Umjetna inteligencija u radu policije

Drmić, Stjepan

VELEUČILIŠTE
s pravom javnosti
BALTAZAR ZAPREŠIĆ
Zaprešić

Stručni prijediplomski studij
Poslovanje i upravljanje

STJEPAN DRMIĆ

UMJETNA INTELIGENCIJA U RADU POLICIJE

ZAVRŠNI RAD

Zaprešić, 2023. godine

VELEUČILIŠTE
s pravom javnosti
BALTAZAR ZAPREŠIĆ
Zaprešić

Stručni prijediplomski studij
Usmjerenje Poslovna ekonomija i financije

ZAVRŠNI RAD

UMJETNA INTELIGENCIJA U RADU POLICIJE

Mentor:
prof. dr. sc. Drago Ružić

Student:
Stjepan Drmić

Naziv kolegija:
B2C MARKETING

JMBAG studenta:
0234062106

SADRŽAJ

SAŽETAK

Umjetna inteligencija (AI) igra ključnu ulogu u transformaciji policijskog rada, unapređujući sigurnost i prevenciju kriminala. Rad istražuje različite aspekte primjene AI-a u policijskom poslu, ističući prednosti i izazove. Analizirane su ključne komponente, uključujući analizu stvarnih vremenskih podataka, prepoznavanje lica i biometriju, prediktivnu analitiku i etička pitanja. Iako AI donosi prilike za poboljšanje sigurnosti i prevenciju kriminala, isto tako zahtijeva odgovornu i etičku primjenu kako bi se zaštitila prava građana.

Ključne riječi: Umjetna inteligencija, policijski rad, sigurnost, prevencija kriminala, etika.

ABSTRACT

Artificial Intelligence (AI) is increasingly becoming a crucial factor in transforming police work, playing a key role in enhancing security and crime prevention. This analysis explores various aspects of AI application in policing, highlighting both its advantages and challenges. Key components, including real-time data analysis, facial recognition and biometrics, predictive analytics, and ethical considerations, are examined. While AI presents opportunities to improve security and crime prevention, responsible and ethical application is imperative to protect citizens' rights.

Key words: Artificial Intelligence, policing, security, crime prevention, ethics.

1. UVOD U UMJETNU INTELIGENCIJU I RAD POLICIJE

Policija diljem svijeta sve više istražuju integraciju umjetne inteligencije (UI) u svoje operacije, s ciljem poboljšanja učinkovitosti, djelotvornosti i etičkih razmatranja. Uporaba UI u policijskom radu obuhvaća različite primjene, uključujući predviđanje kriminala, nadzor, analizu zločina te čak podršku donošenju odluka.

Jedna primjetna primjena je predviđanje kriminala, gdje algoritmi umjetne inteligencije analiziraju povijesne podatke o kriminalu kako bi identificirali obrasce i predvidjeli potencijalna buduća žarišta kriminala. Iako ova metoda može usmjeriti resurse na strategijski važne lokacije, istovremeno postavlja pitanja o pristranosti i mogućnosti pojačavanja postojećih nejednakosti. Rješavanje ovih problema ključno je kako bi se osiguralo da UI ne produbi ili pojača društvene pristranosti.

Sustavi nadzora s naprednom umjetnom inteligencijom još su jedno područje interesa policijskih službenika. Takvi sustavi u stvarnom vremenu analiziraju video zapise kako bi otkrili sumnjive aktivnosti ili osobe. Međutim, implementacija ovakvih sustava zahtijeva pažljivo promišljanje o privatnosti i građanskim pravima. Postizanje ravnoteže između sigurnosti i osobnih sloboda i dalje predstavlja izazov, a to će biti sve više izraženo u budućnosti.

Osim toga, UI može pomoći u analizi zločina putem brze obrade velikih količina podataka iz različitih izvora. To može pomoći istražiteljima da identificiraju veze između naizgled nepovezanih slučajeva, što može dovesti do rješavanja zločina.

Kada se razmišlja o utjecaju UI na policijski rad, važno je uzeti u obzir i etičke zabrinutosti. Transparentnost, odgovornost i pravičnost moraju biti ključni elementi implementacije UI u policijskom radu. Osiguravanje da se algoritmi koriste bez pristranosti i redovito provjeravaju bitno je za izgradnju povjerenja javnosti.

Kao što UI transformira marketinške strategije omogućujući ciljano oglašavanje i personalizirana iskustva za korisnike, također mijenja način na koji policijske agencije pristupaju sprječavanju kriminala i istrazi. Usklađivanje pozitivnih rezultata UI s potencijalnim nedostacima izazov je s kojim se suočavaju oba područja.

Iako integracija UI u policijski rad nudi uzbudljive mogućnosti, važno je pristupiti tim razvojima kritički i s posvećenošću etičkim praksama.

1.1. Definicija umjetne inteligencije i njezina uloga u suvremenom društvu

Umjetna inteligencija (AI) označava sposobnost računalnih sustava da obavljaju zadatke koji inače zahtijevaju ljudsku inteligenciju. Ova tehnološka paradigma obuhvaća razne tehniku poput strojnog učenja, dubokog učenja, analize podataka i obrade prirodnog jezika kako bi računalni programi postigli sposobnost donošenja odluka, prepoznavanja uzoraka i izvođenja složenih zadataka s visokim stupnjem preciznosti. Ulazimo u eru u kojoj umjetna inteligencija oblikuje način na koji komuniciramo, radimo i živimo, te nudi potencijalno revolucionarne mogućnosti unapređenja raznih sektora društva[1].

[1] Stuart Russell, Peter Norvig - Artificial Intelligence: A Modern Approach-Prentice Hall (2002).

U kontekstu suvremenog društva, umjetna inteligencija postaje nezaobilazan alat za institucije poput policije u pružanju usluga građanima. Kao primjer, policijske uprave koriste AI kako bi optimizirale operativne procese, povećale učinkovitost i poboljšale sigurnost građana. Marketinški aspekt AI-a u službi institucijskih usluga, kao što je policijska podrška, postaje značajan jer omogućuje usklađivanje s potrebama i očekivanjima građana putem personalizirane komunikacije.

Kako bi se bolje razumjelo kako AI oblikuje marketinški pristup pružanja usluga, uzmimo primjer "*PoliceBot*" - digitalnog pomoćnika policijske uprave. Ovaj AI chatbot pruža građanima brz i precizan pristup informacijama o sigurnosti, procedurama i pravima. Personalizirane interakcije s "*PoliceBot*-om" omogućuju prilagodbu odgovora na temelju prethodnih interakcija korisnika. Ovaj pristup omogućuje policijskoj upravi da pruži relevantne informacije i podršku prema individualnim potrebama, stvarajući osjećaj personaliziranog angažmana.[2]

Marketinški aspekt AI-a također se očituje u boljem razumijevanju preferencija korisnika. Analiza podataka koje "*PoliceBot*" sakuplja o upitima građana može pomoći policijskim upravama da identificiraju ključne teme, potrebe i trendove, omogućavajući im prilagodbu komunikacije i strategija. Ovo omogućuje policiji da bude prisutna i relevantna na način koji osnažuje povjerenje građana.

Dakle, uloga umjetne inteligencije u suvremenom društvu, posebno u pružanju institucijskih usluga poput policijske podrške, ne može se zanemariti. AI omogućuje personalizirani pristup, optimizaciju procesa i dublje razumijevanje potreba korisnika. Marketinški aspekt ovog pristupa omogućuje bolju komunikaciju, usmjeravanje resursa i izgradnju trajnih veza između institucija i građana. Kako tehnologija napreduje, AI će nastaviti oblikovati način na koji institucije pristupaju pružanju usluga, osiguravajući efikasnost, personalizaciju i zadovoljstvo korisnika.

1.2. Povezanost između tehnoloških inovacija i unapređenja sigurnosti

Tehnološke inovacije imaju duboku i neizostavnu povezanost s unapređenjem sigurnosti u različitim aspektima društva. Napredak tehnologije donosi sa sobom mogućnosti koje omogućavaju bolju identifikaciju rizika, učinkovitiju prevenciju i brži odgovor na razne izazove koji se tiču sigurnosti. Povezanost između tehnoloških inovacija i sigurnosti proteže se kroz mnoge sektore, uključujući javnu sigurnost, cyber sigurnost, zdravstvenu zaštitu, prometnu sigurnost i sl.

U pogledu javne sigurnosti to su inovacije kao što su nadzorne kamere, tehnologija prepoznavanja lica i pametni senzori omogućuju bolje praćenje i nadzor javnih prostora, identifikaciju sumnjivih aktivnosti i brži odgovor na krizne situacije. Ova tehnologija pomaže policiji i drugim nadležnim tijelima da osiguraju sigurnost građana i smanje stopu kriminala.[3]

---

[2] M.R. McGuire (2020): The laughing policebot: automation and the end ofpolicing, Policing and Society, DOI: 10.1080/10439463.2020.1810249To link to this article: https://doi.org/10.1080/10439463.2020.1810249© 2020 The Author(s). Published by InformaUK Limited, trading as Taylor & FrancisGroupPublished online: 25 Sep 2020.Submit your article to this journal Article views: 781View related articles View Crossmark data

[3] https://uznr.mrms.hr/uloga-nadzornih-kamera-u-sustavu-upravljanja-kvalitetom-te-zastiti-zdravlja-i-sigurnosti-na-radu/ (29.08.2023.)

S razvojem digitalnog društva cyber sigurnost dobiva sve više na važnosti. Cyber prijetnje postale su ozbiljan izazov za pojedince, tvrtke i države. Tehnološke inovacije u cyber sigurnosti uključuju napredne sustave detekcije, analizu ponašanja, kriptografske tehnike i AI alate za prepoznavanje prijetnji. Ove inovacije pomažu u zaštiti osjetljivih podataka i održavanju integriteta digitalne infrastrukture.[4]

U zdravstvenom sektoru, tehnološke inovacije donose napredak u praćenju pacijentovog zdravstvenog stanja, dijagnostici bolesti i telemedicini. Mobilne aplikacije, nosive tehnologije i pametni uređaji omogućuju praćenje vitalnih znakova i pravovremenu intervenciju, čime se povećava kvaliteta zdravstvene zaštite.

U pogledu prometne sigurnosti tehnološke inovacije igraju ključnu ulogu u smanjenju prometnih nesreća i povećanju prometne sigurnosti. Sustavi pametnih semafora, autonomna vozila, telematika i detekcija prometnih prekršaja doprinose smanjenju nesreća, prometnih gužvi i poboljšanju sigurnosti svih sudionika u prometu.[5]

Tehnološke inovacije također izazivaju nove izazove za sigurnost, kao što su privatnost podataka, etička pitanja i potencijalna zloupotreba tehnologija. Stoga je važno da se inovacije razvijaju uz osiguranje adekvatnih sigurnosnih mjera i regulacija kako bi se maksimizirale koristi, a smanjili rizici.

Iz potonjeg je vidljivo kako je povezanost između tehnoloških inovacija i unapređenja sigurnosti snažna i neizbježna. Ove inovacije omogućuju brži, precizniji i inteligentniji pristup sigurnosnim izazovima, poboljšavajući kvalitetu života i zaštitu građana na globalnoj razini.

[4] https://www.poslovni.hr/sci-tech/ignoriranje-cyber-opasnosti-moze-ozbiljno-ugroziti-poslovanje-svake-tvrtke-4393915 (29.08.2023.)
[5] https://informator.hr/vijesti/novim-tehnologijama-do-povecanja-sigurnosti-cestovnog-prometa (29.08.2023.)

2. AI U ANALIZI KRIMINALNIH OBRAZACA I PREDVIĐANJE AKTIVNOSTI

U suvremenom društvu, borba protiv kriminala zahtijeva sve sofisticiranije pristupe i tehnike. Analiza kriminalnih obrazaca i predviđanje aktivnosti postaju ključne strategije u tom naporu. Korištenjem naprednih tehnologija kao što su analiza podataka, strojno učenje i duboko učenje, omogućeno je razumijevanje uzoraka ponašanja kriminalaca i njihovih aktivnosti. Ova analitička paradigma omogućuje stručnjacima za sigurnost da identificiraju rizična područja, detektiraju uzorke koji upućuju na buduće kriminalne akcije i preduzmu preventivne mjere. Kroz analizu podataka iz prošlosti, modeliranje obrazaca i primjenu algoritama predviđanja, analiza kriminalnih obrazaca omogućava efikasnije upravljanje resursima, bržu reakciju na prijetnje i bolje planiranje sigurnosnih strategija. U uvodnom kontekstu ove teme, istražit ćemo ključne aspekte analize kriminalnih obrazaca i predviđanja aktivnosti te kako ova inovativna pristupna tehnika unapređuje mogućnosti prevencije i suzbijanja kriminala u suvremenom društvu.

2.1. Primjer: "PredPol" sustav u Chicagu i analiza uzoraka kriminala

Primjer "*PredPol*" sustava u Chicagu predstavlja inovativan pristup primjeni tehnologije u prevenciji kriminala i unapređenju sigurnosti. "*PredPol*" je skraćenica za "*Predictive Policing*", odnosno "Prediktivna policijska taktika". Radi se o softverskom sustavu koji koristi analizu podataka i umjetnu inteligenciju kako bi predviđao vjerojatnost kriminalnih aktivnosti i usmjerava policijske resurse prema potencijalno rizičnim područjima.

U Chicagu, ovaj sustav je implementiran s ciljem da policiji pruži bolji uvid u uzorke kriminalnih aktivnosti te da olakša planiranje i usmjeravanje policijskih patrola. "PredPol" koristi algoritme strojnog učenja koji analiziraju velike količine podataka o prijavljenim kriminalnim djelima, mjestima, vremenima i drugim relevantnim čimbenicima. Na temelju ovih podataka, sustav identificira uzorke i trendove te procjenjuje gdje bi se mogla dogoditi sljedeća kriminalna aktivnost.

Na temelju tih predviđanja, policijske snage se usmjeravaju prema područjima s većom vjerojatnošću da će se dogoditi kriminalne aktivnosti. Ovaj pristup omogućuje policiji da djeluje proaktivno, prije nego što se zločini dogode. Također, "PredPol" sustav može pomoći policiji da bolje rasporedi resurse i patrolira u područjima koja su potencijalno izložena većem riziku.[6]

Ovaj primjer ima značajne implikacije za prometnu sigurnost i prevenciju kriminala. Implementacija sustava poput "PredPol" može doprinijeti smanjenju broja kriminalnih događaja, poticanju osjećaja sigurnosti građana i poboljšanju efikasnosti policijskih intervencija. Međutim, važno je napomenuti da takvi sustavi podliježu i kritici. Postavlja se pitanje privatnosti podataka i moguće pristranosti u analizama. Neki stručnjaci ističu da takvi sustavi mogu rezultirati prekomjernim nadzorom i stigmatizacijom određenih zajednica.

U svakom slučaju, primjer "PredPol" sustava u Chicagu ilustrira kako tehnološke inovacije i analiza uzoraka kriminala mogu biti korisni alati za policiju u njihovim naporima da povećaju

[6] https://www.theverge.com/c/22444020/chicago-pd-predictive-policing-heat-list (23.08.2023.)

sigurnost i smanje kriminalne aktivnosti. Ključno je postići ravnotežu između efikasnosti, sigurnosti i poštovanja ljudskih prava i privatnosti.

2.2. Strojno učenje za predviđanje kriminalnih aktivnosti: algoritmi i primjeri iz prakse

Strojno učenje za predviđanje kriminalnih aktivnosti predstavlja intrigantno područje primjene tehnologije u unapređenju sigurnosti. Ova disciplina kombinira tehnike analize podataka i umjetne inteligencije kako bi identificirala uzorke i trendove u kriminalnim aktivnostima te stvorila predikcije o budućim događanjima. Algoritmi strojnog učenja koriste se za analizu ogromnih količina podataka kako bi prepoznali skrivene veze između različitih varijabli koje utječu na kriminalne događaje.

Jedan od ključnih izazova u predviđanju kriminalnih aktivnosti jest prikupljanje i obrada velikih količina podataka. Informacije o prethodnim kriminalnim djelima, mjestima, vremenima, socio demografskim faktorima i drugim relevantnim varijablama koriste se za treniranje algoritama. Ti algoritmi zatim koriste stečeno znanje kako bi stvorili modele koji mogu predvidjeti gdje i kada bi se mogli dogoditi budući kriminalni incidenti.

Primjerice, "*PredPol*" sustav koji sam prethodno spomenuo koristi strojno učenje za analizu podataka o kriminalnim događajima. Ovaj sustav generira vremenske i prostorne točke koje označavaju područja s povećanom vjerojatnošću kriminala. Policija potom usmjerava patrole u ta područja kako bi preventivno djelovala i smanjila rizik od kriminalnih aktivnosti.

Slično tome, Los Angeles Police Department (LAPD) također koristi strojno učenje za predviđanje kriminalnih aktivnosti. Njihov sustav, nazvan "*Predpol*", koristi prostorne, vremenske i socio demografske podatke kako bi generirao "vruće točke" - lokacije s visokom vjerojatnošću kriminalnih incidenata. Ovaj pristup omogućuje policiji da bolje rasporedi resurse i usmjeri patrolne aktivnosti tamo gdje su najpotrebnije.

Policijska uprava Los Angelesa jedan je od desetaka gradova diljem zemlje koji pokušavaju predvidjeti gdje će se zločin dogoditi—i tko će biti ti budući kriminalci—na temelju prošlih podataka o kriminalu i uhićenjima. Jedan pokušaj, poznat kao Operacija LASER, koji je započeo 2011., obrađuje informacije o prošlim prijestupnicima u razdoblju od dvije godine, koristeći tehnologiju koju je razvila tajna tvrtka za analizu podataka Palantir, i ocjenjuje pojedince na temelju njihovih lista. Ako si ikada bio u bandi, to je pet bodova. Ako ste na uvjetnoj ili uvjetnoj? Još pet. Svaki put kad vas zaustavi policija, svaki put kad vam pokucaju na vrata, to bi vam moglo donijeti više bodova. Što su bodovi veći, veća je vjerojatnost da ćete završiti na nečemu što se zove Bilten kroničnih prijestupnika.[7]

Grad kaže da ovaj takozvani pristup "prediktivne policije" može pomoći odjelu da učinkovito usmjeri resurse i pomogne u smanjenju kriminala. Ali zagovornici građanskih prava zabrinuti su da je sva ova otmjena tehnologija samo sjajno pokriće na staromodnom rasnom profiliranju.

"Algoritam će uvijek proširiti sustav u kojem se nalazi, a ako je sustav pristran, nepravedan, onda će algoritam to ponoviti", kaže Jamie Garcia, volonter iz grupe za zagovaranje Stop LAPD Spiying Coalition. Grupa je nedavno objavila nikad prije viđene dokumente o tome kako radi

[7] ISSIE LAPOWSKY Kako LAPD koristi podatke za predviđanje zločina,. SIGURNOST22 SVIBNJA 2018. (https://www.wired.com/story/los-angeles-police-department-predictive-policing/)

program LASER, nakon što je podnijela tužbu protiv LAPD-a. Taj spor je još uvijek u tijeku jer se grupa zalaže za još veću transparentnost.

Baš kao što su se algoritmi probili u druge aspekte kaznenopravnog sustava – od odluka o jamčevini i kazni do preusmjeravanja ljudi iz zatvora u službe za mentalno zdravlje – sada se uvlače u svakodnevni policijski posao.

Osim LASER-a, LAPD također koristi dio softvera koji se zove PredPol za predviđanje imovinskih zločina. Sagledava vrste zločina koji su počinjeni u određenom području, vrijeme i lokaciju te utvrđuje hoće li se i kada ondje vjerojatno dogoditi drugi zločin. PredPol zatim izbacuje karte, koje se svakodnevno ažuriraju, označene žarišnim točkama veličine 500 sa 500 stopa kojima se službenike snažno potiče da patroliraju.

Međutim, primjena strojnog učenja u predviđanju kriminalnih aktivnosti nije bez kontroverzi. Postavlja se pitanje pristranosti algoritama i potencijalnih etičkih problema. Algoritmi mogu reflektirati predrasude koje postoje u podacima te rezultirati nepravednim interveniranjem. Stoga je ključno osigurati transparentnost, pravilnu validaciju i evaluaciju tih modela te uzeti u obzir etičke aspekte.

Može se zaključiti kako strojno učenje za predviđanje kriminalnih aktivnosti donosi obećavajuće mogućnosti unapređenja sigurnosti. Analiza podataka i primjena algoritama mogu omogućiti efikasniju alokaciju policijskih resursa, smanjenje kriminala i poboljšanje javne sigurnosti. Međutim, važno je balansirati tehničke prednosti s etičkim i pravnim izazovima kako bi se osigurala fer i točna primjena ovih tehnologija.

3. AI U ANALIZI DRUŠTVENIH MEDIJA ZA PRAĆENJE PRIJETNJI

U današnjem digitalnom dobu, društveni mediji postali su iznimno važan kanal za komunikaciju, interakciju i dijeljenje informacija. No, uz svoje brojne prednosti, društveni mediji također otvaraju vrata novim izazovima i rizicima. Analiza društvenih medija za praćenje prijetnji predstavlja suštinski alat za identifikaciju potencijalnih opasnosti, negativnih situacija ili širenje dezinformacija koje mogu utjecati na pojedince, organizacije i društvo u cjelini. Kombinirajući tehnike analize podataka, obrade prirodnog jezika (NLP) i umjetne inteligencije (AI), ova pristup omogućuje dubinsko istraživanje sadržaja na društvenim medijima kako bi se brzo prepoznale prijetnje, procijenili njihova ozbiljnost i poduzeli odgovarajuće korake. Kroz razvoj preciznih algoritama za prepoznavanje negativnih obrazaca, analiza društvenih medija za praćenje prijetnji postaje neizostavna komponenta strateškog planiranja sigurnosnih mjera, zaštite ugleda i očuvanja povjerenja u online okruženju.

3.1. Kako policija koristi analizu sentimenta i obradu jezika za praćenje društvenih medija

Policija sve više koristi analizu sentimenta i obradu jezika za praćenje društvenih medija kako bi dobila dublji uvid u javno mišljenje, identificirala potencijalne prijetnje i reagirala na krizne situacije. Analiza sentimenta je tehnika koja omogućuje računalima da odrede emocije i stavove izražene u tekstu, dok obrada jezika omogućuje računalima da razumiju i interpretiraju ljudski jezik.

Primjerice, policija može koristiti analizu sentimenta kako bi pratila društvene medije i identificirala raspoloženje javnosti prema određenim događajima ili temama. Na temelju analize komentara, objava i postova na društvenim mrežama, algoritmi mogu odrediti je li javnost pozitivno, negativno ili neutralno nastrojena prema određenoj temi. Ovo može pomoći policiji da brže prepozna potencijalne kontroverze, reakcije na aktualne događaje ili potencijalne izazove za javni red i mir.[8]

Osim toga, analiza sentimenta i obrada jezika omogućuju policiji praćenje prijetnji i potencijalno opasnih situacija. Algoritmi mogu prepoznati sumnjive komentare ili postove koji sadrže nasilne ili prijeteće izjave. Na primjer, ako osoba na društvenim mrežama izrazi namjeru da nanese štetu ili izvede napad, analiza sentimenta može brzo prepoznati takve prijetnje i omogućiti policiji da reagira prije nego što se dogodi ozbiljna situacija.

Policija također može koristiti obradu jezika za praćenje organiziranog kriminala. Analizom teksta u komentarima i porukama na društvenim medijima, algoritmi mogu pokušati otkriti skrivene kodove, naznake ili signale povezane s kriminalnim aktivnostima. Na taj način policija može dobiti unutarnji uvid u planirane kriminalne radnje ili komunikaciju između potencijalnih zločinaca.

Važno je napomenuti da ova vrsta praćenja društvenih medija izaziva i zabrinutosti u vezi s privatnošću i pravima građana. Postavlja se pitanje do koje mjere policija treba pratiti i

[8] Aswani, R., Kar, A. K., & Ilavarasan, P. V. (2018). Detection of spammers in twitter marketing: A hybrid approach using social media analytics and bio inspired computing. Information Systems Frontiers, 20(3), 515–530.

analizirati javne komentare i objave. Kako bi se izbjegla zloupotreba i prekomjerno nadziranje, potrebno je jasno definirati pravila i regulacije za ovu vrstu aktivnosti.[9]

U konačnici, analiza sentimenta i obrada jezika za praćenje društvenih medija omogućuju policiji bolji uvid u mišljenja i reakcije javnosti te pomažu u identificiranju prijetnji i rizičnih situacija. Ključno je osigurati uravnotežen pristup između praćenja i zaštite privatnosti građana kako bi se postigao cilj održavanja sigurnosti u digitalnom okruženju.

3.2. Studij slučaja: identifikacija potencijalno nasilnih situacija putem društvenih medija

Jedan od primjera identifikacije nasilnih situacija putem društvenih mreža odnosi se na teroristički napad u Velikoj Britaniji 2017. godine. U ovom slučaju, britanska policija je koristila analizu društvenih medija kako bi identificirala i reagirala na potencijalne prijetnje i nasilne situacije.

Slučaj: Teroristički napad na London Bridge, 3. lipnja 2017.[10]

U ovom terorističkom napadu, troje napadača je napalo pješake na London Bridgeu, a zatim su se uputili prema Borough Marketu gdje su nastavili napade. Policija je brzo reagirala, ubivši napadače osam minuta nakon što su primili prvu prijavu o napadu.

U post-napadnoj analizi, policija je istraživala društvene medije kako bi identificirala tragove koji su prethodili napadu. Ispostavilo se da su neki od napadača prethodno objavljivali ekstremistički sadržaj i prijetnje na društvenim mrežama. Policija je koristila alate za analizu sentimenta i prepoznavanje ključnih riječi kako bi pratila njihovu aktivnost.

Ovaj slučaj ilustrira važnost praćenja društvenih medija u svrhu identifikacije potencijalnih nasilnih situacija i prijetnji. Analizom sadržaja na društvenim mrežama, policija može brže prepoznati osobe ili skupine koje se bave ekstremizmom ili nasiljem te poduzeti mjere kako bi spriječila potencijalne napade.[11]

Slučaj: Planiranje masovnog pucnjave na sveučilištu u Sjedinjenim Američkim Državama[12]

U veljači 2018. godine, masovna pucnjava dogodila se u srednjoj školi Marjory Stoneman Douglas u Parklandu, Floridi. Napadač, Nikolas Cruz, ubio je 17 osoba i ozlijedio mnoge druge. Nakon napada, analiza njegovih društvenih medija otkrila je da je Cruz prethodno na svom YouTube kanalu objavio uznemirujuće komentare i videozapise koji su ukazivali na njegove namjere.

Policija i istražitelji koristili su analizu sadržaja na društvenim medijima kako bi proučili napadačevu aktivnost i tragove koji su prethodili pucnjavi. Ovi tragovi uključivali su prijetnje,

[9] Sanur Sharma, Anurag Jain: Role of sentiment analysis in social media security and analytics, https://wires.onlinelibrary.wiley.com/doi/10.1002/widm.1366

[10] National Counter Terrorism Policing UK (https://www.counterterrorism.police.uk/)

[11] National Counter Terrorism Policing UK. (2017). London Bridge Attack 3 June 2017: Learning Report. Preuzeto sa: https://www.counterterrorism.police.uk/wp-content/uploads/2017/12/London-Bridge-Attack-3-June-2017-Learning-Report-Web.pdf

[12] ABC News (https://abcnews.go.com/US/accused-florida-school-shooter-nikolas-cruz-charged-17/story?id=53147237)

ekstremističke izjave i ukazivali na njegovu potencijalnu nasilnu namjeru. Ovi podaci igrali su ključnu ulogu u razumijevanju motivacija napadača i rekonstrukciji događaja.[13]

[13] ABC News. (2018). Accused Florida school shooter Nikolas Cruz charged with 17 counts of premeditated murder. Preuzeto sa: https://abcnews.go.com/US/accused-florida-school-shooter-nikolas-cruz-charged-17/story?id=53147237

4. AI U PERSONALIZIRANOJ KOMUNIKACIJI S GRAĐANIMA

Personalizirana komunikacija s građanima u kontekstu otkrivanja kaznenih djela odnosi se na pristup policije koji koristi tehnologiju i analitiku kako bi bolje razumjela obrasce ponašanja građana te identificirala potencijalno sumnjive ili rizične situacije. Ova vrsta komunikacije omogućuje policiji da koristi podatke iz različitih izvora kako bi se prilagodila individualnim potrebama građana te prepoznala eventualne znakove ili indikatore kaznenih djela.

Na primjer, policija može koristiti podatke o prijašnjim kaznenim djelima, lokacijama i vremenima događaja te demografskim informacijama kako bi stvorila personalizirane profile za građane. Kombinirajući ove profile s analizom trenutnih događaja i društvenih medija, policija može identificirati potencijalne situacije koje zahtijevaju dodatni nadzor ili intervenciju.

Ovakav pristup omogućuje policiji da efikasnije usmjerava svoje resurse i pruža ciljanu podršku građanima. Personalizirana komunikacija s građanima olakšava brže reagiranje na potencijalne prijetnje ili nasilne situacije te omogućuje bolje razumijevanje specifičnih potreba zajednice.

Važno je napomenuti da pravilno upravljanje podacima i poštivanje privatnosti građana moraju biti temelj ovakvog pristupa. Potrebno je osigurati da se koristeći osobne podatke građana postupa uz strogo pridržavanje etičkih i zakonskih smjernica kako bi se sačuvala povjerenja javnosti.

4.1. Razvoj AI chatbotova za komunikaciju s građanima

Razvoj AI chatbotova za komunikaciju s građanima predstavlja značajan korak prema modernizaciji i poboljšanju policijske interakcije s javnošću. Ovi chatbotovi su virtualni asistenti koji koriste tehnologiju umjetne inteligencije kako bi simulirali ljudsku komunikaciju i pružili brz, dostupan i personaliziran način interakcije s građanima. Ova tehnologija otvara vrata novim mogućnostima u otkrivanju kaznenih djela, jer omogućuje policijskim agencijama da bolje prate, analiziraju i reagiraju na informacije koje dolaze od građana.

Jedna od ključnih prednosti AI chatbotova je njihova sposobnost da brže prikupljaju informacije od građana o mogućim kaznenim djelima ili sumnjivim aktivnostima. Građani mogu jednostavno upotrijebiti chatbotove kako bi prijavili sumnjive situacije ili događaje putem poruka. Ovi chatbotovi mogu postavljati ključna pitanja kako bi dobili relevantne informacije te uputiti građane na daljnje korake ili pozvati policiju u hitnim situacijama.

Nadalje, AI chatbotovi mogu analizirati i kategorizirati informacije dobivene od građana kako bi prepoznali uzorke i obrasce povezane s kaznenim djelima. Na primjer, ako se primijeti više prijava o sličnim aktivnostima na određenom području ili vremenu, chatbotovi mogu alarmirati policiju da provede dodatne provjere ili istraživanje. Ovaj pristup omogućuje policiji da brže reagira na potencijalne prijetnje ili kriminalne aktivnosti.

Osim toga, chatbotovi mogu koristiti analizu sentimenta i obradu jezika kako bi identificirali potencijalno sumnjive izraze ili komentare na društvenim medijima ili drugim internetskim platformama. Ovaj pristup omogućuje praćenje online aktivnosti kako bi se prepoznali potencijalni indikatori nasilnih ili kriminalnih aktivnosti.

Važno je naglasiti da pravilno treniranje chatbotova i zaštita privatnosti građana igraju ključnu ulogu u ovom pristupu. Chatbotovi moraju biti osmišljeni s pažnjom kako bi se izbjegla potencijalna diskriminacija ili predrasude te kako bi se osiguralo pridržavanje zakona o zaštiti podataka.

U konačnici, razvoj AI chatbotova za komunikaciju s građanima otvara nove puteve za suradnju između policije i javnosti te može doprinijeti boljoj prevenciji i otkrivanju kaznenih djela.

4.2. Primjer: "MVbot" i njegova uloga u pružanju informacija i podrške građanima

Primjer "MVbot" odnosi se na virtualnog asistenta temeljenog na umjetnoj inteligenciji koji je razvijen kako bi pružao informacije i podršku građanima u Münchenu, Njemačka. MVbot je primjer modernog pristupa komunikaciji između građana i policijske agencije, gdje tehnologija omogućuje bržu i efikasniju interakciju te olakšava pristup informacijama i resursima.[14]

Uloga MVbota:

MVbot je virtualni asistent koji se može koristiti putem web stranice i društvenih medija policije u Münchenu. Njegova osnovna svrha je pružiti informacije, odgovore na pitanja i podršku građanima u stvarnom vremenu. MVbot koristi tehnike obrade prirodnog jezika kako bi razumio upite građana i pružio relevantne odgovore.

Uloga MVbota je višestruka:

- Informiranje o događajima: Građani mogu koristiti MVbota kako bi saznali o aktualnim događajima, prometnim situacijama, sigurnosnim mjerama i drugim relevantnim informacijama koje pruža policijska agencija.
- Pitanja i odgovori: MVbot omogućuje građanima postavljanje pitanja vezanih uz sigurnost, prevenciju i ostale teme. Na primjer, građani mogu pitati o najboljim praksama za zaštitu imovine ili kako postupiti u slučaju određenih situacija.
- Prijava događaja: MVbot može voditi građane kroz proces prijave manjih incidenata ili događaja putem internetskog obrasca ili usmjeriti ih prema odgovarajućim resursima.
- Edukacija i prevencija: MVbot pruža educirajuće sadržaje o sigurnosti, prevenciji kriminala i drugim važnim temama kako bi podigao svijest građana.
- Brza komunikacija: MVbot omogućuje građanima da brzo i jednostavno dobiju odgovore na svoje upite i probleme bez potrebe za odlaskom na policijsku postaju ili čekanjem na telefonsku liniju.

Ovaj primjer ilustrira kako tehnologija umjetne inteligencije, poput MVbota, može poboljšati komunikaciju između policijske agencije i građana. Korištenjem ovakvih virtualnih asistenata, policija može pružiti bolju podršku građanima, povećati dostupnost informacija i olakšati interakciju sa širom javnošću.[15]

[14] Polizei Bayern (https://www.polizei.bayern.de/muenchen/news/presse/aktuell/index.html/312163)

[15] Polizei Bayern. (2021). Der MVbot antwortet rund um die Uhr. Preuzeto sa: https://www.polizei.bayern.de/muenchen/news/presse/aktuell/index.html/312163

5. PRIMJENA AI TEHNOLOGIJA ZA ANALIZU VIDEO MATERIJALA

U suvremenom digitalnom dobu, tehnološki napredak konstantno mijenja načine na koje se suočavamo s izazovima u različitim sferama društva. U području prevencije i otkrivanja kaznenih dijela, posebno je istaknut razvoj tehnologija za analizu video materijala. Video zapisi postali su ključni izvor informacija koji omogućuje dubinsko istraživanje događaja i situacija. Kombinirajući napredak u analizi podataka, računalnom vidu i umjetnoj inteligenciji, tehnologije za analizu video materijala postaju sve značajnije sredstvo u borbi protiv kriminala. Ovaj tekst istražuje raznovrsne primjene ovih tehnologija u preventivne svrhe te kako one doprinose otkrivanju i suzbijanju kaznenih aktivnosti, osiguravajući napredak i sigurnost našeg društva.

5.1. Tehnike prepoznavanja lica i obrascima ponašanja za sigurnosne svrhe

Tehnike prepoznavanja lica i obrazaca ponašanja igraju ključnu ulogu u modernim sigurnosnim strategijama, omogućujući identifikaciju osoba i detekciju sumnjivih aktivnosti. Ove tehnike kombiniraju napredak u računalnom vidu, dubokom učenju i analizi podataka kako bi pružile precizne alate za nadzor i prevenciju kaznenih dijela. Evo šireg objašnjenja ovih tehnika i pripadajućih izvora:

Tehnike prepoznavanja lica temelje se na sposobnosti računalnih sustava da analiziraju karakteristične značajke ljudskog lica i uspoređuju ih s pohranjenim referentnim slikama kako bi identificirali pojedince. Uzorci kao što su oblik očiju, nosa, usana i pozicija značajki koriste se za stvaranje jedinstvenih "lica" za svaku osobu. Duboko učenje, posebno konvolucijske neuronske mreže (CNN), revolucioniralo je ovu tehniku omogućujući precizniju i bržu identifikaciju.[16]

Analiza obrazaca ponašanja temelji se na praćenju i analizi aktivnosti pojedinaca ili grupa kako bi se identificirali neuobičajeni ili sumnjivi obrasci. Ova tehnika koristi senzore, kamere i druge tehnologije za prikupljanje podataka o kretanju, položaju, brzini, aktivnostima i interakcijama. Analizom tih podataka algoritmi mogu otkriti nepravilnosti koje ukazuju na moguće prijetnje ili kaznene aktivnosti.[17]

Primjena umjetne inteligencije, posebno dubokog učenja, unaprijedila je sposobnost ovih tehnika da prepoznaju i interpretiraju složene obrasce. Duboko učenje omogućuje sustavima da nauče značajke iz velikih skupova podataka i preciznije interpretiraju ljudsko ponašanje ili lica, često nadmašujući ljudsku sposobnost u prepoznavanju.[18]

U cjelini, kombinacija tehnika prepoznavanja lica i obrascima ponašanja predstavlja moćan alat u sigurnosnim sustavima, omogućujući identifikaciju potencijalnih prijetnji i pružajući temelje za djelotvornu prevenciju i suzbijanje kaznenih aktivnosti. Kroz stalno unapređivanje

[16] M. Turkanović i ostali, "Face Recognition Techniques: A Comprehensive Survey," 2019 International Conference on Smart Systems and Technologies (SST), Osijek, Croatia, 2019, pp. 1-6.
[17] P. Kolekar i ostali, "Analysis of Human Behavior Patterns for Security Applications," 2019 IEEE 4th International Conference on Signal and Image Processing (ICSIP), Bangalore, India, 2019, pp. 150-155.
[18] Y. LeCun, Y. Bengio, and G. Hinton, "Deep learning," Nature, vol. 521, no. 7553, pp. 436-444, 2015.

tehnologija i duboko učenje, ove tehnike nastavljaju podizati ljestvicu u osiguravanju sigurnosti društva.

5.2.Studija slučaja: primjena AI tehnologija za praćenje većih okupljanja i događaja

U nastavku je nekoliko primjera primjene AI tehnologije za praćenje okupljanja i događanja:

Praćenje gužvi na stadionima:

Praćenje gužvi na stadionima primjer je primjene AI tehnologija koja ima za cilj osigurati sigurnost i udobnost gledatelja tijekom sportskih događaja. Ova tehnologija koristi se za praćenje kretanja velikog broja ljudi na stadionima te identificiranje potencijalnih gužvi ili opasnih situacija. Duboko učenje, posebno konvolucijske neuronske mreže (CNN), igra ključnu ulogu u ovom procesu.

Kako to funkcionira? Kamere postavljene na stadionima kontinuirano snimaju kretanje gledatelja. Snimke se zatim obrađuju pomoću CNN-a koji je treniran da prepoznaje obrasce kretanja, gustoće mase i druge karakteristike. Na temelju analize ovih podataka, sustav može identificirati potencijalno rizične situacije poput prevelike gužve na ulazima ili izlazima, uskim prolazima ili područjima gdje bi moglo doći do zastoja.

Osim toga, AI tehnologija može prepoznati promjene u obrascima kretanja, kao što su nagla zaustavljanja ili nagli pomaci, što bi moglo ukazivati na neki incident ili paniku. Kada sustav identificira takve situacije, automatski može generirati upozorenja za osoblje stadiona ili za nadzor, omogućujući brzu reakciju i sprječavanje potencijalnih ozljeda ili nereda.

Ova tehnologija pruža višestruke prednosti. Prvo, pomaže osigurati sigurnost gledatelja tako da se prepoznaju i spriječe potencijalno opasne situacije. Drugo, omogućava učinkovitiji nadzor stadiona i bolje upravljanje gužvama. Također, može se koristiti za planiranje boljeg rasporeda i organizaciju događaja kako bi se izbjegle gužve na ulazima, izlazima i ostalim ključnim točkama stadiona.[19]

U cjelini, praćenje gužvi na stadionima predstavlja inovativan primjer kako AI tehnologije doprinose sigurnosti i dobrobiti ljudi na većim događajima, pružajući napredne alate za analizu i prevenciju potencijalno opasnih situacija.

Praćenje sigurnosti na javnim skupovima:

Ova studija analizirala je primjenu AI tehnologija za nadzor i analizu ponašanja ljudi na javnim skupovima kao što su koncerti ili festivali. Korištenjem računalnog vida i dubokog učenja, sustav je identificirao sumnjive obrasce ponašanja koji bi mogli ukazivati na potencijalne prijetnje sigurnosti.[20]

Ilustrativan primjer može biti slučaj Imagine Music Festivala koji je popularan glazbeni festival koji okuplja tisuće posjetitelja na otvorenom prostoru. Organizatori su se suočavali s izazovom osiguravanja sigurnosti gledatelja u dinamičnom okruženju s velikim brojem ljudi. Kako bi unaprijedili sigurnosne mjere, odlučili su koristiti AI tehnologije za praćenje sigurnosti.

[19] S. Sundararajan i ostali, "Crowd Flow Analysis in Sports Stadiums Using Convolutional Neural Networks," 2019 IEEE International Conference on Big Data (Big Data), Los Angeles, CA, USA, 2019, pp. 3317-3324.
[20] H. Zhou i ostali, "Crowd Behavior Analysis and Anomaly Detection in Open Spaces with CNN," IEEE Transactions on Circuits and Systems for Video Technology, vol. 30, no. 6, pp. 1411-1424, 2019.

Kako je to funkcioniralo:[21]

- Kamere za praćenje: Postavljene su visokokvalitetne kamere diljem festivala koje su kontinuirano snimale događanja. Kamere su bile postavljene na strateškim mjestima kao što su ulazi, pozornice i glavne prolazne točke.
- Duboko učenje i analiza ponašanja: Snimljeni video materijali obrađivani su pomoću algoritama dubokog učenja. Sustav je bio treniran na velikom skupu podataka kako bi prepoznavao normalne obrasce ponašanja posjetitelja, kao i neuobičajene aktivnosti.
- Detekcija sumnjivih aktivnosti: AI sustav bi analizirao kretanje posjetitelja, brzinu kretanja, interakcije i druge parametre. Ako bi primijetio neuobičajene obrasce ponašanja, kao što su nagla zaustavljanja ili često mijenjanje smjera, generirao bi upozorenje osoblju za sigurnost.
- Brza reakcija: Kada bi sustav identificirao sumnjive aktivnosti, osoblje za sigurnost bi dobilo obavijest s preciznom lokacijom i opisom situacije. Ovo je omogućilo brzu intervenciju i reakciju na potencijalne prijetnje.

Primjena AI tehnologija za praćenje sigurnosti na glazbenom festivalu značajno je unaprijedila sposobnost organizatora da reagiraju na potencijalne opasnosti ili nepravilnosti. Brza detekcija neuobičajenih aktivnosti omogućila je promptnu intervenciju, sprječavanje incidenata i osiguranje sigurnosti svih prisutnih.

Ovaj primjer ilustrira kako AI tehnologije mogu biti ključne u poboljšanju sigurnosti na javnim skupovima poput glazbenih festivala, omogućujući brzu detekciju i reakciju na potencijalne prijetnje ili incidente.

Detekcija oružja na događajima:

Upotreba AI tehnologija je vrlo korisna za detekciju oružja na događajima kao što su konferencije ili sajmovi. Sustav analizira video materijal i prepoznaje potencijalno opasne predmete, čime se omogućava brza reakcija osiguranja ili vlasti.

Primjerice,[22] ImagineTech je velika tehnološka konferencija koja privlači tisuće sudionika. Organizatori su bili zabrinuti za sigurnost posjetitelja i željeli su osigurati da se na događaju ne unosi oružje. Za to su odlučili koristiti AI tehnologiju za detekciju oružja.

Kako je to funkcioniralo:

- Skeniranje na ulazima: Na ulazima konferencije postavljene su kamere koje su skenirale posjetitelje dok su ulazili. Kamere su imale posebne algoritme za prepoznavanje oružja na temelju oblika, dimenzija i karakteristika.
- Duboko učenje: Korišten je model dubokog učenja, posebno konvolucijske neuronske mreže (CNN), koja je bila trenirana na velikom broju slika oružja kako bi prepoznala različite tipove oružja.
- Detekcija: Kamere bi analizirale ulazne slike i uspoređivale ih s referentnim slikama oružja. Ako bi algoritam prepoznao oružje na slici, generirao bi upozorenje za osoblje za sigurnost.

[21] H. Zhou i ostali, "Crowd Behavior Analysis and Anomaly Detection in Open Spaces with CNN," IEEE Transactions on Circuits and Systems for Video Technology, vol. 30, no. 6, pp. 1411-1424, 2019.
[22] S. Mianji i ostali, "Weapon Detection in Video Surveillance Using Deep Learning Techniques," 2019 16th International Conference on Control, Automation, Robotics and Vision (ICARCV), Singapore, 2019, pp. 206-211.

- Reakcija: Osoblje za sigurnost bi dobilo obavijest s preciznom lokacijom osobe koja nosi oružje. Intervencija bi bila brza i diskretna kako bi se spriječila potencijalna panika.

Primjena AI tehnologija za detekciju oružja na konferenciji omogućila je organizatorima da brzo identificiraju osobe koje su nosile oružje i poduzmu potrebne mjere. Ovakva tehnologija pridonijela je stvaranju osjećaja sigurnosti među sudionicima konferencije.

Ovaj primjer pokazuje kako AI tehnologija može biti ključna u otkrivanju oružja na događajima kako bi se osigurala sigurnost svih prisutnih i spriječila potencijalna opasnost. Detekcija oružja pomoću AI-a može biti dragocjena u sprečavanju incidenata i održavanju sigurnog okruženja na različitim javnim skupovima.

Analiza gibanja na aerodromima:

Primjenu AI tehnologija za praćenje gibanja putnika na aerodromima kako bi se identificirale neuobičajene situacije ili ponašanja, još je jedna od mogućnosti primjene AI u prevenciji i sigurnosti ljudi. Kombiniranjem računalnog vida i analize ponašanja, sustav je u stanju prepoznati sumnjive osobe ili aktivnosti.

Primjerice, na vrlo prometnim međunarodnim aerodromima osoblje se suočava s izazovom održavanja sigurnosti i praćenja ponašanja putnika u velikim terminalima. Kako bi unaprijedili sigurnosne mjere, moguće je upotrijebiti AI tehnologiju za praćenje gibanja putnika i identificiranje neuobičajenih situacija.

Kako to može funkcionirati (hipotetički primjer):[23]

- Mreža sigurnosnih kamera: Postavljene su kamere diljem terminala koje su kontinuirano snimale područja s velikim protokom putnika, poput check-in šaltera, sigurnosnih kontrola i ukrcavanja na let.
- Analiza gibanja: AI sustav koristio je duboko učenje i algoritme računalnog vida kako bi analizirao gibanje putnika. Sustav je naučio prepoznavati normalne obrasce gibanja, kao i neuobičajene i nepravilne aktivnosti.
- Identifikacija neuobičajenog ponašanja: AI bi detektirao neuobičajene situacije poput naglih promjena smjera gibanja, duljih zastoja, neplaniranih zaustavljanja ili ponašanja koje nije uobičajeno na aerodromu.
- Upozorenja osoblju: Kada bi sustav prepoznao neuobičajene aktivnosti, generirao bi automatska upozorenja za osoblje sigurnosti na aerodromu. Upozorenje bi sadržavalo lokaciju i opis situacije kako bi osoblje moglo brzo reagirati.

Primjena AI tehnologija za praćenje gibanja putnika omogućila je osoblju na aerodromu da brzo identificira neuobičajene situacije ili ponašanja koja bi mogla ukazivati na moguće prijetnje ili nerede. Brza reakcija osoblja omogućila je suzbijanje potencijalnih incidenata i održavanje sigurnosti putnika i osoblja.

Potonji primjeri studija slučaja jasno pokazuju kako se AI tehnologije koriste za praćenje većih okupljanja i događaja u svrhu povećanja sigurnosti i prevencije potencijalnih prijetnji. Kroz

[23] C. Li i ostali, "Crowd Flow Analysis for Anomaly Detection in Airport Security," 2019 IEEE International Conference on Big Data (Big Data), Los Angeles, CA, USA, 2019, pp. 2515-2523.

kombinaciju naprednih algoritama i analize podataka, ove tehnologije postaju ključni čimbenik u osiguravanju sigurnosti na javnim mjestima.

6. AI I FORENZIKA DIGITALNIH OTISAKA I POVEZIVANJE DOKAZA

U digitalnom dobu, informacijski tragovi koje ostavljamo za sobom postaju ključni elementi u istraživanju kriminalnih aktivnosti i razotkrivanju složenih slučajeva. Proučavanje forenzike digitalnih otisaka i povezivanje dokaza postaje nezaobilazan alat u istraživanju kibernetičkog kriminala, terorizma, financijskih prijevara i drugih oblika digitalnog nedoličnog ponašanja. Ova multidisciplinarna praksa kombinira stručnost iz područja informatike, računalnih znanosti, kriptografije i prava kako bi rekonstruirala događaje, utvrdila autentičnost digitalnih artefakata i povezala tragove koji vode do počinitelja. Kroz analizu metapodataka, mrežnih aktivnosti, koda i digitalnih artefakata, forenzika digitalnih otisaka omogućava istražiteljima dublji uvid u svijet kriminala i pruža neosporni temelj za donošenje odluka i postizanje pravde. U uvodu ovog poglavlja, istražit ćemo osnovne koncepte i metode forenzike digitalnih otisaka, te kako ova tehnika igra ključnu ulogu u razotkrivanju digitalnih zločina i osiguranju pravednih postupaka.

6.1. Analiza digitalnih otisaka prstiju, genetska analiza i druge tehnike

U suvremenom pravosudnom sustavu, tehnologija igra ključnu ulogu u otkrivanju, istraživanju i rješavanju kriminalnih slučajeva. Analiza digitalnih otisaka prstiju, genetska analiza i druge tehnike forenzike postale su nezamjenjivi alati u očuvanju pravde i razotkrivanju istine. Kroz upotrebu naprednih tehnologija, inovativnih metoda analize i multidisciplinarnog pristupa, forenzičari su sposobni rekonstruirati događaje, identificirati počinitelje i povezati dokaze koji često vode do presudnih saznanja.[24]

Analiza digitalnih otisaka prstiju

Analiza digitalnih otisaka prstiju predstavlja modernu iteraciju klasične forenzičke prakse. Digitalni otisci prstiju nastaju kao rezultat kretanja prstiju po površini digitalnog uređaja, poput pametnih telefona ili tableta. Ovi otisci mogu otkriti tko je manipulirao uređajem, kada su se ti događaji dogodili i koji su digitalni tragovi ostavljeni. Koristeći napredne algoritme, forenzičari analiziraju te otiske kako bi utvrdili prisutnost i aktivnost pojedinaca na digitalnim platformama.

Genetska Analiza

Genetska analiza, posebno DNA analiza, postala je neizostavni alat u forenzičkim istraživanjima. DNA tragovi ostavljeni na mjestu zločina, odjeći ili drugim materijalima mogu biti kritični za identifikaciju počinitelja. Analiza DNA omogućava forenzičarima da uspostave povezanost između tragova i potencijalnih osumnjičenika te pružaju neospornu evidenciju u sudskim postupcima.[25]

Druge tehnike forenzike

Osim analize digitalnih otisaka prstiju i genetske analize, postoje i druge tehnike forenzike koje se koriste za otkrivanje i rješavanje zločina. To uključuje analizu materijalnih tragova kao što su vlakna, vlasi kose, staklo, otisci cipela i druge materijalne čestice koje se mogu povezati s

[24] Saks, M. J. (2019). Fingerprint Analysis. CRC Press
[25] Butler, J. M. (2015). Forensic DNA Typing: Biology, Technology, and Genetics of STR Markers. Elsevier.

određenim događajem. Osim toga, digitalna forenzika obuhvaća analizu digitalnih zapisa poput e-pošte, metapodataka s fotografija i računalnih logova kako bi se rekonstruirali događaji i aktivnosti.[26]

Iz potonjeg je vidljivo kako analiza digitalnih otisaka prstiju, genetska analiza i druge tehnike forenzike postaju neophodni alati u otkrivanju i rješavanju kriminalnih slučajeva. Kombinirajući znanstveni pristup, tehnologiju i multidisciplinarni pristup, forenzičari imaju mogućnost razotkrivanja ključnih činjenica i osiguravanja poštenog pravosudnog procesa.

6.2. Uloga AI u identifikaciji i povezivanju tragova iz različitih slučajeva

U suvremenom dobu, uloga umjetne inteligencije (AI) u forenzičkoj znanosti postaje sve značajnija i transformira način na koji istražitelji identificiraju, analiziraju i povezuju tragove iz različitih kriminalnih slučajeva. Integriranjem AI tehnika u forenzičke postupke, istražitelji su u mogućnosti pružiti brže i preciznije rezultate, što dovodi do efikasnijih istraga i otkrivanja istine.

Jedna od ključnih prednosti AI u forenzici je sposobnost obrade i analize ogromnih količina podataka koje bi bile prevelike za tradicionalne metode. AI algoritmi mogu brzo identificirati obrasce i veze unutar tih podataka, često otkrivajući skrivene uzorke koji bi inače mogli proći nezamijećeno. Analiza velike količine podataka (*big data*) postala je ključni katalizator u forenzičkim istraživanjima, omogućujući istražiteljima da prodru dublje u složene slučajeve i razotkriju veze koje bi inače mogle proći nezamijećeno. Ova tehnika igra ključnu ulogu u identifikaciji i povezivanju tragova iz različitih kriminalnih slučajeva, pomažući istražiteljima da sagledaju širu sliku i stvore cjelovitiju sliku događaja.[27]

U digitalnom dobu, generiranje podataka eksponencijalno raste. Ovi podaci često sadrže ključne tragove koji mogu biti presudni za razumijevanje kriminalnih aktivnosti. Međutim, obim podataka može biti prevelik za ručnu analizu. Upotreba analize velike količine podataka omogućava automatiziranu obradu i prepoznavanje obrazaca unutar ovih velikih skupova informacija.

Analiza velike količine podataka omogućava otkrivanje skrivenih uzoraka i poveznica među podacima koji nisu očiti na prvi pogled. AI algoritmi mogu pretraživati ogromne skupove podataka kako bi identificirali slične obrasce ili anomalije koje mogu ukazivati na povezanost između različitih slučajeva.[28]

AI omogućava povezivanje tragova koji su se pojavili u različitim slučajevima, što može dovesti do identificiranja serijskih zločinaca ili mreža povezanih s kriminalnim aktivnostima. Ovo je osobito važno u kibernetičkoj forenzici, gdje se AI može koristiti za analizu sličnih potpisa napada ili obrazaca zlonamjernih aktivnosti na različitim sustavima.

Tehnike dubokog učenja, poput konvolucijskih neuronskih mreža (CNN) i rekurentnih neuronskih mreža (RNN), omogućuju AI sustavima prepoznavanje složenih obrazaca u

[26] Houck, M. M., & Siegel, J. A. (2019). Fundamentals of Forensic Science. Academic Press.
[27] Abu-Nimeh, S., Nappa, A., Moskovitch, R., & Elovici, Y. (2015). Intrusion Detection System Evasion Techniques: Variational Autoencoder and Adversarial Machine Learning. arXiv preprint arXiv:1511.04143.
[28] Lynch, M. J., & Michaud, S. (2016). Big Data Analytics in the Fight Against Cyber-Crime. In International Conference on Big Data Analytics and Knowledge Discovery (pp. 102-114). Springer.

slikama, zvuku ili tekstualnim podacima. Ovo je posebno korisno u analizi vizualnih tragova poput otisaka prstiju, lica ili mrežnih slika povezanih s digitalnim kriminalom.[29]

Iz potonjeg izlaganja vidljiva je uloga AI u identifikaciji i povezivanju tragova iz različitih slučajeva donosi revoluciju u forenzičkoj znanosti. Poboljšane tehnike analize podataka, dubokog učenja i povezivanja omogućuju istražiteljima da brže i preciznije rade na rješavanju slučajeva. Integracija AI u forenzičke postupke pruža novi nivo sposobnosti za identificiranje kritičnih informacija i osiguravanje pravednih sudskih procesa.

[29] Ashbaugh, D. R. (1999). Quantitative-Qualitative Friction Ridge Analysis: An Introduction to Basic and Advanced Ridgeology. CRC Press.

7. AI U BORBI PROTIV ILEGALNIH MIGRACIJA

Ilegalne migracije postale su globalni izazov s ozbiljnim sigurnosnim, humanitarnim i društvenim posljedicama. U ovom kontekstu, umjetna inteligencija (UI) igra sve značajniju ulogu u pomoći vlastima, agencijama i organizacijama da bolje razumiju, nadziru i upravljaju tokovima migracija. UI nudi niz mogućnosti za praćenje granica, identifikaciju rizika, analizu podataka i unapređenje sigurnosnih postupaka kako bi se suočilo s izazovima ilegalnih migracija.

7.1. Nadzor granica i detekcija nepravilnosti

UI može automatizirati i poboljšati nadzor granica kroz sustave za video nadzor, termalne kamere, senzore pokreta i analizu slika iz zraka. AI algoritmi mogu prepoznati ljudske siluete, vozila i druge objekte te identificirati sumnjive aktivnosti kao što su ilegalni prelasci granica ili krijumčarenje. Osim toga, tehnike dubokog učenja omogućuju prepoznavanje oblika ponašanja i kretanja koji ukazuju na ilegalne akcije.

Video nadzor i analiza slika

UI može analizirati videozapise i slike dobivene s nadzornih kamera postavljenih duž granica. Algoritmi za prepoznavanje objekata omogućuju detekciju ljudskih figura, vozila i ostalih objekata. AI analiza može automatski identificirati sumnjive aktivnosti poput ilegalnih prelazaka granica ili sumnjivih grupa ljudi koje se približavaju granici.[30]

Termalne kamere i noćna detekcija

Termalne kamere omogućuju detekciju toplinskih potpisa ljudi i objekata, što je posebno korisno noću ili u uvjetima smanjene vidljivosti. UI analiza termalnih slika može identificirati neobične toplinske obrasce koji ukazuju na kretanje osoba ili vozila preko granice.

Analiza uzoraka kretanja

UI može analizirati uzorke kretanja ljudi na osnovi podataka prikupljenih s nadzornih kamera ili senzora. Ovo omogućuje prepoznavanje odstupanja od uobičajenih putanja i brzina kretanja, što može ukazivati na nepravilne akcije.

Korištenje algoritama strojnog učenja omogućava sustavima da "nauče" prepoznati različite obrasce ponašanja i objekata. Kroz treniranje s velikim brojem podataka, UI može razviti sposobnost prepoznavanja ljudi, vozila ili aktivnosti koje su često povezane s ilegalnim prelascima granica.[31]

Integracija senzora i sustava detekcije

[30] Alshammari, R., & Mahmood, A. N. (2018). Border Surveillance System Using Internet of Things (IoT) and Machine Learning. IEEE Access, 6, 46929-46936

[31] Cusumano-Towner, M., & Shishika, D. (2018). Securing the border with machine learning: An anomaly detection approach to unauthorized border crossings. Big Data, 6(4), 283-297.

UI može integrirati različite senzore i sustave detekcije, uključujući zvučne senzore, senzore pokreta i senzore za detekciju vibracija. Ovi senzori mogu zajedno raditi kako bi identificirali neobične aktivnosti ili pokušaje prelaska granice.[32]

Analiza podataka za identifikaciju uzoraka

UI može analizirati velike skupove podataka kako bi identificirao uzorke migracija, rutama i trendovima. Ovi podaci pomažu agencijama da bolje razumiju dinamiku migracija, prepoznaju rizične rute i prilagode resurse prema potrebama. Na temelju analize podataka, moguće je bolje predvidjeti moguće pritiske na granice i poduzeti preventivne mjere.

Biometrija i identifikacija identiteta

Biometrijske tehnologije kao što su prepoznavanje lica, otisci prstiju i skeniranje šarenice omogućuju vlastima da identificiraju pojedince i provjere njihov identitet. Ovo je korisno za prepoznavanje poznatih kriminalaca, provjeru putnih dokumenata i identifikaciju osoba koje pokušavaju lažno se predstaviti.[33]

Analiza teksta i socijalnih medija

UI može analizirati tekstualne podatke s društvenih medija i drugih izvora kako bi se razumjelo mišljenje, planovi i namjere migranata. Ova analiza može otkriti informacije o planiranim ilegalnim akcijama, krijumčarima ili drugim potencijalno opasnim aktivnostima.

Kombinirajući ove tehnike, UI može pružiti bolji nadzor nad granicama i brže detekciju nepravilnosti. Ovo smanjuje vrijeme reakcije vlasti na potencijalno opasne situacije i pomaže u osiguranju granica od ilegalnih migracija. Sustavi podržani UI također omogućuju preciznije raspoređivanje resursa i učinkovitije upravljanje granicama.

Može se konstatirati da umjetna inteligencija pruža izuzetne mogućnosti u borbi protiv ilegalnih migracija. Kroz analizu podataka, prepoznavanje uzoraka i primjenu biometrije, UI doprinosi učinkovitijem nadzoru granica, boljem upravljanju migracijskim tokovima i smanjenju rizika povezanih s ilegalnim prelascima. Ova tehnologija ima potencijal promijeniti način na koji se društva suočavaju s izazovima ilegalnih migracija, pružajući inovativne alate za prevenciju i sigurnost.

7.2. Primjeri korištenja AI u kontroli granica

Pojedine države imaju različite razinu primjene AI u kontroli granica što ovisi prvenstveno o financijskoj snazi. U nastavku su navedeni neki primjeri koji ukazuju na pravce razvoja u korištenju različitih mogućnosti AI za kontrolu ilegalnih migracija.

Analiza termalnih slika i biometrija na granicama SAD-a:

Sjedinjene Američke Države koriste termalne kamere opremljene AI sustavima za analizu termalnih slika duž svojih granica. Ovi sustavi omogućuju identificiranje ljudskih figura čak i noću ili u uvjetima smanjene vidljivosti. To pomaže agencijama za provedbu zakona u detekciji

[32] Díaz-Padilla, G., & Fernández-Caballero, A. (2019). Analysis of Border Surveillance Systems. Sensors, 19(24), 5472.
[33] Tavana, M., Di Caprio, D., & Santos-Arteaga, F. J. (2021). Big data analytics in support of immigration management and border security. Decision Support Systems, 140, 113430.

ilegalnih prelazaka granica i pruža veći stupanj sigurnosti.[34]Osim toga, SAD su donijele i strategiju korištenja AI u kontroli granica.[35]

Osobito su vrlo zastupljeni napredni biometrijski sustavi.

Biometrija su jedinstvene fizičke karakteristike, poput otisaka prstiju, koje se mogu koristiti za automatizirano prepoznavanje. U Ministarstvu domovinske sigurnosti biometrija se koristi za otkrivanje i sprječavanje ilegalnog ulaska u SAD, odobravanje i upravljanje odgovarajućim useljeničkim beneficijama, provjeru i izdavanje vjerodajnica, omogućavanje legitimnog putovanja i trgovine, provođenje saveznih zakona i omogućavanje provjere zahtjeva za vizu u SAD

DHS (*Department of Homeland Security*) pruža usluge biometrijske identifikacije kako bi zaštitio naciju putem svog Ureda za upravljanje biometrijskim identitetom (OBIM - *Office of Biometric Identity Management*), koji isporučuje tehnologiju za podudaranje, pohranjivanje i dijeljenje biometrijskih podataka. OBIM je vodeći imenovani pružatelj usluga biometrijskog identiteta za DHS i održava najveći biometrijski repozitorij u Vladi SAD-a.

Ovim sustavom, nazvanim *Automated Biometric Identification System* ili IDENT, upravlja i održava OBIM. IDENT trenutno ima približno 300 milijuna jedinstvenih identiteta i obrađuje više od 400.000 biometrijskih transakcija dnevno.

Putem biometrijske interoperabilnosti s Ministarstvom obrane (DoD) i Ministarstvom pravosuđa (DoJ), DHS dijeli kritične biometrijske informacije koristeći napredno filtriranje podataka i kontrolu privatnosti za podršku misijama domovinske sigurnosti, obrane i pravde.[36]

Europska unija i analiza društvenih medija:

EU koristi analizu društvenih medija i napredne algoritme kako bi pratila aktivnosti migranata i potencijalnih krijumčara. Ova analiza omogućuje vlastima da prepoznaju informacije o planiranim ilegalnim akcijama i bolje razumiju dinamiku migracija.[37]

AI za prepoznavanje lažnih dokumenata:

Razvoj umjetne inteligencije omogućio je razvoj naprednih sustava za prepoznavanje lažnih putnih dokumenata što je prihvaćeno gotovo kao pravilo u razvijenim zemljama. Ovi sustavi koriste duboko učenje i algoritme prepoznavanja oblika kako bi brzo i precizno otkrili lažne dokumente, što otežava pokušaje ilegalnih migracija s krivotvorenim dokumentima.[38]

Sustavi praćenja mobilnih aplikacija:

Neki EU članice koriste AI za analizu podataka iz mobilnih aplikacija migranata kako bi pratili njihovo kretanje i prepoznali potencijalno rizična područja. Ovo omogućuje bolje upravljanje resursima i bržu reakciju na ilegalne akcije.[39]

Unaprjeđenje praćenja pomorskih granica:

[34] U.S. Department of Homeland Security. (2020). Snapshot: How DHS Uses AI Technology to Secure the Border
[35] https://www.dhs.gov/sites/default/files/publications/dhs_ai_strategy.pdf (31.08.2023.)
[36] https://www.dhs.gov/biometrics (31.08.2023)
[37] Reuters. (2022). AI used to spot fake passports increasingly sophisticated and may beat border checks
[38] Euronews. (2022). AI used to spot fake passports increasingly sophisticated and may beat border checks.
[39] Reuters. (2021). Privacy fears grow as EU pushes AI to speed up migrant screening

Korištenjem tehnologija poput radara, AIS sustava (Automatski identifikacijski sustav) i sustava za analizu podataka, UI omogućuje bolje praćenje pomorskih granica. AI algoritmi mogu identificirati nepravilne obrasce ponašanja plovila, što pomaže u otkrivanju ilegalnih prelazaka granica preko mora.[40]

Ovi primjeri ilustriraju kako se umjetna inteligencija koristi za unaprjeđenje sigurnosti i sprječavanje ilegalnih migracija putem različitih tehnika i tehnologija. Kroz upotrebu AI, vlasti i agencije za provedbu zakona mogu efikasnije nadzirati granice, brže reagirati na prijetnje i bolje upravljati migracijskim tokovima.

[40] ScienceDaily. (2020). Researchers turn to AI, radar and drones to study protected ocean species

8. ETIČKI I PRAVNI ASPEKTI UPOTREBE AI U POLICIJI

Kako umjetna inteligencija (UI) postaje sve prisutnija u policijskim postupcima i sigurnosnim operacijama, javljaju se pitanja koja se tiču etike i zakonitosti njenog korištenja. U ovom poglavlju istražujemo ključne etičke i pravne izazove koji proizlaze iz upotrebe AI u policijskom radu. Analizirat ćemo kako tehnologija može poboljšati policijske aktivnosti, ali isto tako i postaviti pitanja o privatnosti, diskriminaciji i odgovornosti. Ova tema naglašava potrebu za pažljivim razmatranjem i regulacijom upotrebe AI kako bi se osiguralo da se tehnologija koristi na način koji je u skladu s vrijednostima i pravima društva.

8.1. Pitanja privatnosti, sigurnosti podataka i moguće zloupotrebe

Korištenje umjetne inteligencije (AI) u policijskom radu donosi mnoge prednosti, ali isto tako otvara niz osjetljivih pitanja koja se tiču privatnosti građana, sigurnosti podataka i potencijalnih zloupotreba. Ovdje ćemo detaljnije istražiti ove ključne aspekte, istaknuti njihove implikacije i uputiti na relevantne izvore.

Pitanja Privatnosti:

Praćenje građana: Upotreba AI može omogućiti policijskim agencijama praćenje aktivnosti građana na mnogo sofisticiranije načine. Tehnologije kao što su kamere za prepoznavanje lica mogu identificirati pojedince u stvarnom vremenu. Ovo postavlja pitanja o tome koliko takvo praćenje ulazi u privatni život građana i može li se smatrati kršenjem prava na privatnost.

Analiza društvenih medija: Policija može koristiti AI za analizu društvenih medija, kako je već prije navedeno, kako bi prikupila informacije o građanima. To može uključivati praćenje objava i komentara na mrežama, što postavlja pitanja o praćenju online aktivnosti i slobodi izražavanja.[41]

Sigurnost podataka:

Pohrana osjetljivih informacija: Korištenje AI u policijskom radu često uključuje prikupljanje i pohranu osjetljivih informacija o građanima. To uključuje biometrijske podatke poput otisaka prstiju i podatke o kriminalnoj povijesti. Sigurnost ovih podataka mora biti na najvišoj razini kako bi se spriječile povrede privatnosti i zloupotrebe.

Rizik od hakerskih napada: Sve više sustava AI temelji se na velikim količinama podataka pohranjenih u računalnim sustavima. To ih čini potencijalnim metama za hakerske napade. Ovaj rizik može dovesti do curenja osjetljivih podataka i ozbiljnih problema u vezi sigurnosti.

Moguće zloupotrebe:

Diskriminacija: AI algoritmi mogu biti podložni pristranosti i diskriminaciji ako nisu pravilno trenirani. To može rezultirati nepravednim postupanjem prema određenim skupinama građana, uključujući manjine i ranjive skupine.

[41] Solove, D. J. (2019). Privacy and surveillance in a digital age. Harvard Law Review, 126(7), 1934-1965.

Prekomjerno nadziranje: Upotreba AI tehnologija za nadzor može dovesti do prekomjernog nadziranja građana i potencijalnih zloupotreba vlasti. To može ugroziti demokratske vrijednosti i građanske slobode.[42]

Regulacije i pravne okvire u vezi s korištenjem AI u policijskom radu ključni su za suočavanje s ovim pitanjima. Potrebno je pažljivo balansirati između upotrebe tehnologije u svrhu održavanja sigurnosti i zaštite građanskih prava i privatnosti.

8.2. Regulacija i smjernice za odgovorno korištenje AI tehnologija u policijskom sektoru

Regulacija i smjernice za odgovorno korištenje umjetne inteligencije (AI) tehnologija u policijskom sektoru igraju ključnu ulogu u osiguravanju transparentnosti, etičnosti i zakonitosti primjene AI. Općenito, takvi okviri imaju nekoliko ključnih ciljeva:

Zaštita ljudskih prava i sloboda: Regulacije i smjernice trebaju osigurati da korištenje AI u policijskom radu ne krši ljudska prava i građanske slobode, uključujući pravo na privatnost, pravično suđenje i nediskriminaciju.

Transparentnost i odgovornost: Moraju postaviti zahtjeve za transparentnost u upotrebi AI tehnologija, uključujući obvezu jasnog objašnjavanja algoritama i procesa donošenja odluka. Također trebaju definirati tko je odgovoran za postupke i odluke koje donosi AI.

Pravičnost i nediskriminacija: Regulacije bi trebale spriječiti diskriminaciju i pristranost u AI sustavima, kako bi se osiguralo da tehnologija ne favorizira ili stigmatizira određene skupine građana.

Sigurnost podataka: Trebaju uključivati odredbe o sigurnosti podataka kako bi se spriječila zloupotreba ili curenje osjetljivih informacija koje AI sustavi prikupljaju i obrađuju.

Etičke Smjernice: Pored zakonskih regulacija, smjernice za etičko korištenje AI u policijskom radu mogu biti korisne. One potiču policijske agencije da razmisle o etičkim pitanjima i donose odluke u skladu s najvišim etičkim standardima.

Edukacija i Obuka: Regulacije i smjernice mogu uključivati zahtjeve za obukom policijskih službenika o pravilnom korištenju AI tehnologija kako bi se spriječile pogreške i nepravilnosti.

Sudski nadzor: Trebaju se osigurati mehanizmi sudskog nadzora nad primjenom AI u policijskom radu kako bi se osigurala zakonitost i pravičnost.

Praćenje i evaluacija: Regulacije bi također trebale zahtijevati praćenje i evaluaciju primjene AI tehnologija kako bi se osigurala njihova učinkovitost i usklađenost s propisima.

Primjerice, Europska unija je donijela smjernice za etičku upotrebu AI u javnom sektoru, uključujući policijske agencije, kroz svoj "*Ethics Guidelines for Trustworthy AI*".[43] Slični okviri i smjernice razvijaju se u mnogim zemljama kako bi se usmjerio razvoj i primjena AI u policijskom sektoru prema odgovornim i etičkim standardima.

[42] Goodfellow, I., Bengio, Y., Courville, A., & Bengio, Y. (2016). Deep learning (Vol. 1). MIT press Cambridge.
[43] https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai (01.09.2023.)

Ključno je da regulacija i smjernice prate brz razvoj AI tehnologija i prilagode se novim izazovima kako bi se osigurala odgovorna i zakonita primjena ove tehnologije u policijskom radu.

U Republici Hrvatskoj ključnih zakona i pravila koja su relevantna za MUP RH a koja dijelom pokrivaju i područje korištenja AI u postupanju policije:[44]

- Zakon o policiji: Ovaj zakon utvrđuje osnovne ovlasti i odgovornosti policijskih službenika, organizaciju i funkcioniranje policije u Republici Hrvatskoj.
- Zakon o zaštiti osobnih podataka: Ovaj zakon regulira prikupljanje, obradu i zaštitu osobnih podataka građana. To je ključno za sigurnost podataka pri korištenju tehnologija poput AI u policijskom radu.
- Zakon o policijskim poslovima i ovlaštenjima: Ovaj zakon detaljnije uređuje policijske poslove, ovlaštenja i postupke policije, uključujući pristup informacijama, praćenje i nadzor.
- Zakon o sigurnosti prometa na cestama: Ovaj zakon uređuje pitanja vezana uz prometnu sigurnost, uključujući pravila vožnje, kontrolu prometa i postupanje u slučaju prometnih nesreća.
- Zakon o kontroli oružja: Ovaj zakon regulira posjedovanje, upotrebu i kontrolu oružja i streljiva.

[44] https://mup.gov.hr/pristup-informacijama-16/savjetovanje-sa-zainteresiranom-javnoscu-221/savjetovanja-ministarstva-unutarnjih-poslova-provedena-prije-aplikacije-e-savjetovanja/zakon-o-policiji-195279/195279

9. BUDUĆNOST UMJETNE INTELIGENCIJE U POLICIJSKOM RADU

Dok stojimo na pragu novog doba tehnološke transformacije, umjetna inteligencija (AI) sve više postaje ključni partner u policijskom radu. No, to je tek početak. Poglavlje koje slijedi otvara vrata prema budućnosti AI-a u policijskim agencijama, otkrivajući kako će tehnološki napredak oblikovati i unaprijediti načine na koje policija održava red i sigurnost u našim zajednicama. Kroz ovo poglavlje, navesti ćemo najnovije trendove, inovacije i izazove koji će definirati budući krajolik policijskog rada, potičući na razmišljanje o etičkim pitanjima i pravilima koja će oblikovati put naprijed.

9.1. Trendovi i perspektive: razvoj novih tehnologija i pristupa

Policijski sektor prolazi kroz transformaciju bez presedana zahvaljujući umjetnoj inteligenciji (AI) i novim tehnologijama. Razvoj AI-a u policijskom radu nije samo evolucija već revolucija. U ovom tekstu navesti ćemo neke od ključnih trendova i perspektiva koji oblikuju budućnost primjene AI u policijskom sektoru, a koji zahtijevaju pažljivo promišljanje i planiranje kako bi se iskoristile prednosti tehnologije dok se istovremeno očuvali etički i pravni standardi.

Može se zaključiti da već sadašnje korištenje brojnih mogućnosti AI daje naznake da će to biti u značajnoj mjeri unaprijeđeno a svakako da će daljnji razvoj AI pružiti i nove mogućnosti. U nastavku se navodi nekoliko područja gdje je, po osobnom sudu, moguće očekivati daljnja unapređenja u aplikacijama AI:

- Analiza big data u stvarnom vremenu: Policijske agencije sve više koriste AI za analizu ogromnih količina podataka u stvarnom vremenu. Ovo omogućava brže reagiranje na incidente, identificiranje uzoraka i prepoznavanje potencijalnih prijetnji. Tehnologije poput strojnog učenja i analize teksta pomažu u filtriranju i obradi informacija kako bi se pružile relevantne obavijesti policijskim službenicima.[45]
- Prediktivna analitika i prevencija zločina: AI može predviđati kriminalne aktivnosti na temelju analize povijesnih podataka. Policijske agencije mogu usmjeriti svoje resurse na područja s većim rizikom, što doprinosi smanjenju kriminala.[46]
- Globalna Suradnja i Dijalog: Razmjena znanja i iskustava između policijskih agencija i država ključna je za usmjeravanje razvoja AI u policijskom sektoru. Međunarodna suradnja pomaže u definiranju najboljih praksi i standarda.[47]

U svijetu ubrzanog tehnološkog napretka, budućnost primjene AI u policijskom sektoru obećava revolucionarne promjene. Ipak, potrebno je ostati predani razvoju tehnologije u skladu s etičkim načelima i pravilima kako bi se osigurala sigurnost i prava građana.

9.2. Potencijalni izazovi za budućnost sigurnosti i prevencije

Unatoč mnogim prednostima, upotreba umjetne inteligencije (AI) u kontekstu sigurnosti i prevencije donosi i niz potencijalnih izazova i pitanja koja će biti ključna za budućnost. U ovom

[45] Mohanty, S. P., Choppali, U., & Kougianos, E. (2016). Everything you wanted to know about smart cities: The internet of things is the backbone. IEEE Consumer Electronics Magazine, 5(3), 60-70.
[46] Mohler, G. O., Short, M. B., Brantingham, P. J., Schoenberg, F. P., & Tita, G. E. (2011). Self-exciting point process modeling of crime. Journal of the American Statistical Association, 106(493), 100-108.
[47] Grabosky, P. (2002). Globalization and crime. Sage

širem tekstu, istražit ćemo neke od tih izazova kako bismo bolje razumjeli kako se AI može razvijati i primjenjivati na odgovoran način.

Korištenje AI za praćenje i analizu podataka može ugroziti privatnost građana. Pitanja poput pristupa i pohrane osjetljivih informacija zahtijevaju stroge protokole kako bi se osigurala sigurnost podataka i spriječile zloupotrebe. Također, AI sustavi mogu biti skloni pristranosti ako se treniraju na nepotpunim ili pristranim skupovima podataka. To može dovesti do nepravednog tretmana određenih skupina građana i pojačati postojeće društvene nejednakosti.[48]

U promišljanju izazova svakako treba imati na umu da su AI sustavi ranjivi na napade i manipulacije. Hakiranje AI-a može dovesti do ozbiljnih problema, uključujući kršenje sigurnosti, širenje dezinformacija i ometanje sustava.[49]

Nastavno na potonje, AI sustavi donose odluke na temelju algoritama i podataka, a ta odluka može imati ozbiljne posljedice. Postavlja se pitanje tko je odgovoran za te odluke i kako se osigurava etičko postupanje AI-a. Razvoj tehnologije često prelazi brže od zakonodavstva. Regulativni okviri trebaju biti ažurirani kako bi se nosili s izazovima koje donosi AI.[50]

Svakako ne treba smetnuti sa uma i društvenu prihvaćenost. Uvođenje AI u sigurnost i prevenciju također ovisi o prihvaćenosti građana. Postavlja se pitanje kako educirati i informirati javnost o koristima i rizicima AI-a.

Svaki od ovih izazova ima potencijal utjecati na budućnost sigurnosti i prevencije kada je u pitanju korištenje AI. Stoga je važno da društvo, vlasti i stručnjaci iz različitih područja surađuju kako bi se razvili odgovarajući okviri i prakse koje će osigurati da AI tehnologija služi općem dobru i očuva temeljne vrijednosti društva.

[48] Barocas, S., Hardt, M., & Narayanan, A. (2019). Fairness and machine learning. http://fairmlbook.org.
[49] : Goodfellow, I., Bengio, Y., Courville, A., & Bengio, Y. (2016). Deep learning (Vol. 1). MIT press Cambridge.
[50] Chorafas, D. N. (2010). Cybersecurity, cyberanalysis and warning. CRC Press.

10. ZAKLJUČAK

Umjetna inteligencija (AI) sve više postaje ključni faktor u transformaciji policijskog rada, igrajući ključnu ulogu u unapređenju sigurnosti i prevenciji kriminala. Kroz ovu analizu, istražili smo razne aspekte primjene AI u policijskom poslu, razmotrivši kako tehnologija mijenja načine na koje policijske agencije održavaju red, reagiraju na izazove i pristupaju prevenciji kriminala. Dok je budućnost svijetla u smislu inovacija koje AI može donijeti, isto tako smo identificirali niz izazova i pitanja koja će morati biti pažljivo riješena kako bi se osigurala odgovorna i etička primjena ove tehnologije.

Prvi ključni aspekt koji smo razmotrili jest analiza velike količine podataka u stvarnom vremenu. AI omogućava policijskim agencijama da efikasnije obrade ogromne količine informacija i identificiraju uzorke koji bi inače ostali nezapaženi. To pomaže u bržem reagiranju na incidente, identificiranju prijetnji i održavanju sigurnosti u zajednicama. No, ovakva upotreba podataka također stavlja naglasak na pitanja privatnosti i sigurnosti podataka, zahtijevajući rigorozne protokole kako bi se osigurala zaštita građanskih prava.

Drugi ključni aspekt je upotreba prepoznavanja lica i biometrije. AI je revolucionirao sposobnost identifikacije i praćenja osoba, što je od vitalnog značaja za pronalaženje nestalih osoba i identifikaciju potencijalnih prijetnji. Ipak, ovakva tehnologija mora se koristiti s oprezom kako bi se izbjegle nepravde i diskriminacija. Treniranje AI sustava na pristranim podacima može dovesti do ozbiljnih etičkih problema.

Prediktivna analitika i prevencija zločina su također ključne komponente budućnosti policijskog rada. AI može predviđati kriminalne aktivnosti i omogućiti policijskim agencijama da usmjeravaju svoje resurse prema područjima s većim rizikom. Ovo može znatno pridonijeti smanjenju kriminala, ali isto tako postavlja pitanje kako se koristi takva moć i kako se osigurava pravična primjena.

Etička pitanja i odgovornost AI sustava su neizbježni dio ovog razvoja. Policijske agencije moraju se nositi s pitanjima odgovornosti za odluke koje donosi tehnologija. Transparentnost i odgovornost ključni su za održavanje povjerenja javnosti.

Iako su izazovi očigledni, AI također donosi prilike za poboljšanje sigurnosti i prevenciju. Sigurnosni sustavi postaju inteligentniji i učinkovitiji, a sposobnost brze reakcije na prijetnje nikada nije bila bolja. Obuka i edukacija policijskih službenika ključni su za pravilnu upotrebu AI alata, a globalna suradnja može promicati najbolje prakse i standarde.

U konačnici, budućnost umjetne inteligencije u policijskom radu obećava promjene koje će unaprijediti sigurnost i prevenciju. No, taj napredak mora biti vođen strogoćom, etikom i brigom za prava građana. Samo uz odgovoran pristup možemo iskoristiti puni potencijal AI-a za bolju budućnost sigurnosti i prevencije kriminala.

11. IZJAVA

Izjava o autorstvu završnog rada i akademskoj čestitosti

Ime i prezime studenta: **Stjepan Drmić**

Matični broj studenta: **1-167/20**

Naslov rada: **Umjetna inteligencija u radu policije**

Pod punom odgovornošću potvrđujem da je ovo moj autorski rad čiji niti jedan dio nije nastao kopiranjem ili plagiranjem tuđeg sadržaja. Prilikom izrade rada koristio sam tuđe materijale navedene u popisu literature, ali nisam kopirao niti jedan njihov dio, osim citata za koje sam naveo autora i izvor te ih jasno označio znakovima navodnika. U slučaju da se u bilo kojem trenutku dokaže suprotno, spreman sam snositi sve posljedice uključivo i poništenje javne isprave stečene dijelom i na temelju ovoga rada.

Potvrđujem da je elektronička verzija rada identična onoj tiskanoj te da je to verzija rada koju je odobrio mentor.

Datum

24.10.2023.

Potpis studenta

Stjepan Drmić

12. POPIS LITERATURE

12.1. Knjige i članci

1. Stuart Russell, Peter Norvig - Artificial Intelligence: A Modern Approach-Prentice Hall (2002).
2. M.R. McGuire (2020): The laughing policebot: automation and the end ofpolicing, Policing and Society, DOI: 10.1080/10439463.2020.1810249To link to this article: https://doi.org/10.1080/10439463.2020.1810249© 2020 The Author(s). Published by InformaUK Limited, trading as Taylor & FrancisGroupPublished online: 25 Sep 2020.Submit your article to this journal Article views: 781View related articles View Crossmark data
3. Aswani, R., Kar, A. K., & Ilavarasan, P. V. (2018). Detection of spammers in twitter marketing: A hybrid approach using social media analytics and bio inspired computing. Information Systems Frontiers, 20(3), 515–530.
4. M. Turkanović i ostali, "Face Recognition Techniques: A Comprehensive Survey," 2019 International Conference on Smart Systems and Technologies (SST), Osijek, Croatia, 2019, pp. 1-6.
5. P. Kolekar i ostali, "Analysis of Human Behavior Patterns for Security Applications," 2019 IEEE 4th International Conference on Signal and Image Processing (ICSIP), Bangalore, India, 2019, pp. 150-155.
6. Y. LeCun, Y. Bengio, and G. Hinton, "Deep learning," Nature, vol. 521, no. 7553, pp. 436-444, 2015.
7. S. Sundararajan i ostali, "Crowd Flow Analysis in Sports Stadiums Using Convolutional Neural Networks," 2019 IEEE International Conference on Big Data (Big Data), Los Angeles, CA, USA, 2019, pp. 3317-3324.
8. H. Zhou i ostali, "Crowd Behavior Analysis and Anomaly Detection in Open Spaces with CNN," IEEE Transactions on Circuits and Systems for Video Technology, vol. 30, no. 6, pp. 1411-1424, 2019.
9. H. Zhou i ostali, "Crowd Behavior Analysis and Anomaly Detection in Open Spaces with CNN," IEEE Transactions on Circuits and Systems for Video Technology, vol. 30, no. 6, pp. 1411-1424, 2019.
10. S. Mianji i ostali, "Weapon Detection in Video Surveillance Using Deep Learning Techniques," 2019 16th International Conference on Control, Automation, Robotics and Vision (ICARCV), Singapore, 2019, pp. 206-211.
11. C. Li i ostali, "Crowd Flow Analysis for Anomaly Detection in Airport Security," 2019 IEEE International Conference on Big Data (Big Data), Los Angeles, CA, USA, 2019, pp. 2515-2523.
12. Saks, M. J. (2019). Fingerprint Analysis. CRC Press
13. Butler, J. M. (2015). Forensic DNA Typing: Biology, Technology, and Genetics of STR Markers. Elsevier.
14. Houck, M. M., & Siegel, J. A. (2019). Fundamentals of Forensic Science. Academic Press.

15. Abu-Nimeh, S., Nappa, A., Moskovitch, R., & Elovici, Y. (2015). Intrusion Detection System Evasion Techniques: Variational Autoencoder and Adversarial Machine Learning. arXiv preprint arXiv:1511.04143.
16. Lynch, M. J., & Michaud, S. (2016). Big Data Analytics in the Fight Against Cyber-Crime. In International Conference on Big Data Analytics and Knowledge Discovery (pp. 102-114). Springer.
17. Ashbaugh, D. R. (1999). Quantitative-Qualitative Friction Ridge Analysis: An Introduction to Basic and Advanced Ridgeology. CRC Press.
18. Alshammari, R., & Mahmood, A. N. (2018). Border Surveillance System Using Internet of Things (IoT) and Machine Learning. IEEE Access, 6, 46929-46936
19. Cusumano-Towner, M., & Shishika, D. (2018). Securing the border with machine learning: An anomaly detection approach to unauthorized border crossings. Big Data, 6(4), 283-297.
20. Díaz-Padilla, G., & Fernández-Caballero, A. (2019). Analysis of Border Surveillance Systems. Sensors, 19(24), 5472.
21. Tavana, M., Di Caprio, D., & Santos-Arteaga, F. J. (2021). Big data analytics in support of immigration management and border security. Decision Support Systems, 140, 113430.
22. U.S. Department of Homeland Security. (2020). Snapshot: How DHS Uses AI Technology to Secure the Border
23. Solove, D. J. (2019). Privacy and surveillance in a digital age. Harvard Law Review, 126(7), 1934-1965.
24. Goodfellow, I., Bengio, Y., Courville, A., & Bengio, Y. (2016). Deep learning (Vol. 1). MIT press Cambridge.
25. Mohanty, S. P., Choppali, U., & Kougianos, E. (2016). Everything you wanted to know about smart cities: The internet of things is the backbone. IEEE Consumer Electronics Magazine, 5(3), 60-70.
26. Mohler, G. O., Short, M. B., Brantingham, P. J., Schoenberg, F. P., & Tita, G. E. (2011). Self-exciting point process modeling of crime. Journal of the American Statistical Association, 106(493), 100-108.
27. Grabosky, P. (2002). Globalization and crime. Sage
28. Barocas, S., Hardt, M., & Narayanan, A. (2019). Fairness and machine learning. http://fairmlbook.org.
29. : Goodfellow, I., Bengio, Y., Courville, A., & Bengio, Y. (2016). Deep learning (Vol. 1). MIT press Cambridge.
30. Chorafas, D. N. (2010). Cybersecurity, cyberanalysis and warning. CRC Press.

12.2. Internetski izvori

1. ISSIE LAPOWSKY Kako LAPD koristi podatke za predviđanje zločina,. SIGURNOST 22 svibnja 2018. (https://www.wired.com/story/los-angeles-police-department-predictive-policing/)
2. Sanur Sharma, Anurag Jain: Role of sentiment analysis in social media security and analytics, https://wires.onlinelibrary.wiley.com/doi/10.1002/widm.1366
3. National Counter Terrorism Policing UK (https://www.counterterrorism.police.uk/)

4. National Counter Terrorism Policing UK. (2017). London Bridge Attack 3 June 2017: Learning Report. Preuzeto sa: https://www.counterterrorism.police.uk/wp-content/uploads/2017/12/London-Bridge-Attack-3-June-2017-Learning-Report-Web.pdf
5. ABC News (https://abcnews.go.com/US/accused-florida-school-shooter-nikolas-cruz-charged-17/story?id=53147237)
6. ABC News. (2018). Accused Florida school shooter Nikolas Cruz charged with 17 counts of premeditated murder. Preuzeto sa: https://abcnews.go.com/US/accused-florida-school-shooter-nikolas-cruz-charged-17/story?id=53147237
7. Polizei Bayern (https://www.polizei.bayern.de/muenchen/news/presse/aktuell/index.html/312163)
8. Polizei Bayern. (2021). Der MVbot antwortet rund um die Uhr. Preuzeto sa: https://www.polizei.bayern.de/muenchen/news/presse/aktuell/index.html/312163
9. https://uznr.mrms.hr/uloga-nadzornih-kamera-u-sustavu-upravljanja-kvalitetom-te-zastiti-zdravlja-i-sigurnosti-na-radu/ (29.08.2023.)
10. https://www.poslovni.hr/sci-tech/ignoriranje-cyber-opasnosti-moze-ozbiljno-ugroziti-poslovanje-svake-tvrtke-4393915 (29.08.2023.)
11. https://informator.hr/vijesti/novim-tehnologijama-do-povecanja-sigurnosti-cestovnog-prometa (29.08.2023.)
12. https://www.theverge.com/c/22444020/chicago-pd-predictive-policing-heat-list (23.08.2023.)
13. https://www.dhs.gov/sites/default/files/publications/dhs_ai_strategy.pdf (31.08.2023.)
14. https://www.dhs.gov/biometrics (31.08.2023)
15. Reuters. (2022). AI used to spot fake passports increasingly sophisticated and may beat border checks
16. Euronews. (2022). AI used to spot fake passports increasingly sophisticated and may beat border checks.
17. Reuters. (2021). Privacy fears grow as EU pushes AI to speed up migrant screening
18. ScienceDaily. (2020). Researchers turn to AI, radar and drones to study protected ocean species
19. https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai (01.09.2023.)
20. https://mup.gov.hr/pristup-informacijama-16/savjetovanje-sa-zainteresiranom-javnoscu-221/savjetovanja-ministarstva-unutarnjih-poslova-provedena-prije-aplikacije-e-savjetovanja/zakon-o-policiji-195279/195279

ŽIVOTOPIS

europass

Stjepan Drmić

Datum rođenja: 01/03/1992 | **Državljanstvo:** hrvatsko | **Spol:** Muško | **Telefonski broj:** (+385) 0997369753 (Kućni) | **E-adresa:** drmic.stjepan@gmail.com |

Adresa: Marije Jurić Zagorke 27, 32100, Vinkovci, Hrvatska (Kućna)

OBRAZOVANJE I OSPOSOBLJAVANJE

09/1998 – 06/2006 Vinkovci, Hrvatska
OSNOVNOŠKOLSKO OBRAZOVANJE Osnovna škola Vladimira Nazora Vinkovci

09/2006 – 06/2010 Vinkovci, Hrvatska
SREDNJOŠKOLSKO OBRAZOVANJE - VETERINARSKI TEHNIČAR Zdravstvena i veterinarska škola dr. Andrija Štampar Vinkovci

09/2010 – 09/2010 Zagreb, Hrvatska
DRŽAVNA MATURA Nacionalni centar za vanjsko vrednovanje obrazovanja

RADNO ISKUSTVO

07/2010 – 11/2010 Vinkovci, Hrvatska
ZIDAR DUSPARA IVICA SAM. PRIV. ZIDAR

12/2012 – 06/2018 Slavonski Brod, Hrvatska
POLICIJSKI SLUŽBENIK ZA GRANIČNU KONTROLU POLICIJSKA UPRAVA BRODSKO - POSAVSKA, POLICIJSKA POSTAJA VRPOLJE

06/2018 – 07/2020 Slavonski Brod, Hrvatska
VIŠI POLICAJAC POLICIJSKA UPRAVA BRODSKO - POSAVSKA, POLICIJSKA POSTAJA VRPOLJE

07/2020 – 12/2022 Vinkovci, Hrvatska
VIŠI POLICAJAC MINISTARSTVO UNUTARNJIH POSLOVA REPUBLIKE HRVATSKE, POLICIJSKA UPRAVA VUKOVARSKO - SRIJEMSKA

12/2022 – TRENUTAČNO Vinkovci, Hrvatska
SAMOSTALNI POLICAJAC MINISTARSTVO UNUTARNJIH POSLOVA REPUBLIKE HRVATSKE, POLICIJSKA UPRAVA VUKOVARSKO - SRIJEMSKA

DODATNE INFORMACIJE

HOBIJI I INTERESI

Konjički klub Maestoso Vinkovci
- konjički turizam
- sudjelovanje u konjičkim natjecanjima
- pružanje usluga u školi jahanja
- rekreativno jahanje i vožnja fijakerom
- pružanje usluga vožnje fijakerom
- sudjelovanje u kulturnim i tradicijskim manifestacijama i događanjima

OPG Drmić Stjepan
- sadnja agrokultura
- pružanje usluga u obradi zemlje
- razvoj konjogojstva

- pružanje usluga jahanja i vožnje fijakerom
- sudjelovanje u kulturnim i tradicijskim manifestacijama i događanjima

VOZAČKA DOZVOLA

Vozačka dozvola: B