

Ivona Leskur*
Filozofski fakultet, Univerzitet u Beogradu

Bezbednosni izazovi pametnih gradova – kibernetička sigurnost i privatnost podataka u strateško-pravnim okvirima iz sociološke perspektive

SAŽETAK

U radu se istražuju bezbednosni izazovi pametnih gradova, sa posebnim osvrtnom na kibernetičku sigurnost i privatnost podataka u strateško-pravnim okvirima iz sociološke perspektive. Savremeni gradovi suočavaju se sa izazovima populacionog rasta i ekološke krize, što je dovelo do razvoja koncepta pametnih gradova. Pametni gradovi koriste informaciono-komunikacione tehnologije za unapređenje gradskog života, ali implementacija ovih tehnologija donosi i značajne rizike, naročito u oblasti zaštite podataka i kibernetičke bezbednosti. Analiza je obuhvatila Ustav Republike Srbije, Krivični zakonik, Zakon o informacionoj bezbednosti, Zakon o zaštiti podataka o ličnosti, Strategiju za borbu protiv visokotehnološkog kriminala i Strategiju razvoja informacione bezbednosti. Ustav pruža osnovnu zaštitu podataka o ličnosti, dok Zakon o zaštiti podataka o ličnosti detaljno uređuje prava i obaveze u vezi sa obradom podataka. Krivični zakonik definiše krivična dela protiv bezbednosti računarskih podataka, a Zakon o infor-

* ivonaleskur@gmail.com

macionoj bezbednosti postavlja mere za zaštitu informaciono-komunikacionih sistema. Strategije razvoja informacione bezbednosti i borbe protiv visokotehnološkog kriminala naglašavaju važnost zaštite građana, ali im nedostaje kontinuitet u implementaciji i prilagođavanju brzim tehnološkim promenama. Krićka analiza ukazuje na potrebu za koherentnim strateškim i legislativnim okvirom koji bi obezbedio efikasnu zaštitu građana u digitalnom okruženju pametnih gradova. U radu se zaključuje da Srbija ima dobre zakonske temelje za zaštitu kibernetićeke bezbednosti, ali je neophodno unaprediti implementaciju i kontinuirano ažurirati strateške dokumente kako bi se adekvatno odgovorilo na nove izazove.

KLJUČNE REĆI: *pametan grad, kibernetićeke bezbednost, privatnost podataka*

UVOD

Savremeni rizici, odnosno suoćavanje sa izazovima pre svega populacionog rasta i ekološke krize, nameću potrebu da se problemima uređenja i organizacije gradskog prostora obrađuju u razvojnim agendama na svetskom, evropskom i nacionalnom nivou. a ideja kojoj se najviše pažnje pridaje u akademskim, naućnim i politićkim krugovima jeste vizija o pametnom gradu.

Iako meću naućnicima ne postoji saglasnost oko jedne sveobuhvatne definicije, ono što je zajednićko svim definicijama pametnog grada i ono što je *differentia specifica* u odnosu na slićne koncepte koji se često i naizmenićno upotrebljavaju (preduzetnićki grad, digitalni grad, inteligentni grad) jeste implementacija informaciono-komunikacionih tehnologija u svrhe unapređenja gradskog života. Dok se polažu velike nade u sve naprednije digitalne tehnologije i njihovu mogućnost da reše narastajuće probleme u urbanim zonama, raste i bojazan od rizika koje njihova implementacija u gradskim područjima nosi, a najveću pažnju javnosti, ali i naućnika privlaće pitanja zaštite podataka i, generalno, pitanja bezbednosti na internetu, odnosno kibernetićeke bezbednosti.

ZNAĆAJ KIBERNETIĆKE BEZBEDNOSTI U KONTEKSTU PAMETNIH GRADOVA U SRBIJI

Može se dovesti u pitanje relevantnost bavljenja temom kibernetićeke, odnosno „sajber” (cyber) bezbednosti u pametnim gradovima.

vima u kontekstu Srbije imajući u vidu da u našoj državi još uvek ne postoji nijedan pametan grad. Međutim, ono u čemu se ogleda važnost ove teme jesu brojne inicijative i planirani projekti koji nam ukazuju na mogućnost pametnog razvoja gradova u Srbiji kroz planska dokumenta (Milošević, et al., 2019: 8). U kreiranje pametnih gradova u Srbiji su se uključile privatne korporacije, kao što je kineska kompanija Huawei koja je kreirala rešenja za više od 160 pametnih gradova u preko 100 zemalja sveta, a sa kojom je sklopljen ugovor o implementaciji i razvoju 5G mreže u Srbiji (Prigoda, Bogavac i Čekeřevac, 2022: 75).

Dakle, iako u našoj zemlji još uvek ne postoji transparentna, planska i usmerena orijentisanost ka pametnoj urbanizaciji, na osnovu pokrenutih inicijativa od strane gradskih vlasti sa drugim „stejkholderima”, pre svega sa privatnim kompanijama, u gradovima širom Srbije, a ne samo u Beogradu kao glavnom gradu, može se videti da postoji namera da se postepeno ugrađuju digitalni sistemi i usluge koji služe „opametnjivanju” gradskog područja, kao što su ugradnja senzora za parking, senzori na semaforima i slično. Recimo, 2019. godine najavljivano je da će Niš postati prvi pametan grad u Srbiji¹, potom je 2022. bilo reči o Indiji kao prvom pametnom srpskom gradu², a protekle (2023) godine Pirot je bio prvi grad u Srbiji koji je krenuo u izradu strategije o pametnom gradu³. U aprilu tekuće godine u Kragujevcu je predstavljena Mapa puta pametnih gradova u Srbiji, a istovremeno je predstavljen i pilot-projekat Kragujevca kao prvog pametnog srpskog grada⁴.

Kao što se iz priloženog može videti, Srbija počinje da prati globalni trend sve brže implementacije digitalnih tehnologija u gradsko „tkivo”. Iako se ovo postepeno uključivanje u diskusije o pamet-

1 „Niš – grad naprednih tehnologija i prvi 'pametan grad' u Srbiji”, Niške vesti, <https://niskevesti.rs/nis-grad-naprednih-tehnologija-i-prvi-pametni-grad-u-sbiji/> pristupljeno 28.6.2024.

2 „Indija na korak do 'pametnog grada'”, Vojvodina uživo, <https://vojvodinauzivo.rs/indija-na-korak-do-pametnog-grada/> pristupljeno 28.6.2024.

3 „Pametnim rešenjima do pametnog grada – Započela izrada Strategije za uspostavljanje pametnog grada u Pirotu”, SKGO, <https://www.skgo.org/vesti/detaljno/3182/pametnim-resenjima-do-pametnog-grada-zapocela-izrada-strategije-za-uspostavljanje-pametnog-grada-u-pirotu> pristupljeno 28.6.2024.

4 „Projekat mape puta pametnih gradova za Srbiju pokrenut iz Kragujevca”, Grad Kragujevac, <https://kragujevac.ls.gov.rs/vest/sr/64548/projekat-mape-puta-pametnih-gradova-za-srbiju-pokrenut-iz-kragujevca.php> pristupljeno 28.6.2024.

nim gradovima može protumačiti kao zakasnelo imajući u vidu da neki evropski, američki i azijski gradovi već više od tri decenije rade na projektima pametne urbanizacije, kašnjenje u odnosu na svetske trendove u sferi pametnih gradova i svoju trenutnu početnu poziciju Srbija može da iskoristi kao osnovu za sveobuhvatno i temeljno planiranje i koordinaciju svih aspekata pametne urbanizacije, a samim tim i za bavljenje rizicima koje digitalizacija urbanog prostora sa sobom nosi, čime bi se mogli predupređiti propusti sa kojima su se mnogi gradovi širom sveta već suočili i time ugrozili bezbednost svojih građana. Kao jedna od glavnih preporuka koja se navodi, kako u akademskim tako i u korporativnim izveštajima radi sprečavanja potencijalnih opasnosti od implementacije IKT u gradsku infrastrukturu, ističe se zakonska i strateška regulacija procesa koji doprinose razvijanju pametnih gradova. Primera radi, Singapur, često navođen kao jedan od najreprezentativnijih primera pametnog grada, 2013. godine pokrenuo je Nacionalni plan za kibernetičku bezbednost (National Cyber Security Master Plan) kao sastavni deo strategije „pametne nacije”⁵. Cilj našeg rada bio je da uvidimo da li slični nacionalni planovi, strategije ili zakoni postoje na nivou Srbije, odnosno da li postoji strateški i zakonski okvir kojim bi se na nacionalnom nivou za sve gradove na teritoriji Republike Srbije regulisala kibernetička bezbednost i obezbedila zaštita podataka građana u slučaju izgradnje pametnih gradova. Pretnje koje nastaju u virtuelnom, odnosno kibernetičkom prostoru predstavljaju opasnost za sve aspekte gradskog sistema i često ne ostaju na nivou virtuelnog, već se manifestuju i na materijalnom nivou, ostavljajući posledice po gradsku infrastrukturu, ekonomiju, prirodne resurse i energetska snabdevanje. Raznovrsnost tih pretnji, kao i razornost njihovih eventualnih posledica zahteva sistematičan i detaljan pregled koji prevazilazi obime ovog rada, te smo se u ovom istraživanju, imajući u vidu da je u pitanju sociološki rad, fokusirali isključivo na rizike i bezbednost u vezi sa građanima, kao sastavnim elementima svakog nacionalnog društva.

5 “Smart Nation Singapore” predstavlja zvaničnu inicijativu pokrenutu od strane Ministarstva za digitalni razvoj i informacije Singapura, a singapurška Vlada odobrila je zakone i javne politike namenjene zaštiti ličnih i osetljivih podataka. <https://www.smartnation.gov.sg/about-smart-nation/secure-smart-nation/personal-data-protection-laws-and-policies/> pristupljeno 30.6.2024.

TEHNO-OPTIMIZAM I TEHNOLOŠKI RIZICI

Insistiranje na značaju da grad postane pametan i takmičenje gradskih vlasti da baš njihov grad bude prvi u Srbiji koji će dobiti taj epitet ukazuju na diskurs koji nije prisutan samo u našoj zemlji već se neguje u inicijativama za osnivanje pametnih gradova širom sveta, a to je narativ da je pametan grad superioran u odnosu na onaj grad koji to nije. Pametan grad nastoji da se predstavi kao neideo-loški, zdravorazumski, apolitični koncept, oko kog nema razloga da se neko ne složi. Naučnici, stručnjaci i inženjeri koji razvijaju tehnologije svoj rad vide kao ideološki neutralan i objektivan, koji može doneti dobro svima. Slično tome, biznis akteri i lokalne vlade smatraju da su njihove inicijative za izgradnju pametnih gradova inkluzivne, pragmatične i naučno zasnovane. Ono odakle potiče nedostatak kritike i neosnovani optimizam relevantnih aktera u vezi sa pametnim gradovima jeste tehno-optimizam, odnosno vera da se svi problemi, pa i oni gorući u gradovima, mogu rešiti implementacijom digitalnih tehnologija. Koncept pametnog grada je upravo i nastao u skladu sa principima ekološke modernizacije, odnosno tehnokratskog pristupa životnoj sredini po kom je svaki problem sadašnjice moguće rešiti „tehno-institucionalnim popravkama” (Hajer, 1995: 32). Pristalice ekološke modernizacije u tehnološkom razvoju vide rešenje za postizanje ravnoteže između očuvanja životne sredine i neodustajanja od ekonomskog progresa, odnosno tehnologiju posmatraju kao činilac koji će pomiriti tri dimenzije održivosti, a to su socijalna, ekonomska i ekološka. Ovakva optimistična percepcija uloge tehnologije kao univerzalnog rešenja za narastajuće probleme današnjice sprečava kritički pristup i preispitivanje nedostataka i potencijalnih problema koje te tehnologije mogu da donesu. Kako neki autori zapažaju, integracija pametnih tehnologija ne samo da nije doprinela rešavanju, već je dodatno zakomplikovala već postojeće probleme, i pritom dovela do stvaranja novih (Dodge and Kitchin, 2018: 205). Funkcionisanje pametnog grada počiva na umreženosti što većeg broja uređaja i korisnika, i dok, sa jedne strane, ta umreženost može imati pozitivne implikacije, kao što je brža razmena informacija ili efikasnije donošenje odluka, sa druge, ona doprinosi ranjivosti čitavog komunikacionog sistema jer potencijalne posledice više nisu ograničene na manji broj učesnika već se one efektom domina šire kroz čitav sistem. Osim toga, empirijske analize su pokazale da digitalne tehnologije mogu dovesti do novih

varijacija već postojećih problema u gradu. Naime, gledajući kroz istoriju kriminala postoji otkako postoje i urbana društva, te briga za bezbednost u pametnim gradovima ne predstavlja ništa novo, ali ono što je specifično u savremenom kontekstu pametnih gradova jeste način na koji se kriminalne aktivnosti izvode (*ibid*). Digitalne tehnologije omogućavaju izvršiocima da svoja dela počine sa ogromnih razdaljina, i to često uz mogućnost da ne budu uopšte detektovani, a samim tim i da ne odgovaraju za počinjeno delo. Pored toga, zahvaljujući softverskim alatima, napadi u „sajber” prostoru se danas mogu izvesti uz minimalne rizike i troškove, što je u pozitivnoj korelaciji sa motivacijom potencijalnih počinitelaca da se odluče da izvedu kriminalni akt (*ibid*).

Svi ovi faktori ukazuju na to da je neophodno objektivno i slojevito analiziranje prednosti i rizika koje sa sobom donosi implementacija IKT u urbanim područjima. To bi mogao biti zadatak svakog grada ili države pojedinačno u skladu sa svojim kontekstualnim specifičnostima. U ovom radu nećemo se osvrnati na komparaciju koristi i opasnosti od digitalnih tehnologija u gradovima, već ćemo samo ukratko obrazložiti koji su najveći bezbednosni izazovi po pojedinačne građane i zašto su oni značajni.

KIBERNETIČKA SIGURNOST I PRIVATNOST PODATAKA GRAĐANA

Deo kritike koji je privukao najveću pažnju javnosti u vezi sa uvođenjem IKT u gradove jesu pitanja etičke prirode. Naime, smatra se da se u okviru koncepta pametnog grada normalizuje narušavanje privatnosti stanovnika i manipulisanje njihovim stilovima života koji bivaju usmeravani ka ekološkoj potrošnji i turizmu (Vanolo, 2014: 894). Kako prikupljanje i analiza velikih podataka predstavljaju osnovno sredstvo za funkcionisanje pametnog grada (Kešić, 2023: 37), javila se zabrinutost zbog potencijalne zloupotrebe podataka radi nadzora stanovnika i ograničavanja građanskih sloboda. Smatra se da upotreba tehnologije u upravljanju može dovesti do determinizma podataka i normalizacije modela anticipativnog upravljanja (Dimitrijević, 2023: 95). To znači da se analizom podataka oblikuju profili pojedinaca i predviđaju njihove preferencije, odnosno anticipiraju se potencijalni proizvodi koje će kupiti, usluge

koje će koristiti, mesta na koja će ići, procenjuje se vrednost njihovog biznisa, verovatnoća da otplate kredit ili da plate određenu cenu za nešto (Kitchin, Cardullo and Di Felicianantonio, 2018: 9). Takvo profilisanje građana može da dovede do sortiranja stanovnika po određenim kategorijama, što znači da neke kategorije mogu da dobiju privilegovan status, dok, istovremeno, neke druge kategorije stanovništva mogu da budu marginalizovane i diskriminizovane (*ibid*). Osim anticipativnog upravljanja, kao problem se javlja i determinizam podataka, koji se odnosi na situaciju u kojoj pojedinci nisu samo profilisani, procenjeni i sortirani na osnovu onoga što su već učinili (proizvoda koji su kupili, mesta na kom su locirani i slično), već i na osnovu predikcija o tome šta bi mogli u budućnosti da učine (Ramirez prema Dimitrijević, 2023: 93). Prediktivna analitika podataka se tako koristi kako bi se procenili potencijalni događaji u budućnosti, i na osnovu toga donele odluke. Na primer, američka policija se koristi ovim strategijama kako bi predvidela koje lokacije su najpodložnije kriminalu, pa se tako donose odluke o područjima grada u koje preventivno treba usmeriti više policijskih patrola (Kitchin, Cardullo and Di Felicianantonio, 2018: 10). U pametnom gradu menja se uloga gradske uprave, pa ona postaje kontrolor (Dimitrijević, 2023: 88), odnosno nove tehnologije transformišu metode upravljanja društvom, zahvaljujući čemu vlast postaje tehnokratska, automatizovana, prediktivna i zasnovana na algoritmima (Kitchin, Cardullo and Di Felicianantonio, 2018: 8). Tehničkim jezikom i terminologijom pokušavaju da se prikriju relacije moći (Vanolo, 2014: 890), a građanin se svodi na nadziranog, kontrolisanog subjekta i potrošača koji predstavlja samo izvor za uzimanje podataka (Dimitrijević, 2023: 93).

Fukoova interpretacija Bentamovog koncepta „panoptikona” podseća nas na asimetrične odnose moći između nadzornika i nadziranih, odnosno, u kontekstu digitalizacije, između onih koji upravljaju tokovima podataka (privatne kompanije i nacionalne vlade) i izvora podataka (građani). Bentamov „panoptikon”, kao svojevrsni oblik arhitekture za nadziranje, imao je za cilj da oni koji su posmatrani budu u svakom trenutku svesni da su posmatrani i samim tim da budu podstaknuti da internalizuju oblike ponašanja koji se od njih očekuju, a kasnije, u vreme kada je Fuko sredinom sedamdesetih pisao „Disciplinu i kaznu”, moglo bi se reći da je ta arhitektura poprimila drugačiji oblik gde se više nije odnosila na cilindrični toranj iz kog nadzornik bilo kog trenutka može da posmatra zatvorenike,

već na CCTV kamere raspoređene svuda po gradu. Više od pedeset godina kasnije, od kada je Fuko ukazao na ulogu koju informacione tehnologije mogu imati u kontroli građana i inženjeringu društva, suočavamo se sa pojavom koja se više ne može objasniti „panopticismom“, to jest procesom internalizacije očekivanih poželjnih oblika ponašanja usled straha od kazne ili posledica, jer u slučaju savremenih digitalnih tehnologija u virtuelnom prostoru korisnici više nisu ni svesni da su nadzirani, ne znaju ko, ni u kom trenutku prikuplja podatke o njima, ne znaju šta se od njih očekuje, te samim tim ne mogu ni da biraju koje obrasce ponašanja će usvojiti (Rathbone, 2022).

Imajući sve ovo u vidu, može se reći da su izvori nesigurnosti po bezbednost pojedinaca u budućim pametnim gradovima višestruki, te je neophodan zakonski i regulativni okvir koji bi osigurao da će podaci koje građani svesno ili nesvesno emituju u informacioni sistem biti zaštićeni i da neće doprineti viktimizaciji stanovništva. Iako već postoje brojne inicijative i agende da se reguliše sajber bezbednost na različitim nivoima, od međunarodnog, preko evropskog kroz politike Evropske unije, do nacionalnog i lokalnog nivoa, ne postoji koherentan strateški i legislativni sistem koji bi uređivao sajber bezbednost u kontekstu pametnih gradova u Srbiji. Formiranje regulacionog sistema u sferi kibernetičke bezbednosti bilo bi od velikog značaja kako bi se stvorio mehanizam garancije zaštite privatnosti i sloboda građana. Zadatak države je da bude taj garant i da štiti svoje građane, makar i od sebe same, te smo se upravo iz tog razloga odlučili da pitanja kibernetičke bezbednosti građana posmatramo kroz javnopolitički diskurs u Srbiji.

POSTAVKA I NALAZI ISTRAŽIVANJA

U prethodnom delu rada pokušali smo da objasnimo razloge zbog kojih je važno baviti se kibernetičkom bezbednošću građana u savremenim društvima u kontekstu nastajanja pametnih gradova. Sada ćemo izložiti postavke na kojima počiva naše istraživanje o datoj temi.

Kao što je već navedeno, cilj ovog istraživanja bio je da se otkrije da li se u strateškim i legislativnim dokumentima u Republici Srbiji obrađuju problemi i izazovi kibernetičke bezbednosti i zaštite građana.

Kako u Srbiji još uvek ne postoje ni pametni gradovi, ni nacionalni planski dokumenti koji bi uredili potencijalnu buduću „pametnu” urbanizaciju, smatrali smo da je važno da uvidimo postoje li osnove za zaštitu od rizika u sferi digitalne realnosti, kako bi se stvorili dobri temelji za očuvanje bezbednosti građana kada se krene sa masovnom i intenzivnom digitalizacijom urbanih prostora. Metod koji smo primenili kako bismo došli do odgovora na postavljeno pitanje je metod analize sadržaja. Imajući u vidu da Šušnjić definiše komunikaciju kao „proces u kom neki pojedinac ili *institucija* nastoji da prenese neku poruku, preko određenih tehničkih sredstava, do određene grupe ljudi s namerom da izazove određene efekte u njihovom verovanju, stavovima i ponašanju” (Šušnjić, 1973: 249), smatrali smo analizu sadržaja najprikladnijim metodom za ispitivanje strateških nacionalnih dokumenata kao nosioca komunikacije, to jest poruka, od državnih tela ka široj javnosti, odnosno građana, naročito što svrha analize sadržaja može, između ostalog, biti otkrivanje fokusa institucionalne pažnje (Fajgelj, 2014: 375). U ovom istraživanju biće primenjen **namerni uzorak**, koji nastaje tako što istraživač na osnovu svoje stručnosti i uvida u osobenosti populacije vrši izbor svake jedinice u skladu sa predmetom istraživanja, odnosno radi dobijanja odgovora na istraživačka pitanja (Manić, 2017: 159). Za ovaj tip uzorka smo se opredelili oslanjajući se na Holstijevu procenu da je njegova primena pogodna kada se svaki izvor ne smatra podjednako značajnim za potrebe istraživanja, pa se uzorak formira tako što se odaberu jedinice koje se smatraju najtipičnijim za osnovni skup, što implicira da postoji kriterijum na osnovu kog se određuje šta se smatra tipičnom karakteristikom proučavane populacije (Holsti, 1968 prema Manić, 2017: 159). Ako istraživač bira svaku jedinicu uzorka po svom nahodanju, verujući da je tako izabrani uzorak reprezentativan za ceo osnovni skup, u tom slučaju formira *uzorak zasnovan na subjektivnom sudu* (Žižić, Lovrić i Pavličić, 1996: 141), što je vrsta namernog uzorka koju smo koristili u našem istraživanju.

Dokumenta koja su ušla u naš uzorak su: Ustav Republike Srbije, Krivični zakonik Republike Srbije, Zakon o informacionoj bezbednosti, Zakon o zaštiti podataka o ličnosti, Strategija za borbu protiv visokotehnološkog kriminala i Strategija razvoja informacione bezbednosti.

U Ustavu kao krovnom legislativnom dokumentu navodi se član 42, Zaštita podataka o ličnosti, kojim se jemči zaštita podataka o ličnosti i zabranjuje upotreba podataka o ličnosti izvan svrhe za koju

su prikupljeni (Ustav Republike Srbije, 2021). Stavke navedene u ovom članu se dalje uređuju zakonom, i to Zakonom o zaštiti podataka o ličnosti, koji uređuje „pravo na zaštitu fizičkih lica u vezi sa obradom podataka o ličnosti i slobodni protok takvih podataka, načela obrade, prava lica na koja se podaci odnose, obaveze rukovalaca i obrađivača podataka o ličnosti, kodeks postupanja, prenos podataka o ličnosti u druge države i međunarodne organizacije, nadzor nad sprovođenjem ovog zakona, pravna sredstva, odgovornost i kazne u slučaju povrede prava fizičkih lica u vezi sa obradom podataka o ličnosti” (Zakon o zaštiti podataka o ličnosti, 2018). U okviru Krivičnog zakonika, dvadeset sedmom glavom se jasno definišu krivična dela protiv bezbednosti računarskih podataka i dalje se pojedinačnim članovima uređuju segmenti kao što su računarska sabotaža, pravljenje i unošenje računarskih virusa, računarske prevare, ograničavanje pristupa javnoj računarskoj mreži i slično (Krivični zakonik RS, 2019). Zakon o informacionoj bezbednosti iz 2016. godine najopširnije od svih dokumenata uređuje mere zaštite od bezbednosnih rizika u informaciono-komunikacionim sistemima, dok Strategija razvoja informacione bezbednosti u RS za period od 2017. do 2020. godine kao prioritetsnu oblast definiše informacionu bezbednost građana, informacionu bezbednost zemlje i borbu protiv visokotehnološkog kriminala. Strategija za borbu protiv visokotehnološkog kriminala reguliše aktivnosti koje za cilj imaju suzbijanje visokotehnološkog kriminala koji se, prema zakonodavnom okviru Republike Srbije, odnosi na krivična dela kod kojih se „kao objekat ili sredstvo izvršenja krivičnih dela javljaju računari, računarski sistemi, računarske mreže, računarski podaci, kao i njihovi proizvodi u materijalnom ili elektronskom obliku” (Strategija za borbu protiv visokotehnološkog kriminala, 2018).

Pregledom navedenih dokumenata i analizom njihovog sadržaja može se zaključiti da su problemi u vezi sa kibernetičkom bezbednosti građana dotaknuti i delimično obrađeni u zakonodavnom i strateškom okviru Republike Srbije. Od navedenih dokumenata, Zakon o informacionoj bezbednosti najtemeljnije obrađuje rizike koji direktno utiču na potencijalnu eksploataciju podataka građana i na njihovu bezbednost. Iz strategije razvoja informacione bezbednosti takođe se može videti da u diskursu javnih politika u Srbiji postoji svest o opasnostima koje digitalne tehnologije donose i njihovim reperkusijama na građane, međutim, problem sa ovom strategijom je što je njen period važenja istekao 2020. godine, a nova nije sači-

njena. Isto se odnosi i na strategiju za borbu protiv visokotehnološkog kriminala koja se odnosila na period 2019–2023. godine. Dakle, nedostaje kontinuiran rad na problemima kibernetičke bezbednosti građana, što može biti posebno problematično imajući u vidu brz i nepredvidiv razvoj tehnologija.

ZAKLJUČAK

U ovom radu analizirani su bezbednosni izazovi pametnih gradova sa posebnim osvrtom na kibernetičku sigurnost i privatnost podataka u strateško-pravnim okvirima Republike Srbije. Kroz pregled Ustava, Krivičnog zakonika, Zakona o informacionoj bezbednosti, Zakona o zaštiti podataka o ličnosti, Strategije za borbu protiv visokotehnološkog kriminala i Strategije razvoja informacione bezbednosti, ustanovljeno je da su ključni aspekti zaštite kibernetičke bezbednosti i privatnosti građana delimično pokriveni zakonodavstvom. Međutim, analiza je pokazala da nedostatak kontinuiranog rada na strateškim dokumentima predstavlja značajan izazov. Strategije razvoja informacione bezbednosti i borbe protiv visokotehnološkog kriminala, čiji je period važenja istekao, ukazuju na potrebu za ažuriranim i sveobuhvatnim pristupom u regulisanju sajber bezbednosti. Srbija je u procesu praćenja globalnog trenda digitalizacije urbanih prostora, ali je važno da se ti procesi sprovedu uz adekvatnu zakonsku i stratešku regulaciju kako bi se obezbedila efikasna zaštita građana. Poseban izazov predstavlja brzina tehnoloških promena, koja zahteva fleksibilne i prilagodljive strategije. Da rezimiramo, iako Srbija ima solidne zakonske temelje za zaštitu kibernetičke bezbednosti građana, neophodno je unaprediti implementaciju postojećih zakona i razviti kontinuirane i ažurirane strateške dokumente. Ovo će omogućiti efikasniju zaštitu građana u kontekstu razvoja pametnih gradova i odgovarati na nove izazove koje donosi digitalizacija urbanih prostora.

LITERATURA

- Dimitrijević, L. (2023). Strategije razvoja pametnih gradova: determinizam podataka i tehnološki suverenitet. *Sociološki pregled*, 57(1): 76–101.
- Dodge, M., and Kitchin, R. (2018). The challenges of cybersecurity for smart cities. *Creating smart cities*. Routledge.
- Fajgelj, S. (2014). *Metode istraživanja ponašanja*. Beograd: Centar za primenjenu psihologiju.
- Hajer, M. (1995). *The Politics of Environmental Discourse. Ecological Modernization and the Policy Process*. New York: Oxford University Press.
- Kesić, D. B. (2023). „Pametni” gradovi: nova paradigma urbanog razvoja. *Sociološki pregled*, 57(1): 32–52.
- Kitchin, R., Cardullo, P., and Di Felicianantonio, C. (2018). Citizenship, Justice and the Right to the Smart City. *The Programmable City Working Paper 41*; <https://progcity.maynoothuniversity.ie/>
- Krivični zakonik, „Službeni glasnik Republike Srbije”, br. 35/2019.
- Manić, Ž. (2017). *Analiza sadržaja u sociologiji*. Beograd: „Čigoja štampa” i Institut za sociološka istraživanja Filozofskog fakulteta u Beogradu.
- Milošević, M. et al. (2019). Smart City: Modeling Key Indicators in Serbia Using IT2FS. *Sustainability*, 11(13), 3536; <https://doi.org/10.3390/su11133536>.
- Prigoda, L., Bogavac, M. i Čekerevac, Z. (2022). Srbija i pametni gradovi. *FBIM Transactions*, 10(1): 70–85. DOI 10.12709/fbim.10.10.01.08
- Rathbone, M. (2022). Panopticism, impartial spectator and digital technology. *Indo-Pacific Journal of Phenomenology*, 22(1), e2064720. <https://doi.org/10.1080/20797222.2022.2064720>
- Strategija razvoja informacione bezbednosti u Republici Srbiji za period od 2017. do 2020. godine, „Službeni glasnik Republike Srbije”, br. 53/2017.
- Strategija za borbu protiv visokotehnološkog kriminala za period 2019–2023. godine, „Službeni glasnik Republike Srbije”, br. 71/2018.
- Ustav Republike Srbije, „Službeni glasnik Republike Srbije”, br. 115/2021.
- Vanolo, A. (2014). Smartmentality: The Smart City as Disciplinary Strategy. *Urban Studies*, 51(5): 883–898.

Zakon o zaštiti podataka o ličnosti, „Službeni glasnik Republike Srbije”, br. 87/2018.

Zakon o informacionoj bezbednosti, „Službeni glasnik Republike Srbije”, br. 77/2019.

Žižić, M., Lovrić, M. i Pavličić, D. (1996). *Metodi statističke analize*. Beograd: Ekonomski fakultet Univerziteta u Beogradu.

Linkovi

„Niš – grad naprednih tehnologija i prvi 'pametan grad' u Srbiji”, Niške vesti, 28.11.2019. <https://niskevesti.rs/nis-grad-naprednih-tehnologija-i-prvi-pametni-grad-u-sbiji/> pristupljeno: 28.6.2024.

„Indija na korak do 'pametnog grada'”, Vojvodina uživo, 22.10.2022. <https://vojvodinauzivo.rs/indija-na-korak-do-pametnog-grada/> pristupljeno: 28.6.2024.

„Pametnim rešenjima do pametnog grada – Započela izrada Strategije za uspostavljanje pametnog grada u Pirotu”, SKGO, 6.6.2023. <https://www.skgo.org/vesti/detaljno/3182/pametnim-resenji-ma-do-pametnog-grada-zapocela-izrada-strategije-za-uspostavljanje-pametnog-grada-u-pirotu> pristupljeno: 28.6.2024.

„Projekat mape puta pametnih gradova za Srbiju pokrenut iz Kragujevca”, Grad Kragujevac, 10.4.2024. <https://kragujevac.ls.gov.rs/vest/sr/64548/projekat-mape-puta-pametnih-gradova-za-srbiju-pokrenut-iz-kragujevca.php> pristupljeno: 28.6.2024.

Smart Nation Singapore, Government's Personal Data Protection Laws and Policies <https://www.smartnation.gov.sg/about-smart-nation/secure-smart-nation/personal-data-protection-laws-and-policies/> Accessed 30.6.2024.

SECURITY CHALLENGES OF SMART CITIES – CYBERSECURITY AND DATAPRIVACY IN STRATEGIC-LEGAL FRAMEWORKS FROM A SOCIOLOGICAL PERSPECTIVE

SUMMARY

In light of the increasing integration of information and communication technologies into the infrastructure of smart cities, this paper explores how issues of cybersecurity and data privacy are addressed in strategic documents that regulate urban technological systems. Smart cities play a key role in shaping modern urban practices through their ability to use technology to improve the quality of life for residents and the efficiency of city services. The research will begin with a comprehensive review of relevant literature that deals with the security issues of smart cities, with particular emphasis on the critical school of thought within the 3RC model, which considers the differences between technology-oriented ('hard') and human-oriented ('soft') approaches. The methodology relies on a secondary analysis of available strategic documents of cities from various global contexts, with special emphasis on analyzing the regulatory framework for the future development of smart cities in Serbia. The choice of Serbia as a case study is particularly relevant because our country represents an example of how transitional societies adapt their legal and technological frameworks in the context of integration into broader European and global trends, providing insight into unique challenges and solutions in regulating cybersecurity and data privacy. Through the comparison of selected strategic-legislative systems as case studies, we aim to identify key security policies and mechanisms for protecting citizens' privacy. The research aims to discover how cyber risks are recognized and effectively addressed through existing strategies, and to determine the impact of sociological perspectives and insights on the formation and implementation of these policies. The results of the study will provide deeper insights into the effectiveness of current regulations and will suggest recommendations for their improvement, aligned with dynamic social and technological changes in urban environments. The analysis is expected to highlight key weaknesses and potentials for improvement in the field of cybersecurity and privacy protection, emphasizing the importance of adaptive security practices in global urban development.

KEYWORDS: *smart cities, cybersecurity, data privacy.*