. (ur.), *Big data, Crime and Social Control*, Routledge Frontiers of Criminal Justice, 2018, str. 108–128.

Summary

Ivan Vidaković *

THE USE OF PREDICTIVE POLICING DESIGNED FOR LAW ENFORCEMENT AUTHORITIES: THE EUROPEAN UNION PERSPECTIVE **

Artificial intelligence has become an integral facet of everyday life. Simultaneously, criminal law has not remained impervious to modernisation processes, primarily facilitated through the integration of artificial intelligence systems into traditional activities, processes, stages, and actions. Predictive policing systems, designed to anticipate future criminal offences, including the area where the offence might be committed, the perpetrator, and the potential victim, have served for many years as effective tools for redirecting law enforcement efforts from reactive to preventive measures. However, the expeditious processing of vast amounts of data carries inherent risks, chiefly manifested in data quality, transparency, and accuracy. Given the implications of employing predictive policing systems within the purview of law enforcement authorities, any associated risks necessitate careful regulation and control to ensure the acceptability of such systems. A significant endeavour to address and mitigate these risks is evident in the European Union's efforts to regulate artificial intelligence through the Artificial Intelligence Act, representing one of the most comprehensive attempts in this domain. In assessing the proposed regulation, this paper primarily scrutinises the fragmented approach to defining artificial intelligence and the risk-based approach, a crucial aspect for the regulation of predictive policing systems. The evaluation of predictive systems extends to an exploration of their purpose, discerning the concrete implications of their use for fundamental human rights and freedoms. Subsequently, the paper delves into an analysis of past practices, examining specific systems and countries to elucidate practical challenges encountered in their application within a legal framework, as evidenced by relevant court decisions. The concluding section of the paper concentrates on scrutinising the European Union's regulation of artificial intelligence. This examination seeks to determine whether predictive policing systems align with the stringent criteria established for high-risk systems, as initially outlined in the proposal, or whether a more restrictive perspective, possibly entailing the complete prohibition of their use as outlined through the amendments to the Artificial Intelligence Act, is the correct interpretation.

Keywords: Artificial Intelligence Act, high-risk AI systems, predictive policing systems, quality of data, risk-based approach, transparency

* Ivan Vidaković, mag. iur., 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>.

** This article is a product of work that has been fully supported by the Josip Juraj Strossmayer University of Osijek, Faculty of Law Osijek, under the project IP-PRAVOS-18 'Artificial Intelligence and Criminal Law'.