PREGLEDNI ZNANSTVENI ČLANAK

UDK: 004.77
DOI: 10.59245/ps.32.2.3
Primljeno: kolovoz 2022.

KRUNOSLAV ANTOLIŠ *

Pametni gradovi i informacijsko-komunikacijske tehnologije

Sažetak

Svjedoci smo velikih tehnoloških promjena u današnjemu modernom svijetu. Sve te tehnološke promjene i nove IoT (engl. Internet of Things) tehnologije, kojoj je hrvatski pandan IS (internet stvari) olakšavaju svakodnevni život, ali donose i mnoge ranjivosti, rizike i prijetnje. Svaka ranjiva situacija u pametnom gradu može dovesti do ozbiljnih ugroza za cijeli grad te prouzročiti goleme posljedice. Oslonac na nove IKT (informacijsko-komunikacijske tehnologije) sustave u pametnom gradu donosi i brojne digitalne tragove, koji izuzeti na zakonit način od zakonom ovlaštene osobe mogu znatno pridonijeti u istraživanju sigurnosnih ugroza i sankcioniranju počinitelja kaznenih djela i prekršaja. No da bi cjelokupni IKT potporni sustav bio izvor digitalnih dokaza, sveukupna rješenja moraju biti zakonom utemeljena i usklađena s europskim i nacionalnim normama. Kompilacije, ali i komparativne metode primijenjene u radu imaju za cilj uočavanje najboljih praksi, međunarodnih, ali i domaćih pristupa integriranja IKT-a u koncept pametnih gradova, primjerice u Zadru. U radu će se primijeniti metode znanstvenog istraživanja deskripcije konkretnih primjera pametnih gradova i njihovih rješenja u pojedinim ključnim segmentima za njihovo funkcioniranje i optimiziranje resursa. Metode analize i sinteze u definicijskom poimanju pametnih gradova, na korištenim izvorima, tj. tekstovima iz domaće i strane literature, imale su za cilj predstaviti razne pristupe, ali i nove paradigme važne za daljnji razvoj koncepta pametnih gradova.

Ključne riječi: *pametni gradovi, ranjivosti, rizici, prijetnje, informacijsko-komunikacijske tehnologije.*

* izv. prof. dr. sc. Krunoslav Antoliš, glavni policijski savjetnik, Veleučilište kriminalistike i javne sigurnosti, Policijska akademija „Prvi hrvatski redarstvenik“, MUP RH, Zagreb, Hrvatska.

1. UVOD

U suvremenom tehnologijom determiniranom svijetu veliku ulogu imat će pametni gradovi. No da bismo se mogli sustavno pozabaviti tom problematikom, potrebno je prije svega odrediti što čini okvir pametnoga grada. Bilo bi dobro i odrediti što je točno zajednica, jer ta definicija može uvjetovati odnose i veze između suvremenih gradova i sela te tokova ljudi. Prije nego što se odlučimo izgraditi pametan grad, moramo znati i odgovor na pitanje zašto to želimo.

Proučiti zajednicu znači proučiti i upoznati njezine građane, njezino poslovanje i njezine sustave donošenja odluka. Pritom je važno oslanjati se na inicijative koje bi trebale definirati uloge, odgovornosti i ciljeve, a iz kojih bi trebala proizići tzv. politike pametnih gradova. Ukratko, ljudi, procesi i tehnologija tri su načela uspjeha pametne gradske inicijative. Gradovi moraju proučavati svoje građane i zajednice te stvoriti politike i ciljeve kako bi se zadovoljile potrebe građana. Zatim se može pomoću tehnologije sve to implementirati. Dakle, dolazak novih informacijsko-komunikacijskih tehnologija uvelike je poboljšao kvalitetu života građana. Iako su te tehnologije olakšale naš život, njihova upotreba također donosi rizike. Koncept pametnoga grada privukao je veliku pozornost u tehničkom svijetu. Nove tehnologije, uz jednostavnu i brzu komunikaciju, građanima omogućuju goleme uštede, primjerice bolje iskorištavanje i uporabu izvora energije. Uporaba i razvoj IKT sustava također donose rizike i prijetnje, koje je potrebno osvijestiti. Kako svemu tome pristupiti, možda je dobar primjer Peter Calthorpe (rođen 1949.). Riječ je o arhitektu, urbanom dizajneru i urbanistu iz San Francisca, jednom od osnivača Kongresa za novi urbanizam, zagovaračke skupine sa sjedištem u Chicagu osnovane 1992. koja promiče prakse održive gradnje. Zbog svojih radova na redefiniranju modela urbanog i prigradskog razvoja u Americi, časopis Newsweek proglasio ga je jednim od dvadeset pet inovatora na vrhuncu. Poznat je i po zagovaranju tzv. kineskog urbanističkog pristupa sedam načela, koja su:

1. Potreba očuvanja prirode, ekologije, agrarnog krajolika i mjesta kulturne baštine.
2. Potreba stvaranja okoliša – susjedstva mješovite namjene i mješovitih prihoda.
3. Potreba dizajniranja prohodnih ulica i kvartova po mjeri čovjeka – primjerenih ljudima.
4. Prednost biciklističkim mrežama i ulicama bez automobila, primjerice stvoriti prostor kolnika samo za bicikle.
5. Povećati gustoću cestovne mreže, a istodobno ograničiti veličinu gradskih blokova.
6. Razviti sustav brzog autobusnog prijevoza.

Mnogi gradovi u razvoju diljem svijeta pate od sve veće prometne gužve. Veliki troškovi prometnog zagušenja, uključujući neodrživo vrijeme putovanja na posao i zagađenje (npr. Binkman 2016, Simeonova i sur. 2019, Lu i sur. 2017), naveli su urbaniste da se zalažu za nove ili proširene sustave javnog prijevoza. Međutim, njihova je izgradnja često vrlo skupa, posebno za gradove s ograničenim budžetom. Kako bi prevladali tu prepreku, mnogi se gradovi okreću sustavima brzog autobusnog prijevoza (BAP) koji osiguravaju namjenske trake s pravom prolaska za gradske

autobuse te koriste mrežu strateški lociranih postaja za preuzimanje i iskrcavanje putnika. Pružaju slične prijevozne usluge kao podzemna ili laka željeznica, ali su jeftiniji za razvoj i rad, visokokvalitetan tranzit i pristupačan BAP.

7. Uskladiti gustoću prometa s tranzitnim kapacitetima.

2. RAZNI PRISTUPI DEFINICIJI PAMETNOGA GRADA

Deakin, primjerice, definira pametan grad kao onaj koji se koristi informatičkim tehnologijama kako bi zadovoljio zahtjeve tržišta te ističe da je uključenost zajednice u proces nužna za pametan grad. Stoga, pametni grad bio bi onaj koji ne samo da posjeduje IKT u pojedinim područjima nego je i tu tehnologiju implementirao tako da pozitivno utječe na lokalnu zajednicu. Pametni grad može se definirati i kao integracija postojeće konstrukcije s novim informacijskim i komunikacijskim tehnologijama kako bi se stvorio sveobuhvatan sustav učinkovitih urbanih e-usluga. Spomenuto povezuje fizičku infrastrukturu, infrastrukturu informacijske tehnologije, društvenu te poslovnu infrastrukturu radi ojačanja kolektivne inteligencije grada (Chen, 2021, prema Maruf et al., 2020). Također, događa se da se nova tehnologija suočava s brojnim tehničkim, društvenim, ekonomskim izazovima i problemima (Chen, 2021, prema Al-Saidi i Zaidan, 2020). Autori Ismagilova et al. (2020) navode kako su pametni gradovi dizajnirani na infrastrukturi temeljenoj na IKT-u koji omogućuje internet stvari, a podržava društvenu i urbanu međusobnu povezanost na temelju veće interakcije građana i vladine učinkovitosti.

Karakteristike pametnoga grada su i učinkovitija upotreba fizičke infrastrukture (ceste, izgrađeni okoliš i druga fizička sredstva) putem umjetne inteligencije i analize podataka kako bi se podržao snažan i zdrav ekonomski, društveni i kulturni razvoj. No važno je i komuniciranje s lokalnim zajednicama u upravljanju i odlučivanju pomoću otvorenih inovacijskih procesa, veće učinkovitosti gradskih institucija putem e-uprave s naglaskom na sudjelovanje građana. Tu je i nezaobilazno učenje te prilagođavanje, a time i učinkovitije i brže reagiranje na promjenjive okolnosti, poboljšavajućih korisnost grada.

Pametan grad ne podrazumijeva samo tehnološke promjene nego i promjenu životnih uvjeta te ulaganja u ljudski kapital (Ståhlbröst et al. 2015, prema Neirotti i sur., 2014). Pametni gradovi sastoje se od različitih vrsta IoT senzora, uključujući one za kontrolu prometa, parkirne senzore, prometnu rasvjetu itd (Chen, 2021, prema Nakano i Washizu, 2021).

Tehnologije usvojene u pametnim gradovima uglavnom su najsuvremenije te se ne mogu naći izvan takvih gradova, pa upravo zbog toga važni podaci koje te tehnologije podupiru mogu biti zanimljivi i sa stajališta ugroženosti različitim napadima (Vorakulpipat et al. 2021). Pametni gradovi odnose se na upotrebu novih tehnoloških rješenja za poboljšanje kvalitete života građana, interakcije s gradskom upravom te promicanje održivog razvoja (Ismagilova et al., 2020, prema Chourabi i sur. 2012; Yahia i dr. 2019; Yu i Xu 2018).

Prema određenim izvorima (Chen, 2021), unutar pametnoga grada postoje brojne podjele na podsustave, kao što su pametna vlada (implementacija poslovnih procesa te pružanje visokokvalitetnih usluga), pametna zdravstvena zaštita (koristi tehnologije, primjerice nosivi

uređaji, mobilni internet za dinamički pristup informacijama, povezivanje ljudi, zdravstvenih ustanova i institucija), pametna energija (pametna energetska mreža koja može poduprijeti dvosmjernu komunikaciju i električne struje između različitih entiteta u mreži), pametni prijevoz (za smanjenje prometnih gužvi, povećanje razine sigurnosti, uštedu vremena, smanjenje potrošnje goriva, koriste sustave upozorenja vozača, sustave praćenja i evidentiranja prekršaja...), pametna zgrada (senzori i mrežna tehnologija za komunikaciju između građevinske opreme).

Može se zaključiti kako se pametnim gradovima smatraju oni koji uz bolju i veću primjenu modernih tehnologija omogućuju poboljšanje usluga građanima, bolju iskorištenost resursa te smanjivanje negativnog utjecaja na okoliš. Sigurnost i privatnost ne utječu samo na pametni grad u cjelini nego i na njegove pametne sastavnice koje uključuju zdravstvo, obrazovanje, prijevoz, tvornice, zgrade (Vorakulpipat et al. 2021).

Poželjni oblici inteligencije u pametnim gradovima su sljedeći. Orkestrirajuća inteligencija, poradi koje gradovi uspostavljaju institucije i načine rješavanja problema koji se temelje na zajednici, primjerice kao u Bletchley Parku, gdje je tim na čelu s Alanom Turingom dešifrirao nacističku Enigmu. To je među prvim primjerima pametnoga grada.

Inteligencija za osnaživanje u sklopu čega gradovi osiguravaju otvorene platforme, eksperimentalne objekte i pametnu gradsku infrastrukturu kako bi se implementirale inovacije u pojedinim četvrtima. Kista Science Cityju u Stockholmu i Cyberport u Hong Kongu mjesta su gdje se mogu vidjeti te inovacije, a slične su strukture napravljene i u Melbourneu. Kada je gradska infrastruktura napredna zbog prikupljanja podataka u realnom vremenu, uz analizu i prediktivno modeliranje u svim gradskim četvrtima, tada govorimo o inteligenciji instrumentacije. Postoji mnogo kontroverzi u vezi toga, osobito kada je riječ o nadzoru u pametnim gradovima. Primjeri instrumentalne inteligencije provedeni su u Amsterdamu.

Pametni prostor još se naziva „ambijentalna inteligencija“ ili „digitalno radno okružje“, tj. prostor u kojem bi se isplatilo raditi već danas, a sutrašnjica će teško moći proći bez takve poslovne okoline. Lokalnim upravama neće biti pametno samo pokazati ledinu blizu važnih prometnica pa očekivati da projektanti osmisle neku, kao, zgodnu poduzetničku zonu koju će osloboditi od plaćanja komunalnih naknada. U svijetu hibridnog rada i povezanih stvari vladat će ambijentalna inteligencija. Riječ je o konceptu koji čine senzori i aktuatori, korisnička sučelja, industrijska komunikacijska sučelja, komunikacijski protokoli, programska podrška sustava i programski alati koji omogućuju da se pomoću sustava i komponenti visokog stupnja integracije, kao što su osobna i industrijska računala, specijalizirana mjerna i upravljačka oprema te komunikacijski sustavi opće namjene izrade uređaji i sustavi koji će prepoznavati potrebe korisnika i pomagati im u njihovu životnom i radnom okružju, kao i aktivnostima. Ambijentalna inteligencija koncept je za buduće društvo znanja u kojem inteligentna korisnička sučelja omogućuju međusobnu komunikaciju korisnika i računala, kao i njihovu interakciju s okruženjem u realnom vremenu. U osnovi su tog koncepta korisniku usmjerena računala, olakšan pristup korisnika, kao i kontrola i podrška korisnikove interakcije. Ambijentalna inteligencija danas se znanstveno izučava na Sveučilištu u Zagrebu putem sljedećih sadržaja: dizajn uređaja ili sustava za pomoć korisniku u njegovu radu i življenju, organiziranje sustava kao mreže specijaliziranih uređaja,

korištenje standardiziranih protokola, sučelja i komponenti, procjena i na odgovarajući način korištenje svojstava industrijskih uređaja, podsustava i metoda, planiranje i organiziranje vođenja projekta od zamisli do ostvarenja, kritiziranje i argumentiranje odluke i ideje pri komunikaciji s drugim timovima čiji projekti čine cjelinu, odabir odgovarajućih osjetila, analiziranje potreba korisnika, prezentiranje rezultata javnosti, analiziranje potreba korisnika metodom „design thinking", projektnog rada i projektnog dokumentiranja te popularnog i stručnog izvještavanja. Prvobitna ideja uklopljena je u koncept društveno korisnog učenja.

3. PRIMJERI RAZVOJA PAMETNIH GRADOVA U SVIJETU I KOD NAS

Brojni su se gradovi odlučili na razvitak u smjeru onih pametnih te sustavno nastoje provoditi strategije za prilagodbu postojeće imovine i mreža. Najpoznatiji primjeri takvih gradova su Busan, Tokio, London, New York, Pariz, Amsterdam, Reykjavik, Dubai, Stockholm, Santander (Ismagilova et al., 2020, prema Forbes 2019; Peris-Ortiz et al., 2016; Simonofski et al., 2019), Beč, Toronto, Kopenhagen, Hong Kong i Barcelona (Pérez-Martınez, Martinez--Ballesté i Solanas, 2013, prema Activa, 2012).

U Nizozemskoj, točnije Rotterdamu, prometna uprava prati oko 22.000 vozila u kretanju svako jutro, a regionalna agencija za okoliš prikuplja podatke o kvaliteti zraka po satu na širem području grada, što je više od 175.000 opažanja godišnje (Zoonen, 2016).

Kopenhagen je primjer vodećih zelenih gradova u svijetu zbog smanjenja emisije CO_2. U gradu je uvedena i pametna LED rasvjeta sa senzorima pokreta koji automatski smanjuju razinu osvjetljenja kada senzor očita da nema prolaznika te se tako smanjuje svjetlosno onečišćenje i štedi električna energija (Fischer, 2017). Cilj je da Kopenhagen do 2025. postane neutralan u odnosu na ugljikovodike te da se smanje štetni utjecaji na stanovnike (posljedice svjetlosnog i zvučnog onečišćenja, onečišćenja zraka te konzumacije konvencionalno uzgojenog voća i povrća).

Fischer (2017) u svojem članku navodi i Amsterdam kao jedan od najpametnijih gradova na svijetu. Naveo je platformu Social Glass putem koje se prikupljaju i povezuju podaci s raznih društvenih mreža, koji se potom analiziraju kako bi se došlo do informacija o raspoloženju, stanju i željama građana. To je zapravo sustav koji može procesirati velike količine podataka te iz njih izvući iskoristive zaključke, primjerice može otkriti gužve u prometu, ali i okupljanja građana tijekom festivala, doznati koji su im sadržaji najatraktivniji te s kojim se problemima suočavaju.

Indija je objavila planove za razvoj 100 pametnih gradova diljem zemlje za pokretanje gospodarskog rasta uz stvaranje tehnoloških rješenja za interakciju građana (Ismagilova et al., 2020, prema Praharaj i sur. 2018).

Kada je riječ o suvremenoj i naprednoj tehnologiji, Kina je jedna od najpoznatijih zemalja, a njezin je pristup doveo do brojnih projekata utemeljenih na politikama za potencijalno preoblikovanje gospodarskih struktura, transformaciju gospodarskog razvoja, poboljšanje konkurentnosti radnika, kao i učinkovitosti vlade u smislu upravljanja energijom i okolišem (Ismagilova et al., 2020, prema Yu i Xu 2018).

Prema Jupiter Researchu, Šangaj je broj jedan u svijetu za 2022. zahvaljujući vodećoj svjetskoj platformi podataka o građanima. Riječ je o gradu koji ima više od 1000 različitih usluga za svoje stanovnike (Knezović, 2022).

Osim Šangaja, i ostali azijski gradovi (Seul, Peking) u vrhu su zahvaljujući mogućnostima i tehnologijama vezanim uz pametne gradove. Njihove platforme za upravljanje podacima te digitalizirano upravljanje komunalnim i javnim uslugama izrazito su napredne.

U Hrvatskoj su primjeri pametnih gradova Zadar, Split i Dubrovnik. Pametne govornice u Zadru je postavio Hrvatski Telekom, a one pružaju besplatni Wi-Fi. Također, ondje se mogu kupiti karte za međugradski prijevoz, kao i one za parkiranje. U Dubrovniku je razvijena prva pametna parkirališna aplikacija, a u Splitu je Ericsson Nikola Tesla razvio IT rješenja, aplikaciju za pametni parking (Fischer, 2017). U Dubrovniku se također može naći Bigbelly, bio spremnik za prikupljanje otpada, kao i LED svjetiljka s integriranim multifunkcionalnim senzorskim sklopom radi smanjenja razine osvijetljenosti ako nema prolaznika. U Splitu se koriste solarni paneli za proizvodnju električne energije, pametni kontejneri, inteligentne prskalice na zelenim javnim površinama, potom prilagođeno paljenje javne rasvjete, alarmiranje nadležnih službi u slučaju kriznih situacija te podaci i informacije o javnom prijevozu u realnom vremenu. Krk kao prvi hrvatski pametni otok ima mrežu e-punionica, car/bike sharing, moderniziranu javnu LED rasvjetu, pametne klupe i kante za otpad, sustav koji prati popunjenost parkirališnih mjesta, pametni sustav upravljanja vodoopskrbom, kanalizacijom te sustavom pročišćavanja otpadnih voda.

Neki od ostalih hrvatskih gradova koje se smatraju pametnima su Ivanec, Jastrebarsko, Karlovac, Labin, Makarska, Pleternica, Poreč, Pula, Rijeka, Umag, Zagreb i Koprivnica. U Republici Hrvatskoj dostupni su brojni izvori financiranja od kojih su najvažniji Europski strukturni i investicijski fondovi. Iako je uvođenje „pametnih“ rješenja u hrvatske gradove jako skupo, uvijek je važno slušati i uvažiti mišljenja građana te barem napraviti procjenu poboljšanja kvalitete života koja bi nastala kao posljedica uvođenja određenog pametnog rješenja.

4. PRIVATNOST U PAMETNIM GRADOVIMA

Iako pametni gradovi olakšavaju život i čine ga jednostavnijim, povezanost i međuovisnost čine ga ranjivim na sigurnosne napade, kao i napade na privatnost (Sookhak et al., 2019). Prema najnovijim istraživanjima, ljudi su zabrinuti za privatnost te se pitaju tko i zašto koristi njihove osobne podatke (Zoonen, 2016).

Autori Cui et al. (2018) ističu kako osjetljive informacije koje se dijele s trećom stranom, a posebice kriptirana komunikacija između i unutar virtualne stvarnosti, čine podatke ranjivim, a naročito one koje senzori pohranjuju, pa sve to čini problem ugroze privatnosti realnim. Pametni gradovi ranjivi su na ugroze privatnosti, primjerice podatke kao što su identitet, lokacija, zdravstveno stanje, način života pa bi bilo opasno otkrivati to nepouzdanim ili neovlaštenim subjektima, kako u fizičkom tako i u virtualnom svijetu (Zhang et al., 2017).

Zabrinutost za privatnost ljudi, autor Zoonen (2016) podijelio je na shemu dva po dva u kojoj identificira četiri vrste mogućih osjetljivosti koje ljudi mogu imati o podacima pametnog

grada. Prva su vrsta osobni podaci koji se koriste u uslužne svrhe. Riječ je o podacima koje grad prikuplja o svojim stanovnicima, primjerice podaci o rođenju, smrti, braku, stanovanju (prvi kvadrant). Svrha je tih podataka poboljšanje gradskih usluga. Izazovi privatnosti u tom su kvadrantu umjereni jer je ta vrsta podataka sastavni dio upravljanja gradom, ali postoji kontinuirani rizik od prelaska percepcije tih podataka u drugi kvadrant. Druga su vrsta osobni podaci koji se koriste radi nadzora (drugi kvadrant), primjerice policijski podaci o prekršajima i slično, podaci o javnom prijevozu i oni lučkih vlasti. Kombinacija vrlo osobnih podataka prikupljenih i korištenih u svrhu nadzora i državne kontrole čine ovaj kvadrant vrlo spornim među zagovornicima privatnosti. Treća su vrsta neosobni podaci koji se upotrebljavaju radi nadzora. To se odnosi na sve vrste podataka koji se ne mogu povezati s pojedincem te se upotrebljavaju radi nadzora i kontrole, primjerice praćenja sporta i gužve. Takvi podaci nisu osjetljivi jer ne nadziru pojedinca nego skupine (primjerice u prometu). Pritom se koristi softver za prepoznavanje lica u gužvama pa su prakse njegove uporabe izazvale građanske, političke i pojedinačne sumnje, a u SAD-u su održavani prosvjedi tvrdeći da takav način rada izaziva rasističko profiliranje s predrasudama. Posljednja, četvrta vrsta su neosobni podaci prikupljeni radi usluge, s ciljem dobrobiti građana. Toj skupini pripadaju podaci za praćenje kvalitete zraka, buke i vode, pametnoga gospodarenja otpadom te svi podaci koje gradovi objave na svojim portalima. Iako većinom nisu opasni za politiku i vladu, zabrinutost se javlja jer se prilikom metoda profiliranja može omogućiti ponovna identifikacija pojedinaca iz agregatnih i anonimiziranih podataka.

Kao primjer problema privatnosti autor Zoonen (2016) u svojem je članku istaknuo kante sa senzorima. Svijet je upoznat s pametnim kantama za otpad, uvedene su radi smanjenja troškova i poboljšanja učinkovitosti. No autor skreće pozornost na to kako neke vrste pametnih kanti uključuju samo senzor koji mjeri razinu otpada, a druge pak omogućuju istodobnu provjeru autentičnosti korisnika putem pristupa pametnoj kartici te u tome uočava problem privatnosti. Tako postoje kante koje mjere samo ako je regalno skladište puno i treba ga isprazniti. Važno je napomenuti da u tom slučaju nije poznato tko je ubacio otpad, ali sustav osigurava da će se kanta isprazniti na vrijeme. Zaključak je da njihovi osobni podaci u kombinaciji sa svrhom usluge vjerojatno neće izazvati zabrinutost. S druge, pak, strane, odlaganje otpada u takve spremnike može zahtijevati provjeru autentičnosti kartice osobe koja želi baciti svoje smeće. Iako autentifikacija i sprečavanje nezakonitog otpada mogu biti glavna svrha tog sustava, to također omogućuje prikupljanje osobnih podataka o tome tko koliko baca u određenu kantu pa autor u tom slučaju skreće pozornost na problem privatnosti.

5. SIGURNOST U PAMETNIM GRADOVIMA

Autor Chen (2021) u svojem je detaljno razrađenom članku naveo da je jedan od sigurnosnih izazova kod pametnih zgrada kršenje privatnosti, a to je zbog visokofrekventnih podataka o potrošnji energije korisnika koji se prenose s pametnih brojila korisnika na druge subjekte pametne mreže, što ugrožava privatnost korisnika. Pritom se lako mogu otkriti osjetljive informacije, primjerice vrsta električne opreme koja se koristi, je li zgrada prazna ili puna. Kao sljedeći izazov autor je naveo prisluškivanje, pri čemu se ponovno može narušiti

privatnost dobivanjem privatnih podataka o korisniku. Potom, sigurnosni je izazov i promjena ili ponavljanje poruke, primjerice izmjena poruke za mjerenje pametnog mjerača podataka ili umetanje nove poruke o potrošnji.

Pregled sigurnosnog krajolika identificirao je sigurnosne prijetnje kao što su kod pametnih mreža ranjivost protokola, privatnosti, prisluškivanja i napada na uređaje povezane s internetom. Sustavi za automatizaciju zgrada imaju prijetnje nesigurnih protokola te nedostatka izvorne provjere autentičnosti dugog životnog ciklusa uređaja, kod bespilotnih letjelica sigurnosni problem uključuje ometanje komunikacije, kod pametnih vozila presretanje komunikacije, za IoT senzore prijetnje mogu biti kvar senzora ili održavanje povjerljivosti podataka, a za sigurnost platforme u oblaku sigurnosne prijetnje mogu biti zlonamjerne unutarnje prijetnje, napadi uskraćivanja usluge te ranjivosti sustava i aplikacija (Ismagilova et al., 2020, prema Baig i sur. 2017).

Sigurnosni izazovi u pametnom prijevozu bili bi obustava poruke, širenje lažne informacije (lažni certifikati, upozorenja), uskraćivanje usluge (slanje velike količine nevažnih poruka pa se blokira komunikacijski kanal), krivotvorenje identiteta (hakiranje osobnih iskaznica te ulazak u mrežu da se obmane druga vozila), prisluškivanje (na bežičnoj komunikaciji u automobilskoj mreži) i hardverska manipulacija (manipulacija semaforom da je uvijek zeleno) (Chen, 2021).

Prijetnja sigurnosti, kako navode autori Cui et al., (2018), jesu i Botnet aktivnosti u pametnim gradovima temeljene na IoT-u. Botnet mreže mogu predstavljati velike i ozbiljne prijetnje IoT sustavima, primjerice mreža Mirai Botnet koja može zaraziti uređaje (npr. web kamere, pisače i usmjerivače) te infekciju proširiti na mnoge heterogene IoT uređaje te na kraju prouzročiti distribuirane napade uskraćivanjem usluga.

U automobilskoj industriji, točnije u autima bez vozača, može se pojaviti hakiranje sustava pa hakeri mogu izvesti udaljeni napad, primjerice kontrolirati upravljanje automobilom te prouzročiti nesreću (Cui et al., 2018).

U pametnom zdravstvu i zdravstvenim tehnologijama sigurnosni su problemi izrazito opasni jer je riječ o pacijentima. Posljedice mogu biti zakonske kazne, financijski gubici, narušavanje ugleda. Tu je također prisutan problem privatnosti. Zlonamjerni softver može pristupiti mnogim informacijama (poruke, pozivi, povijest) te ih prosljeđivati. Korisnici također upotrebljavaju razne stranice o zdravstvu, a potencijalne ranjivosti su da napadač može ukrasti korisnikovu sesiju, dobiti pristup neovlaštenim resursima i ukrasti podatke (osobna iskaznica).

Najčešće prijetnje privatnosti su mrežna krađa identiteta (vrsta prijetnji u kojoj se korisnika navodi na otkrije osobne podatke), kolačići (bilježe sve prijave te ih prijavljuju tamo gdje je dizajner kolačića to odredio), neželjena pošta (poruke koje se šalju primatelju bez njegova dopuštenja) te elektronička trgovina (plaća se putem formulara upisom broja kreditne kartice, a taj je podatak vidljiv svima koji imaju ovlasti za pristup).

Neke prijetnje mogu biti manipulacija senzorima, primjerice kada zlonamjerni napadači generiraju lažne podatke kako bi manipulirali rezultatima senzora kao što su odluke, nadalje mogu pokrenuti napade uskraćivanjem usluga, ometajući senzore kako bi umanjili kvalitetu

inteligentnih usluga u pametnom gradu (Zhang et al., 2017). Autori Ismagilova et al. (2020) istaknuli su da je upotreba umjetne inteligencije (UI) uvelike poboljšala privatnost i sigurnost. Pametni sustav siguran je samo ako ima mogućnost praćenja svojih radnih uvjeta i pravodobnog otkrivanja sumnjivih događaja (Cui et al., 2018).

Potencijalna rješenja za sigurnosne prijetnje mogu biti širi skup sustavnih intervencija, primjerice sigurnost za dizajn, korektivna sigurnosna zakrpa i zamjena, osnivanje timova stručnjaka za hitne intervencije te promjene u postupcima nabave i kontinuirani profesionalni razvoj (Ismagilova et al., 2020, prema Kitchin i Dodge, 2019). Kad je riječ o sigurnosti i privatnosti, upotreba umjetne inteligencije također može pomoći i to na razne načine koji se već koriste u nekim pametnim gradovima, a to su senzori za otkrivanje pucnjave, videonadzor i analitika, dronovi te kibernetska sigurnost (Ismagilova et al., 2020, prema Srivastava et al., 2017). S druge strane, neki stručnjaci smatraju da upotreba tih tehnologija, primjerice dronova, može rezultirati raznim tehnološkim i društvenim problemima vezanim uz privatnost, javnu i kibernetsku sigurnost (Ismagilova et al., 2020, prema Vattapparamban i sur., 2016).

Autori Cui et al. (2018) upozoravaju na sigurnosne zahtjeve povezane s osiguranjem pametnih gradova, a autentifikacija je osnovni zahtjev za različite slojeve pametnog sustava. Potrebna je za dokazivanje identiteta i osiguravanje kako bi samo ovlašteni klijenti mogli pristupiti uslugama u heterogenom sustavu. Povjerljivost je drugi zahtjev, a njezina je svrha spriječiti informacije od napada ili izlaganja pogrešnom izvoru. Dostupnost je sljedeći, a znači da bi sve usluge i svi uređaji trebali biti dostupni kada je to potrebno. Potom osiguranje integriteta, tj. cjelovitosti razmijenjenih podataka, jer IoT prikupljaju velike količine podataka u kratkom vremenu, što iziskuje cloud servise koji mogu skladištiti tu količinu podataka. Autori naglašavaju kako se za očuvanje privatnosti primjenjuju neke gotove tehnike sigurnosti i privatnosti, kao što su enkripcija, anonimnost te kontrola pristupa (Zhang et al., 2017).

Osim tehničkih rješenja, svakako su potrebni obrazovanje i obuka (programeri bi trebali imati sposobnost razvoja stabilnog i otpornog koda), bolja regulativa i bolje upravljanje (Cui et al., 2018). Nove internetske tehnologije promoviraju usluge temeljene na cloudu, mrežno povezivanje uređaja, real world korisnička sučelja, korištenje pametnih telefona, pametnih mjerača te tako otvaraju nove načine za rješavanje problema. Online suradničke platforme za upravljanje podatkovnim senzorima su internetske usluge baze podataka koje vlasnicima senzora omogućuju registraciju i povezivanje uređaja kako bi mogli unositi podatke u online bazu podataka za pohranu te time programerima olakšavaju povezivanje s bazom podataka i izgradnju vlastitih aplikacija.

U Londonu sustav upravljanja prometom, poznat kao SCOOT, optimizira trajanje zelenog svjetla na prometnim raskrižjima prenoseći natrag magnetometar i induktivne podatkovne petlje na superračunalo. Grad Santander u Cantabriji, sjevernoj Španjolskoj, ima 20.000 senzora koji povezuju zgrade, infrastrukturu, promet, mreže i komunalne usluge, nude fizički prostor za eksperimentiranje i provjeru funkcije interneta stvari, kao što su interakcijski i upravljački protokoli, tehnologije uređaja i usluge podrške kao što su otkrivanje, upravljanje identitetom i sigurnost. Senzori ondje prate razinu onečišćenja, buke, prometa i parkiranja.

Elektroničke kartice (poznate kao pametne kartice) druga su zajednička platforma u okvirima pametnoga grada. Te kartice posjeduju jedinstveni šifrirani identifikator koji vlasniku omogućuje prijavu u niz državnih usluga (ili e-usluga). Jedinstveni identifikator omogućuje vladama prikupljanje podataka o građanima za bolje pružanje usluga i utvrđivanje zajedničkih interesa grupa. Ta je tehnologija implementirana u Southamptonu.

6. ZAKONSKI PREDUVJETI ZA USPOSTAVU PAMETNIH IKT SUSTAVA – ZADAR

Projektni pristup videonadzornom sustavu koridora ulica i semaforiziranih raskrižja u Zadru primjer je toga što je tehnološki i projektnom dokumentacijom bilo potrebno obuhvatiti: sustav videonadzorne zaštite javne površine grada; sustav videonadzorne zaštite prostorija smještaja Nadzornog centra na centralnoj lokaciji; sustav protuprovalne zaštite prostorija smještaja Nadzornog centra na centralnoj lokaciji; sustav kontrole pristupa prostorija smještaja Nadzornog centra na centralnoj lokaciji.

Unapređenjem i povezivanjem digitalne infrastrukture poboljšat će se prometni sustav. Preventivnim, pak, mjerama za zaštitu sustava i nadzor javnih površina, osoba i imovine, putem povezivanja sustava tehničke zaštite, podići će se sigurnost imovine i građana.

Sve je bilo potrebno prilagoditi uvažavajući niz europskih normi iz područja inteligentnih transportnih sustava, elektroničke naplate, cestovnog prijevoza i prometne telematike.

- HRN EN ISO 14819-1:2014 Inteligentni transportni sustavi -- Informativne poruke o prometu i putovanju u sustavu kodiranja prometnih informacija -- 1. dio: Protokol za kodiranje u sustavu prijenosa podataka putem radija -- Uporaba ALERT-C u kanalu za prijenos podataka o prometu (RDS-TMC) (ISO 14819-1:2013; EN ISO 14819-1:2013)
- HRN EN ISO 14819-2:2014 Inteligentni transportni sustavi -- Informativne poruke o prometu i putovanju u sustavu kodiranja prometnih informacija -- 2. dio: Kodovi za događaje i informacije u sustavu prijenosa podataka putem radija -- Uporaba ALERT-C u kanalu za prijenos podataka o prometu (RDSTMC) (ISO 14819-2:2013; EN ISO 14819-2:2013)
- HRN EN ISO 14819-3:2014 Inteligentni transportni sustavi -- Informativne poruke o prometu i putovanju u sustavu kodiranja prometnih informacija -- 3. dio: Određivanje lokacije u sustavu prijenosa podataka putem radija -- Uporaba ALERT-C u kanalu za prijenos podataka o prometu (RDS-TMC) (ISO 14819-3:2013; EN ISO 14819-3:2013)
- HRS CEN ISO/TS 17574:2017 Elektronička naplata -- Smjernice za izradu sigurnosnog profila (ISO/TS 17574:2017; CEN ISO/TS 17574:2017)
- HRN EN 12795:2008, Cestovni prijevoz i prometna telematika -- Namjenska komunikacija kratkog dosega (NKKD) -- NKKD podatkovni sloj: pristup mediju i kontrola logičke poveznice (EN 12795:2003)

- HRN EN 13372:2008, Cestovni prijevoz i prometna telematika (CPPT) -- Namjenska komunikacija kratkog dosega -- Profili za CPPT aplikacije (EN 13372:2004)
- HRN EN ISO 14814:2008, Cestovni prijevoz i prometna telematika -- Automatska identifikacija vozila i opreme -- Referentna arhitektura i nazivlje (ISO 14814:2006; EN ISO 14814:2006)
- HRN EN ISO 14815:2008, Cestovni prijevoz i prometna telematika -- Automatska identifikacija vozila i opreme -- Specifikacije sustava (ISO 14815:2005; EN ISO 14815:2005)
- HRN EN ISO 14816:2008/A1:2019, Cestovni prijevoz i prometna telematika -- Automatska identifikacija vozila i opreme -- Brojčano označivanje i struktura podataka (ISO 14816:2005/Amd 1:2019; EN ISO 14816:2005/A1:2019)
- HRN EN ISO 17262:2012/A1:2019, Inteligentni transportni sustavi -- Automatska identifikacija vozila i opreme -- Brojčano označivanje i struktura podataka (ISO 17262:2012/Amd 1:2019; EN ISO 17262:2012/A1:2019)

Tu je važno spomenuti usklađenost s nacionalnom regulativom, vezanom uz mogućnost uspostave videonadzora, što proizlazi i iz odredbi:

- Zakona o kaznenom postupku – člankom 177. stavak 1. i 2.
- Zakona o prekršajima – člankom 157. stavak 1.
- Zakona o nadzoru državne granice – člankom 45.
- Zakona o minimalnim mjerama zaštite u poslovanju s gotovim novcem i vrijednostima – člankom 7. stavak 1. točka 3.
- Zakona o javnom okupljanju – člankom 5. p
- Zakona o sprječavanju nereda na športskim natjecanjima – člankom 16., pravilima iz članka 6. stavka 4. i uvjetima iz članka 8. stavka 4.
- Zakona o sigurnosti prometa na cestama – čl. 283. p.

Da bi sve bilo moguće koristiti radi izuzimanja digitalnih dokaza, potrebne su i određene tehnološke karakteristike sustava: detekcija pokreta kod određenih objekata; prepoznavanje registracijskih pločica, marke i tipa vozila; prepoznavanje osoba; mogućnost pohrane i pretraživanja zapisa radi identifikacije počinitelja kaznenog djela ili prekršaja; korištenje zapisa kao dokaza; brzina, sigurnost i protočnost prometa te njegov opseg; nadzor graničnih i ilegalnih prijelaza. Sustav bi morao imati jednu ili više nadzornih jedinica, odnosno središte iz kojeg bi se zaštićenim videokamerama nadziralo više lokacija.

Jednako tako, sustav bi trebao imati stalnu i promjenljivu lokaciju nadziranja, što bi se postiglo postavljanjem dodatnog broja kamera koje bi se uključivale po potrebi. Pitanje korištenja tehničkih snimki u kaznenom i prekršajnom postupku iznimno je složeno i postoje različita rješenja koja nude različiti pravni sustavi, a protežu se između formalnih kriterija valjanosti dokaza i kriterija načela pretežitog interesa. Kod formalnih kriterija valjanosti dokaza tehničke snimke smatraju se dokazima ako su načinjene u kaznenom postupku, odnosno prema uvjetima formalno zadanim zakonskim propisom. U pravnim sustavima

kod kojih vrijedi načelo pretežitog interesa postoji mogućnost uporabe tehničkih snimki te drugih dokaza pribavljenih na nezakonit način ako interes pravde i pravičnosti preteže nad interesom zaštite dobara koja bi se mogla pojaviti kao zaštitni objekt striktnog pridržavanja pravila o dokazivanju.

Kad je riječ o našem pravnom sustavu, on je zasnovan na definiranju dokaza u kaznenom postupku. Naime, članak 10. stavak 1. Zakona o kaznenom postupku jasno propisuje da se sudske odluke ne mogu temeljiti na dokazima pribavljenim na nezakonit način (nezakoniti dokazi).

Pravne osnove koje su sadržane u Zakonu o kaznenom postupku prikazane su u članku 333., koji govori o snimkama, ispravama i predmetima pribavljenim provedbom radnji iz članka 332. Ako se izvidi kaznenih djela ne bi mogli provesti na drugi način ili bi to bilo moguće samo uz nerazmjerne teškoće, na pisano obrazloženi zahtjev državnog odvjetnika sudac istrage može protiv osobe za koju postoje osnove sumnje da je sama počinila ili zajedno s drugim osobama sudjelovala u kaznenom djelu iz članka 334. ovog Zakona, pisanim, obrazloženim nalogom odrediti posebne dokazne radnje kojima se privremeno ograničavaju određena ustavna prava građana.

Temeljem Zakona o policijskim poslovima i ovlastima, policija je ovlaštena za snimanje na javnim mjestima. Iz Zakona o sigurnosti prometa na cestama, članak 283., proizlazi da se brzina kretanja vozila utvrđuje pomoću uređaja za mjerenje brzine kretanja vozila, tahografskog zapisa ili neposrednim praćenjem s vozilom. Fotografija i videozapis s podacima o utvrđenoj brzini, tahografski zapis i zapisnik o očitanju na radaru koji nema zapis ili brzinomjer, služe kao dokaz o utvrđenoj brzini kretanja vozila. Kao dokaz u prekršajnom postupku mogu se koristiti tehničke snimke, službene bilješke i zapisnici.

U poredbenom pravu nije bilo posebnih poteškoća s uporabom snimki nastalih na javnim mjestima za dokazivanje u kaznenom postupku. Iako je videosnimanje, primjerice, u Velikoj Britaniji najčešće, u njihovu pravnom sustavu uopće ne postoji izričit zakonski izvor koji regulira navedeno područje, nego se snimanje provodi oslanjanjem na opća pravna načela o nepostojanju zaštite privatnosti u takvim okolnostima.

U američkom se pravu od 1967. smatra da osobu na javnome mjestu ne može štititi imunitet od toga da je uočavaju druge osobe, prema odluci Saveznog vrhovnog suda u predmetu Katz. U odluci je sud utvrdio da građani ne mogu očekivati privatnost na događajima koji su dostupni javnosti s obzirom na to da policijski službenici ionako mogu uočiti takve događaje.

7. ZAKLJUČAK

Pametni gradovi rezultat su tehnološkog napretka i odraz velike inovacije u ICT-ju. Građani se unutar pametnih gradova spajaju putem pametnih telefona te umjetnih i integriranih alata kao što je IoT, što dovodi do znatnog poboljšanja načina života. Razvojem takve tehnologije raste i težnja za povećanjem sigurnosti koja mora biti zakonski utemeljena.

Zabrinutost ljudi proizlazi i iz percepcije određenih podataka, primjerice osobnih i neosobnih, a njihova se zabrinutost razlikuje ovisno o svrsi za koju se ti podaci prikupljaju,

primjerice za usluge, nadzor i sl., o čemu se govori u istraživanjima provedenim radi jačanja percepcije privatnosti u sklopu kampanja uvođenja Opće uredbe o zaštiti podataka. Fizički sloj kao izvor digitalnih dokaza kod pametnih gradova mora biti otporan na različite uređaje za prisluškivanje ili blokiranje komunikacije, pogotovo kod pružanja osjetljivih informacija kada rizik od ugroze raste, a prijetnje su izvjesnije i mora ih se predvidjeti, kao što je to slučaj u osiguravanju kretanja štićenih osoba.

Opravdano je i potrebno proširiti svijest o prijetnjama u pametnim gradovima, za što je nužna edukacija stručnjaka, ali i građana koji su dio pametnoga grada, a s formalno-pravnog stajališta potrebno je stvaranje zakonskih osnova koji će osigurati i štititi građane i imovinu. Pritom treba staviti naglasak na jasno i nedvosmisleno informiranje o mogućnostima, ali i ranjivostima novih tehnologija te o načinima zaštite od novih oblika ugroza koje nove IKT tehnologije donose prilikom implementacije IoT koncepata u pametnim gradovima.

LITERATURA

1. Chen, M. (2021). Smart city and cyber-security; technologies used, leading challenges and future recommendations. Energy Reports Volume 7, November 2021, Pages 7999-8012. Preuzeto s: https://doi.org/10.1016/j.egyr.2021.08.124.
2. Fischer, I. (2017). 12 INTELIGENTNIH RJEŠENJA KOJA SU ZAUVIJEK PROMIJENILA ŽIVOT GRAĐANIMA Pametni gradovi donose nova radna mjesta i veće prihode poduzetnicima jutarnji.hr. Preuzeto s: https://www.jutarnji.hr/vijesti/12-inteligentnih-rjesenja-koja-su-zauvijek-promijenila-zivot-gradanima-pametni-gradovi-donose-nova-radna-mjesta-i-vece-prihode-poduzetnicima-6717852.
3. HRN EN 12795:2008, Cestovni prijevoz i prometna telematika – Namjenska komunikacija kratkog dosega (NKKD) – NKKD podatkovni sloj: pristup mediju i kontrola logičke poveznice (EN 12795:2003) http://31.45.242.218/HZN/Todb.nsf/wFrameset2?OpenFrameSet&Frame=Down&Src=%2FHZN%2FTodb.nsf%2F66011c0bda2bd4dfc1256cf300764c2d%2Fabec508c60c160c4c125710f003c6f7c%3FOpenDocument%26AutoFramed.
4. HRN EN 13372:2008, Cestovni prijevoz i prometna telematika (CPPT) − Namjenska komunikacija kratkog dosega − Profili za CPPT aplikacije (EN 13372:2004) http://31.45.242.218/HZN/Todb.nsf/cd07510acb630f47c1256d2c006ec863/5dd6c820de686f27c12571100032752b?OpenDocument&AutoFramed.
5. HRN EN ISO 14814:2008, Cestovni prijevoz i prometna telematika − Automatska identifikacija vozila i opreme − Referentna arhitektura i nazivlje (ISO 14814:2006; EN ISO 14814:2006) https://repozitorij.hzn.hr/upload/eglasilo_2008/Oglasnik508.pdf.
6. HRN EN ISO 14815:2008, Cestovni prijevoz i prometna telematika − Automatska identifikacija vozila i opreme − Specifikacije sustava (ISO 14815:2005; EN ISO 14815:2005) https://repozitorij.hzn.hr/upload/eglasilo_2008/Oglasnik508.pdf.

7. HRN EN ISO 14816:2008/A1:2019, Cestovni prijevoz i prometna telematika − Automatska identifikacija vozila i opreme − Brojčano označivanje i struktura podataka (ISO 14816:2005/Amd 1:2019; EN ISO 14816:2005/A1:2019) https://repozitorij.hzn.hr/norm/HRN+EN+ISO+14816%3A2008%2FA1%3A2019.
8. HRN EN ISO 14819-1:2014 Inteligentni transportni sustavi − Informativne poruke o prometu i putovanju u sustavu kodiranja prometnih informacija − 1. dio: Protokol za kodiranje u sustavu prijenosa podataka putem radija − Uporaba ALERT-C u kanalu za prijenos podataka o prometu (RDS-TMC) (ISO 14819-1:2013; EN ISO 14819-1:2013) https://repozitorij.hzn.hr/norm/HRN+EN+ISO+14819-1%3A2014.
9. HRN EN ISO 14819-2:2014 Inteligentni transportni sustavi − Informativne poruke o prometu i putovanju u sustavu kodiranja prometnih informacija − 2. dio: Kodovi za događaje i informacije u sustavu prijenosa podataka putem radija − Uporaba ALERT-C u kanalu za prijenos podataka o prometu (RDSTMC) (ISO 14819-2:2013; EN ISO 14819-2:2013) https://repozitorij.hzn.hr/norm/HRN+EN+ISO+14819-2%3A2014.
10. HRN EN ISO 14819-3:2014 Inteligentni transportni sustavi − Informativne poruke o prometu i putovanju u sustavu kodiranja prometnih informacija − 3. dio: Određivanje lokacije u sustavu prijenosa podataka putem radija − Uporaba ALERT-C u kanalu za prijenos podataka o prometu (RDS-TMC) (ISO 14819-3:2013; EN ISO 14819-3:2013) https://repozitorij.hzn.hr/norm/HRN+EN+ISO+14819-3%3A2021.
11. HRN EN ISO 17262:2012/A1:2019, Inteligentni transportni sustavi − Automatska identifikacija vozila i opreme − Brojčano označivanje i struktura podataka (ISO 17262:2012/Amd 1:2019; EN ISO 17262:2012/A1:2019) https://repozitorij.hzn.hr/norm/HRN+EN+ISO+17262%3A2012%2FA1%3A2019.
12. HRS CEN ISO/TS 17574:2017 Elektronička naplata − Smjernice za izradu sigurnosnog profila (ISO/TS 17574:2017; CEN ISO/TS 17574:2017) http://31.45.242.218/HZN/Todb.nsf/wFrameset2?OpenFrameSet&Frame=Down&Src=%2FHZN%2FTodb.nsf%2FNormaSve%2F11f96642fa783b8bc12581790024fe9f%3FOpenDocument%26AutoFramed.
13. Ismagilova, E., Hughes, L., Rana, N. i Dwivedi, Y. (2020). Security, Privacy and Risks Within Smart Cities: Literature Review and Development of a Smart City Interaction Framework. Information Systems Frontiers.10.1007/s10796-020-10044-1. Preuzeto s https://www.researchgate.net/publication/343123843_Security_Privacy_and_Risks_Within_Smart_Cities_Literature_Review_and_Development_of_a_Smart_City_Interaction_Framework.
14. Knezović, G. (2022). Pametni grad broj 1 u svijetu za 2022. je Šangaj. mreza.bug.hr. Preuzeto s: https://mreza.bug.hr/pametni-grad-broj-1-u-svijetu-za-2022-je-sangaj/.
15. Pérez-Martínez, P. A., Martínez-Ballesté, A., i Solanas, A. (2013). Privacy in smart cities: A case study of smart public parking. Paper presented at the PECCS 2013 - Proceedings of the 3rd International Conference on Pervasive Embedded Computing

and Communication Systems, 55–59. Preuzeto s: https://www.researchgate.net/publication/289736601_Privacy_in_Smart_Cities_A_case_tudy_of_smart public_parking.

16. Sookhak, M. H., Tang, Y. He, i F. R. Yu, „Security and Privacy of Smart Cities: A Survey, Research Issues and Challenges“, in IEEE Communications Surveys & Tutorials, vol. 21, no. 2, pp. 1718–1743, Secondquarter 2019, doi: 10.1109/COMST.2018.2867288. Preuzeto s https://ieeexplore.ieee.org/abstract/document/8447209.
17. Ståhlbröst, A., Padyab, A. M., Sällström, A., i Hollosi, D. (2015). Design of Smart City Systems from a Privacy Perspective. IADIS International Journal on WWW/Internet Vol. 13, No.1, pp. 1–16 ISSN: 1645–7641. Preuzeto s: http://www.diva-portal.org/smash/get/diva2:979841/FULLTEXT01.pdf.
18. Vorakulpipat, Chalee. Ryan K. L. Ko, Qi Li, Ahmed Meddahi, „Security and Privacy in Smart Cities“, Security and Communication Networks, vol. 2021, Article ID 9830547, 2 pages, 2021. https://doi.org/10.1155/2021/9830547.
19. Zakon o javnom okupljanju − članak 5. p https://www.zakon.hr/z/444/Zakon-o-javnom-okupljanju.
20. Zakon o kaznenom postupku − članak 177. stavak 1. i 2. https://www.zakon.hr/z/174/Zakon-o-kaznenom-postupku.
21. Zakon o minimalnim mjerama zaštite u poslovanju s gotovim novcem i vrijednostima − članak 7. stavak 1. točka 3. https://www.zakon.hr/z/449/Zakon-o-minimalnim-mjerama-za%C5%A1tite-u-poslovanju-s-gotovim-novcem-i-vrijednostima.
22. Zakon o nadzoru državne granice – članak 45. https://www.zakon.hr/z/450/Zakon-o-nadzoru-dr%C5%BEavne-granice .
23. Zakon o prekršajima – članak 157. stavak 1. https://www.zakon.hr/z/52/Prekr%C5%A1ajni-zakon.
24. Zakon o sprječavanju nereda na športskim natjecanjima – članak 16. pravilima iz članka 6. stavka 4. i uvjetima iz članka 8. stavka 4. https://www.zakon.hr/z/445/Zakon-o-sprje%C4%8Davanju-nereda-na-%C5%A1portskim-natjecanjima.
25. Zhang, K., J. Ni, K. Yang, X. Liang, J. Ren i X. S. Shen, „Security and Privacy in Smart City Applications: Challenges and Solutions“ in IEEE Communications Magazine, vol. 55, no.1, pp. 122–129, January 2017, doi: 10.1109/MCOM.2017.1600267CM. Preuzeto s https://ieeexplore.ieee.org/document/7823349.
26. Zoonen, L. (2016). Privacy concerns in smart cities. Government Information Quarterly. 33. 10.1016/j.giq.2016.06.004. Preuzeto s https://www.researchgate.net/publication/304746305_Privacy_concerns_in_smart_cities.

Abstract

Krunoslav Antoliš

Smart cities and information and communication technologies

We are witnessing great technological changes in today's modern world. All these technological changes and the new IoT (Internet of Things) technology, which has a Croatian counterpart, IS (Internet of Things), make everyday life easier but also bring many vulnerabilities, risks and threats. Any vulnerable situation in a smart city can lead to serious threats to the entire city and cause massive consequences. Relying on new ICT (Information Communication Technology) systems in a smart city also brings numerous digital traces, which, if extracted legally from a person authorized by law, can significantly contribute to investigating security threats and sanctioning perpetrators of criminal acts and misdemeanours. However, for the entire ICT support system to be a source of digital evidence, the overall solutions must be legally based and harmonized with European and national norms. The compilations and the comparative methods applied in work aim to observe the best practices and international as well as domestic approaches to integrating ICT into the concept of smart cities, for example, in Zadar. The paper will apply scientific research methods to describe concrete examples of smart cities and their solutions in certain key segments for their functioning and resource optimization. The method of analysis and synthesis in the definition of smart cities, based on the sources used, i.e. texts from domestic and foreign literature, aimed to present various approaches but also new paradigms important for the further development of the concept of smart cities.

Keywords: smart cities, vulnerabilities, risks, threats, information and communication technologies.