**Ivana D. Miljuš***

**Pregledni naučni članak**
**UDK: 004.8:351.74**
**doi: https://doi.org/10.56461/SPZ_25303KJ**
**Primljeno: 14. 2. 2025.**
**Prihvaćeno: 6. 9. 2025.**

# ALGORITMI VEŠTAČKE INTELIGENCIJE ZA „OCENU RIZIKA“ U DOMENU SAVREMENOG PROGNOZIRAJUĆEG RADA POLICIJE

***Sažetak***

Policijski „algoritmi za ocenu rizika” aktiviraju inherentne rizike po ostvarivanje osnovnih ljudskih prava. Značaj teme proizlazi iz ubrzanog razvoja sistema veštačke inteligencije i nedavnog formulisanja međunarodnopravnog okvira za njihovu upotrebu. Autorka polazi od hipoteze da međunarodnopravni i evropskopravni okvir suštinski uspostavljaju ograničenu zabranu primene AI sistema u prediktivnom radu policije. Cilj istraživanja je ukazivanje na potrebu redefinisanja u određenoj meri osnovnih instituta krivično procesnog prava. Dominantan metod istraživanja je uporednopravni. Osnovni rezultati ogledaju se u povezivanju rada AI algoritama sa krivično procesnim pravom, pravom na slobodu i bezbednost, pravom na pravično postupanje.

**Ključne reči:** policija, ocena rizika, veštačka inteligencija, pravo na slobodu i bezbednost, pravo na pravičan postupak.

* Docent, Pravni fakultet Univerziteta u Beogradu, Beograd, Srbija.
E-mail: *ivana.miljus@ius.bg.ac.rs*
ORCID: *https://orcid.org/00000001-8147-4061*

## ARTIFICIAL INTELLIGENCE ALGORITHMS FOR "RISK ASSESSMENT" IN THE FIELD OF MODERN PREDICTIVE POLICING

***Summary***

The work of "risk assessment" algorithms within the framework of predictive policing is based on a risk-based, future-oriented approach, risk generation, and a specific type of police intervention towards individuals. Modern algorithms use AI elements to enhance police efficiency and support more informed decision-making, but they also carry numerous inherent risks to the protection of fundamental human rights and freedoms. The significance of this topic stems from the rapid development of AI systems, the practices of applying AI algorithms in Europe and global, and the recent formulation of international and European legal frameworks for the use of AI systems, which also impact the field of predictive policing. The author starts from the fundamental hypothesis that the international and European legal framework does not introduce an apsolute ban on the use of AI systems in predictive policing but essentially establishes a limited prohibition and introduce basic safeguards for the application of AI systems, as a result of balancing the expansion of AI technology development, its benefits and risks. The aim of the research is to highlight the need for a certain degree of redefinition of the fundamental institutes and principles of criminal procedural law, guarantees of the right to liberty and security, and the requirements of the right to a fair trial, as well as to identify the principles and basic guidelines for the application of AI systems in predictive policing. Two important principles for the application of AI algorithms are: 1. the essential/significant/dominant role of humans in decision-making, which implies that a human carefully evaluates the algorithm's report by assigning its limited value in decision-making or not assigning it any value at all (depending on the algorithm's shortcomings or the absence of safeguards for the use of AI systems); 2. the transparency of the AI algorithm's operation concerning an individual's right to review the data, functioning, and outcome of the algorithm. The main research results are reflected in linking the functioning of predictive algorithms with criminal procedural law, the principle of adversarial proceedings/contradictory, the right to liberty and security, the right to fair procedure, and identifying fundamental safeguards and risks highlighted by comparative legal practice and international legal documents.

**Keywords*:*** police, "risk assessment algorithms", artificial intelligence (AI), right to liberty and security, right to a fair procedure.

## 1. Uvod

„Pristupi krivičnoj pravdi utemeljeni na riziku" (*risk-based approaches to criminal justice*) jesu pristupi i prakse kontrole kriminaliteta zasnovani na paradigmi rizika. Podrazumevaju upotrebu raznovrsnih aktuarskih metoda, alata i prognozirajućih tehnologija u cilju prevencije kriminaliteta. Prevencija zasnovana na faktorima rizika dominantna je u kontroli kriminaliteta od osamdesetih godina prošlog veka, a naučnici su koristili statističke i geo-prostorne analize da bi odredili nivoe rizika od zločina (Mehozay & Fisher, 2019, pp. 524-426). Na pristup utemeljen na riziku nadovezuje se koncept „pre-crime društva".[1] Pristup baziran na riziku i prognozirajući rad policije „idu u korak" sa njim. Deo su šireg koncepta orijentisanog ka budućnosti. „Pre-crime" je noviji koncept, koji pojam preuzima iz književnosti (vid. Nenadić, 2017, p. 158). Njegov neposredni *ratio* bio je borba protiv terorizma. Usmeren ka neizvesnoj budućnosti, on egzistira uz tradicionalan koncept „post-crime društva" koji primenjuje klasično krivično pravo, usmereno na krivična dela iz prošlosti. „Pre-crime", kako to objašnjava Nenadić (2021a, p. 269), počiva na „preokupaciji društva budućim krivičnim delima (budućnošću i bezbednošću) i tendenciji krivičnopravnog sistema da se bavi anticipiranjem krivičnih dela". Temelji se na predviđanju pretnji, kombinaciji imaginacije i akcije, logici „zamisli scenario/najgori scenario – deluj u sadašnjosti uz prinudu – predupredi scenario". Zender u svom radu (2007, p. 262), od pre skoro dve decenije, nalazi da se društvo nalazi na pragu prelaska iz „post-crime" u „pre-crime društvo", u kojem mogućnost sprečavanja rizika konkuriše reakciji na učinjena kaznena dela, čak je i nadmašuje.

Primeri aktivnosti u sadašnjosti u cilju prevencije određenih krivičnih dela, u opštem smislu zasnovani na riziku, jesu profilisanje, javni registri osuđenih za krivična dela protiv polne slobode učinjena prema maloletnim licima, vršenje „preventivnih nadzora policije" nad „osuđenim seksualnim 'predatorima'" (vid. Škulić, 2019, pp. 43-49), preventivno lišenje slobode potencijalnih učinilaca krivičnih dela nasilja u porodici i navijača iz kategorije „huligana" (vid. Nenadić, 2017, pp. 162-166). „Pre-crime" okvir nadmašuje okvir zasnovan na riziku. Specifičnosti prevencije zasnovane na riziku ogledaju se u „primeni okvira rizika na identifikovanu pretnju, 'verovatniju i izračunljivu budućnost', sprečavanje ponavljanja krivičnih dela, korišćenje ranijih osuda za ocenu budućeg kriminalnog rizika, formiranje sumnje

[1] Kriminološki pojam „pre-crime" vezuje se za sociološki pojam „društva rizika" (*Risk Society*). Urlih Bek (Urlich Beck), nemački sociolog, 1986. godine u svom kapitalnom delu o „društvu rizika" (*Risikogesellschaft*), prevedenom na engleski jezik (Ritter, 1992, p. 34), piše: „U 'društvu rizika' prošlost gubi moć da određuje sadašnjost. Njeno mesto zauzima budućnost, dakle, nešto nepostojeće, izmišljeno, fiktivno, 'uzrok' trenutnog iskustva i delovanja. Danas postajemo aktivni da bismo sprečili, ublažili ili preduzeli mere predostrožnosti protiv problema i kriza sutrašnjice […]".

da će se ponovo učiniti krivično delo na temelju ponašanja u prošlosti, postavci da je prestupništvo u prošlosti i sumnja da će se ponoviti osnov za prinudnu intervenciju države" (McCulloch & Wilson, 2016, pp. 3-9). Za lice pod rizikom pronalazi se i izraz „unapred osumnjičeni", „osoba koja privlači pažnju", koja možda nikada nije bila predmet istrage za konkretno krivično delo, ali ga algoritam izdvaja i stavlja pod nadzor u određenom cilju (Sachoulidou, 2023, p. 22).

„Algoritmi za ocenu rizika" su vrsta prediktivnog analitičkog alata, softvera koji primenjuje određene tehnike kojima se kao rezultat generiše i klasifikuje prognoza izvršenja/ponavljanja krivičnog dela / rizik od bekstva / nepojavljivanja pred sudom i verovatne lokacije eventualnih budućih krivičnih dela. Koriste se u prognozirajućem radu policije, u određenoj meri u radu pravosudnih organa, probacijskih službi. Pružaju informacije policijskim službenicima za prognoziranje i određene vidove intervencija u cilju sprečavanja krivičnih dela. Kompjuterizacija alata za ocenu rizika dovela je do mogućnosti da se analiziraju i povezuju veliki skupovi podataka. Korišćenje veštačke inteligencije (dalje u tekstu: AI) vodi brojnim složenim etičkim i pravnim pitanjima, te zahteva etičke i pravne garancije i nadzor. U radu se analiziraju prakse pojedinih država Evrope sa osvrtom na praksu primene algoritama u SAD.

## 2. Algoritmi za prognoziranje rizika u okvirima prediktivnog/prognozirajućeg rada policije

Preko četrdeset godina paradigma rizika ostvaruje povećan uticaj u oblasti policijskih praksi (Mythen, 2020, p. 167). Prediktivni/prognozirajući rad policije realizuje se pre izvršenja krivičnog dela u odnosu na potencijalne učinioce, potencijalne žrtve i potencijalne lokacije izvršenja krivičnog dela, ali u širem smislu i nakon izvršenja krivičnog dela, u pravcu prognoziranja identiteta „učinioca". Prediktivni policijski softveri utemeljeni su na ideji o predvidivosti i algoritamskoj izračunjivosti kriminala (Egbert & Krasmann, 2019, p. 3). Temelje se na zapažanju da krivična dela slede određene obrasce (Kaufman, Egbert & Leese, 2019, p. 674).

Rezultati rada pojedinih kompjuterskih programa koji analiziraju veliku količinu podataka pokazali su značajan uspeh u policijskom rešavanju slučajeva.[2] Međutim, slikovito se zapaža da „nije moguće pravilno odvojiti rizike zločina koje treba sprečiti i rizike sprečavanja zločina" (Strikwerda, 2021, p. 423). Izdvajaju se fundamentalni izazovi za ostvarivanje osnovnih ljudskih prava i sloboda generisani upotrebom „algoritama za ocenu rizika": 1. nesrazmerno zadiranje u pravo

[2] Od 2007. godine, kada je započelo eksperimentalno uvođenje programa „Keycrime" u Milanu, do 2014. godine, rešeni slučajevi pljački komercijalnih objekata porasli su sa nešto više od 27% na više od 61%, sa vrhuncem od 81%, u pogledu pljački u apotekama (Polizia Moderna, 2015, p. 3).

na privatnost; 2. netransparentnost i neobjašnjivost rada algoritma, nemogućnost objašnjavanja kako se došlo do rezultata u vidu ocene rizika, takozvani efekat „*black box*"; 3. efekat diskriminacije; 4. rizici za pretpostavku nevinosti i stigmatizaciju. Centralni rizik sa krivično-procesnog aspekta je rizik za pretpostavku nevinosti. Otvara opciju ponovnog razmatranja njene zaštite i regulative pitanja da li policija mora da ispuni standard individualizovane sumnje pre nego što algoritmu dostavi podatke potrebne za generisanje izveštaja o riziku, odnosno pre ikakve intervencije u vezi sa krivičnim postupkom (Sachoulidou, 2023, p. 23).

### *2.1. Primer alata SyRI*

Značajni primeri upotrebe prognozirajućih algoritama u Evropi beleže se u Holandiji, koja na državnom nivou primenjuje „algoritme za ocenu rizika". Izdvajamo primenu ovih algoritama u povezanom kontekstu sa radom policije i tužilaštva. U pogledu alata SyRI (*System Risk Indication*) za prevenciju i borbu protiv prevara i prognoziranje prevara, Okružni sud u Hagu, u odluci broj C/09/550982/ HA ZA 18/388, 2020. godine (The Hague District Court, 2020), rešavao je u građansko-pravnom predmetu. Ocenio je da zakonodavstvo o ovom alatu, iako ima legitiman cilj – borbu protiv prevara u određenim oblastima (socijalnog osiguranja, radnog prava), njihovu prevenciju i ekonomsko blagostanje – povređuje pravo na privatnost iz čl. 8 Evropske konvencije o ljudskim pravima i osnovnim slobodama (dalje u tekstu: EKLJP). Izveštaj o riziku od prevara, generisan u šiframa a potom dešifrovan, mogao se proslediti tužilaštvu i policiji po zahtevu. Policija je mogla da koristi izveštaj zajedno sa drugim dokazima kao osnov za sprovođenje mera iz svoje nadležnosti. Iz odluke Suda sledi nalaz da se zahtevi upotrebe algoritama odnose najpre na *tačnost i potpunost* unosnih podataka i *pravo na zaštitu privatnosti* unosnih podataka koje algoritam analizira i generiše rezultat u vidu „pogodaka" o rizičnim fizičkim/pravnim licima.

Sud u Hagu poziva se na princip iz prakse ESLJP-a da država koja primenjuje nove tehnologije pronađe pravi balans između koristi od upotrebe i zadiranja u ostvarivanje prava na poštovanje privatnog života, te da se pred zakonodavca postavlja zahtev da „obezbedi dovoljno efikasan okvir u kojem se svi uključeni interesi mogu izvagati na transparentan i proverljiv način" (The Hague District Court, 2020, par. 6.6.). U ovom slučaju nije bio ispunjen zahtev „pravičnog balansa" između društvenog interesa kojem služi zakonodavstvo i narušavanja privatnog života, te se nije moglo govoriti o „dovoljno opravdanom zadiranju u privatni život". Korišćeni su podaci iz baza različitih institucija o zaposlenju, dugovima, zdravstvenom osiguranju i lični podaci građana. Model rizika, indikatori rizika i podaci za obradu nisu bili javni, niti poznati uključenim stranama, zbog čega nije ni bilo moguće da se

proceni ispunjenje zahteva proporcionalnosti – neophodnosti zadiranja u privatni život s obzirom na željeni legitimni cilj. Zakonodavstvo nije utvrdilo obavezu da se lica čiji se podaci obrađuju informišu o tome niti da se obaveste da je napravljeno obaveštenje o riziku. Pogođeni nisu mogli da osporavaju izveštaj pre donošenja odluke nadležnih organa. Velike količine podataka kvalifikovane su kao podaci za obradu, uključujući i posebne lične podatke, i korišćeni su profili rizika, pa je identifikovano da postoji rizik od nenamernog povezivanja na osnovu predrasuda, kao što su niži socio-ekonomski status ili imigrantsko poreklo (The Hague District Court, 2020, par. 6.93). Pravo na privatnost u kontekstu zaštite podataka dotiče prava na jednako postupanje u jednakim slučajevima i zaštitu od diskriminacije, stereotipizacije i stigmatizacije (The Hague District Court, 2020, par. 6.24). Tužioci su tvrdili da ljudska intervencija u donošenju odluke nije bila smislena, jer agent nije imao način da razume kako je izveštaj o riziku generisan i koja kombinacija informacija je dovela do konačne odluke, ali Sud nije utvrdio da li je ljudska intervencija bila značajna (vid. Elyounes, 2021, pp. 503-506).

## 3. Policijski AI „algoritmi za ocenu rizika" i profilisanje

Ugrađivanje AI u „algoritme za ocenu rizika", povećano oslanjanje državnih organa mnogih država na rezultate AI aplikacija produbljuju izazove i rizike u oblasti prava na slobodu i bezbednost ličnosti, pravo na pravično postupanje, pravo na privatnost. Teorija postavlja opštu pretpostavku da AI prema svojim osobinama odgovara aktuelnoj tendenciji kontrole kriminaliteta, ali da „najvećim delom ne odgovara postignutom nivou zajemčenih ljudskih prava (Stevanović, 2022, p. 344).

Unapređivanje AI i potreba da se poveže i obradi velika količina podataka da bi se znatno brže došlo do preciznijeg rezultata doveli su do upotrebe AI u oblasti prognozirajućeg rada policije i brojnih AI aplikacija za procenu rizika. Savremene prakse pokazale su da se AI i automatizovani sistemi koriste da bi se prognoziralo u određenom periodu eventualno izvršenje krivičnih dela određene prirode/vrste[3], pre svega krivična dela sa elementima nasilja, imovinska krivična dela, seksualni delikti, krivična dela u vezi sa vatrenim oružjem i krivična dela terorizma. *Ratio* njihove upotrebe je unapređenje efikasnosti prediktivnog rada policije i potkrepljenija procena rizika, utemeljena na brojnim podacima iz različitih baza podataka. Na nivou Evropske unije, konstatuje se da se „sve veća upotreba AI u sferi krivičnog

[3] Utset (2021, pp. 176-177), na temelju premise da algoritmi mašinskog učenja najbolje funkcionišu ako se treniraju na velikom broju primera, zaključuje da će biti najkorisniji za veoma česta krivična dela, krivična dela u vezi sa drogom i krivična dela protiv imovine, te da će policijsko prediktivno delovanje dovesti do većeg broja hapšenja za ova krivična dela.

prava posebno temelji na obećanju da ima potencijal da *smanji određene vrste kriminala* i dovede do *objektivnih odluka*" (European Parliament resolution on artificial intelligence in criminal law and its use by the police and judicial authorities in criminal matters (2020/2016(INI) – EU Resolution 2020/2016(INI), 2021).

Policijski „algoritmi za ocenu rizika" prema svom predmetu odnose se na: 1. *određena lica* – ocena rizika od vršenja krivičnih dela/recidivizma; 2. *određene lokacije* – ocena rizika da će se u određenim oblastima/geografskim lokacijama ostvariti krivično delo. U ovom kontekstu AI se pripisuje funkcija da putem analize istorijskih podataka o kriminalu i identifikovanjem obrazaca *pomogne* policiji da predvidi „potencijalna žarišta kriminala" (*hot spots*) i proaktivno raspodeli svoje snage da bi sprečila krivična dela, što naročito može biti od značaja u velikim gusto naseljenim gradovima (Situmeang *et al*., 2024, p. 1967).

„Algoritmi za ocenu rizika" sa elementima AI primenjuju se i u odlučivanju o krivičnom gonjenju/primeni oblika diverzionog postupanja. Upečatljiv primer je korišćenje u okrugu u Velikoj Britaniji, u okvirima pilot-projekta, algoritma *Harm Assessment Risk Tool* (HART), baziranom na obliku mašinskog učenja[4]. U Holandiji je izraženo korišćenje policijskih algoritama i u odnosu na maloletna lica (Top600). Softveri za ocenu rizika obrađuju podatke kao što su uzrast/starost, rod, zanimanje, krivična evidencija, da bi identifikovali lica sklona da učine teška krivična dela (Golunova, 2023, p. 51). Prognoze u pogledu lokacija zasnivaju se na dostupnim informacijama o predstojećim događajima (npr. veliki sportski događaji), vremenskim uslovima i stopama kriminala u prošlosti (Golunova, 2023, p. 51).

Rad algoritma Dalia (*Dynamic Evolving Learning Integrated Algorithm*) sa AI tehnologijama, koji koristi policija u Italiji, usmeren je na profilisanje specifičnog pojedinca i verovatne lokacije za izvršenja budućih verovatnih krivičnih dela. Zasniva se na velikoj bazi policijskih podataka o eventualnim krivičnim delima pojedinaca/grupe, prikupljanju velike količine podataka, analiziranju inkriminisanih događaja, identifikovanju ponavljanja krivičnih dela. Predmet analize su i podaci o osumnjičenima prikupljeni iz svedočenja, što može uključivati „specifične identifikacione detalje poput procene starosti, visine, telesne građe, boje kože, kose, očiju, odeće i akcenta", informacije o oružju, vozilu koje je korišćeno, koji se kombinuju sa policijskim izveštajima i krivičnim evidencijama i snimcima video-nadzornih kamera (Fair Trials-Automating Injustice, n.d., p. 20).

Algoritam HART-a zasnivao se na velikom skupu podataka (predmetima iz određenog perioda u kojima su lica bila lišena slobode u policijskim stanicama), 34 varijable, od kojih se velika većina odnosila na „kriminalnu prošlost" (29) a preostale

[4] Mašinsko učenje podrazumeva skup kompjuterskih metoda koje omogućavaju da mašina uči na osnovu iskustava iz prošlosti (podataka za analizu), automatski iznalazi obrasce iz podataka, na osnovu kojih može da daje prognoze za budućnost (vid. Häuselmann, 2022, pp. 48-49).

na policijske obaveštajne podatke i podatke o karakteristikama/obeležjima ličnosti (starost, rod, forme boravišnog poštanskog koda koji praktično kategorizuje pojedince na osnovu socijalnih i geo-demografskih podataka), te na namernom favorizovanju „opreznih grešaka" u kojima su nivoi rizika precenjeni (Oswald *et al*., 2018, p. 227). Kreiran je da pomogne policiji u proceni rizika od izvršenja kaznenih dela u određenom periodu u odnosu na lica koja je policija lišila slobode. Angažovanje AI smatralo se racionalnim zbog ogromnog broja neophodnih informacija i nekoliko hiljada predmeta koje je bilo potrebno obraditi na godišnjem nivou (Stevanović, 2022, p. 352). Pojedinci su svrstavani u tri kategorije – visokorizični (u riziku da učine teška krivična dela), umereno rizični, podložni diverzionom tretmanu (u riziku da učine lakša krivična dela), niskorizični (bez rizika od izvršenja krivičnog dela). Istraživanja u vezi sa ovim alatom doprinela su i formiranju smernica za postupanje koje obuhvataju, između ostalog: 1. postavku da mašina ne zamenjuje ljudsku inteligenciju, već je dopunjuje i pojačava (*zahtev savetodavne uloge algoritma*, zadržavanja diskrecione ocene čoveka); 2. ocenu da li su podaci koji se obrađuju pribavljeni, obrađeni i zadržani u skladu sa pravom, saglasno principu neophodnosti u vezi sa legitimnim ciljem; 3. zahtev kvaliteta podataka koji se obrađuju, odsustva predrasuda; 4. postavljanje pitanja da li su objašnjiva pravila odlučivanja i uticaj svakog faktora na konačan rezultat (vid. Oswald *et al*., 2018, pp. 244-249).

Prognoze policije u odnosu na lica potencijalno vode određenim aktivnostima policije – stavljanje označenih lica pod neki vid nadzora/konstantni nadzor, racije, saslušanja, unošenje u policijske evidencije, zaustavljanje i pretresanje i drugi oblici preventivnih lišenja slobode ili aktivnosti socijalnih službi. Upozorava se da su dugoročne društvene implikacije grešaka u prognozi narušavanje poverenja u sposobnost policije da obavlja svoj posao, što može da dovede do smanjenja ukupnog efekta odvraćanja jer sposobnost policije zavisi od spremnosti građana koji poštuju zakon da podele informacije sa policijom (Utset, 2021, p. 175). Prakse automatizovane ocene rizika u sferi prognozirajućeg rada policije pokazala su da su ocene rizika proizvodile procesne posledice u vidu tužilačkih predloga strožih kazni i predloga za određivanje pritvora, policijska hapšenja za učinjena krivična dela (Fair Trials-Automating Injustice, n.d., pp. 11-12).

Upotreba „algoritama za procenu rizika", u okvirima prognozirajućeg rada policije, započela je u SAD[5], policijskim departmanima Santa Kruz i Los Anđeles (PredPol), odakle se širi u države Evrope. Praksa u pojedinim evropskim i u američkim državama pokazala je da su neki podaci unošeni u algoritam sadržali diskriminacije direktno (podaci o etničkoj pripadnosti), ili indirektno (podaci o poštanskim kodovima, zaustavljanjima i pretresanjima, finansijske informacije o licima).

[5] U SAD, nekoliko država, poput Kalifornije i Ilinoisa, donelo je posebne zakone o policijskim algoritmima (Raji & Sholademi, 2024, p. 73).

Kao kriterijumi za ocenu rizika korišćeni su policijska hapšenja u određenom periodu i kontakti sa javnim tužilaštvom (u Amsterdamu Top600 za modeliranje rizika i profilisanje). Beleže se slučajevi u kojima su podaci suštinski bili u vezi sa ponašanjem drugih lica, u kojima su odnosna lica bila žrtve ili označeni kao svedoci/potencijalni svedoci krivičnopravno relevantnog događaja (u Amesterdamu Top400 za modeliranje rizika). Kriterijumi za ocenu rizika u pogledu vršenja krivičnih dela bili su i podaci koji nisu u vezi sa krivičnim delima/potencijalnim krivičnim delima, na primer odsustvo iz škole, učestalost promene osnovne škole (Top400). Pojedini su se direktno odnosili na raniji život roditelja/staratelja, bliskih lica sa kojima maloletno lice živi, prijatelja/poznanika (ProKid).

Postavlja se *pitanje tačnosti* rezultata rada AI, čak i ako se eliminišu predrasude (Utset, 2021, p. 175). Osnovni zahtev pravičnog postupanja je da uputstva o upotrebi AI aplikacija sadrže upozorenja donosiocima odluka/korisnicima o mogućim greškama, čime se upućuje na neophodnu kontrolu čoveka. Istraživanja pokazuju da je praksa primene algoritma PRECOBS u Nemačkoj utemeljena na principima ljudskog odlučivanja i procene i da dominantnu ulogu u prognozirajućem radu zadržavaju patrolni policajci i policijski analitičari (Egbert & Krasmann, 2019, p. 6).

AI aplikacijama za ocenu rizika pripisuje se informativna uloga u prognozirajućem radu policije. Ukazuje se na temelnji rizik – da li je odluka o lišenju slobode „*adekvatno potkrepljena*", te da li je lišenje slobode arbitrerno (Golunova, 2023, p. 54). Problem manjkavosti skupa podataka (policijskih i drugih) iz kojih algoritmi uče (nepotpunost, predrasude[6]), te tačnost informacija u vidu rezultata algoritma vodi na teren pravičnog postupanja. Ova sfera obuhvata informisanje pojedinca da je u postupku donošenja odluke i preduzimanja mera na osnovu nje primenjen AI sistem, preispitivanje tačnosti isporučene informacije i transparentnost podataka i rada algoritma. Ukazuje se na važnost obezbeđivanja da alati budu podrška u donošenju odluke, a da ne zamene prosuđivanje korisnika (Alikhademi *et al*., 2021, p. 9). Zahtev zadržavanja „čoveka u petlji"[7], generalno istican u vezi sa upotrebom AI sistema, proizlazi iz inherentnog rizika da se policijski službenici prekomerno uzdaju u rezultat rada AI.

Postavlja se pitanje postojanja drugih informacija i činjenica, osim rezultata algoritma. Ovaj zaključak se može izvesti i iz analize stavova Evropskog suda za ljudska prava (dalje u tekstu: ESLJP) o saglasnosti preventivnog lišenja slobode sa

[6] Nenadić i Miljuš (2021, pp. 299-300) naglašavaju da je AI sklona predrasudama i uvećavanju postojećih unosnih predrasuda u sistem, osvrću se na pristrasnost automatizacije koju odlikuje sklonost ka generalizaciji i odsustvo individualnosti.

[7] Zahtev *human-in-the loop* naglašen je u krivično-procesnom domenu i u oblasti odgovornosti pojedinca za aktivnosti AI iz koje se ostvaruju krivična dela/međunarodna krivična dela, pre svega međunarodna krivična dela u užem smislu (vid. Škulić & Miljuš, 2024, p. 246, pp. 268-269, pp. 275-276).

pravom na slobodu i bezbednost ličnosti. Naime, ESLJP preispituje da li se u konkretnom slučaju može proceniti da postoji „dovoljno činjenica i informacija" koje bi se prema standardu „objektivnog posmatrača" mogle kvalifikovati kao „dovoljne" za zaključak o eventualnim budućim „konkretnim i specifičnim krivičnim delima" (*Ostendorf v. Germany*, predstavka broj 15598/08, presuda ECHR, 7. 3. 2013, par. 80).

## 4. AI sistemi u prognozirajućem radu policije iz vizure pravnog okvira Saveta Evrope

Nakon više opštih preporuka i uputstava donetih u okvirima Saveta Evrope[8] za primenu AI sistema u kontekstu ljudskih prava i sloboda, Savet Evrope usvaja 22. oktobra 2020. godine Rezoluciju Pravda putem algoritma – Uloga AI u policijskim i krivičnim pravosudnim sistemima (Justice by algorithm – The role of artificial intelligence in policing and criminal justice systems, Parliamentary Assembly Resolution 2342 (2020) – CoE Resolution 2342 (2020)). U tekstu Rezolucije konstatuje se raširena primena AI u svetu i u državama članicama u radu policije i krivičnom pravosuđu[9], upotreba nekih AI sistema/razmatranje njihove upotrebe. Domen primene AI je prepoznavanje lica, prognozirajuće policijsko delovanje, identifikacija potencijalnih žrtava krivičnih dela, ocena rizika u postupcima odlučivanja o pritvoru, kaznama, uslovnom otpustu, identifikovanje „hladnih slučajeva" podobnih za rešavanje modernom forenzičkom tehnologijom.

Temeljna ideja je da se upotreba AI u okvirima rada policije, kao i pravosuđa, ne zabrani zbog potencijalnih značajnih koristi, već da se pravno reguliše na nivou država članica („pravni osnov za svaku aplikaciju AI i obradu relevantnih podataka"). Pravo država o upotrebi AI u ovim domenima treba da počiva na univerzalno prihvaćenim osnovnim etičkim principima: 1. transparentnosti, koji obuhvata aspekt pristupačnosti i objašnjivosti i zahteva da se obezbedi da procesi donošenja odluka u AI aplikacijama budu objašnjivi i korisnicima i pogođenim licima; 2. pravde i pravičnosti koja obuhvata nediskriminaciju; 3. odgovornosti čoveka za odluke i dostupnost pravnih lekova; 4. bezbednosti i sigurnosti; 5.

[8] Recommendation CM/Rec(2020)1 of the Committee of Ministers to member States on the human rights impacts of algorithmic systems, Committee of Ministers, 8 April 2020; Unboxing Artificial Intelligence: 10 steps to protect Human Rights, Council of Europe Commissioner for Human Rights, 2019; Guidelines on Artificial Intelligence and data protection, Consultative Committee of the Convention for the protection of individuals with regard to automatic processing of personal data (Convention 108), 25 January 2019; European Ethical Charter on the use of artificial intelligence (AI) in judicial systems and their environment, CEPEJ(2018)14, December 2018.

[9] U našoj literaturi zapaža se težnja da u krivičnom pravosuđu pojedinih država AI dobije ulogu „velike pomoći sudijama u odlučivanju" (Avramović, 2023, p. 170, p. 174).

privatnosti i zaštite podataka (CoE Resolution 2342 (2020), para. 4.1-4.5). Nameće se pozitivna obaveza državama da podvrgavaju AI aplikacije nezavisnom i delotvornom etičkom nadzoru, da obezbede da njihova upotreba bude podložna efikasnom sudskom nadzoru i sprovode početne i periodične, transparentne procene uticaja na ljudska prava.

Istovremeno, upozorava se na osnovne rizike po ostvarivanje principa transparentnosti i odgovornosti: uskraćivanje pristupa izvornom kodu od strane privatnih kompanija na osnovu intelektualne svojine; opasnost nepružanja informacija/objašnjenja potrebnih za osnovno razumevanje funkcionisanja AI sistema; opasnost da neke procese u okviru rada sistema AI čovek neće biti sposoban da razume; zamagljivanje predrasuda i jačanje postojećih predrasuda; nemogućnost da lica na koja se primenjuje AI lako preispituju pojedine tehnike. Ističe se zabrinutost u pogledu jednog od motiva uvođenja AI – donošenje potkrepljenijih odluka. Čovek koji koristi AI sistem usled manjkavosti u domenu transparentnosti neće biti sposoban da donosi odluke na temelju potpunih informacija (CoE Resolution 2342 (2020), par. 7.4).

Komitet ministara Saveta Evrope usvojio je 17. maja 2024. godine Okvirnu konvenciju o AI, ljudskim pravima, demokratiji i vladavini prava (*Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law* – CoE Framework Convention, 2024), otvorenu za potpisivanje na Konferenciji u Viljnusu 5. septembra 2024. godine.[10] Okvirna konvencija prvi je opšti međunarodnopravno obavezujući sporazum čiji je predmet celokupan „životni ciklus sistema AI", sa aspekta ljudskih prava. Odraz je pristupa da se utvrde univerzalni standardi uticaja AI sistema na ljudska prava umesto redefinisanja postojećih ugovora o ljudskim pravima u kontekstu AI (Morawska, 2024, p. 43). Konvencija formuliše sedam načela: ljudsko dostojanstvo i individualna autonomija, jednakost i nediskriminacija, poštovanje privatnosti i zaštita ličnih podataka, transparentnost i nadzor, odgovornost i obaveze, pouzdanost i sigurne inovacije. Sadrži zahteve upućene državama da se identifikuje sadržaj generisan od strane AI (načelo transparentnosti i nadzora iz čl. 8), obezbede mere pouzdanja u sisteme AI i poverenja u njihove rezultate „adekvatnim kvalitetom" i „bezbednošću" (načelo pouzdanosti iz čl. 12), dostupnost pristupačnih i delotvornih pravnih lekova za kršenja ljudskih prava pred nacionalnim organom (čl. 14).

Dostupnost pravnih lekova u bliskoj je vezi sa pravom na informisanje da je upotrebljen AI sistem prilikom generisanja prognoza/donošenja odluke i sa načelom transparentnosti. Transparentnost je suštinski ograničena transparentnost,

[10] Konvenciju su 5. septembra potpisale Andora, Gruzija, Island, Norveška, Republika Moldavija, San Marino, Velika Britanija, Izrael, SAD i Evropska unija, a Crna Gora 5. novembra 2024. godine.

u meri da omogući dovoljno razumevanje funkcionisanja sistema i procesa odlučivanja stručnjacima i licima na koje se prognoze AI primenjuju.[11] Limitirana je i tehničkom izvodljivošću. Suština je otkrivanje informacija, što se u smislu tradicionalnog krivičnog procesnog prava može izjednačiti sa otkrivanjem dokaza/uvidom u spise predmeta. Ogleda se u obezbeđivanju da se postigne „pravi balans između različitih suprotstavljenih interesa" (privatnost, poverljivost, nacionalna bezbednost, zaštita prava trećih, javni red, nezavisnost pravosuđa, „druga razmatranja i zakonski zahtevi") i neophodna prilagođavanja u relevantnim okvirima, a da se pri tome ne menja osnovni režim prava o ljudskim pravima (Explanatory Report, par. 62). Odstupanja od transparentnosti moguća su u interesu javnog reda, bezbednosti i drugih važnih javnih interesa, kako je predviđeno međunarodnim instrumentima ljudskih prava i, gde je to neophodno, da bi se ostvarili ovi ciljevi (Explanatory Report, čl. 14 (99)). Obaveza država je da obezbede dostupnost relevantnih informacija o sistemima AI koji mogu značajno uticati na ljudska prava. Mere države moraju da zadovolje standard „dovoljne mere", da lica koja su pogođena mogu da *ospore odluke* koje su donete/ili da budu informisana suštinski o korišćenju sistema.

## 5. Akt o veštačkoj inteligenciji EU o prognozirajućim policijskim algoritmima

Policija i pravosudne institucije u Evropi koriste AI sisteme da bi uticali na odluke u krivičnom pravosuđu, informisali/podržali donošenje odluka (Nikolinakos, 2023, p. 382, fn. 139 (A)). Na nivou Evropske unije napominje se da prognozirajuće policijsko delovanje, iako može da analizira date skupove podataka za identifikaciju obrazaca i korelacija, ne može da pruži pouzdana predviđanja o ponašanju pojedinca. Načelno se *protivi policijskoj upotrebi AI* za predviđanje ponašanja pojedinaca/grupa na osnovu „istorijskih podataka i prethodnog ponašanja, članstva u grupama, lokacije ili bilo kojih drugih takvih karakteristika, pokušavajući da identifikuje osobe koje će verovatno učiniti krivično delo" (EU Resolution (2020/2016(INI), par. 24). Istovremeno, formulišu se stavovi koji faktički upućuju na neophodnost da se održi *suštinska/značajna uloga čoveka u odlučivanju*.[12] U

[11] Načelo transparentnosti prema redaktorima Konvencije (Explanatory Report to the Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law) ima dva aspekta – „objašnjivost" i „interpretabilnost". Prvi je sposobnost da se pruže „dovoljno razumljiva" objašnjenja zašto sistem AI pravi prognoze / generiše sadržaj / preporučuje / donosi odluke. Drugi je sposobnost *razumevanja kako sistem AI donosi prognoze*/odluke, mera u kojoj se izlazi sistema AI mogu učiniti dostupnim i razumljivim stručnjacima i laicima. Podrazumeva omogućavanje *razumevanja unutrašnjeg funkcionisanja, logike i procesa donošenja odluka* sistema AI korisnicima, uključujući i pogođena lica (Explanatory Report, par. 60-61).

[12] Iz smernica i upozorenja u Rezoluciji EU sledi: 1. AI sistem treba da bude u „službi ljudi"; 2. operater uvek mora da poseduje „*krajnju kontrolu*" i „*mogućnost isključivanja*" AI sistema;

nauci se govori o dovoljnoj i smislenoj diskreciji službenika, velikom uticaju ljudske diskrecije, koja sprečava da algoritam postane *de facto* donosilac odluka (Elyounes, 2021, p. 515). O formiraju standarda zadržavanja čoveka u postupku odlučivanja govori i američka sudska praksa (Cowger, 2020, p. 47). Važno je posedovati svest o tendenciji pojedinaca da odviše veruju u „naizgled objektivnu i naučnu prirodu" AI instrumenta i ne razmatraju opciju da njihovi rezultati mogu da budu „netačni, nepotpuni, irelevantni/diskriminatorski" (EU Resolution (2020/2016(INI), par. 15). Rezolucija se osvrće na temeljna prava pojedinca iz zakonodavstva EU: 1. pravo pojedinca da se ne podvrgne odluci koja ima pravne posledice / značajno utiče na njega, zasnovanoj *isključivo* na automatizovanoj obradi podataka"; 2. zabrana profilisanja koje vodi diskriminaciji prema fizičkim licima na osnovu posebnih kategorija ličnih podataka (EU Resolution (2020/2016(INI), par. 15).

Zakon o veštačkoj inteligenciji (*The Artificial Intelligence Act*) Evropskog parlamenta i Saveta Evropske unije (EU Regulation 2024/1689), čija celovita primena je odgođena dvadeset četiri meseca od stupanja na snagu, 1. avgusta 2024. godine (dalje u tekstu: EU AI Act) ipak ne uvodi apsolutnu zabranu upotrebe prognozirajućih AI algoritama u radu policije. Opredeljenje je rezultat vaganja zahteva za izričitu potpunu zabranu primene AI u prognozirajućem radu policije[13], generalnog potencijalnog značaja upotrebe AI i priznavanja da rad „algoritama za ocenu rizika" i upotreba AI sistema nose ozbiljne inherentne pretnje po ljudska prava i slobode. Odražava načelno opredeljenje za put regulisanja AI u vidu uvođenja zaštitnih garancija od zloupotreba primene AI i povrede osnovnih prava i sloboda. Akt formuliše načelno zabranu faznih i međusobno uslovljenih aktivnosti („zabranjene AI prakse") – plasiranje na tržište, stavljanje u pogon i upotreba sistema AI

3. „ako se ljudi *samo oslanjaju* na podatke, profile i preporuke mašine, neće moći da sprovedu nezavisnu ocenu"; 4. „mora se izbegavati *prekomerna zavisnost*" od rezultata koje pružaju AI sistemi (EU Resolution (2020/2016(INI), par. E; par. 15).

[13] Dominantan argument u prilog zabrani AI sistema u prediktivnom radu policije odnosi se na rizik diskriminacije na osnovu rase, državljanstva, ekonomsko-socijalnog statusa. Praksa upotrebe AI algoritama ukazala je da unosni podaci kojima se kreira i trenira AI sadrže predrasude na štetu manjinskih grupa u Evropi (vid. Fair Trials, 2021). O zalaganju organizacija civilnog društva za zabranu, vid. Nikolinakos 2023, p. 383, fn. 142 (C).

Kada se ukazuje na opasnosti primene AI sistema u prognozirajućem radu policije, navodi se primer Santa Kruza, Kalifornija. Santa Kruz je među prvim gradovima koji su pre više od deceniju uveli prognozirajuće algoritme, prvi grad u SAD koji je zabranio upotrebu prognozirajućih prediktivnih alata, a kasnije, sledeći druge gradove, i softvera za prepoznavanje lica (vid. Sturgill, 2020). Nekoliko gradova u SAD obustavilo je korišćenje sistema prognozirajućeg policijskog delovanja. Policijska odeljenja Njujorka i Kembridža, Masačusetsa, ukinula su ove programe zbog nedostatka efikasnosti, efekta diskriminacije i praktičnog neuspeha, okrenuvši se zajedničkom policijskom delovanju, što je dovelo do opadanja stope kriminala (EU Resolution (2020/2016(INI)), 2021, par. 24).

za prognoziranje rizika da će fizička lica učiniti krivično delo.[14] Zabrana praktično obuhvata uže područje svog delovanja. Pojedini autori dovode u pitanje njenu delotvornost ako se koristi argument ljudske intervencije i široki opšti izuzetak u domenu nacionalne bezbednosti (Levano, 2024, p. 6). Zebnju u pogledu efikasnosti zabrane produbljuje i američka sudska praksa koja razmatra pitanje da li je primenom AI alata zloupotrebljena diskreciona ocena čoveka (vid. *State of Wisconsin v. Eric L. Loomis*) i činjenica da su pionir u primeni prognozirajućih AI alata koji se upotrebljavaju i za odlučivanje o krivičnoj sankciji i potpisnici Okvirne konvencije o AI, upravo SAD.

Prva ograda zabrane upotrebe AI sistema u prognozirajućem radu odnosi se na sisteme *AI zasnovane isključivo* na temelju izrade profila[15] fizičkog lica i proceni njegovih osobina i obeležja ličnosti (Poglavlje II, čl. 5 (d) EU AI Act). Druga je da se sistemi AI mogu primenjivati kao instrument *podrške čoveku* u odlučivanju ako njihovoj upotrebi prethodi ocena čoveka o učešću lica u ostvarivanju krivičnog dela, u vidu postojanja relevantnog stepena sumnje (ocena zasnovana na „objektivnim i proverljivim činjenicama direktno povezanim sa krivičnim delom"). Ovo odgovara ranijem stavu EU da prognozirajuće delovanje policije u kojem se koriste AI sistemi *ne može biti jedini osnov za intervenciju policije* (EU Resolution (2020/2016(INI), 2021, par. 24).

Potrebno je da ovlašćeno službeno lice policije/javni tužilac oceni relevantan stepen sumnje da je pojedinac svojom radnjom zašao u kriminalnu zonu, preduzeo barem kažnjive pripremne radnje za ostvarenje krivičnog dela. Rezultat algoritma može samo da potkrepljuje ocenu da postoji opasnost da će lice učiniti krivično delo, koja esencijalno predstavlja osnov za preventivnu intervenciju policije – lišenje slobode. Formalni razlog formulisanja ove praktično relativne zabrane počiva na garanciji pretpostavke nevinosti,[16] čiji je efekat zahtev da se ocena rizika od vršenja

[14] Predlog Evropske komisije bio je usmeren da se AI prognozirajući sistemi označe kao visokorizični. Evropski parlament je predložio potpunu zabranu. Ukazuje se da je rešenje u AI EU Akt-u plod kompromisa koji u suštini ne ide dalje od zabrane potpuno automatizovanog donošenja odluka u zakonodavstvu EU i zaštite ličnih podataka (vid. Vogiatzoglou, 2025, pp. 28-29).

[15] „Izrada profila" prema Opštoj uredbi o zaštiti podataka (EU) 2016/679 (General Data Protection Regulation 2016/679 – GDP) jeste bilo koji oblik *automatizovane obrade ličnih podataka* koji se „sastoji od upoređivanja ličnih podataka za procenu određenih ličnih aspekata pojedinca, posebno za analizu ili prognoziranje" aspekata u vezi sa njegovim, između ostalog, ličnim sklonostima, interesima, pouzdanošću, ponašanjem, lokacijom ili kretanjem tog pojedinca (čl. 4, st. 1, tač. 4 GDP).

[16] Interesantno je utemeljenje zabrane primene AI sistema u prognozirajućem radu policije na pretpostavki nevinosti. Sud pravde EU „iskristalisao" je stav primenjujući Direktivu o pretpostavci nevinosti – „izrazito minimalistički pristup u tumačenju pretpostavke nevinosti", njenoj primeni isključivo u krivičnom postupku, u uskom domenu, sferi odlučivanja o krivici, isključujući čak i odlučivanje o pritvoru (vid. Nenadić, 2021b, pp. 44-50).

krivičnog dela u budućnosti temelji na *stvarnom/realnom ponašanju lica* (par. 42 Preambule). *Ratio* označavanja neprihvatljivog rizika su sledeći zaključci: 1. oduzimanjem slobode pojedincima i pre nego što su učinila krivično delo za koje su profilisani preusmerava se pažnja sa stvarnog kriminalnog ponašanja na nejasne i diskriminatorske pojmove rizika i sumnje; 2. AI sistemi „nisu pouzdani dokazi stvarne/potencijalne kriminalne aktivnosti i nikada ne bi smeli da se koriste kao 'opravdanje za bilo kakvu policijsku akciju'" (Nikolinakos, 2023, p. 383, fn. 142 (B)). Prognoza rizika od izvršenja krivičnog dela ne može da se zasniva samo na profilisanju, osobinama ili karakteristikama ličnosti kao što su tipične koje se izdvajaju u praktičnom radu: državljanstvo lica, mesto rođenja, mesto boravišta, broj dece, visina duga, marka automobila. Potrebno je da čovek oceni da postoji „razumna sumnja" u pogledu krivičnog dela na bazi objektivno proverljivih činjenica.

Treća ograda, opšti izuzetak u primeni AI sistema, jeste postojanje legitimnog cilja zaštite nacionalne bezbednosti. Četvrta se formuliše u par. 42 Preambule. Zabrana primene AI u prognozirajućem radu policije ne isključuje AI sisteme usmerene na: 1. *targetiranje sumnjivih transakcija* – upotreba analitike rizika „radi ocene izvršenja finansijskih prevara preduzeća na temelju sumnjivih transakcija"; 2. *profilisanje područja/lokacija* – upotreba instrumenata za analizu rizika u cilju predviđanja verovatnoće lokalizacije narkotika / nezakonite robe od strane carinskih tela, na primer na temelju poznatih krijumčarskih ruta. Nije zabranjen softver koji nadzire platne transakcije sa inostranim računima da bi prepoznao obrasce koji ukazuju na pranje novca (Voigt & Hullen, 2024, p. 43), što pravda i hitnost zbog opcije lakog premeštanja imovine i uništavanja dokaza (vid. Matić-Bošković, 2022, p. 464). U pogledu profilisanja područja, ispoljava se zabrinutost da li će praksa rezultirati diskriminacijama pojedinaca (ComputerWeekly, 2022).

## 6. Zaključak

Opasnosti primene policijskih AI „algoritama za ocenu rizika" odnose se na podatke koji se obrađuju (verodostojnost, relevantnost, dozvoljenost obrade), ispravno funkcionisanje sistema i da čovek izgubi krajnju kontrolu nad radom algoritma. Zabrana primene AI sistema u prediktivnom radu policije praktično nije apsolutna. Suštinski, uspostavlja se ograničena zabrana i izgrađivanje pravnog okvira koji obuhvata načela i standarde za regulisanje AI sistema u domenu pravnih sistema država. Podrazumeva minimalizovanje uloge AI sistema. Rezultat rada AI sistema može da ima karakter jedne informacije, veoma limitiranog značaja i kredibiliteta, podržavajućeg faktora / potpore za ocenu rizika. Dva važna načela su: 1. *dominantna uloga čoveka* u odlučivanju – obazrivo vrednovanje izveštaja algoritma

tako što će mu čovek pripisati limitiranu vrednost za odlučivanje / uopšte ga neće vrednovati, u zavisnosti od nedostataka algoritma / nepostojanja zaštitnih garancija za upotrebu AI; 2. *transparentnost rada* algoritma AI, u vezi sa pravom pojedinca da preispituje podatke, funkcionisanje i rezultat algoritma.

Prognozirajući rad policije može imati reperkusije na krivični postupak u sferi policijskog hapšenja zbog postojanja osnovane sumnje u pogledu konkretnog krivičnog dela/faze u ostvarenju krivičnog dela (kažnjive pripremne radnje, pokušaj) i ocene opasnosti da će lice ponoviti izvršenje konkretnog i specifičnog krivičnog dela, dovršiti pokušano krivično delo, ili izvršiti krivično delo kojim preti. Uslov je postojanje relevantnog stepena sumnje u pogledu krivičnog dela u prošlosti i konkretna opasnost od krivičnog dela u bliskoj budućnosti. Lišenje slobode mora biti u određenom cilju u konkretnom krivičnom postupku. Zamislimo da je policija upotrebila AI softver koji je generisao izveštaj o visokom stepenu rizika. Ključni rizici su da lice lišeno slobode nije informisano o primeni AI sistema, da su pojedini predmetni podaci nepotpuni, nemaju dokazni značaj, nisu u vezi sa konkretnim krivičnopravnim događajem ili sadrže diskriminaciju. Načelo raspravnosti, u određenoj meri redefinisano, zahteva da je osumnjičeni upoznat sa primenom AI sistema, analiziranim podacima i funkcionisanjem algoritma u *dovoljnoj meri* da preispituje izveštaj o riziku i odluku o lišenju slobode, ako je ocena rizika uticala na odlučivanje.

## Literatura

Alikhademi, K., Drobina, E., Prioleau, D., Richardson, B., Purves, D. & Gilbert, J. E. 2021. A Review of Predictive Policing from the Perspective of Fairness. *Artificial Intelligence and Law*, 30, pp. 1-17. Dostupno na: https://doi.org/10.1007/s10506-021-09286-4, 23. 1. 2025.

Avramović, D. S. & Jovanov, I. D. 2023. Sudijska (ne)pristrasnost i veštačka inteligencija. *Strani pravni život*, 67(2), pp. 161-177.

Bech, U. 1992. *Risk Society: Towards a New Modernity* (prevod dela: *Risikogesellschaft: Auf dem Weg in eine andere Moderne*. Frankfurt, 1986, prev. Ritter, M.). London/ Newbury Park/ New Delhi: Sage Publications.

Cowger, A. R. 2020. *The Threats of Algorithms and AI to Civil Rights, Legal Remedies, and American Jurisprudence: One Nation under Algorithms*. Lanham: Lexington Books.

Egbert, S. & Krasmann, S. 2019. Predictive Policing: Not yet, but soon Preemptive? *Policing and Society*, pp. 1-15, Dostupno na: https://doi.org/10.1080/10439463.2019.1611821, 23. 1. 2025.

Elyounes, D. A. 2021. "Computer Says No!": The Impact of Automation on the Discretionary Power of Public Officers. *Vanderbilt Journal of Entertainment and Technology Law*, 23(3), pp. 451-516.

Golunova, V. 2023. Artificial Intelligence and the Right to Liberty and Security. In: Quintavalla, A. & Temperman, J. (eds.), *Artificial Intelligence and Human Rights*. Oxford: Oxford University Press, pp. 45-60. Dostupno na: https://doi.org/10.1093/law/9780192882486.003.0003, 22. 1. 2025.

Häuselmann, A. 2022. Disciplines of AI: An Overview of Approaches and Techniques. In: Custers, B. & Fosch-Villaronga, E. (eds.), *Law and Artificial Intelligence: Regulating AI and Applying AI in Legal Practice*. The Hague: Asser Press, pp. 43-72.

Kaufman, M., Egbert, S. & Leese, M. 2019. Predictive Policing and the Politics of Patterns. *The British Journal of Criminology*, 59(3), pp. 674-692.

Matić Bošković, M. 2022. Cybercrime Money Laundering Cases and Digital Evidence. *Strani pravni život*, 66(4), pp. 451-467.

McCulloch, J. & Wilson, D. 2016. *Pre-crime – Pre-emption, Precaution and the Future*. London/New York: Routledge.

Mehozay, Y. & Fisher, E. 2019. The Epistemology of Algorithmic Risk Assessment and the Path towards a Non-penology Penology. *Punishment & Society*, 21(5), pp. 523-541.

Morawska, E. H. 2024. Council of Europe Standards and Activities Related to AI: Towards a Framework Convention on AI and Human Rights. In: Balcerzak, M. & Kapelańska-Pręgowska, J. (eds.), *Artificial Intelligence and International Human Rights Law: Developing Standards for a Changing World*. Cheltenham/Northampton: Edward Elgar Publishing, pp. 25-44.

Mythen, G. 2020. Against the Odds? Unraveling the Paradoxes of Risk Prevention in Counter-Radicalization Strategy. In: Pratt, J. & Anderson, J. (eds.), *Criminal Justice, Risk and the Revolt against Uncertainity*. Cham: Palgavre Machmillan, pp. 167-190.

Nenadić, S. 2017. Pre-crime koncept Zakona o sprečavanju nasilja u porodici – obaveze države i rizici po povredu ljudskih prava. *Strani pravni život*, 61(1), pp. 155-167.

Nenadić, S. 2021a. *Pretpostavka nevinosti sa posebnim osvrtom na praksu Evropskog suda za ljudska prava*. Beograd: Službeni glasnik.

Nenadić, S. 2021b. Pretpostavka nevinosti u pravu EU – korak napred, dva koraka nazad. *Crimen – časopis za krivične nauke*, XII (1), pp. 38-52.

Nenadić, S. & Miljuš, I. 2022. Krivična pravda u eri veštačke inteligencije. U: Kostić, J. & Matić Bošković, M. (eds.), *Digitalizacija u kaznenom pravu i pravosuđu*, tematski zbornik radova međunarodnog značaja, međunarodni naučni skup. Beograd: Institut za uporedno pravo i Institut za kriminološka i sociološka istraživanja u saradnji sa Pravosudnom akademijom, pp. 291-315.

Nikolinakos, N. T. 2023. *EU Policy and Legal Framework for Artificial Intelligence, Robotics and Related Technologies - The AI Act*. Cham: Springer.

Oswald, M., Grace, J., Urwin, S. & Barnes, G. C. 2018. Algorithmic Risk Assessment Policing Models: Lessons from the Durham HART Model and 'Experimental' Proportionality. *Information & Communications Technology Law*, 27(2), pp. 223-250.

Raji, I. & Sholademi, D. B. 2024. Predictive Policing: The Role of AI in Crime Prevention. *International Journal of Computer Applications Technology and Research*, 13(10), pp. 66-78.

Sachoulidou, A. 2023. Going beyond the "Common Suspects": To Be Presumed Innocent in the Era of Algorithms, Big Data and Artifcial Intelligence. *Artifcial Intelligence and Law*, pp. 1-54. Dostupno na: https://doi.org/10.1007/s10506-023-09347-w, 27. 1. 2025.

Situmeang, S. M. T. Mahdi, U., Zulkarnain, P. D., Aziz, H. A. & Nugroho, T. 2024. The Role of Artificial Intelligence in Criminal Justice. *Global International Journal for Innovative Reasearch*, 2(8), pp. 1966-1981.

Stevanović, A. 2022. Uloga veštačke inteligencije u kontroli kriminaliteta. U: Kostić, J. & Matić Bošković, M. (eds.), *Digitalizacija u kaznenom pravu i pravosuđu*, tematski zbornik radova međunarodnog značaja, međunarodni naučni skup. Beograd: Institut za uporedno pravo i Institut za kriminološka i sociološka istraživanja u saradnji sa Pravosudnom akademijom, pp. 343-362.

Strikwerda, L. 2021. Predictive Policing: The Risks Associated with Risk Assessment. *The Police Journal: Theory, Practice and Principles*, 94(3), pp. 422-436.

Škulić, M. 2019. *Krivična dela protiv polne slobode*. Beograd: Službeni glasnik.

Škulić, M. & Miljuš, I. 2024. Artificial Intelligence – Enhanced Uncrewed Aerial Vehicles/Drones in Armed Conflict: Legal Gaps and de lege ferenda Recommendations. In: Безверхов А. Г. (ed.), *Современное международное право: проблемы и вызовы*: *сборник трудов* по итогам Международной научно-практической конференции. Самара: Издательство Самарского университета, pp. 242-279.

Utset, M. A. 2021. Predictive Policing and Criminal Law. In: McDaniel, J. L. M. & Pease, K. G. (eds.), *Predictive Policing and Artificial Intelligence*. London/New York: Routledge, pp. 163-182.

Vogiatzoglou, P. 2025. *Mass Data Surveillance and Predictive Policing: Contested Foundations and Human Rights Impact*. Oxon/New York: Routledge.

Voigt, P. & Hullen, N. 2024. *The EU Al Act: Answers to Frequently Asked Questions*. Berlin: Springer.

Zender, L. 2007. Pre-crime and Post-criminology. *Theoretical Criminology*, 11(2), pp. 261-281.

### *Internet izvori*

ComputerWeekly. 2022. EU Lawmakers Propose Limited Ban on Predictive Policing Systems. Dostupno na: https://www.computerweekly.com/news/252516238/EU-lawmakers-propose-limited-ban-on-predictive-policing-systems, 22. 1. 2025.

Fair Trials, 2021. Fair Calls for Ban on the Use of AI to 'Predict' Criminal Behaviour. Dostupno na: https://www.fairtrials.org/articles/news/fair-trials-calls-ban-use-ai-predict-criminal-behaviour/, 22. 1. 2025.

Fair Trials - Automating Injustice: The Use of Artificial Intelligence & Automated Decision-Making Systems in Criminal Justice in Europe. Dostupno na: https://www.fairtrials.org/articles/news/fair-trials-calls-ban-use-ai-predict-criminal-behaviour/, 22. 1. 2025.

Levano, J. 2024. Predictive Policing in the AI Act: Meaningful Ban or Paper Tiger?. *European Law Blog*. Dostupno na: https://europeanlawblog.eu/2024/07/05/predictive-policing-in-the-ai-act-meaningful-ban-or-paper-tiger/, 27. 1. 2025.

Polizia Moderna, 2015. La chiave del crimine. Dostupno na: https://www.poliziadistato.it/statics/16/la-chiave-del-crimine.pdf, 27. 1. 2025.

Sturgill, K. 2020. Santa Cruz Becomes the First U.S. City to Ban Predictive Policing. *Los Angeles Times*. Dostupno na: https://www.latimes.com/california/story/2020-06-26/santa-cruz-becomes-first-u-s-city-to-ban-predictive-policing, 27. 1. 2025.

### *Sudska praksa*

*Ostendorf v. Germany*, Application no. 15598/08, judgment ECtHR, 7. March 2013. Dostupno na: https://hudoc.echr.coe.int/, 23. 1. 2025.

Supreme Court of Wisconsin, Case No. 2015AP157-CR, *State of Wisconsin v. Eric L. Loomis*, 13.07.2016. Dostupno na: https://law.justia.com/cases/wisconsin/supreme-court/2016/2015ap000157-cr.html, 17. 1. 2025.

The Hague District Court, C-09-550982-HA ZA 18-388, 05-02-2020. Dostupno na: https://gdprhub.eu/index.php?title=Rb._Den_Haag_-_C/09/550982/HA_ZA_18/388, 17. 1. 2025.

### *Pravni izvori*

CoE Framework Convention, 2024. Council of Europe, Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law Council of Europe Treaty Series - No. 225, Vilnius, 5.IX.2024. Dostupno na: https://rm.coe.int/1680afae3c, 28. 1. 2025.

CoE Resolution 2342 (2020). Council of Europe, Parliamentary Assembly Resolution 2342 (2020) Justice by Algorithm – The Role of Artificial Intelligence in Policing and Criminal Justice Systems. Dostupno na: https://pace.coe.int/en/files/28805/html, 28. 1. 2025.

Guidelines on Artificial Intelligence and data protection, Consultative Committee of the Convention for the protection of individuals with regard to automatic processing of personal data (Convention 108), 25 January 2019, T-PD(2019)01, Directorate General of Human Rights and Rule of Law. Dostupno na: https://rm.coe.int/guidelines-on-artificial-intelligence-and-data-protection/168091f9d8, 28. 1. 2025.

GDP Regulation, 2016. General Data Protection Regulation (EU) 2016/679 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 and on the free movement of such data, and repealing Directive 95/46/EC (Text with EEA relevance). *OJ* L 119, 4.5.2016. Dostupno na: https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng, 31. 1. 2025.

EU AI Act, 2024. European Union, The Artificial Intelligence Act – Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Text

with EEA relevance). *OJ* L 2024/1689, 12.7.2024. Dostupno na: https://eur-lex.europa.eu, 21. 1. 2025.

European Ethical Charter on the use of artificial intelligence (AI) in judicial systems and their environment, European Commission for the Efficiency of Justice, 3-4, December 2018, CEPEJ(2018)14. Dostupno na: https://rm.coe.int/ethical-charter-en-for-publication-4-december-2018/16808f699c, 28. 1. 2025.

EU Resolution (2020/2016(INI)), 2021. European Parliament resolution of 6 October 2021 on artificial intelligence in criminal law and its use by the police and judicial authorities in criminal matters (2020/2016(INI). Dostupno na: https://www.europarl.europa.eu/doceo/document/TA-9-2021-0405_EN.html, 29. 1. 2025.

Unboxing Artificial Intelligence: 10 steps to protect Human Rights, Council of Europe, Commissioner for Human Rights, May 2019. Dostupno na: https://www.coe.int/en/web/commissioner/-/unboxing-artificial-intelligence-10-steps-to-protect-human-rights, 28. 1. 2025.