

Ненад Р. Путник¹
Јана М. Марковић²
Универзитет у Београду, Факултет безбедности
Београд (Србија)

342.738:004.056
351.777.81:[711.45:004.7
Прејледни научни рад
Примљен 12/02/2025
Измењен 23/02/2025
Прихваћен 26/02/2025
doi: [10.5937/socpreg59-56735](https://doi.org/10.5937/socpreg59-56735)

БЕЗБЕДНОСТ И ПРИВАТНОСТ У ПАМЕТНИМ ГРАДОВИМА

Сажетак: Глобални тренд растуће урбанизације и експанзије градова последњих деценија проузроковао је бројне проблеме у њиховом функционисању. Убрзан развој информационо-комуникационих технологија појавио се као решење за те проблеме, и довео до настанка такозваних *паметних градова*. Паметни град осмишљен је као нов модел града који генерише и обрађује енормне количине дигиталних података са циљем оптимизације градске инфраструктуре и побољшања услова живота. Употреба нових технологија је, међутим, отворила многа питања и изазвала забринутост у вези са начином употребе тих технологија и могућностима злоупотребе прикупљених података. У раду су описане кључне карактеристике архитектуре паметног града и анализирана питања угрожавања безбедности и приватности грађана која она отвара. Извори и облици угрожавања безбедности и приватности у паметним градовима су бројни, међусобно испреплетени и захтевају подрбну анализу са техничко-технолошког, социолошког и правног аспекта.

Кључне речи: паметан град, информационо-комуникационе технологије, безбедност, приватност, подаци о личности

УВОД

Градови су одувек били не само тачка окупљања већ и центар друштвеног и политичког живота, развоја региона и националне економије. Они су успутна или коначна тачка људи који мигрирају тражећи основне или боље услове за живот. Процењује се да ће у урбаним срединама у 2050. години живети чак 68,4 процената укупног становништва (Population Data Portal UNFPA, n. d.), што је нешто више од две трећине укупне популације.

¹ nputnik@fb.bg.ac.rs; <https://orcid.org/0000-0002-6374-7270>

² jana.markovic@fb.bg.ac.rs; <https://orcid.org/0009-0003-0676-8213>

Са увећањем броја становника у градовима, расте и потреба за развојем градске инфраструктуре како би се задовољиле потребе њихових житеља оличене у широком спектру производа и услуга. Неки од најважнијих проблема који се притом јављају односе се на комуналне услуге – обезбеђивање довољне количине електричне енергије и воде, одлагање отпада, загађење ваздуха, загушење саобраћаја, услове становања, као и повећање стопе криминалитета.

Тренд урбанизације је, истовремено, актуелизовао изазове одрживог развоја, а унапређење квалитета живота наметнуо као императив урбаног развоја. Решење за многе изазове урбаног и одрживог развоја виђено је у примени савремене информационо-комуникационе технологије (у даљем тексту: ИКТ), што је довело до настанка концепта паметних градова.

У контексту ИКТ, паметни градови се могу посматрати и као систем међусобно повезаних и умрежених система кроз које се размењује огромна количина дигиталних података. Такви системи пак имају своје техничко-технолошке слабости и рањивости. Они су изложени не само ризицима техничких кварова, грешкама у њиховом пројектовању и коришћењу, већ и злоупотребама од стране злонамерних актера у физичком и сајбер свету. Безбедносним ризицима нису изложени само ИКТ системи, већ и сви подаци који се у њима обрађују и складиште. Посебно осетљиву категорију података представљају подаци о личности који су у тесној вези са захтевом за очувањем приватности грађана (General Data Protection Regulation, 2018). Стога је разумљив захтев да се безбедност ИКТ система и дигиталних података у паметним градовима континуирано оцењује и унапређује (Marković, 2023).

ПОЈАМ И КАРАКТЕРИСТИКЕ ПАМЕТНОГ ГРАДА

Концепт паметног града заснива се на употреби савремених технологија које треба да помогну градској управи у пружању широког спектра услуга, са циљем побољшања квалитета привредног и друштвеног живота. Унапређење услуга у здравству, успостављање дигиталног приступа јавној управи, смањење емисије угљен-диоксида, управљање отпадом, саобраћајним гужвама и паркинзима, увођење интелигентних система уличне расвете, уградња паметних бројила за електричну енергију, пројектовање паметних зграда, неке су од области живота у граду које могу да буду унапређене „паметним технологијама“. Паметни градови, или како се још називају, дигитални градови, технолошки градови, жичани градови, свеприсутни градови, интелигентни градови, градови информација, градови знања, паметне заједнице, креативни градови и одрживи градови (Praharaј & Nan, 2019, str. 1) повезују људе са технологијом, баратајући огромном количином података међу којима се налазе и они посебно осетљиве природе, у које спадају и подаци о личности.

Паметни градови представљају урбана подручја која употребом ИКТ прикупљају, генеришу и обрађују податке, како би стекли бољи увид у понашање и перформансе потрошача (грађана) и та подручја учинили ефикаснијим и одрживијим. Иако се за паметне градове превасходно везује екстензивна и интелигентна употреба ИКТ које омогућавају управљање подацима и информацијама, паметни град је много више од

паметних технологија. Паметни град је концепт који захтева холистички приступ за разумевање његове архитектуре и примене. Холистички приступ подразумева повезаност неколико димензија у концепт паметног града: технологија, одрживост, екологија, социјална и економска димензија.

Иако међу теоретичарима нема сагласности у вези са универзалном дефиницијом паметног града, издвајамо једну коју је, након опсежне анализе, понудила Рената Дамери (Renata Paola Dameri). Ова ауторка паметни град формулише као „добро дефинисану географску област, у којој високе технологије као што су ИКТ, логистика, производња енергије и тако даље, сарађују на стварању користи за грађане у смислу благостања, укључивања и учешћа, квалитета животне средине, интелигентног развоја; област којом управља добро дефинисан скуп субјеката, који су у стању да утврде правила и политику за градску управу и развој“ (Dameri, 2013, стр. 2549).

КОМПОНЕНТЕ ПАМЕТНОГ ГРАДА И ЊЕГОВА АРХИТЕКТУРА

Разумевање концепта паметног града укључујући и разумевање његове архитектуре, дакле, захтева холистички приступ који реферише на свеукупност људских, друштвених, културних, еколошких, економских и технолошких фактора. Ипак, иако је улога људског, друштвеног и институционалног капитала препозната, чини се да је примарни нагласак био и остао на технологији.

Најчешће идентификоване компоненте паметног града су: паметно управљање (у вези са учешћем у одлучивању, јавном администрацијом и јавним услугама); паметан људски капитал (у вези с људима, њиховим образовањем и запослењем, социјалним интеракцијама и интеграцијама); паметно окружење (у вези с природним ресурсима, нпр. уређеност простора, загађење, одрживост зграда); паметно живљење (у вези с квалитетом живота); паметна економија (у вези с иновацијама, пословањем и предузетништвом, тржиштом, конкурентношћу) и паметна мобилност (у вези с транспортом и уопште доступношћу услуга) (Lombardi, Giordano, Farouh & Yousef, 2012, стр. 139). Наведене компоненте уједно представљају и такозване апликације паметног града.

Група аутора (Gil-Garcia, Pardo & Nam, 2015, стр. 78) понудила је концептуални оквир за сагледавање и разумевање паметног града тако што је проширила оквир који је извела анализом академске литературе. Према овим ауторима, кључне компоненте паметног града су: технологија и подаци (информационо-комуникационе и друге технологије, подаци и информације), физичко окружење (природна животна средина и еколошка одрживост, изграђено окружење и градска инфраструктура), друштво (економија знања и про-бизнис окружење, људски капитал и креативност, управљање, ангажовање и сарадња) и влада (институционално уређење, градска управа и управљање, јавне услуге). Карактеристике града могуће је сагледати кроз одрживост (инфраструктуре и владе, енергетска одрживост и климатске промене, решавање загађења и отпада, социјална, економска и здравствена одрживост), квалитет живота (економско и емоционално благостање), урбанизацију (техничка,

инфраструктурна, владина, економска) и паметна решења (у економском, социјалном и еколошком аспекту) (Silva, Khan & Han, 2018, str. 699).

Паметни градови данашњице генеришу огромне количине података. Тим подацима је неопходно управљати, јер управљати подацима значи управљати паметним градом. Треба управљати подацима који се добијају из физичког света, као и онима који се аутоматизовано обрађују, генеришу и анализирају у информационим системима. Стога, аспекте управљања подацима могуће је сагледати као аспекте перцепције, интеграције, облака³, апликација и пословних слојева архитектуре паметног града (Ahmed, 2020, str. 2). Подаци који се *џерцејцијом* прикупе са сензора, *инџејришу* се у хетерогене мреже, да би се у *облаку* складиштили за паметне апликације, а потом, заједно са подацима насталим из *самостјалних ајликација*, користили за пружање услуга. Обухватан приказ архитектуре паметног града даје група аутора која прави разлику између шест слојева: физички или слој перцепције; мрежни или комуникациони слој; слој виртуелизације; слој анализе података и рударења⁴ и апликациони слој (Al-Turjman, Zahmatkesh & Shahroze, 2019).

Укратко, можемо рећи да се паметни град у техничко-технолошком смислу заснива на сензорима за прикупљање података (попут оних који детектују температуру ваздуха, број возила на раскрсници, људи у тржним центрима и сл.), јединицама или системима за аутоматизовано управљање и контролу (какви су на пример SCADA системи), хетерогеним мрежама за пренос података, као и дигиталним базама података и моћним серверима за обраду података.

Сви побројани елементи спадају у категорију Интернет ствари⁵ јер су међусобно повезани рачунарским мрежама путем којих комуницирају, заједно са свим другим уређајима који су повезани на интернет. Поред овог хардверског слоја, архитектура паметног града увек укључује и софтвер (апликације) преко којих се корисницима обезбеђује пружање услуга.

УТИЦАЈ ПАМЕТНИХ ТЕХНОЛОГИЈА НА БЕЗБЕДНОСТ И ПРИВАТНОСТ

Људи су склони томе да дефинишу безбедност као постојање заштите и осећаја безбедности у свакодневном животу. Ова врста безбедности, која се у професионалној литератури назива онтолошка безбедност, показује да је људима највише важно оно што Ентони Гиденс назива могућношћу да живот иде даље као и обично, „способност да наставе“. То укључује не само физичку безбедност већ и социјалну и материјалну безбедност те информисану безбедност (способност разумевања света око себе,

³ Облак (енгл. *Cloud*) јесте простор на интернет мрежи за складиштење података којима се може приступити путем интернет везе.

⁴ Рударење (енгл. *Data mining*) се може схватити као процес сортирања великих скупова података с циљем идентификовања образаца.

⁵ Интернет ствари (енгл. *Internet of Things – IoT*) у основи представља мрежу међусобно повезаних уређаја који прикупљају податке и размењују их са другим ИОТ уређајима путем интернет мреже.

промена које се у њему дешавају и давање значења тим променама), затим заштиту људских права и грађанских слобода, као и заштиту од социјално девијантних феномена, насиља и тероризма (Danilović Hristić, 2016).

Једна од општеприхваћених дефиниција коју је поставио Бери Бузан, „да је безбедност заправо слобода од претњи“ (Buzan, 1983), даје интерпретацију на много вишем нивоу опште (државне или националне) безбедности, али се може применити и на ниво урбаног окружења и осећај који корисници формирају не само о градском простору већ и о дигиталном простору у коме се одвија већи део активности савременог урбаног човека. Основа за насилно (криминално, сексистичко или расистичко) понашање према одређеним категоријама становништва лежи у општој друштвеној и економској ситуацији друштва која се преноси на улице градова. Стварност и озбиљност насиља на улицама доводе до свеопштег осећаја несигурности у заједницама – а несигурност урбаних простора узрокује њихово смањење или злоупотребу. Велика промена у истраживању ове теме догодила се од 1960-их, посебно током 1980-их и 1990-их, захваљујући, између осталог, интересовању феминистичких група за одређене теме, али и појави насилног и хулиганског понашања у градовима, учесталом тероризму, као и развоју нових технологија (видео-надзор, GPRS, GIS, CCTV, DVR) и њиховој масовној примени у 21. веку (Danilović Hristić, Stefanović & Putnik, 2021).

Нове, „паметне“, технологије, које су у основи паметних градова, генератор су велике количине података. Велики број сензора који су инсталирани у паметним градовима прикупљају и шаљу податке на више нивое дигиталне архитектуре како би се они складиштили, обрадили и користили за доношење одлука, односно за унапређење квалитета услуга које се обезбеђују становништву. Подаци се на овом месту могу схватити и у контексту података из база података владиних и корпоративних тела. Додајмо томе и податке које прикупљају грађани, посетиоци или друге заинтересоване стране. У великој мери, грађани користе паметне аутомобиле или паметне куће и зграде, паметне телефоне и сатове и све паметне уређаје у дому или канцеларији преко којих обављају своје свакодневне задатке или задовољавају социјалне потребе. Иако осмишљени као уређаји који треба да унапреде квалитет живота, ови извори података истовремено постају и извор опасности по безбедност и приватност. У самој основи, паметни градови су унапредили и заменили традиционалне уређаје електронским. Тако, да би грађани могли да користе разне врсте паметних система, они претходно морају дати своје личне податке овим паметним системима. Међу подацима који се прикупљају налазе се и поверљиви подаци правних ентитета (државних и недржавних субјеката), као и подаци о личности који укључују име и презиме, матични број грађана, порески број, број осигурања, број телефона, број идентификационог документа, фотографије, видео и тонске записе особе, отиске прстију, ДНК, податке о локацији и кретању и слично.

Заштита података подразумева континуирану активност на спровођењу техничких, организационих и кадровских мера које се предузимају у односу на процењен ризик по угрожавање података и инфраструктуре која их подржава. Ова активност увек обухвата два аспекта: један који се односи на заштиту инфраструктуре и технологије кроз које подаци протичу, и други који се односи на саме податке који се

генеришу, обрађују и користе.⁶ Безбедност података обухвата заштиту њихове поверљивости, интегритета и расположивости. Поверљивост обезбеђује приватност и заштиту поверљивих података, интегритет штити податке од модификације, док расположивост обезбеђује да подаци буду доступни ауторизованим корисницима. Сваки од три наведена аспекта безбедности података може бити угрожен. Напади на поверљивост усмерени су на неовлашћено праћење и приступ информацијама, напади на интегритет усмерени су на упад у систем како би изменили ускладиштене информације, а напади на доступност усмерени су на ускраћивање неке услуге или рушење система. Критични аспекти управљања подацима укључују и информације о томе који се подаци чувају, како су класификовани, где се чувају, како се користе и са ким се деле.

Ахмед указује на постојање различитих врста приватности појединаца: приватност идентитета, телесна приватност, територијална приватност, приватност мобилности, приватност комуникација и трансакција (Ahmed, 2020, str. 4).⁷ Реч је дакле о великој количини разноврсних података који се међусобно разликују по формату, величини, сложености, сврси, власништву и сл. У вези са тим, када се говори о паметним градовима, није могуће изоставити такозване велике податке⁸ који се генеришу и користе за подршку развоју и одрживости паметних градова. Анализи великих података може у великој мери да допринесе вештачка интелигенција (ВИ, енгл. *Artificial Intelligence*). У основи, комбиновање Интернет ствари и ВИ ефикасан је начин да се надограде постојећи системи паметних градова. Уз наведено, употреби великих података допринело је коришћење технологије облака као глобалне мреже сервера.

У свом стицају, употреба нових (паметних) технологија (Интернет ствари, облак и ВИ), изазива подозрење једног дела популације, узроковано сумњом да се подацима не управља на адекватан начин, те да се они чак и намерно злоупотребљавају. Стога, паметни градови изазивају забринутост у погледу безбедности и приватности и поновно актуелизују Бентамову идеју Паноптикона. У идеји „паметног Паноптикона“ град (држава или неки наддржавни ентитет) прикупљене податке користи не само за надзор грађана већ и за комерцијалну (зло)употребу личних података прикупљених у паметним градовима. Перцепција грађана је таква да они имају малу или никакву контролу над тим шта компаније, градске власти или владе држава раде са њиховим подацима (McClain, Faverio, Anderson & Park, 2023, str. 4).

У Приручнику за локалне и регионалне владе Програма ОУН за насеља, наводи се да „поверење у јавне институције опада у многим деловима света, делом због недостатка транспарентности, необезбеђене дигиталне инфраструктуре и ограничених могућности за представљање и учешће заједнице“ (UN-Habitat, 2021, str. 47). Стога је

⁶ У вези са наведеним, треба имати на уму да је информационо-комуникациона инфраструктура у основи сваке друге критичне инфраструктуре. Многи сајбер напади циљају управо владе и уопште националне критичне инфраструктуре. Сходно карактеристикама критичне инфраструктуре, поремећаји на једној инфраструктури могу се рефлектовати и на цео град.

⁷ Упоредити са седам типова приватности (Finn, Wright & Friedewald, 2013) или различитим типовима активности које имају различит степен приватности (Evans, 2018, str. 493).

⁸ Велики подаци (енгл. *Big Data*) представљају енормно велики број неструктурираних података који се континуирано умножавају, док се само један део њих користи за доношење одлука.

јасно да је подршка и учешће грађана у успостављању, развоју и одржавању паметног града неопходна и незаобилазна. Од укључености грађана у креирање јавних политика и одлучивање о важним питањима, зависи да ли ће паметни градови опстати или ће бити укинати (Thomas, Mula, Vang & Dan, 2015).⁹

Са друге стране, важно је истаћи и постојање такозваног парадокса приватности (Young & Quan-Haase, 2013) који говори о томе да су грађани, са једне стране, забринути за приватност, док са друге стране не воде довољно рачуна о превентивним мерама и властитој безбедности у дигиталном свету. Илустративан је податак да је најпопуларнији пин код који се користи „1234“ (DataGenetics, n. d.). Такође, широко је распрострањена и пракса коришћења истих параметара за логовање на две или више апликација, или пак бесконачно дељење података путем друштвених мрежа. Поменути парадокс истраживала је Ван Зунен (Van Zoonen). Закључак спроведеног истраживања говори о томе да забринутост грађана у вези са приватношћу варира у зависности од тога о којим подацима је реч, у коју сврху се прикупљају и користе (обрада података у сврху пружања услуге изазива најмању забринутост, док највећи степен забринутости изазива сврха надзора) и које организације или особе прикупљају и користе податке – безлични (псеудонимизовани или анонимизовани) подаци изазивају најмању забринутост, а подаци о личности највећу (2016).

Друго истраживање из 2023. године је потврдило претпоставку да врста прикупљених података највише утиче на перцепцију и забринутост грађана, док време обраде података најмање на то утиче. Међу подацима чије прикупљање највише изазива забринутост налазе се осетљиви и подаци о личности, попут видео-снимака, података о броју људи и њиховој локацији (Emami-Naeini et al., 2023).

Налази истраживања о употреби софтверских апликација говоре о томе да мањи степен забринутости изазивају оне апликације које су општег карактера, какве су, на пример, веб-прегледачи или апликације за размену електронске поште. Већу забринутост узрокују апликације које су повезане са личним подацима, као што су друштвене мреже и банкарске апликације (Bergström, 2015, стр. 421).

У истраживању које је спроведено у Сједињеним Америчким Државама чак 81% испитаника је изразило забринутост у погледу начина на који приватне компаније прикупљају њихове податке, односно 71% њих у погледу како то чини влада (McClain, Faverio, Anderson & Park, 2023, стр. 3). Питање приватности у контексту надзора од стране владе привукло је пажњу бројних аутора. Неки аутори су пронашли везу између прихватљивости надзора и начина на који перципирају саму владу. Тако, „индивидуална прихватљивост владиног надзора зависи од њихове перцепције владе и јавних послова“ (Nam, 2018, стр. 540), односно од поверења које грађани имају у владу. Такође, једна од студија наглашава важну улогу друштвеног утицаја и реципроцитета на прихватање технологија које захтевају масовно прихватање и реципрочно откривање информација које траже разне апликације (Fox et al., 2021, стр. 12). У неким студијама, као варијабла истраживања укључена је националност и

⁹ Торонто је пример града у којем иницијатива паметног града није прихваћена и усвојена. Као главни разлог издваја се забринутост грађана за приватност њихових података. Грађани су сматрали да иницијатива занемарује људе и њихове потребе дајући енормну предност квантификацији и контроли свега што би у паметном граду постојало (Сессо, 2019).

национална култура, као фактор који утиче на понашање и перцепције испитаника (Budak, Rajh & Recher, 2017; Hallinan, Friedewald & McCarthy, 2012; Thompson et al., 2020).

Важно је напоменути да су последњих деценија развијени безбедносни стандарди који имају за циљ заштиту дигиталних података. Најпознатији међу њима је, свакако, сет стандарда ИСО 27000. Такви стандарди значајно доприносе безбедности података и заштити приватности грађана. Па ипак они, сами по себи, нису гаранција безбедности, будући да се непрекидно појављују нове технологије (са новим рањивостима) и, на њима засноване, софтверске апликације. Стога је неопходно обезбедити да све технологије и апликације које се користе за потребе паметног града имају и одржавају оптималан ниво безбедности и приватности. Обезбеђивање највишег нивоа заштите уједно је и кључно за даљи развој тржишта електронске трговине, од којих у великој мери зависи и развој паметног града. Уз то, неопходна је константна активност на (ре)дефинисању, имплементацији и хармонизацији националних и међународних безбедносних политика и стратегија, закона и стандарда (Putnik, Milošević & Cvetković, 2022, str. 338–339). Стога, безбедност и приватност представљају вишедимензионални проблем чија решења зависе од технолошких и социоекономских фактора, али и од доносилаца политичких одлука. Незаобилазан аспект заштите јесте и захтев за подизање свести и едукацију грађана чиме би се осигурао виши ниво безбедносне културе грађана и смањила подложност манипулацији.

ЗАКЉУЧАК

Концептом паметног града, са једне стране, обухваћена је употреба ИКТ која подразумева коришћење хардвера, софтвера и рачунарских мрежа док се, са друге стране, наглашава унапређење квалитета живота грађана у различитим областима као што су: инфраструктура, енергија, транспорт, природни ресурси, јавне услуге и сл., коришћењем претходно генерисаних великих података.

Да би паметни град испунио своју основну намену и унапредио квалитет услуга које пружа својим грађанима и посетиоцима, велике количине података морају да буду прикупљене, анализиране и припремљене за доношење одлука. Том процесу у великој мери доприносе паметне технологије: велики подаци, Интернет ствари, облак и ВИ. У вези са наведеним циљем, градови настоје да унапреде постојеће, односно, имплементирају нове технологије које своје место проналазе у свим секторима економског, еколошког, политичког, друштвеног и културног аспекта. Многе од тих технологија захтевају активно учешће корисника да би могле да испуне свој потенцијал, односно њихов пристанак за активно дељење података са различитим апликацијама. Са друге стране, неке од технологија (попут видео-надзора на јавним просторима или различитих сензора) прикупљају податке без сагласности грађана. Ова чињеница је важна јер може водити злоупотребама личних података – незаконитом профилисању индивидуалних корисника на основу података који су наводно анонимни.

Питање заштите података и приватности заузима средишње место у академским расправама које тематизују концепт паметног града. Забринутост грађана услед развоја технологија које омогућавају прикупљање и обраду њихових података једно је од кључних питања како у научним круговима, тако и у практичној, политичкој,

сфери. Забринутост грађана варира у односу на врсту података који се прикупљају, апликације које се користе, сврху и циљ обраде, као и у односу на субјекте који податке прикупљају и користе.

Мудро управљање паметним градом стога захтева озбиљна истраживања јавног мњења, како би доносиоци одлука на адекватан начин регулисали управљање подацима у паметном граду. На тај начин, постиже се транспарентност и укључивање грађана у доношење одлука од којих у великој мери зависи имплементација паметних технологија и развој паметног града. У демократским државама, доносиоци одлука настоје да смање ниво забринутости грађана за приватност и истовремено да задобију њихову подршку за развој паметних апликација. Томе свакако претходи доношење адекватног правног оквира који треба да гарантује транспарентност и учешће заједнице у одлучивању.

Концепт паметног града, на крају, отвара многа питања на која је потребно дати одговоре у будућности. Са аспекта информационе безбедности потребно је евалуирати актуелна и потенцијална решења за безбедност и заштиту података из перспективе нових претњи које се свакодневно појављују. Са социолошког аспекта значајан допринос се може очекивати од оних истраживања која за циљ имају перцепцију грађана у вези са питањима њихове безбедности и приватности. Подједнако значајна би била и анализа постојећег правног оквира у овој области – конкретних институционалних и законодавних решења која су усвојена са циљем заштите безбедности и приватности података у паметним градовима.

Nenad R. Putnik¹
Jana M. Marković²
University of Belgrade, Faculty of Security Studies
Belgrade (Serbia)

SECURITY AND PRIVACY WITHIN SMART CITIES

(Translation *In Extenso*)

Abstract: The global trend of increasing urbanization and expansion of cities in recent decades has caused numerous problems in their functioning. The rapid development of information and communication technologies has emerged as a solution to these problems and led to the emergence of so-called smart cities. A smart city is conceived as a new model of a city that generates and processes enormous amounts of digital data with the aim of optimizing urban infrastructure and improving living conditions. However, the use of new technologies has raised many questions and caused concerns about the way these technologies are used and the possibilities of misuse of collected data. The paper describes the key characteristics of the smart city architecture and analyzes the issues of threats to the security and privacy of citizens opened up by it. The sources and forms of threats to security and privacy in smart cities are numerous, interconnected and require a detailed analysis from a technical-technological, sociological and legal perspective.

Keywords: smart city, information and communication technologies, security, privacy, personal data

INTRODUCTION

Cities have always been not only a gathering point, but also a centre of social and political life, regional development and national economy. They are a temporary or final point to which people migrate searching for basic or better living conditions. It is estimated that in 2050, as many as 68.4% of the world's population will live in urban environments (Population Data Portal UNFPA, n. d.), which accounts for slightly more than two thirds of the total population.

With the increasing number of inhabitants in cities, there is also a growing necessity for the development of city infrastructure to meet the needs of their inhabitants reflected in a broad range of products and services. Some of the most important problems arising

¹ nputnik@fb.bg.ac.rs; <https://orcid.org/0000-0002-6374-7270>

² jana.markovic@fb.bg.ac.rs; <https://orcid.org/0009-0003-0676-8213>

from it refer to communal services – ensuring sufficient amount of electric power and water, waste disposal, air pollution, traffic congestion, housing conditions, as well the increasing crime rate.

The urbanization trend has simultaneously emphasized the challenges of sustainable development and imposed life quality improvement as an imperative of urban development. The solution to many challenges of urban and sustainable development has been seen in the application of modern information and communication technologies (hereinafter: ICTs), leading to the emergence of the smart city concept.

Within the context of ICTs, smart cities can also be seen as a system of mutually connected and networked systems through which an enormous amount of digital data is exchanged. However, these systems have their technical-technological weaknesses and vulnerable spots. They are exposed not only to the risks of technical failures, errors in their design and use, but also to their misuse by ill-intentioned actors in the physical and cyber worlds. Not only ICT systems are exposed to security risks, but also all data processed and stored in them. A particularly vulnerable data category are personal data which are closely related to the requirement for keeping citizens' privacy (General Data Protection Regulation, 2018). Therefore, it seems justified to request that the security of ICT systems and digital data in smart cities should be continually evaluated and improved (Marković, 2023).

THE URBAN CITY CONCEPT AND CHARACTERISTICS

The urban city concept is based on the use of modern technologies that should help city administration in providing a broad range of services with the aim of improving the quality of economic and social life. The improvement of healthcare services, establishing a digital approach to public administration, reduction of carbon-dioxide emission, waste, traffic jams and parking management, introduction of street lights intelligent systems, installation of smart electricity meters, and designing smart buildings are some of the areas of city life that may be improved by "smart technologies". Smart cities, also called digital cities, technological cities, wire cities, omnipresent cities, intelligent cities, information cities, knowledge cities, smart communities, creative cities and sustainable cities (Praharaj & Han, 2019, p. 1), connect people with technology, handling a large amount of data some of which have a particularly vulnerable nature, including personal data.

Smart cities are urban areas which, through the use of ICTs, collect, generate and process data in order to get a better insight into the behaviour and performances of consumers (citizens) and to make those areas more efficient and sustainable. Although smart cities are mainly associated with the extensive and intelligent use of ICTs ensuring data and information management, a smart city is much more than just smart technologies. A smart city is a concept that demands a holistic approach to understanding its architecture and application. Such holistic approach implies connecting several dimensions in a smart city concept: technology, sustainability, ecology, social and economic dimensions.

Although theoreticians do not agree about a universal definition of a smart city, we will single out the one provided, after a comprehensive analysis, by Renata Paola Dameri.

This author formulates a smart city as “a well-defined geographical area, in which high technologies such as ICTs, logistics, energy production etc. cooperate in creating benefits for residents in terms of well-being, inclusion and participation, environment quality, intelligent development: an area defined by a well-defined set of subjects which are able to establish rules and policies for the city administration and development” (Dameri, 2013, p. 2549).

SMART CITY COMPONENTS AND ARCHITECTURE

Understanding the smart city concept, including its architecture, therefore, requires a holistic approach referring to the totality of human, social, cultural, ecological, economic and technological factors. However, although the role of human, social and institutional capital has been recognized, it seems that the primary emphasis was and is on technology.

Most frequently identified components of a smart city are: smart management (in terms of participation in decision-making, public administration and public services); smart human capital (in terms of people, their education and employment, social interactions and integrations); smart environment (in terms of natural resources, e.g., space organization, pollution, building sustainability); smart living (in terms of the quality of life); smart economy (in terms of innovation, business operations and entrepreneurship, market, competitiveness) and smart mobility (in terms of transport and availability of services in general) (Lombardi, Giordano, Farouh & Yousef, 2012, p. 139). The above-listed components are at the same time the so-called smart city applications.

A group of authors (Gil-Garcia, Pardo & Nam, 2015, p. 78) has offered a conceptual framework for considering and understanding a smart city by expanding the framework derived by the analysis of academic literature. According to these authors, the key components of a smart city are: technology and data (information and communication technologies and other technologies, data and information), physical environment (natural environment and ecological sustainability, built environment and urban infrastructure), society (knowledge economy and pro-business environment; human capital and creativity, management, engagement and cooperation) and government (institutional order, city administration and management, public services). It is possible to see city characteristics through sustainability (infrastructure and government sustainability, energy sustainability and climate change, resolving pollution and waste issues, social, economic and healthcare sustainability), quality of life (economic and emotional well-being), urbanization (technical, infrastructural, government, economic) and smart solutions (in economic, social and ecological aspects) (Silva, Khan & Han, 2018, p. 699).

Today's smart cities generate huge amounts of data. These data need to be managed because managing data means managing a smart city. It is necessary to manage both data received from the physical world and those automatically processed, generated and analyzed in information systems. Therefore, data management aspects can be seen as aspects of perception, integration, cloud³, applications and business layers of smart city architecture (Ahmed, 2020, p. 2). The data collected through *perception* from sensors are *integrated* into

³ *Cloud* is the space on the Internet for storing data that may be accessed via Internet connection.

heterogeneous networks in order to be stored in *cloud* for smart applications and then, together with the data coming from *independent applications*, used for providing services. A comprehensive view of smart city architecture is given by a group of authors distinguishing six layers: network layer; communication layer; virtualization layer; data analysis layer, data mining⁴ layer, and application layer (Al-Turjman, Zahmatkesh & Shahroze, 2019).

Succinctly, we may say that a smart city in technical-technological terms is based on data-collecting sensors (like those detecting air temperature, number of cars at a crossing, number of people in shopping centres etc.), units or systems for automated management and control (, for example, SCADA systems), heterogeneous networks for data transfer, as well as digital data bases and powerful servers for data processing.

All the above-listed elements belong to the category of the Internet of Things⁵ because they are mutually connected by computer networks through which they communicate, along with all other devices connected to the Internet. Apart from this hardware layer, smart city architecture always includes software (applications) which ensures provision of services to users.

IMPACT OF SMART TECHNOLOGIES ON SECURITY AND PRIVACY

People tend to define security as the existence of protection and the feeling of security in everyday life. This sort of security, which is called ontological security in expert literature, shows that what people find most important is, according to Anthony Giddens, the possibility of life proceeding as usual, “the ability to go on”. This involves not only physical security, but also social and material security, as well as information security (the ability of understanding the surrounding world, changes occurring in it and giving a meaning to those changes), protection of human rights and civic freedoms, as well as protection against of socially deviant phenomena, violence and terrorism (Danilović Hristić, 2016).

One of the generally accepted definitions given by Barry Buzan – “that security is actually freedom from threats” (Buzan, 1983), gives an interpretation at a much higher level of general (state or national) security, but it can also be applied to the level of urban environment and the feeling that may be formed by users not only about the city space, but also about the digital space in which the larger part of today’s urban man takes place. The basis for violent (criminal, sexist or racist) behaviour towards certain categories or population lies in the general social and economic situation of society that is transferred onto city streets. The reality and gravity of violence in streets lead to a general feeling of insecurity in communities – and insecurity of urban spaces causes their reduction or abuse. A large change in researching this topic has been recorded since 1960s, particularly during 1980s and 1990s, owing to, among other things, the interest of feminist groups in certain topics, as well as the emergence of violent and hooligan behaviour in cities, increasing

⁴ *Data mining* may be understood as a process of sorting large sets of data with the aim of identifying patterns.

⁵ *Internet of Things (IoT)* is essentially a network of interconnected devices which collect data and exchange them with other IoT devices via the Internet.

terrorism, as well as the development of new technologies (video-surveillance, GPRS, GIS, CCTV, DVR) and their mass application in the 21st century (Danilović Hristić, Stefanović & Putnik, 2021).

New, “smart” technologies, which lie in the foundation of smart cities, generate large amounts of data. Numerous sensors installed in smart cities collect and send data to higher levels of digital architecture for the purpose of their storage, processing and use in decision-making, i.e., improving the quality of services provided to residents. In this place, data may also be understood in the context of data from the data bases of government and corporate bodies and, in addition, data collected by citizens, visitors or other stakeholders. Citizens largely use smart cars or smart houses and buildings, smart phones and watches, and all smart devices at home or at work, through which they perform their daily tasks and fulfil their social needs. Although conceived as devices for improving the quality of life, these data sources at the same time become a source of threats to security and privacy. In their very essence, smart cities have improved and replaced traditional devices by electronic ones. Therefore, in order to use different types of smart systems, citizens must first give their personal data to these smart systems. Among collected data, there are also confidential data of legal entities (governmental and non-governmental subjects), as well as personal data that include citizens’ first name and family name, identification number, tax number, insurance number, telephone number, ID number, personal photographs, videos and audio recordings, fingerprints, DNA, location and movement data etc.

Data protection implies a continued activity of implementing technical, organizational and personnel measures undertaken in relation to the assessed risk regarding threats to data and supporting infrastructure. This activity always covers two aspects: the one referring to the protection of infrastructure and technology through which data flow, and the one referring to the very data which are generated, processed and used.⁶ Data security covers their confidentiality, integrity and availability. Confidentiality ensures privacy and protection of confidential data; integrity protects data from modification, while availability ensures authorized users’ access to data. Each of the three above-mentioned aspects of data security may be threatened. Attacks on confidentiality are directed at unauthorized monitoring and access to information; attacks on integrity are directed at system intrusions in order to modify stored information, while attacks on accessibility are directed at preventing a service or at destroying the system. Critical aspects of data management also include information about the method of storing data, how they are classified, where they are kept, how they are used and who they are shared with.

Ahmed points to the existence of different types of individuals’ privacy: identity privacy, body privacy, territorial privacy, mobility privacy, communication and transaction privacy (Ahmed, 2020, p. 4).⁷ Namely, it is a large amount of various data which differ by their format, size, complexity, purpose, ownership etc. In that respect, speaking of smart

⁶ In relation to this, it should be kept in mind that the information-communication infrastructure is in the foundation of any other critical infrastructure. Many cyberattacks are directed exactly at governments and national critical infrastructures in general. In line with the characteristics of critical infrastructure, disturbances may be reflected on the entire city.

⁷ Cf. seven types of privacy (Finn, Wright & Friedewald, 2013) or different types of activities with a different degree of privacy (Evans, 2018, p. 493).

cities, it is impossible to omit so-called big data⁸ generated and used for supporting the development and sustainability of smart cities. The analysis of big data can be largely contributed by Artificial Intelligence (AI). Basically, combining the Internet of Things and AI is an efficient way of upgrading the existing smart city systems. In addition, the use of big data has also been contributed by the use of cloud technology as a global server network.

In its entirety, the use of new (smart) technologies (Internet of Things, cloud, and AI) causes suspicion among one part of the population who believe that data are not managed in an adequate manner, and that they are even intentionally abused. Therefore, smart cities cause concern regarding security and privacy and once again revive Bentham's idea of the panopticon. In the idea of "smart Panopticon", the city (state or some supranational entity) uses collected data not only for citizen surveillance, but also for the commercial use (abuse) of personal data collected in smart cities. The citizens' perception is that they have little or no control over what companies, city authorities or state governments do with their data (McClain, Faverio, Anderson & Park, 2023, p. 4).

The Guidelines for local and regional governments within the United Nations Human Settlements Programme state that "trust in public institutions is decreasing in many parts of the world due to the lack of transparency, unprotected digital infrastructure and limited opportunities for the presentation and participation of the community" (UN-Habitat, 2021, p. 47). Therefore, it is clear that citizens' support and participation in establishing, developing and sustaining a smart city are necessary and unavoidable. Whether smart cities will survive or be abolished depends exactly on the citizens' inclusion in creating public policies and decision-making about important matters (Thomas, Mula, Vang & Dan, 2015).⁹

Furthermore, it is also important to emphasize the existence of the so-called privacy paradox (Young & Quan-Haase, 2013) which speaks that citizens are, on the one hand, concerned about privacy, while, on the other hand, there is no sufficient care about preventive measures and own security in the digital world. It is an illustrative fact that the most popular PIN used is "1234" (DataGenetics, n. d.). In addition, there is also a widespread practice of using the same parameters for logging into two or more applications and, also, endless data sharing via social networks. This paradox has been explored by Van Zoonen. The conclusion of the conducted research shows that the citizens' concern about privacy varies depending on the type of data, the purpose of their collection and use (data processing for the purpose of providing services causes the lowest degree of concern, while the highest degree of concern is caused by the purpose of surveillance) and the organization or person(s) collecting and using data – impersonal (pseudonymized or anonymized) data cause the lowest smallest degree of concern, while personal data cause the highest degree of concern (2016).

The research conducted in 2023 confirms the assumption that the type of collected data mostly affects the citizens' perception and concern, while data processing time affects is at the lowest level. Data whose collection causes the largest concern include sensitive

⁸ *Big Data* are an enormous amount of non-structured data which are continuously multiplied, while only one part of them is used for decision-making.

⁹ Toronto is an example of a city in which the smart city initiative was not accepted and adopted. The main reason for this is the citizens' concern for their data privacy. The citizens believed that this initiative neglected people and their needs, while prioritizing the quantification and control of everything that would exist in a smart city (Cecco, 2019).

and personal data, such as video-recordings, data about the number of people and their location (Emami-Naeini et al., 2023).

The research findings about the use of software applications indicate that a lower degree of concern is caused by those applications which are of general character, for example, web browsers or applications for exchanging e-mails. Greater concern is caused by the applications related to personal data, such as social networks and banking applications (Bergström, 2015, p. 421).

The research conducted in the USA, as many as 81% of the respondents expressed concern about the manner in which private companies collect their data, while 71% expressed concern about the manner it is done by the government (McClain, Faverio, Anderson & Park, 2023, p. 3). The issue of privacy in the context of surveillance by the government has drawn the attention of many authors. Some of them find the connection between acceptability of surveillance and the manner of perception of the government itself. Namely, "individual acceptability of the government surveillance depends on their perception of the government and public affairs" (Nam, 2018, p. 540), or on the citizens' trust in the government. Moreover, one of the studies emphasizes the important role of social impact and reciprocity in accepting technologies that require mass acceptance and reciprocal disclosure of information required by various applications (Fox et al., 2021, p. 12). Some studies also include nationality and national culture as a variable, or a factor affecting the respondents' behaviour and perceptions (Budak, Rajh & Recher, 2017; Hallinan, Friedewald & McCarthy, 2012; Thompson et al., 2020).

It is important to note that the past few decades have witnessed the development of security standards aimed at protecting digital data. The best-known among them is definitely the set of standards ISO 27000. These standards substantially contribute to data security and the citizens' privacy protection. Nevertheless, these standards on their own are not a guarantee of security because of the constant emergence of new technologies (with new vulnerabilities) and software applications based on them. That is why it is necessary to ensure that all technologies and applications used for smart city needs have and maintain an optimal level of security and privacy. Ensuring the highest level of protection is also of key importance for further development of electronic trade markets, on which the development of a smart city largely depends. Moreover, constant activity is necessary on (re)defining, implementing and harmonizing national and international security policies and strategies, laws and standards (Putnik, Milošević & Cvetković, 2022, pp. 338–339). Therefore, security and privacy are a multidimensional problem whose solutions depend on technological and socio-economic factors, as well as on political decision-makers. An unavoidable aspect of protection is also the requirement for raising citizens' awareness and education, which would ensure a higher level of citizens' security culture and reduce their susceptibility to manipulation.

CONCLUSION

The smart city concept, on the one hand, covers the use of ICTs which implies the use of hardware, software and computer networks while, on the other hand, it emphasizes the advancement of the quality of citizens' life in different spheres, such as: infrastructure, energy, transport, natural resources, public services etc., by using previously generated big data.

For a smart city to fulfil its main purpose and improve the quality of services it provides to its citizens and visitors, great amounts of data must be collected, analyzed and prepared for decision-making. This process is largely contributed by smart technologies: big data, Internet of Things, cloud and artificial intelligence. In relation to the above-mentioned aim, cities try to improve the existing technologies or to implement new ones which find their place in all sectors of economic, environmental, political, social and cultural aspects. Many of these technologies demand users' active participation in order to fulfil their potential, i.e., their consent for active data sharing on various. On the other hand, some of these technologies (e.g., video-surveillance of public space or different sensors) collect data without citizens' consent. This fact is important because it may lead to abuses of personal data – illegal profiling of individual users based on allegedly anonymous data.

The issue of data protection and privacy takes the central place in academic debates thematizing the smart city concept. Citizens' concern due to the development of technologies enabling the collection and processing of their data is one of the key issues both in scientific circles and in the practical political sphere. Citizens' concern varies in relation to the type of data to be collected, the applications used, processing purpose and aim, as well as in relation to the subject collecting and using data.

Therefore, wise management of smart cities demands serious public opinion surveys in order to enable decision-makers to regulate adequately data management in a smart city. In that manner, transparency and inclusion of citizens in decision-making is achieved, on which the implementation of smart technologies and the smart city development largely depend as well. In democratic countries, decision-makers try to reduce the level of citizens' concern about privacy and, at the same time, to win their support for the development of smart applications. This is certainly preceded by creating an adequate legal framework which should guarantee transparency and participation of the community in decision-making.

Finally, the smart city concept raises numerous issues that need to be answered in the future. From the perspective of information security, it is necessary to evaluate current and potential solutions to data security and protection from the perspective of new threats occurring on a daily basis. From the sociological aspect, an important contribution may be expected from the research aimed at the citizens' perception regarding the issues of their security and privacy. Equally important would also be the analysis of the existing legal framework in this sphere – specific institutional and legislative solutions adopted with the aim of protecting data security and privacy in smart cities.

REFERENCES / ЛИТЕРАТУРА

- Ahmed, S. (2020). Security and Privacy in Smart Cities: Challenges and Opportunities *International Journal of Engineering Trends and Technology*, 68 (2), 1–8. DOI: [10.14445/22315381/IJETT-V68I2P201](https://doi.org/10.14445/22315381/IJETT-V68I2P201).
- Al-Turjman, F., Zahmatkesh, H., Shahroze, R. (2019). An overview of security and privacy in smart cities' IoT communications. *Trans Emerging Tel Tech*, e3677. DOI: [10.1002/ett.3677](https://doi.org/10.1002/ett.3677).
- Bergström, A. (2015). Online privacy concerns: A broad approach to understanding the concerns of different groups for different uses. *Computers in Human Behavior*, 53, 419–426. DOI: [10.1016/j.chb.2015.07.025](https://doi.org/10.1016/j.chb.2015.07.025).

- Buzan, B. (1983). *People, states, and fear: the national security problem in international relations*. Wheatsheaf Books.
- Budak, J., Rajh, E., Recher, V. (2017). Citizens' privacy concerns: does national culture matter?. In: M. Friedewald et al. (eds.). *Surveillance, Privacy and Security*, 36–51. Routledge.
- Cecco, L. (2019, June 6). 'Surveillance capitalism': critic urges Toronto to abandon smart city project. *The Guardian*. Available at: <https://www.theguardian.com/cities/2019/jun/06/toronto-smart-city-google-project-privacy-concerns>.
- Dameri, R. P. (2013). Searching for smart city definition: a comprehensive proposal. *International Journal of computers & technology*, 11 (5), 2544–2551.
- DataGenetics. (n. d.). *PIN analysis*. Available at: <http://www.datagenetics.com/blog/sep-tember32012/>.
- Danilović Hristić, N. (2016). Languish After Safety in the Urban Life. In: *Conference Proceedings, Fourth International Conference and Exhibition, On Architecture: Scale of Design – From Micro to Macro, STRAND*, 14, 43–51.
- Danilović Hristić, N., Stefanović, N., Putnik, N. (2021). The Real Effects of The Use of Security Cameras in Public Urban Spaces and Controversies Related to Privacy Protection. In: A. Gül, Ö. Demirel & S. Seydoşoğlu (eds.). *The Proceeding Book - 1st International Architectural Sciences and Applications Symposium*, 1296–1303. ISPEC Publishing House.
- Emami-Naeini, P., Breda, J., Dai, W., Kohno, T., Laine, K., Patel, S., Roesner, F. (2023). Understanding People's Concerns and Attitudes Toward Smart Cities. In: A. Schmidt et al., (eds.). *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems (CHI '23)* (Article No.: 71, 1–24). New York: Association for Computing Machinery. DOI: [10.1145/3544548.3581558](https://doi.org/10.1145/3544548.3581558).
- Evans, L. (2018). The privacy parenthesis: Private and public spheres, smart cities and big data. *Creating smart cities*, 194–204. DOI: [10.4324/9781351182409](https://doi.org/10.4324/9781351182409).
- Finn, R. L., Wright, D., Friedewald, M. (2013). Seven Types of Privacy. In: S. Gutwirth et al. (eds.). *European Data Protection: Coming of Age*, 3–32. Dordrecht: Springer. DOI: [10.1007/978-94-007-5170-5_1](https://doi.org/10.1007/978-94-007-5170-5_1).
- Fox, G., Clohessy, T., Van der Werff, L., Rosati, P., Lynn, T. (2021). Exploring the competing influences of privacy concerns and positive beliefs on citizen acceptance of contact tracing mobile applications. *Computers in Human Behavior*, 121, 106806. DOI: [10.1016/j.chb.2021.106806](https://doi.org/10.1016/j.chb.2021.106806).
- General Data Protection Regulation, 2018. <https://gdpr-info.eu/>
- Gil-Garcia, J. R., Pardo, T. A., Nam, T. (2015). What makes a city smart? Identifying core components and proposing an integrative and comprehensive conceptualization. *Information Policy*, 20 (1), 61–87. DOI: [10.3233/IP-150354](https://doi.org/10.3233/IP-150354).
- Hallinan, D., Friedewald, M., McCarthy, P. (2012). Citizens' perceptions of data protection and privacy in Europe. *Computer Law & Security Review*, 28 (3), 263–272. DOI: [10.1016/j.clsr.2012.03.005](https://doi.org/10.1016/j.clsr.2012.03.005).
- Lombardi, P., Giordano, S., Farouh, H., Yousef, W. (2012). Modelling the smart city performance. *The European Journal of Social Science Research*, 25 (2), 137–149. DOI: [10.1080/13511610.2012.660325](https://doi.org/10.1080/13511610.2012.660325).

- Marković, J. (2023). Information security in the function of business continuity management. *Savremene studije bezbednosti*, 1 (2), 11–28. DOI: [10.5937/ssb202301011M](https://doi.org/10.5937/ssb202301011M). [In Serbian].
- McClain, C., Faverio, M., Anderson, M., Park, E. (2023). *How Americans View Data Privacy*. Pew Research Center. Available at: <https://www.pewresearch.org/internet/2023/10/18/how-americans-view-data-privacy/>.
- Nam, T. (2018). What determines the acceptance of government surveillance? Examining the influence of information privacy correlates. *The Social Science Journal*, 56, 530–544. DOI: [10.1016/j.soscij.2018.10.001](https://doi.org/10.1016/j.soscij.2018.10.001).
- Population Data Portal UNFPA. (n. d.). *Percentage of population residing in urban areas*. Available at: <https://arcg.is/1DuzC1>.
- Praharaj, S., Han, H. (2019). Cutting through the clutter of smart city definitions: A reading into the smart city perceptions in India. *City, Culture and Society*, 18, 100289. DOI: [10.1016/j.ccs.2019.05.005](https://doi.org/10.1016/j.ccs.2019.05.005).
- Putnik, N. R., Milošević, M. M., Cvetković, V. N. (2022). Ransomware as a security threat – Social and criminal legislation aspects. *Sociološki pregled*, 56 (1), 328–353. DOI: [10.5937/socpreg56-36845](https://doi.org/10.5937/socpreg56-36845).
- Silva, B. N., Khan, M., Han, K. (2018). Towards sustainable smart cities: A review of trends, architectures, components, and open challenges in smart cities. *Sustainable cities and society*, 38, 697–713. DOI: [10.1016/j.scs.2018.01.053](https://doi.org/10.1016/j.scs.2018.01.053).
- Thomas, V., Mullagh, L., Wang, D., Dunn, N. (2015). Where's Wally? In Search of Citizen Perspectives on the Smart City. In: D. Kim et al. (eds.). *Proceedings of the 8th Conference of the International Forum on Urbanism (IFoU)*. Basel: MDPI. DOI: [10.3390/ifou-A001](https://doi.org/10.3390/ifou-A001).
- Thompson, N., McGill, T., Bunn, A., Alexander, R. (2020). Cultural factors and the role of privacy concerns in acceptance of government surveillance. *Journal of the Association for Information Science and Technology*, 71 (9), 1129–1142. DOI: [10.1002/asi.24372](https://doi.org/10.1002/asi.24372).
- United Nations Human Settlements Programme [UN-Habitat]. (2021). *Centering People in Smart Cities: A playbook for local and regional governments*. United Nations. Available at: <https://unhabitat.org/programme/people-centered-smart-cities/people-centered-smart-cities-playbooks>.
- Van Zoonen, L. (2016). Privacy Concerns in Smart Cities. *Government Information Quarterly*, 33 (3), 472–480. DOI: [10.1016/j.giq.2016.06.004](https://doi.org/10.1016/j.giq.2016.06.004).
- Young, A. L., Quan-Haase, A. (2013). Privacy protection strategies on Facebook: The Internet privacy paradox revisited. *Information, Communication & Society*, 16 (4), 479–500. DOI: [10.1080/1369118X.2013.777757](https://doi.org/10.1080/1369118X.2013.777757).