

TEHNOLOGIJE PAMETNIH GRADOVA U PREVENCIJI KRIMINALA U REPUBLICI SRBIJI: UPOREDNA ANALIZA SA MEĐUNARODNIM STANDARDIMA

Kristina Atanackovic¹, Radovan Radovanovic²

Rezime: Urbanizacija i tehnološki razvoj donose nove izazove u oblasti bezbednosti, naglašavajući potrebu za inovativnim pristupima u prevenciji kriminala. Pametne tehnologije, poput video-nadzora sa veštačkom inteligencijom, analize velikih podataka i IoT senzora, sve više se koriste u globalnoj borbi protiv kriminala. Ovaj rad ispituje primenu tehnologija pametnih gradova u prevenciji kriminala u Republici Srbiji, sa posebnim osvrtom na njihovu usklađenost sa međunarodnim standardima. Cilj je identifikovati ključne izazove u implementaciji i predložiti rešenja za unapređenje bezbednosnih strategija. Analiza obuhvata prednosti i ograničenja postojećih sistema, poređenje sa međunarodnim praksama i mogućnosti za njihovo unapređenje. Posebna pažnja posvećena je ulozi digitalne infrastrukture, zakonodavnog okvira i institucionalne saradnje u jačanju mera prevencije kriminala. Rezultati ukazuju na potrebu modernizacije i prilagođavanja bezbednosnog sistema Republike Srbije globalnim trendovima kako bi se pametne tehnologije efikasnije koristile.

Ključne reči: pametni gradovi, prevencija kriminala, video nadzor, međunarodni standardi, analiza.

SMART CITY TECHNOLOGIES IN CRIME PREVENTION IN THE REPUBLIC OF SERBIA: A COMPARATIV ANALYSIS WITH INTERNATIONAL STANDARDS

Abstract: Urbanization and technological development bring new challenges in the field of security, emphasizing the need for innovative approaches to crime prevention. Smart technologies, such as AI-powered video surveillance, data analysis, and IoT sensors, are increasingly used in the global fight against crime. This paper examines the application of smart city technologies in crime prevention in the Republic of Serbia, focusing on their compliance with international standards. The aim is to identify key challenges in implementation and propose solutions for improving security strategies. The study highlights the advantages and limitations of existing systems, comparing them with international practices to determine opportunities for enhancement. Special attention is given to the role of digital infrastructure, legal regulations, and institutional cooperation in strengthening crime prevention efforts. The findings emphasize the need for modernization and adaptation of Serbia's security framework to align with global trends, ensuring more effective use of smart technologies.

Key words: smart cities, crime prevention, video surveillance, international standards, analysis

1. TEHNOLOGIJE PAMETNIH GRADOVA

Razvoj pametnih gradova predstavlja jedan od ključnih trendova u urbanom planiranju i bezbednosnoj politici savremenih društava. Upotreba inovativnih tehnologija, poput video-

¹Spec. krim, krisatanackovic@gmail.com

²Prof. dr, Kriminalističko-policijski univerzitet, Cara Dušana 196 Beograd, radovan.radovanovic@kpu.edu.rs

nadzora sa veštačkom inteligencijom, senzorskih sistema, analitike velikih podataka, biometrijskih sistema za identifikaciju lica, automatizovanih sistema prepoznavanja lica i vozila i pametnih komunikacionih platformi omogućava bržu reakciju nadležnih organa, povećava efikasnost policijskog rada i smanjuje mogućnost izvršenja krivičnih dela. Njihova svrha je unapređenje policijskog rada, bolja koordinacija hitnih službi i povećanje poverenja građana u institucije. Razvoj pametnih gradova bazira se na integraciji različitih tehnoloških sistema koji omogućavaju proaktivno delovanje u sprečavanju kriminala i povećanju bezbednosti građana.

Pregled ključnih tehnologija pametnih gradova u prevenciji kriminala:

- Video-nadzor i veštačka inteligencija (eng. „Artificial Intelligence“)
- IoT (eng. „Internet of things“) senzori
- Prediktivna analitika i analiza velikih podataka
- Sisteme automatskog prepoznavanja tablica (eng. „Automatic License Plate Recognition“)

Sistemi video-nadzora sa veštačkom inteligencijom koriste algoritme za prepoznavanje lica, analizu ponašanja i identifikaciju sumnjivih aktivnosti u realnom vremenu. Radi ilustracije u Londonu je postavljene veliki broj kamera koje uz pomoć veštačke inteligencije vrše analizu podataka za detekciju i koriste se za prevenciju kriminala. Ovakav sistem omogućava policiji da brzo reaguje u situacijama u kojima je neophodna intervencija, smanjujući tako vreme odziva i povećavajući sigurnost građana.[1]

Internet stvari (IoT) predstavlja mrežu povezanih uređaja koji komuniciraju međusobno i sa centralnim sistemima, omogućavajući prikupljanje i analizu podataka u realnom vremenu. U kontekstu prevencije kriminala, IoT senzori se koriste za nadzor javnih prostora, detekciju sumnjivih aktivnosti i poboljšanje odgovora bezbednosnih službi. Na primer, zvučni senzori mogu identifikovati zvukove pucnjeva, lomljenja stakla ili vriska, automatski upozoravajući nadležne službe na potencijalne incidente. Pametna rasveta, koja reaguje na pokret ili anomalije u okolini, može smanjiti stopu kriminala povećanjem vidljivosti na mestima visokog rizika. Takođe, senzori za prepoznavanje pokreta i vibracija ugrađeni u javnu infrastrukturu mogu pomoći u sprečavanju vandalizma i krađa. Ove tehnologije omogućavaju sigurnosnim službama da brzo reaguju na pretnje i poboljšaju efikasnost patroliranja, dok istovremeno smanjuju potrebu za stalnim fizičkim nadzorom. Međutim, njihova implementacija zahteva adekvatnu zaštitu privatnosti građana i usklađenost sa pravnim regulativama kako bi se sprečile zloupotrebe podataka i neproporcionalno nadziranje određenih društvenih grupa.[2]

Prediktivna analitika koristi podatke o prethodnim kriminalnim događajima za predviđanje budućih kriminalnih aktivnosti. Na osnovu istorijskih podataka, policijske službe mogu identifikovati "vruće tačke" u gradovima, gde je verovatnije da će se dogoditi krivična dela. Policija Los Anđelesa koristi „PredPol“, model za predviđanje kriminala, koji usmerava patrolne jedinice na područja sa povećanim rizikom od kriminala. Ovaj sistem je pomogao da se smanje stope određenih vrsta kriminala, uključujući provale i napade. Prediktivna analitika nije bez izazova, jer se mora obezbediti da sistemi ne izazovu diskriminaciju ili prekomernu upotrebu resursa u specifičnim zajednicama.[3]

Sistemi automatskog prepoznavanja tablica koriste kamere sa naprednim softverskim algoritmima za automatsko prepoznavanje registarskih tablica vozila. Ovi sistemi se sve više primenjuju u gradovima kao deo pametnih sigurnosnih rešenja i mogu imati ključnu ulogu u prevenciji kriminala. ALPR tehnologija omogućava prikupljanje podataka o vozilima koja

ulaze u određena područja, bilo da je reč o javnim mestima, zgradama ili kritičnim infrastrukturnim tačkama.[4] ALPR se koristi u kombinaciji sa bazama podataka za upoređivanje registarskih brojeva, što omogućava identifikaciju vozila koja su povezana sa kriminalnim radnjama, kao što su pljačke, krađe ili nesreće. Takođe, može se koristiti za praćenje sumnjivih vozila, detekciju vozila koja su ukradena ili vozila koja krše saobraćajne propise. Ova tehnologija takođe omogućava brže reagovanje od strane policije jer omogućava identifikaciju vozila u realnom vremenu.

Analiza velikih podataka u kriminalističkim istragama značajna je zbog obrade podataka iz različitih izvora: Uključuje društvene mreže, mobilne uređaje, saobraćajne kamere i transakcione podatke, kao i za predviđanje kriminala korišćenjem istorijskih podataka, AI modeli mogu identifikovati obrasce kriminalnog ponašanja i predložiti proaktivne mere. Ovakva analiza uključuje i Integraciju sa policijskim sistemima: Omogućava povezivanje podataka iz različitih izvora radi brže analize i donošenja odluka. Primer: Chicago koristi sistem „Strategic Decision Support Centers“ koji analizira velike podatke za usmeravanje patrola.[5]

2. TEHNOLOGIJE PAMETNIH GRADOVA U PREVENCIJA KRIMINA U REPUBLICI SRBIJI

U Republici Srbiji koncept pametnih gradova još uvek se razvija, ali pojedini gradovi i opštine već primenjuju napredne tehnologije za unapređenje bezbednosti. Integracija digitalnih platformi, unapređenje video-nadzora i uvođenje prediktivnih modela analize kriminala predstavljaju korake ka modernizaciji sistema javne bezbednosti. Međutim, postavlja se pitanje u kojoj meri su ove tehnologije usklađene sa međunarodnim standardima, pre svega u kontekstu zaštite privatnosti, etike i efikasnosti.

Evropska unija postavila je stroge regulative u oblasti zaštite podataka (GDPR), dok Sjedinjene Američke Države koriste širok spektar tehnologija u prevenciji kriminala uz različite pristupe u regulaciji njihove primene. Azijski pametni gradovi, predvođeni NR Kinom i Singapurom, ističu se naprednim sistemima nadzora i analize podataka, ali istovremeno otvaraju debatu o balansu između bezbednosti i zaštite privatnosti građana. Republika Srbija, kroz Strategiju razvoja veštačke inteligencije za period 2025–2030, prepoznaje značaj pametnih tehnologija u različitim sektorima, uključujući bezbednost. Ova strategija pruža osnovu za uvođenje AI rešenja u oblasti prevencije kriminaliteta, slično kao u razvijenim pametnim gradovima poput Londona, Singapura i Njujorka. Međunarodni primeri pokazuju da su pametni video-nadzor, analiza podataka u realnom vremenu i prediktivno modelovanje kriminala ključne komponente uspešnih bezbednosnih sistema u pametnim gradovima. Pametni video-nadzor postaje ključni alat u urbanim sredinama Republike Srbije. Sistem koji je implementiran u Beogradu, Nišu i Novom Sadu, predstavlja jednu od najsavremenijih metoda za nadzor i prevenciju kriminala. Ovaj sistem koristi kamere visoke rezolucije, opremljene veštačkom inteligencijom za prepoznavanje lica i registarskih tablica [6]. U saradnji sa kompanijom Huawei, u Beogradu je postavljeno više od 1.000 pametnih kamera na ključnim lokacijama, sa ciljem poboljšanja efikasnosti policijskih intervencija. Sistemi za automatsko prepoznavanje registarskih tablica (ALPR – Automatic License Plate Recognition) omogućavaju: Praćenje kretanja sumnjivih vozila kroz umrežene baze podataka, prepoznavanje ukradenih vozila i alarmiranje policijskih patrola, analizu saobraćajnih prekršaja i povezivanje sa drugim sistemima za kažnjavanje. Ova tehnologija se već

primenjuje u Srbiji, ali u manjem obimu u odnosu na vodeće države poput Velike Britanije i NR Kine, gde ALPR igra ključnu ulogu u sprečavanju kriminala i terorizma.[7]

Video-nadzor predstavlja efikasan alat za praćenje školskog okruženja, uključujući učenike, nastavnike i ostalo osoblje. S obzirom na porast različitih oblika kriminalnih aktivnosti u obrazovnim ustanovama, postavljanje sigurnosnih kamera postaje ne samo potreba već i važan deo odgovornosti školskih uprava. Kontinuirani nadzor doprinosi smanjenju incidenata kao što su nasilje, uznemiravanje i ometanje nastavnog procesa. Osim toga, video-nadzor omogućava školskim upravama da prate kretanje učenika i prepoznaju nedozvoljene aktivnosti, uključujući vandalizam, upotrebu opojnih supstanci, fizičke sukobe, neovlašćen ulazak u školske prostore i krađe. Ključne prednosti ove tehnologije obuhvataju povećanje bezbednosti, efikasniju kontrolu disciplina učenika i zaposlenih, kao i podršku policijskim službama kroz mogućnost daljinskog nadzora i brže reakcije u kriznim situacijama. Ilustracije radi, sve osnovne škole na teritoriji gradske opštine Palilula u Beogradu, povezane su sa policijskom stanicom putem sistema video-nadzora. Ovaj sistem omogućava policijskim službenicima da u realnom vremenu prate dešavanja u školskim dvorištima i njihovoj neposrednoj okolini, koristeći savremene tehnologije za nadzor i analizu podataka. Uključivanjem policije u nadzor školskih objekata postiže se veći nivo bezbednosti učenika i nastavnog osoblja, a istovremeno se omogućava efikasnija upotreba ljudskih resursa. Ovakav pristup doprinosi ranom otkrivanju i sprečavanju potencijalnih bezbednosnih rizika, kao i identifikaciji osoba koje dolaze u školski prostor sa nepoželjnim namerama. Sistem funkcioniše neprekidno, snimajući dešavanja u i oko škola 24 sata dnevno, tokom cele godine, čime se obezbeđuje stalna kontrola i evidencija svih aktivnosti u školskom okruženju.[8]

Internet stvari (IoT – Internet of Things) omogućava povezivanje različitih senzora i sistema u jedinstvenu mrežu nadzora. IoT uređaji u službi prevencije kriminala mogu obuhvatati:

- Pametne interfonске sisteme koji omogućavaju verifikaciju posetilaca u stambenim zgradama.
- Senzore kvaliteta vazduha koji mogu otkriti prisustvo eksploziva ili štetnih hemikalija.
- Senzori pokreta na uličnoj rasveti.
- Nosive kamere za policijske službenike koje omogućavaju bolju transparentnost i dokazni materijal.

U Sjedinjenim Američkim Državama IoT tehnologije se koriste za poboljšanje hitnih intervencija i smanjenje nasilja na javnim mestima, dok EU postavlja regulative o zaštiti privatnosti u vezi sa IoT uređajima. IoT tehnologije postepeno nalaze primenu u urbanim sredinama Srbije, sa posebnim fokusom na javnu bezbednost. Pametna rasveta implementirana je u Beogradu i Nišu, a instalacija LED rasvete sa senzorima pokreta omogućava povećanu osvetljenost u rizičnim zonama, čime se smanjuju šanse za kriminalne aktivnosti u večernjim satima. [9]

3. UPOREDNA ANALIZA SA MEĐUNARODNIM STANDARDIMA

Upoređujući pravni okvir Republike Srbije sa međunarodnim standardima, mogu se uočiti ključne razlike u regulativi i pristupu:

Tabela 1 Uporedna analiza

Zemlja/Regulativa	Pristup zaštiti podataka	Upotreba AI i biometrijskih sistema	Transparentnost nadzora
Evropska unija / (GDPR, Direktiva 2016/680)	Strogi propisi, ograničen pristup podacima, zahteva se saglasnost građana	Ograničena upotreba, zabrana masovnog prepoznavanja lica u javnim prostorima (osim u izuzetnim slučajevima)	Visok nivo transparentnosti, države članice obavezne da imaju nezavisne nadzorne organe [10]
SAD / (različite regulative po državama, npr. CCPA u Kaliforniji)	Slabiji standardi zaštite podataka, kompanije mogu koristiti lične podatke u komercijalne svrhe	Široka primena u privatnom sektoru (npr. Amazon, Clearview AI), državne regulative variraju	Umeren nivo transparentnosti [11]
Kina / (Cybersecurity Law, National AI Strategy)	Minimalna zaštita privatnosti, svi podaci su pod kontrolom države	Masovni nadzor i analiza podataka u realnom vremenu, integracija AI sa policijskim bazama	Nizak nivo transparentnosti, država ima potpunu kontrolu nad nadzornim sistemima [12]
Srbija / (Zakon o zaštiti podataka o ličnosti, Zakon o policiji)	Delimično usklađeno sa GDPR, ali nedovoljna kontrola primene	Ograničena primena AI i biometrije, pravni okvir nije precizan za napredne nadzorne tehnologije	Potrebno unapređenje transparentnosti i bolja regulativa [13], [14]

Primena tehnologija pametnih gradova u prevenciji kriminala donosi niz pravnih i etičkih izazova, koji se odnose na zaštitu privatnosti, regulisanje nadzora i usklađivanje sa

međunarodnim standardima. Dok napredne tehnologije povećavaju bezbednost i efikasnost rada policije, njihova zloupotreba ili neadekvatna primena mogu ugroziti osnovna prava građana.

Podaci u Tabeli ukazuju na značajne razlike u regulaciji pametnih tehnologija između država. Dok Evropska unija postavlja visoke standarde zaštite privatnosti, Sjedinjene Američke Države i NR Kina imaju drugačiji pristup – SAD favorizuje privatni sektor, dok NR Kina daje prioritet državnom nadzoru. Republika Srbija se nalazi u fazi tranzicije, sa zakonima koji su delimično usklađeni sa GDPR-om, ali uz nedovoljnu implementaciju i nadzor.

Ključni izazovi uključuju implementacije

- Masovni nadzor građana – kamere sa prepoznavanjem lica i algoritmi veštačke inteligencije mogu dovesti do prekomernog nadzora i narušavanja privatnosti.
- Rizik od zloupotrebe podataka – neadekvatna zaštita baza podataka može omogućiti neovlašćen pristup osetljivim informacijama.
- Profilisanje i diskriminacija – algoritmi veštačke inteligencije mogu sadržavati pristrasnosti koje vode ka diskriminaciji određenih društvenih grupa.

Etičke dileme su ključni aspekt rasprave o implementaciji tehnologija pametnih gradova, a neki od ključnih etičkih pitanja su:

- Gde je granica između legitimnog nadzora i narušavanja prava građana?
- Ko kontroliše prikupljene podatke i ko snosi odgovornost za moguće zloupotrebe?
- Kako sprečiti diskriminaciju i neetične odluke AI sistema?
- Može li prekomerni nadzor narušiti demokratske vrednosti i osnovna ljudska prava?

Upravo zbog ovih dilema, mnoge zemlje insistiraju na uvođenju nezavisnih regulatornih tela i strožih mehanizama nadzora nad primenom pametnih tehnologija u bezbednosne svrhe.

U Republici Srbiji pravna regulativa koja uređuje upotrebu nadzornih tehnologija u prevenciji kriminala uključuje nekoliko ključnih zakona i propisa: Zakon o zaštiti podataka o ličnosti – usklađen sa Opštom uredbom o zaštiti podataka (GDPR) koji reguliše prikupljanje, obradu i čuvanje podataka građana, zatim Zakon o policiji koji definiše nadležnosti policije u korišćenju tehničkih sredstava i digitalnih alata za nadzor i istragu, potom Krivični zakonik koji uređuje sankcije za neovlašćeno prikupljanje i obradu ličnih podataka i Zakon o informacionoj bezbednosti koji postavlja standarde za zaštitu informacionih sistema i prevenciju sajber kriminala.

Iako je regulativa Republike Srbije delimično usklađena sa EU standardima, izazov ostaje u nenoj praktičnoj primeni i nadzoru. Trenutno, upotreba AI analiza snimaka, biometrijskih sistema i prediktivne policije nije dovoljno precizno regulisana, što ostavlja prostor za pravne nesigurnosti. Za razliku od EU, SAD i NR Kine, Republika Srbija nema jasne smernice o korišćenju AI i biometrijskih sistema u javnim prostorima i nalazi se u ranoj fazi razvoja pravnog okvira za pametne gradove. Pred Republikom Srbijom je značajan put ka usklađivanju sa međunarodnim standardima.

Preporuke za Republiku Srbiju ogledale bi se u dodatnom usklađivanju zakona sa međunarodnim standardima – posebno GDPR, kako bi se osigurala bolja zaštita privatnosti. Neophodno je unaprediti nadzor nad primenom tehnologija, što je moguće kroz formiranje

nezavisnog tela za kontrolu nad digitalnim nadzorom i AI primenom. Takođe je neophodno povećati transparentnost kroz javne debate, uključiti građane u procese donošenja odluka o nadzornim tehnologijama, kao i razviti etičke smernice za upotrebu AI i biometrijskih sistema u saradnji sa stručnjacima iz oblasti prava, IT-a i ljudskih prava.

4. ZAKLJUČAK

Tehnologije pametnih gradova mogu značajno poboljšati prevenciju kriminala, ali je njihova efikasnost uslovljena pravnim i etičkim okvirima. Republika Srbija je na putu ka implementaciji pametnih tehnologija u oblasti bezbednosti, ali se suočava sa brojnim izazovima. Iako su sistemi pametnog video-nadzora, IoT senzora i prediktivne analitike već uvedeni u pojedinim gradovima, njihov puni potencijal tek treba da se realizuje. Ključni problemi uključuju nedovoljnu zakonsku regulativu, zabrinutost u vezi sa privatnošću građana i potrebu za većim ulaganjima u tehnološku infrastrukturu. Primena naprednih tehnologija u prevenciji kriminala otvara pitanje zaštite privatnosti i ljudskih prava. Dalji razvoj pametnih gradova u Srbiji zahteva usklađivanje sa evropskim regulativama, edukaciju stručnjaka u oblasti digitalne bezbednosti i aktivno uključivanje građana u procese digitalizacije bezbednosnih sistema. Pametne tehnologije mogu značajno doprineti prevenciji kriminaliteta, ali samo ukoliko se primenjuju transparentno i odgovorno.

LITERATURA

Tom Sorell, AI-related data ethics oversight in UK policing, *Policing: A Journal of Policy and Practice*, Volume 18, 2024, paae016, <https://doi.org/10.1093/police/paae016>.

Mohler, G. O., Short, M. B., Malinowski, S., Johnson, M., Tita, G. E., Bertozzi, A. L. and Brantingham, P. J. Randomized controlled field trials of predictive policing. *Journal of the American Statistical Association*, 110(512), 1399–1411, 2015.

Mouha, Radouan Ait Radouan Ait. "Internet of things (IoT)." *Journal of Data Analysis and Information Processing* 9.02, 77, 2021.

Brčić, Terezija. "Učinci inteligentnih transportnih sustava na upravljanje prometom u pametnim gradovima." *Diplomski rad, Sveučilište u Rijeci, Pomorski fakultet*, 2023.

Arietti, Rachael. "Do real-time crime centers improve case clearance? An examination of Chicago's strategic decision support centers." *Journal of Criminal Justice* 90, 102145, 2024.

MUP Srbije, Digitalizacija bezbednosnih sistema i pametni gradovi u Srbiji, 2023.

Milenković, D. Uvođenje Huawei Safe City sistema u Beograd. „Tehnologija i društvo“, 7(3), 68–81, 2022.

Kekić, Dalibor, Spasić D. "Učešće policije u video-nadzoru u školama na području policijske uprave za grad Beograd– tradicija, stanje i perspektive razvoja [Participation of Police in Video-Control in Schools in the Area of Police Department for City OF Belgrade-Tradition, the State and Prospects of Development]." *Bezbednost u obrazovno-vaspitnim ustanovama i video-nadzor* 98-110, 2018.

Jovanović M. Primena pametne rasvete u urbanim sredinama Srbije. Zbornik radova Fakulteta tehničkih nauka, 28(2),112-127, 2023.

Uredba (EU) 2016/679 Evropskog parlamenta i veća, <https://eur-lex.europa.eu/legal-content/HR/TXT/?uri=CELEX%3A32016R0679>, mart 2025.

California Consumer Privacy Act (CCPA), <https://oag.ca.gov/privacy/ccpa>, mart 2025.

Cybersecurity Laws and Regulations China 2025, <https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/china>, mart 2025.

Zakon o zaštiti podataka o ličnosti Srbije, https://www.paragraf.rs/propisi/zakon_o_zastiti_podataka_o_licnosti.html, mart 2025.

Zakon o policiji Srbije, https://www.paragraf.rs/propisi/zakon_o_policiji.html, mart 2025.