VARSTVOSLOVJE,
letn. 20
št. 1
str. 5–24

Zasebnost v pametnih mestih ali zasebnost za pametne ljudi?

Damjan Fujs, Blaž Markelj

Namen prispevka:

Mesta postajajo tehnološko naprednejša, zlasti, da bi zadostila potrebam vedno večjega števila ljudi. Tehnologija, predvsem »pametna« tehnologija, daje posamezniku udobje v zameno za njegovo zasebnost. Dostop do storitev je mogoč s pomočjo številnih programskih rešitev, tudi aplikacij na mobilnih napravah. Ob nevestni uporabi aplikacij ter nepoznavanju pomena varovanja zasebnosti je tveganje za poseg v zasebnost veliko. Namen prispevka je izpostaviti stališče ljudi do zasebnosti v pametnih mestih ter predstaviti, kaj so tehnologije, ki sestavljajo pametno mesto.

Metode:

Predstavljene ugotovitve so podprte z deskriptivnimi dognanji, ki temeljijo na virih in literaturi ter izvedeni raziskavi, ki smo jo analizirali s pomočjo statističnih metod.

Ugotovitve:

Poznavanje koncepta pametnih mest je na slovenskem področju izjemno slabo. Glavne ugotovitve raziskave kažejo, da ljudje niso pripravljeni bivati v pametnih mestih. Skrbi jih nivo potrebnega računalniškega znanja, ki izhaja iz posameznikovega nepoznavanja pametnih mest. Podatke, pridobljene v pametnih mestih, bi morala upravljati država in ne zasebna podjetja.

Omejitve/uporabnost raziskave:

Znanstvenih objav na temo zasebnosti v pametnih mestih je malo. Omejitev predstavlja tudi ciljna skupina, ki ni na družabnih omrežjih (predvsem starejša populacija), zato bi bilo smiselno izvesti raziskavo tudi med starejšo populacijo.

Praktična uporabnost:

Izsledki raziskave nam pokažejo posameznikovo poznavanje pomena zasebnosti v pametnih mestih, kar predstavlja izhodišče za nadaljnje aplikativno in znanstveno delo na omenjenem področju.

Izvirnost/pomembnost prispevka:

Prispevek na izviren način obravnava aktualno tematiko, katere pomembnost bo v prihodnosti še naraščala.

UDK: 004

Ključne besede: zasebnost, pametna mesta, Splošna uredba o varstvu osebnih podatkov, pametna tehnologija, pametna skupnost

Privacy in Smart Cities or Privacy for Smart People?

Purpose:

Cities are becoming technologically advanced in order to fulfil the needs of constantly increasing number of people. Namely, technology, especially smart one, provides individuals commodity in return for their privacy. Negligent use of applications and lack of knowledge on importance of safeguarding privacy induce great risk for privacy encroachment. The purpose of this paper is to emphasise the attitude of individuals toward privacy in smart cities and to present the technology of smart city.

Design/Methods/Approach:

The findings, presented in paper, are based on descriptive analysis of sources and literature and statistical analysis of research results.

Findings:

Knowledge on smart city concept in Slovenia is extremely poor. The main findings of this research show that people do not want to live in smart cities. They are worried about the needed level of computer knowledge, which even further shows, how little people know on smart cities. The data acquired in smart cities should be in the jurisdiction of the country and not in the hands of private companies.

Research Limitations/Implications:

There are few scientific publications on privacy in smart cities. Another limitation is the focus group of people, who do not use social networks, especially the older population. Therefore, it would be wise to conduct research among this population.

Practical Implications:

Findings of the research could be basis for lectures on awareness of privacy in smart cities and for guidelines for future work regarding more effective privacy protection.

Originality/Value:

The paper addresses topical issue, whose importance will continue to increase in the future.

UDC: 004

Keywords: privacy, smart cities, General Data Protection Regulation, smart technology, smart community

1 UVOD

»Vemo, kje se nahajate. Vemo, kje ste se nahajali v preteklosti. Več ali manj nam je znano, o čem razmišljate.« (Eric Schmidt)[1]

Skoraj petindvajset let je minilo od tega, ko se je pojavilo prvo digitalno[2] mesto Amsterdam (angl. *digital city of Amsterdam*), ki je bilo rezultat desettedenskega socialnega eksperimenta. Povod za gradnjo digitalnega mesta so dale različne skupine, ki so si želele javni digitalni prostor (pojav novega medija), kjer lahko ljudje komunicirajo in se spoznavajo ter sodelujejo s predstavniki lokalnih oblasti. Pomembno vlogo pri tem je odigrala skupina računalniških zanesenjakov »Hacktic«, ki je zagovarjala prosti dostop do interneta in bila prvi ponudnik interneta za širšo javnost (angl. *access for all – XS4ALL*) (van den Besselaar, 2005). Po mnenju Anthopoulosa (2017) je ravno primer digitalnega mesta Amsterdam sprožil vpeljavo pametnih stvari v t. i. kiber-fizični prostor[3] in s tem pojav sodobnih pametnih mest, ki vključujejo širok nabor informacijsko-komunikacijskih tehnologij (v nadaljevanju IKT). Da se neko mesto poistoveti z izrazom pametno mesto, ni nujno, da v svoj koncept delovanja vpelje IKT, kajti mnogo pametnih rešitev je opredeljenih v organizacijskih politikah in v dobrih praksah mest po svetu.

Sodobna družba je deležna socialnih, ekonomskih, kulturnih ter tehnoloških sprememb. Ravno zaradi tega, ker smo družba znanja in informacij, predstavljamo razvojni kapital, ki ga je treba skrbno varovati. Da bi čim bolje varovali svoje »premoženje«, se je treba v prvi vrsti zavedati, kaj je tisto, kar nas ogroža (Sotlar in Tominc, 2012). Kaj je pravzaprav glavna težava pametnih mest, ki so del kibernetskega prostora? Bernik in Meško (2011) opozarjata na široko dostopnost in rabo IKT, ki odpirajo vrata v kibernetski prostor, kar je lahko tudi način oz. tarča za izvajanje kriminalitete. Avtorja tudi ugotavljata, da je v družbi prisotno pomanjkanje ozaveščenosti o kibernetski kriminaliteti tako v zasebnem kot poslovnem svetu. Resolucija o strategiji nacionalne varnosti Republike Slovenije (ReSNV-1, 2010) opredeljuje t. i. nadnacionalne vire ogrožanja, med katere spadajo tudi kibernetske grožnje in zlorabe informacijskih tehnologij in sistemov, kamor bi lahko uvrstili tudi pametna mesta. Pametna mesta so dandanes načrtovana s težnjo k trajnostnemu razvoju, da bi bolj strateško in preudarno upravljala sredstva in surovine, kar je posledica finančne krize iz leta 2008. Enotnega kriterija za mednarodno definicijo pametnih mest ni, tako da si vsaka država po svoje interpretira kriterije za naziv pametno mesto. Številni avtorji menijo, da bo raznovrstna tehnologija v pametnih mestih izboljševala razmere in prispevala

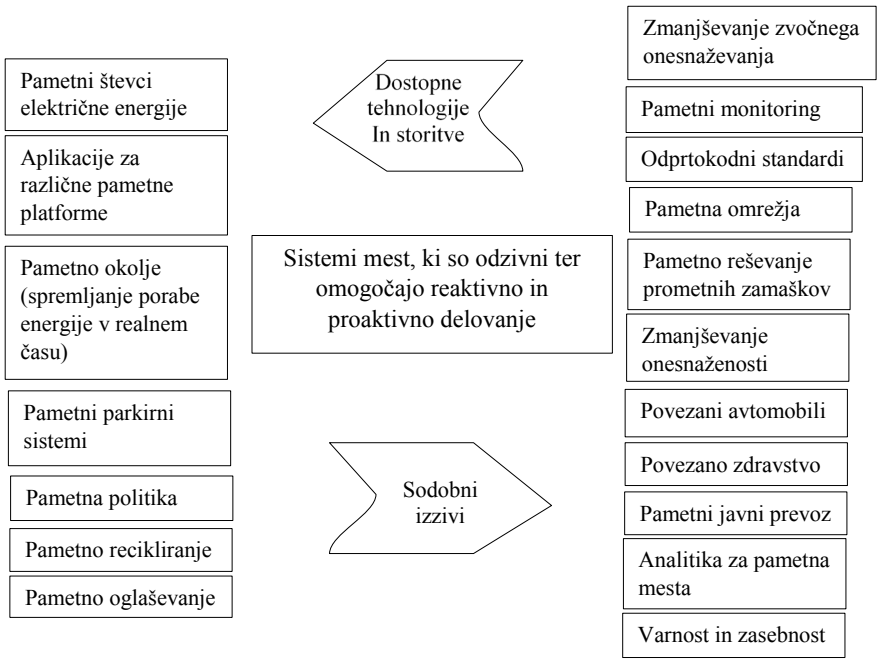
1 *Eric Schmidt je nekdanji generalni direktor podjetja Google in sedanji predsednik uprave podjetja Alphabet, ki je starševsko podjetje prej omenjenemu Googlu ter nekaterim ostalim vodilnim tehnološkim gigantom, kot so: Nest (naprave za pametne domove), Fiber (super hitri internet), Google Capital (investicije v dolgotrajne tehnološke trende) itd.*

2 *Leta 1993 se pojavi izraz digitalno mesto, nadalje pa avtorji uporabljajo izraze, kot so inteligentna mesta, inovativna mesta, povezana mesta, kreativna mesta ter zdaj že vsesplošno sprejeti pojem pametna mesta. Ahvenniemi, Huovila, Pinto-Seppä in Airaksinen (2017) namesto pojma pametna mesta predlagajo nov termin, ki vključuje trajnostni vidik mest – k trajnostnemu razvoju naravnana pametna mesta (angl. smart sustainable cities).*

3 *Rajkumar, Lee, Sha in Stankovic (2010) kiber-fizični prostor (angl. cyber-physical space) opredeljujejo kot pametni sistem, kjer s pomočjo računalnikov in senzorjev spremljamo dogajanje okrog sebe.*

finančna sredstva (gospodarski vidik), spet drugi menijo, da bi pametna mesta morala biti v osnovi narejena za izboljšanje storitev, ki se jih poslužujejo prebivalci (sociološki vidik) (Beretta, 2018).

1.1 Tehnologija pametnih mest ter izzivi



Slika 1: Shematični prikaz dostopnih tehnologij in storitev ter sodobnih izzivov, ki spremljajo razvoj pametnih mest (vir: Kim, Ramos in Mohammed, 2017)

Slika 1 prikazuje shemo, ki predstavlja že obstoječe tehnologije v pametnih mestih in sodobne izzive, s katerimi se srečujejo vsi tisti, ki se ukvarjajo z razvojem pametnih mest. Tehnologija pametnih mest je skladna s tehnološko podporo interneta stvari (angl. *internet of things*, v nadaljevanju IOT[4]), kar pomeni, da se številni senzorji[5] (RFID, IR, GPS, laserski skenerji itd.) preko specifičnih protokolov povezujejo v omrežje, kar omogoča komunikacijo in izmenjavo informacij v pametnih mestih. Kljub vsem tehnološkim in organizacijskim rešitvam pa se pojavljajo novi sodobni izzivi, za katere še nimamo razvitih pametnih prijemov, da

4 *Kim et al. (2017) opozarjajo na ranljivost pametnih naprav, kajti povprečni čas za vdor v pametno napravo (ko se le-ta poveže v sicer zaščiteno omrežje), ki je del IOT, znaša šest minut (360 sekund). Vidimo, da bo treba velik poudarek nameniti samemu razvoju programske opreme, ki bo moral biti dovolj robusten, da ne bo prihajalo do varnostnih vrzeli in s tem posledično tudi do ogrožanja zasebnosti.*

5 *Tipičen primer uporabe senzorjev v pametnih mestih se nanaša na reguliranje temperature. Senzorji na podlagi zunanje temperature določajo temperaturo v notranjih prostorih. Temperaturni senzorji v pametnih mestih so nadgrajeni do te mere, da regulirajo temperaturo tudi glede na vlažnost zraka, kar bistveno prispeva k zmanjšanju stroškov ogrevanja (do 40 odstotkov prihranka) ter k udobnosti bivanja (Lefèvre, v tisku).*

bi se z njimi soočali. Završnik (2010) navaja, da moramo biti pri izbiri tehnologije pozorni, ker ima nekatera tehnologija dvojno možnost uporabe. Na eni strani ogrožajo življenje, na drugi ga rešujejo, po eni strani odvzemajo svobodo, po drugi strani jo dajejo. Te ugotovitve lahko apliciramo tudi v sfero pametnih mest, kjer npr. na eni strani senzorji omogočajo spremljanje zdravstvenega stanja, po drugi strani pa so neka »živa tarča« napadov s strani hekerjev, ki želijo pridobiti te podatke.

2 KONCEPT ZASEBNOSTI IN INFORMACIJSKA VARNOST V PAMETNIH MESTIH

Završnik (2010) navaja, da se vsebina koncepta zasebnosti spreminja in da je z zasebnostjo mogoče trgovati. Podobno je tudi v pametnih mestih, kjer npr. senzorji, ki so postavljeni na določenih lokacijah, po mestu zbirajo podatke o številu pešcev in kolesarjev. Ti podatki nam, posameznikom, ne povedo skoraj nič, mnogo pa razkrijejo tistim, ki so odločevalci v mestu. Na podlagi števila pešcev in kolesarjev na merjenih lokacijah odločevalci lažje razporejajo finančna sredstva za dograditev pločnikov, športnih parkov itd.

Chan, Bateman in Olafsson (2016) poudarjajo, da informacijska varnost s svojo celovitostjo ščiti tudi zasebnost, kar lahko apliciramo tudi v področje pametnih mest. Elmaghraby in Losavio (2014) menita, da sta varnost in varovanje dokaj podobna pojma, ki pa se razlikujeta. Pri varnosti (»nič slabega se še ni zgodilo«) vlagamo več časa in sredstev v prevencijo, medtem ko pri varovanju (»nekaj se dogaja«) uporabljamo različne mehanizme, da bi odpravili oz. vsaj omilili dejanske grožnje. Kibernetska varnost se v tem primeru osredotoča na varnost računalniških sistemov ter na varnost izmenjave podatkov in za to predvideva sankcije (kazensko pravo). Računalniški sistemi v pametnih mestih so jedro težave varovanja informacij, zato se moramo osredotočiti na t. i. CIA model, ki zagotavlja informacijsko varnost; zaupnost (angl. *confidentiality*), celovitost (angl. *integrity*) in dostopnost (angl. *availability*) informacij, in kar posledično zagotavlja tudi zasebnost v pametnih mestih.

Ena izmed osnovnih nalog države je, da v svojih zakonodajnih okvirih zagotavlja pravico do zasebnosti, kar je pri »gradnji« pametnih mest in zagotavljanju informacijske varnosti ključnega pomena. Zato kot primer izpostavljamo Ustavo Republike Slovenije (Ustava RS, 1991), ki koncept utemeljenega pričakovanja zasebnosti zagotavlja v štirih členih (35. člen, 36. člen, 37. člen in 38. člen). Splošni 35. člen se nanaša na varstvo pravic zasebnosti in osebnostnih pravic ter zagotavlja človekovo telesno in duševno nedotakljivost ter nedotakljivost zasebnosti in osebnostnih pravic. 36. člen se dotika prostorske oziroma teritorialne zasebnosti ali t. i. nedotakljivosti stanovanja. S perspektive načrtovanja in delovanja pametnih mest pa je bolj pomemben oz. uporaben 37. člen Ustave RS (1991), ki zagotavlja tajnost pisem in drugih občil oziroma komunikacijsko zasebnost. Omenja tudi, da samo zakon lahko predpiše, da se na podlagi odločbe sodišča za določen čas ne upoštevata varstvo tajnosti pisem in drugih občil ter nedotakljivost človekove zasebnosti, če je to nujno za uvedbo ali potek kazenskega postopka ali za varnost države. Iz besedila 38. člena Ustave RS

(1991), ki zagotavlja informacijsko zasebnost, pa lahko razberemo, da je zakonsko zagotovljeno varstvo osebnih podatkov in da ima vsak posameznik pravico se seznaniti z zbranimi osebnimi podatki, ki se nanašajo nanj, in pravico do sodnega varstva ob njihovi zlorabi (Ustava RS, 1991).

Da je zasebnost zelo pomembna dobrina posameznika, priča dejstvo, da je bila pravica do zasebnosti deklarirana že leta 1948 v Splošni deklaraciji o človekovih pravicah, ki jo je sprejela in razglasila generalna skupščina Združenih narodov (Sotlar in Trivunović, 2012). Ziegeldorf, Morchon in Wehrle (2014) pojasnjujejo, da se je koncept zasebnosti zgodovinsko gledano bolj ali manj nanašal na telesno zasebnost. V sedemdesetih letih 20. stoletja pa se prvič pojavi izraz »informacijska zasebnost«[6]. Glede na to, da pametna mesta operirajo z velikim podatkovjem, moramo dajati poudarek na zaščito le-teh in to zato, da bi preprečili poseg v zasebnost. Zato je pomembno, da zasebnost preučujemo in jo hkrati varujemo v najboljši možni meri.

Z zasebnostjo[7] se bolj podrobno po besedah Završnika in Levičnika (2014) ukvarjamo od leta 2013, ko je Edward Snowden širši javnosti prikazal množično vohunjenje. Avtorja tudi ugotavljata, da so Snowdnova odkritja na strah pred tujimi obveščevalnimi službami vplivala tudi na področju Slovenije. Podobno v svoji doktorski tezi meni tudi Williams (2017), kjer navaja, da so ravno Snowdnova odkritja privedla do tega, da je bil leta 2013 na spletni strani www.dictionary.com najbolj iskan termin *privacy* (slov. zasebnost).

Po besedah Ziegeldorfa et al. (2014) se dandanes v sferi IOT pojavljajo trije ključni elementi, ki oblikujejo informacijsko zasebnost:

- Individualno zagotavljanje kontrole nad zbiranjem in procesiranjem osebnih podatkov.
- Ob uporabi »pametnih stvari« je treba poznati morebitna tveganja glede zasebnosti.
- Zavedati se je tudi treba, da se lahko osebni podatki razširijo izven meja kontrolirane zasebnosti.

Glede na to, da so pametni sistemi preko aplikacij povezani z mobilnimi napravami, se je treba osredotočiti na zagotavljanje informacijske varnosti in varovanje zasebnosti. Weber (2015) opozarja, da je na trgu še vedno ogromno aplikacij, ki zbirajo podatke o lokaciji brez neposredne privolitve uporabnika, medtem ko Markelj in Zgaga (2016) opozarjata na problem mlajših uporabnikov pametnih mobilnih naprav, ki so nepoučeni glede potencialnih groženj in ne uporabljajo varnostnih mehanizmov, ki zagotavljajo višjo stopnjo informacijske varnosti.

2.1 Grožnje zasebnosti v pametnih mestih

Ziegeldorf et al. (2014) ugotavljajo, da naprave, ki so povezane v IOT in so del pametnih mest, predstavljajo nove možnosti interakcij oz. povezljivosti med

6 *Informacijska zasebnost je v takratnih časih pomenila »imeti pravico odločati, kaj lahko drugi vedo o meni«.*

7 *Beseda zasebno je protipomenka besedi javno. Javno je nekaj, kar ni skrito in ga je mogoče dojemati s čutili. Iz tega lahko sklepamo, da je beseda »zasebnost« nekaj, kar je zasebno in ni namenjeno širši javnosti, torej nekaj, kar je skrito (Kanduč et al., 2012).*

napravami, kar lahko privede tudi do novih groženj zasebnosti. Po njihovem mnenju bo IOT v prihodnosti igral zelo pomembno vlogo v vsakdanu slehernega posameznika, ker so po svetu že uveljavljene institucije, ki se ukvarjajo z razvojem naprednejših tehnologij za vzpostavitev globalnega IOT omrežja. Da bo IOT globalno pomembna tržna niša, priča tudi dejstvo, da se v organizacije za razvoj IOT združujejo najboljši in najbolj napredni laboratoriji iz celega sveta (na primer Auto-ID lab). Prej omenjeni avtorji tudi menijo, da zaradi narave razvoja IOT tehnologij, lahko delimo grožnje zasebnosti v pametnih mestih v naslednjih sedem sklopov:

- **Identifikacija**: na podlagi zbranih podatkov s pomočjo različnih naprav (predvsem s kamerami ter senzorji za prepoznavo obraza in glasu) bo mogoče določiti posameznika.
- **Lokalizacija in sledenje**: na podlagi pretočnih podatkov mobilne naprave in povezovanja na bazne postaje ter GPS je mogoče izslediti osebo.
- **Profiliranje**: s pomočjo zbranih osebnih podatkov je mogoče profilirati posameznika. (Facebook ima na primer možnost, da na podlagi določenih algoritmov zazna spolne prestopnike).
- **Interakcije in predstavitve, ki kršijo zasebnost**: treba se je zavedati, da nas lahko ob uporabi tehnologije opazujejo druge osebe, ki z »gledanjem čez ramo« zbirajo podatke o nas in s tem kršijo našo zasebnost.
- **Prenos naprav**: ko se odločimo za prodajo naprave, ki hrani podatke je pomembno, da poskrbimo za trajni izbris podatkov. Moramo se držati načela: »kupi enkrat, imej za vedno«.
- **Napadi na inventar**: napadi na vse vrste pametnih stvari, ki so povezane v IOT. Gre za sofisticirano obliko prestrezanja podatkov s strani nepooblaščenih oseb.
- **Neposredno povezovanje**: Zgodi se lahko, da se dva sistema, ki prej nista bila povezana in bi morala biti popolnoma izolirana drug od drugega, povežeta. Na podlagi tega je možno reidentificirati anonimizirane oz. psevdonimizirane podatke.

Zgoraj naštete grožnje so povezane s pametnimi mesti tako, da napadalci manipulirajo s tehnologijo, ki je dostopna v pametnih mestih. Pri tem ne gre za višjo in nedostopno tehnologijo, ampak za preproste tehnične rešitve, ki olajšujejo življenje v mestu.

Številni avtorji menijo, da so zbrani lokacijski podatki jedro težav v pametnih mestih. Lokacijski podatki, zbrani v pametnih mestih, vsebujejo širok nabor informacij, ki lahko razkrijejo npr. posameznikovo politično prepričanje, zdravstveno stanje ter socialni status (Elmaghraby in Losavio, 2014). Težava pri pametnih mestih je tudi, komu dati legitimen dostop do podatkov in kateri podatki so dostopni širši javnosti (torej posredovani v javno uporabo). Pri tem je stroka razdeljena na dva dela, en del podpira uporabo velikega podatkovja[8] (angl.

8 *Še vedno ni enotne opredelitve, kaj pravzaprav je veliko podatkovje. Splošno uporabljena definicija je, da gre za veliko količino različnih in različno pridobljenih podatkov, na podlagi katerih je mogoče prepoznati neke vzorce obnašanja (Lueks, Alpár, Hoepman in Vullers, 2017).*

big data), češ da spodbujajo ekonomično rast mest ter omogočajo največji možni izkoristek udobja. Po drugi strani pa se strokovnjaki za urbanizem zavzemajo za čim manjšo uporabo velikih podatkov, ki po njihovem mnenju znižujejo kreativnost in vodijo do neke vrste »robotskih mest«, kjer ni mesta za deviantnost[9] (van Zoonen, 2016). Cilj uporabe velikega podatkovja je, da se na podlagi statističnih analiz enormnih količin zbranih podatkov nadomestijo človekovo znanje, izkušnje in intuicija z namenom, da se izognemo sprejemanju napačnih odločitev, ki temeljijo na človekovi subjektivnosti. Lex Machina[10] je primer uporabe velikega podatkovja na sodišču, ko se združita pravo in tehnologija. Pretekle raziskave na Vrhovnem sodišču v Združenih državah Amerike so pokazale, da so napredni algoritmi sposobni boljšega predvidevanja kot za to priučeni posamezniki oz. strokovnjaki. Podobna raziskava je bila izvedena tudi na Evropskem sodišču za človekove pravice, kjer so strokovnjaki razvili sistem za predvidevanje odločitev na podlagi preteklih že odločenih zadevah. Sistem se je pokazal kot izjemno natančen in to kljub temu, da je temeljil zgolj na tekstovni bazi podatkov o primeru in posebej razvitih algoritmih (Završnik, 2017). Tehnologijo, kot je Lex Machina, bi lahko uporabili tudi v pametnih mestih, kjer bi npr. senzorji javljali najprimernejšo oz. najvarnejšo pot do končnega cilja, pri čemer bi tehnologija analizirala podatke, ki so na voljo v realnem času.

Avtorica van Zoonen (2016) ugotavlja, da je ljudi strah za njihovo zasebnost, vendar na drugi strani niso pripravljeni narediti nič za dosego le-te, še več, pripravljeni so se odpovedati delu zasebnosti; še vedno je najbolj priljubljena PIN koda 1234 in še vedno je veliko ljudi, ki uporablja eno geslo za več spletnih mest. Avtorica nadalje omenja, da veliko ljudi kljub nezaupanju do družabnih omrežij objavlja svoje zasebno življenje in ga daje na vpogled drugim. Vse to našteto pa je pokazatelj paradoksa zasebnosti v pametnih mestih, kar pomeni, da še tako veliko število tehnologij in varnih rešitev pri uporabi le-te ne odtehta človekovega voljnega ravnanja, da bi deloval v smeri zaščite svoje zasebnosti in v smeri doseganja informacijske varnosti.

Gharaibeh et al. (2017) vidijo grožnje zasebnosti ter njihove rešitve v pametnih mestih v naslednjih 15 sklopih[11]:

- **Modifikacija podatkov (angl. *data modification*)**: Vrši se na način, da s pomočjo spreminjanja, brisanja ter prirejanja lahko škodujemo celovitosti izmenjanih podatkov. Rešitev za tako težavo je uvedba infrastrukture javnih ključev (enkripcija).
- **Masquerade napad (angl. *masquerade attack*)**: certifikati, ki so izdani na podlagi infrastrukture javnih ključev (angl. *public key infrastructure*), so zlorabljeni na način, da predstavljajo neko drugo entiteto (primer: sporočilo, ki bi moralo biti poslano s strani Janeza, je v bistvu poslano s strani Jožeta.). V tem primeru je pomembno, da ob zaznani grožnji prekličemo certifikat.

9 *Emile Durkheim ugotavlja, da je odklonskost univerzalno družbeno dejstvo in normalen družbeni pojav, ki se pojavlja v vseh družbah in v kateremkoli času (Haralambos in Holborn, 2004).*

10 *Napredno analitično orodje, ki je bilo razvito z namenom predvidevanja sodb in sodnih stroškov v primeru sodnih postopkov zoper intelektualno lastnino (Završnik, 2017).*

11 *Nekatere besede so ohranjene v izvirniku, torej v angleškem jeziku, ker v Sloveniji še ni enakovrednih sopomenk.*

- **Ponavljajoči se napadi (angl. *replay attack*)**: zlonamerne entitete kontinuirano pošiljajo podatke za pridobitev dostopa do sistema. Rešitev je v pomnjenju podatkov o dostopu na podlagi preteklih sporočil in primerjava z novimi.
- **MitM napad (angl. *man-in-the-middle attack*)**: Gre za napad s posrednikom, kjer napadalec prestreza, beleži in spreminja podatke o šifriranem prometu med dvema entitetama, kjer ti dve entiteti mislita, da imata neposredno komunikacijo in ne posumita, da je vmes neki tretji člen. Te težave je mogoče rešiti z različnimi kriptirnimi algoritmi.
- **Sybil napad (angl. *sybil attack*)**: Imitacija več identitet, ki jih napadalec izkorišča za manipulacijo ocene ugleda, kar omogoča izkoriščanje in goljufanje drugih uporabnikov. Tudi v tem primeru se za zaščito pred tovrstnimi napadi uporablja infrastruktura javnih ključev, ki dodeli identiteto entitetam (digitalni podpis), kar identitetam daje legitimnost in unikatnost.
- **Lažno lociranje (angl. *GPS spoofing*)**: V tem primeru so ranljivi avtomobili, ker gre za lažno predstavljanje geolokacijskih podatkov; avtomobil, ki je na točki A, se bo predstavil kot da deluje na točki B, kar lahko vodi do nesreč. Te nepravilnosti je mogoče odpraviti s tehničnimi rešitvami, ki zaznajo vsako nenormalno odstopanje oz. nihanje geolokacijskih podatkov.
- **Ponarejanje sporočil (angl. *broadcast tampering*)**: V sistem avtomobila apliciramo lažne podatke, spremenimo lahko npr. parametre o vzmetenju, izklopimo ABS itd. V tem primeru za zaščito uporabljamo avtentikacijo ter digitalna potrdila, ki onemogočijo tovrstne napade. Četudi napadalec vstopi v sistem preko digitalnega potrdila, nas še vedno varuje CRL[12] (*Certificate Revocation List*).
- **Prisluškovanje in analiza pretoka podatkov (angl. *eavesdropping and traffic analysis*)**: Gre za tipično ogrožanje zasebnosti v pametnih mestih, pri čemer že zadostujejo enkripcija ter ostale kriptirne rešitve.
- **DoS napadi (angl. *DOS attack*)**: Zaradi obremenjenosti sistema z veliko količino podatkov ta ne more več učinkovito delovati. DoS napade je težko preprečiti zaradi same infrastrukture omrežja.
- **Zlonamerna programska oprema (angl. *malware*)**: Gre za napade z različno škodljivo programsko opremo, kot so virusi, črvi, trojanski konji itd. Za preprečevanje tovrstnih napadov veliko naredimo z znanjem informacijske varnosti in s previdnostjo. Tehnične rešitve pa so predvsem uporaba antivirusnih programov ter posodabljanje sistema.
- **Napad z grobo silo (angl. *brute force*)**: Napadalci poskušajo s pomočjo različnih ključev (gesel) priti do avtoriziranega dostopa v sistem. NIST[13] v svojih smernicah predlaga uporabo kriptirnih algoritmov ter robustna in varna gesla.
- **Napadi na čas (angl. *timing attack*)**: »Timing« napadi v sodobnem svetu predstavljajo velik izziv. Gre za časovno kritične aplikacije, ki omogočajo

12 *Po besedah Lueksa et al. (2017) je CRL črni seznam, ki vsebuje niz preklicanih digitalnih potrdil, kar omogoča sistemu, da preveri, ali ima neka oseba kljub digitalnemu potrdilu vstop v sistem.*

13 *National Institute of Standards and Technology.*

zgodnje opozarjanje na katastrofo. Napad na te aplikacije se izvrši na način, da nam aplikacija grozečo katastrofo javi z zamikom. Rešitve so v časovnih žigih in v ECDSA[14] algoritmu.

- **(angl. *conflict collision*)**: Ranljive so predvsem RFID[15] naprave, ki so v tem primeru nesposobne pravilno prebrati in obdelati zbrane podatke (RFID bralnik prebere eno kodo, kljub temu, da sprejme dve).
- **Varnost vozlišč (angl. *node security*)**: Za zagotavljanje varnosti in zasebnosti IOT senzorjev je treba zagotoviti varnost ter zanesljivost vozlišč in komunikacij.
- **Napadi na naprave z omejenimi kapacitetami (angl. *security attacks on devices with limited computational and storage resources*)**: Brezžična senzorska omrežja so sestavni del IOT infrastrukture, kar pomeni, da so tudi sestavni del pametnih mest.

Gharaibeh et al. (2017) v 15 sklopih predstavljajo grožnje zasebnosti v pametnih mestih predvsem s tehnološkega vidika. V naši raziskavi smo se osredotočili na vedenje, poznavanje in obnašanje posameznika v povezavi z zagotavljanjem in varovanjem zasebnosti, ker je pomembno, da se ljudje v prvi vrsti zavedajo groženj zasebnosti. Tehnološke rešitve ne pomagajo veliko, če posameznik sam ni pripravljen delovati samovarovalno (npr. povezovanje v nezaščitena brezžična omrežja kljub temu, da imamo možnost uporabe brezžičnega omrežja, zaščitenega z avtentikacijo), tako lahko rečemo, da nam nič ne pomaga, če imamo zelo varne tehnološke naprave v pametnih mestih, če pa jih ne znamo pravilno uporabljati.

3 UPORABLJENE METODE

3.1 Opis instrumentarija

S pomočjo odprtokodne aplikacije za spletno anketiranje (www.1ka.si) smo sestavili vprašalnik, ki je bil dostopen od 14. 8. 2017 do 14. 9. 2017. Na spletni vprašalnik je v tem času odgovorilo nekaj več kot 300 posameznikov, vendar jih je od tega v celoti končalo anketo 197, zato smo druge (132 nepopolno izpolnjenih vprašalnikov) izločili. Cilji raziskave so bili pridobiti informacije o poznavanju koncepta pametnih mest ter kakšen je odnos posameznikov do zasebnosti v pametnih mestih. Sodelovanje v anketi je bilo prostovoljno in anonimno. Podatke, ki smo jih pridobili s pomočjo spletne ankete, smo statistično obdelali in analizirali s pomočjo programa SPSS (*Statistical Package for Social Sciences*).

Vprašalnik, s katerim so posamezniki s pomočjo sedemstopenjske Likertove lestvice ocenjevali poznavanje koncepta zasebnosti v pametnih mestih, je obsegal 20 spremenljivk. Anketiranci so na lestvici od 1 do 7 (1 – sploh se ne strinjam, 2 – se ne strinjam, 3 – delno se ne strinjam, 4 – niti/niti, 5 – delno se strinjam, 6 – se strinjam, 7 – se popolnoma strinjam) opredelili, v kolikšni meri se strinjajo z določenimi trditvami o pametnih mestih. Drugi del vprašalnika se je nanašal na demografijo anketirancev.

Kaiser-Meyer-Olkinova mera primernosti vzorca (KMO) v našem primeru znaša 0,817, kar pomeni, da so podatki ustrezni za izvedbo faktorske analize.

14 *Eliptic Curve Digital Signature Algorithm.*

15 *Radio Frequency IDentification*

Na podlagi Bartlettovega testa pa lahko zavrnemo tudi ničelno hipotezo, ker znaša vrednost 0,000, kar pomeni, da je ustreznost vzorca optimalna in da korelacijska matrika ni enotska (Šifrer in Bren, 2011). Preverili smo tudi asimetrijo in sploščenost: vrednosti Skewness in Kurtosis znašata v našem primeru med –3 in 3, kar po besedah Šifrer in Bren (2011) pomeni, da so podatki porazdeljeni normalno in ni treba izločiti nobene spremenljivke.

3.2 Opis vzorca

Tabela 1: Izobrazba sodelujočih v anketi

Odgovori	*N*	%
Osnovna šola	1	1
Srednja šola	114	58
Višješolski program	8	4
Visokošolski program	25	12
Univerzitetni program	39	19
Magisterij	10	5

Spletna anketa je bila opravljena po principu snežne kepe (ljudi smo povabili k raziskavi preko družabnega omrežja Facebook). V raziskavi je sodelovalo 197 anketirancev, od tega 99 moških in 98 žensk. Tabela 1 prikazuje, da je največ anketirancev dokončalo srednjo šolo (58 odstotkov), 19 odstotkov jih je imelo dokončan univerzitetni študijski program, 12 odstotkov pa visokošolski študijski program. Nadalje jim sledijo anketiranci z dokončanim magisterijem (5 odstotkov) ter anketiranci z dokončanim višješolskim programom (4 odstotki), le en anketiranec pa je imel dokončano osnovno šolo. Anketirancev z dokončanim doktoratom v tej raziskavi ni bilo.

120 anketirancev (61 odstotkov) je prihajalo iz vzhodne kohezijske regije in 77 anketirancev (37 odstotkov) iz zahodne kohezijske regije.

Tabela 2: Starostna skupina

Odgovori	*N*	%
do 20 let	16	8
21–40 let	178	90
41–60 let	3	2

Tabela 2 prikazuje, da je bilo največ anketirancev v času raziskave starih med 21 in 40 let (90 odstotkov), sledijo jim anketiranci s starostjo do 20 let (8 odstotkov). Najmanj odgovorov smo prejeli od anketirancev, ki so bili v času raziskave stari med 41 in 60 let (2 odstotka).

4 PREDSTAVITEV IN INTERPRETACIJA REZULTATOV RAZISKAVE

V nadaljevanju predstavljamo ugotovitve naše raziskave glede opredelitve anketirancev do zasebnosti v pametnih mestih. Mnenje ljudi glede zasebnosti v pametnih mestih je ključnega pomena, kajti ljudje so tisti, ki morajo tehnologijo sprejeti, in ljudje so tisti, ki soustvarjajo kakovosten skupen življenjski prostor, kar nam pripomore k odločitvam o izboljšanju mesta. Na začetku analiziranja smo opravili faktorsko analizo z metodo glavnih komponent (tabela 3), s katero smo zmanjšali število spremenljivk (s pomočjo pravokotne rotacije Varimax z normalizacijo).

Prvi faktor, s katerim smo pojasnili 20 odstotkov skupne variance, smo poimenovali »Zakonodaja«. Drugi faktor, s katerim smo pojasnili 18,5 odstotkov skupne variance, smo poimenovali »Komoditeta«. Tretji faktor, s katerim smo pojasnili 7,5 odstotkov skupne variance, smo poimenovali »Poznavanje koncepta pametnih mest. Četrti faktor, s katerim smo pojasnili 6,4 odstotkov skupne variance, smo poimenovali »Računalniško znanje«. Peti faktor, s katerim smo pojasnili 5,3 odstotkov skupne variance, smo poimenovali »Grožnje zasebnosti«. Šesti faktor, s katerim smo pojasnili 5,1 odstotkov skupne variance pa smo poimenovali »Paradoks zasebnosti«.

Tabela 3: Rotirana faktorska matrika. Zmanjšanje števila spremenljivk.

Rotirana faktorska matrika[a]						
	Faktorji					
	1	2	3	4	5	6
Pomembno je, da sem s strani upravljavcev obveščen o kršitvi varstva osebnih podatkov, če se ti nanašajo name.	,873					
Pomembno mi je, da je pravica do zasebnosti opredeljena v Ustavi Republike Slovenije.	,844					
Pomembno mi je, da imam pravico do pozabe oz. izbrisa podatkov v pametnih mestih.	,779					
Pomembno mi je, da vem, kateri podatki se zbirajo o meni v pametnih mestih.	,754					
Pomembno mi je, da so podatki, ki so pridobljeni v pametnih mestih, upravljani s strani države in ne s strani zasebnih podjetij.	,556					
Zbiranje podatkov o moji lokaciji predstavlja zame poseg v zasebnost.	,521		-,358		,358	
Močno si želim, da bi bival v pametnem mestu.		,802				
Investiranje v pametna mesta je dobra naložba.		,772				
V zameno za sponzorsko majico sem pripravljen sprejeti splošne pogoje in si namestiti aplikacijo za pametna mesta.		,658				
Z veseljem bi uporabljal mobilne aplikacije, ki merijo stanje v mestu (temperatura, kvaliteta zraka, trenutno število ljudi, trenutno število ter vrsta avtomobilov, število turistov in iz katere države prihajajo itd.).		,553			-,309	
Moji osebni podatki v pametnih mestih bi bili popolnoma varni.		,502	,411			
Zelo dobro poznam koncept pametnih mest.		,464	-,459	,347	,387	
Dobrodošlo je, da imajo mesta čim več podatkov o meni.			,657			
Vseeno mi je, če bodo pametna mesta zbirala podatke o meni brez mojega dovoljenja.		,301	,657			
Želim si, da bi namesto policijskih patrulj uvedli drone, ki bi nadzirali stanje na ulicah v mestu.			,580			

Tabela 3: Nadaljevanje

Rotirana faktorska matrika[a]						
	Faktorji					
	1	2	3	4	5	6
Pametna mesta bi zahtevala ogromno računalniškega znanja.				,828		
Skrbi me, da bodo pametna mesta ogrožala mojo zasebnost.	,343			,568	,332	
Vsakič, ko naložim kako aplikacijo, preberem splošne pogoje.					,807	
V mestu se večkrat povežem v brezplačno WI-FI omrežje, ki ne zahteva gesla (nezaščiteno omrežje).						,806
Na družabnem omrežju (Facebook, Instagram, Twitter itd.) večkrat objavim fotografijo z lokacijo, kjer je bila posneta.						,629
Metoda ekstrakcije: Principal Component Analysis. Metoda rotacije: Varimax with Kaiser Normalization.						
a. Rotacija konvertirana v 8 iteracijah.						

S Cronbachovim koeficientom alfa (α) smo izračunali zanesljivost vprašalnika, kar v našem primeru znaša 0,724, kar pomeni, da je ta del vprašalnika srednje zanesljiv. Po besedah Šifrer in Bren (2011) lahko Cronbach alfa (α) zavzame vrednost med 0 in 1, pri čemer pomeni 0 popolno nezanesljivost in 1 popolno zanesljivost, medtem ko $\alpha > 0{,}8$ pomeni visoko zanesljivost in $0{,}6 < \alpha < 0{,}8$ srednjo zanesljivost. Skupna varianca vseh izločenih faktorjev pa je 62,8 odstotka. V nadaljevanju bomo predstavili rezultate opisne statistike po posameznih spremenljivkah, razvrščenih v posamezni faktor.

Tabela 4: Opisna statistika spremenljivk faktorja »Zakonodaja«

	Aritmetična sredina	**Standardni odklon**	**% Se strinjam (5+6+7)**
Pomembno je, da sem s strani upravljavcev obveščen o kršitvi varstva osebnih podatkov, če se ti nanašajo name.	6,4	1,06	96
Pomembno mi je, da je pravica do zasebnosti opredeljena v Ustavi Republike Slovenije.	6,3	1,20	93
Pomembno mi je, da vem, kateri podatki se zbirajo o meni v pametnih mestih.	6,1	1,45	88
Pomembno mi je, da imam pravico do pozabe oz. izbrisa podatkov v pametnih mestih.	6,0	1,28	90
Pomembno mi je, da so podatki, ki so pridobljeni v pametnih mestih, upravljani s strani države in ne s strani zasebnih podjetij.	5,2	1,62	69
Zbiranje podatkov o moji lokaciji predstavlja zame poseg v zasebnost.	5,5	1,57	80

Iz tabele 4 je razvidno, da je anketirancem najbolj pomembno, da so s strani upravljavcev obveščeni o kršitvi varstva osebnih podatkov, če se le-ti nanašajo na njih. Kar se tiče zakonodaje pa jim je najmanj pomembno, če so podatki upravljani

s strani države in ne s strani zasebnih podjetij. Na podlagi rezultatov, ki so prikazani, lahko rečemo, da bo nova Uredba o varstvu podatkov (Uredba (EU) 2016/679 Evropskega parlamenta in sveta o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES, 2016; v nadaljevanju Splošna uredba o varstvu podatkov, 2016) prinesla novosti, ki bo uporabnikom (v našem primeru prebivalcem) nudila večjo zaščito in varovanje zasebnosti. Pri faktorju »Zakonodaja« smo želeli izvedeti, kakšen je odnos ljudi do različnih pravnih okvirjev (vključujoč Splošno uredbo o varstvu podatkov).

Tabela 5: Opisna statistika spremenljivk faktorja »Komoditeta«

	Aritmetična sredina	Standardni odklon	% Se strinjam (5+6+7)
Močno si želim, da bi bival v pametnem mestu.	3,7	1,45	26
Investiranje v pametna mesta je dobra naložba.	4,6	1,44	59
V zameno za sponzorsko majico sem pripravljen sprejeti splošne pogoje in si namestiti aplikacijo za pametna mesta.	2,8	1,78	18
Z veseljem bi uporabljal mobilne aplikacije, ki merijo stanje v mestu (temperatura, kvaliteta zraka, trenutno število ljudi, trenutno število ter vrsta avtomobilov, število turistov in iz katere države prihajajo itd.).	4,6	1,77	61
Moji osebni podatki v pametnih mestih bi bili popolnoma varni.	3,1	1,48	19

Na podlagi tabele 5 lahko ugotovimo, da imajo anketiranci zelo pozitiven odnos do uporabe mobilnih aplikacij v zvezi s pametnimi mesti in bi jih z veseljem uporabljali, da bi dosegali večjo komoditeto oz. udobnost. Velika večina anketirancev pa kljub pripravljenosti do prenosa aplikacije ni pripravljena sprejeti splošnih pogojev aplikacije v zameno za sponzorsko majico. Faktor »Komoditeta« nam daje pregled nad tem, kakšno udobje lahko v pametnih mestih pričakujemo in kakšen odnos imajo anketiranci do osebnih podatkov.

Tabela 6: Opisna statistika spremenljivk faktorja »Poznavanje koncepta pametnih mest«

	Aritmetična sredina	Standardni odklon	% Se strinjam (5+6+7)
Zelo dobro poznam koncept pametnih mest.	3,5	1,64	30
Dobrodošlo je, da imajo mesta čim več podatkov o meni.	2,4	1,46	9
Vseeno mi je, če bodo pametna mesta zbirala podatke o meni brez mojega dovoljenja.	1,6	0,98	3
Želim si, da bi namesto policijskih patrulj uvedli drone, ki bi nadzirali stanje na ulicah v mestu.	2,6	1,69	19

Na podlagi tabele 6 lahko zaključimo, da anketirancem ni vseeno, če bodo pametna mesta zbirala podatke brez njihovega dovoljenja oz. privolitve. Večina anketirancev se ne strinja s trditvijo »Zelo dobro poznam koncept pametnih mest«. Faktor »Poznavanje koncepta pametnih mest« se nanaša na to, kako dobro ljudje poznavajo pametna mesta in kakšen odnos imajo do podatkov.

	Aritmetična sredina	Standardni odklon	% Se strinjam (5+6+7)
Pametna mesta bi zahtevala ogromno računalniškega znanja.	5,3	1,44	76

Tabela 7: Opisna statistika spremenljivk faktorja »Računalniško znanje«

Tabela 7 prikazuje, da večina anketirancev meni, da bodo pametna mesta zahtevala ogromno računalniškega znanja (programiranje, visoka računalniška pismenost, široko poznavanje informacijskih tehnologij itd.). Pri faktorju »Računalniško znanje« smo uporabili zgolj eno spremenljivko, ker koncept pametnih mest kot tak temelji na trajnostnem razvoju in za to ni potrebnega nobenega poznavanja računalništva.

	Aritmetična sredina	Standardni odklon	% Se strinjam (5+6+7)
Skrbi me, da bodo pametna mesta ogrožala mojo zasebnost.	4,6	1,56	59
Vsakič, ko naložim kako aplikacijo, preberem splošne pogoje.	2,6	1,68	17

Tabela 8: Opisna statistika spremenljivk faktorja »Grožnje zasebnosti«

Iz tabele 8 lahko razberemo, da bodo pametna mesta ogrožala zasebnost posameznika. Na drugi strani pa je le malo tistih, ki se dejansko vedejo »samovarovalno« in preberejo splošne pogoje pri namestitvi aplikacije. Faktor »Grožnje zasebnosti« prikazuje odnos anketirancev do zasebnosti in kako je lahko le ta ogrožena (strah pred ogroženo zasebnostjo in branje splošnih pogojev pri nalaganju aplikacije).

	Aritmetična sredina	Standardni odklon	% Se strinjam (5+6+7)
V mestu se večkrat povežem v brezplačno Wi-Fi omrežje, ki ne zahteva gesla (nezaščiteno omrežje).	4,3	1,99	56
Na družabnem omrežju (Facebook, Instagram, Twitter itd.) večkrat objavim fotografijo z lokacijo, kjer je bila posneta.	3,5	2,08	41

Tabela 9: Opisna statistika spremenljivk faktorja »Paradoks zasebnosti«

Iz tabele 9 lahko razberemo, da se velika večina anketirancev v mestu večkrat poveže v brezplačno Wi-Fi omrežje, ki ne zahteva gesla (nezaščiteno omrežje), kar je zopet pokazatelj, da se uporabniki ne zavedajo groženj informacijski tehnologiji v pametnih mestih. Znano je namreč, da so nezaščitena Wi-Fi omrežja zelo ranljiva za napade, kar lahko privede do posega v zasebnost, prestrezanja gesel, razkritja občutljivih informacij itd. Faktor »Paradoks zasebnosti« se nanaša na uporabo brezplačnega Wi-Fi omrežja v mestu in na objavljanje fotografij z lokacijo na družabnih omrežjih, s čimer lahko obrazložimo, da gre v tem primeru za ključen pojav, kjer se ljudje zavedajo groženj, pa vendarle niso pripravljeni veliko storiti za dosego večje stopnje zasebnosti.

Tabela 10: Poznate naslednje strani oz. projekte: ezavod.si, smartis.si, smartiscity.eu, smartcitymaribor.si

Poznate naslednje strani oz. projekte: ezavod.si, smartis.si, smartiscity.eu, smartcitymaribor.si?	**Frekvenca**	**Odstotek (%)**
(Da, vse)	2	1
(Da, vendar ne vseh naštetih)	52	25
(Ne)	145	69

Na podlagi tabele 10 ugotavljamo, da večina anketirancev še ne pozna koncepta pametnih mest, ki so jih zasnovala slovenska podjetja. 69 odstotkov anketirancev ne pozna omenjenih projektov, zgolj 1 odstotek anketirancev v celoti pozna projekte, 25 odstotkov anketirancev pa pozna le nekatere strani oz. projekte.

5 RAZPRAVA

Pametna mesta so pred našimi vrati. S pojavom novih tehnologij, vplivom globalizacije in organizacijskih rešitev, ki jih le-te ponujajo pa za sabo prinašajo tudi določen del tveganja. Zato je pomembno, da ravnamo v smeri zagotavljanja informacijske varnosti in ozaveščanja prebivalcev. V naši raziskavi smo ugotovili, da ljudje koncepta pametnih mest še ne poznajo. Na vprašanje: »*Poznate naslednje strani oz. projekte: ezavod.si, smartis.si, smartiscity.eu, smartcitymaribor.si*?« sta pritrdilno odgovorila le dva anketiranca, kar je na neki način skrb vzbujajoče. Zavedati se moramo, da danes dostopna tehnologija predstavlja tako prednosti kot slabosti. Prednosti so vsekakor v tem, da smo s pomočjo tehnologije povezani bolj kot prej in da imamo dostop do informacij praktično od koderkoli in od kjerkoli. Slabosti pa se kažejo predvsem v nepoučenosti uporabnikov, ki velikokrat ne razumejo, da je zagotavljanje zasebnosti in varovanje informacij izjemnega pomena. Tako lahko rečemo, da bomo poleg pametnih mest potrebovali tudi pametne ljudi, ki bodo delovali v smeri zagotavljanja varnosti informacij in v smeri varovanja zasebnosti.

Opisna statistika spremenljivk faktorja »Zakonodaja« predstavlja predvsem novosti, ki jih prinaša nova Splošna uredba o varstvu podatkov (2016). V naši raziskavi tako ugotavljamo, da bo ta prinesla mnogo pozitivnih sprememb, s katero naši anketiranci v veliki večini soglašajo (obvestilo o kršitvi varstva osebnih podatkov s strani upravljavcev, vedenje o tem, kateri podatki se zbirajo o nas, pravica do pozabe oz. izbrisa osebnih podatkov).

Velika večina anketirancev je s povprečno vrednostjo (5,3) prepričana, da bi pametna mesta zahtevala ogromno računalniškega znanja. Ta dognanja so sicer v nasprotju z Anthopoulosovimi (2017) tezami, v katerih pojasnjuje, da je v pametnih mestih veliko rešitev snovanih na podlagi organizacijskih reštev, ki nimajo nič opraviti s tehnologijo. Zato je pomembno, da ljudi izobražujemo tako v smeri računalniške pismenosti kot tudi v smeri ozaveščanja o samih konceptih pametnih mest in kaj le-ti prinašajo za slehernega posameznika. Zanimiva je tudi ugotovitev, da bi lahko v pametnih mestih prišlo do pojava paradoksa zasebnosti, kar pomeni, da ljudje kljub zavedanju groženj ne bodo delovali samozaščitno in bodo s tem posledično sprejeli tveganja, kar lahko vodi do »oškodovanja«

zasebnosti. Tako smo pri opisni statistiki spremenljivk faktorja »Paradoks zasebnosti« ugotovili, da se ljudje v veliki večini povezujejo v nezaščitena Wi-Fi omrežja, torej tista, ki ne zahtevajo vnosa gesla za dostop do omrežja, kar je veliko varnostno tveganje za prestrezanje podatkov in prisluškovanje. Manjši delež anketirancev pa tudi večkrat objavi fotografijo z lokacijo, kjer je le-ta bila posneta. Ob tem se seveda pojavlja vprašanje, ali se anketiranci sploh zavedajo kakšne podatke, na podlagi prostovoljne privolitve (samovoljno objavljanje lokacije), dajejo na vpogled ostalim uporabnikom različnih družabnih omrežij. Objavljanje fotografij z lokacijo je seveda zaželjeno in nesporno, če se želimo pohvaliti prijateljem in ostalim deležnikom na družabnih omrežjih, vendar pa ne smemo pozabiti na to, da gre vendarle za razkrivanje zasebnosti. Še bolj sofisticiran način za razkrivanje osebnih podatkov in s tem posledično zasebnosti je zbiranje podatkov o lokaciji brez naše privolitve. Lahko bi rekli, da gre za zlorabo. Na podlagi tega ugotavljamo, da bodo družabna omrežja odigrala pomembno vlogo pri načrtovanju pametnih mest. Brandt, Bendler in Neumann (2016) so v študiji, ki so jo izvedli na področju San Francisca, s pomočjo analitike družabnih omrežij (Twitter) natančno oblikovali vzorce in vozlišča lokacij, od koder ljudje najpogosteje tvitajo. Ti podatki pa odločevalcem (upravljavcem) v mestu pripomorejo k analizi najboljših lokacij z največjo gostoto turizma. Na teh stičiščih se lahko postavijo razne trgovine in ostale potrošniške institucije, ki omogočajo dodaten dotok financ in boljšo rabo prostora ter bolj učinkovito načrtovanje novih urbanih rešitev. Na podlagi pametnih mest so se tako začeli oblikovati novi termini, kot so: pametni turizem, pametni ekosistemi, pametno upravljanje itd.

Dne 25. 5. 2018 se bo začela uporabljati[16] nova Splošna uredba o varstvu podatkov (2016), ki bo povzročila spremembo nacionalne zakonodaje o varstvu osebnih podatkov in bo imela velik vpliv na upravljanje z zasebnostjo tudi v pametnih mestih. Novost, ki jo prinaša, je med drugim tudi ureditev privolitve za obdelavo osebnih podatkov (prostovoljna, izražena z jasnim pritrdilnim dejanjem in izraža nedvoumno soglasje k obdelavi). Zakonito in izrecno določen mora biti tudi namen zbiranja oz. obdelovanja osebnih podatkov. Pri tem bo pomembno, kako bodo načrtovalci pametnih mest vključili razno tehnologijo in ostale rešitve, da bodo skladne s Splošno uredbo o varstvu osebnih podatkov. Rezultati analize zajemajo mnenja večine mlade populacije, zato bi bilo raziskavo smiselno izvesti tudi na starejših prebivalcih, ki niso odraščali s pametno tehnologijo in imajo verjetno drugačen odnos do »novih stvari«.

6 ZAKLJUČEK

Lopez, Rios, Bao in Wang (2017) navajajo, da je zasebnost del informacijske varnosti in kot taka služi za širše poznavanje varnostne problematike. Avtorji tudi navajajo, da je ravno zasebnost tisti ključni člen, ki mora biti v pametnih mestih najbolj varovana, ker je zaradi zbiranja in obdelave podatkov najbolj ranljiva. Zasebnost pa je ranljiva zato, ker so senzorji in računalniki »pomanjšani« do te mere, da jih naše oko več ne zazna oz. so skriti, kar je težava, saj niti ne vemo, od

16 *Sicer je Splošna uredba o varstvu osebnih podatkov (2016) stopila v veljavo že 24. 5. 2017.*

koga in kje smo opazovani, kaj šele, da vemo, kdo obdeluje te zbrane podatke. Po mnenju anketirancev je najbolj primerno, da podatke, ki so zbrani v pametnih mestih, upravlja država, kar je na neki način logično, saj s tem zagotovimo določeno stopnjo pravne varnosti in nadzor nad podatki ter zmanjšamo tveganje za prevlado kapitalskih interesov (trgovanje z informacijami – zlorabe). Vsekakor pa bo k zaščiti posameznika in njegove zasebnosti pripomogla Splošna uredba o varstvu podatkov (2016), ki se bo začela uporabljati 25. 5. 2018.

Strnemo torej lahko, da sta človek in njegova zasebnost tisti glavni komponenti, ki jih moramo varovati in imeti v mislih, ko načrtujemo pametna mesta. To pa lahko storimo s kakovostnimi programskimi rešitvami in z vključevanjem različnih strokovnjakov.

Članek zaključujemo z razlago naslova »Zasebnost v pametnih mestih ali zasebnost za pametne ljudi?«, ki se ne nanaša toliko na pojasnitev urbanistične problematike, temveč nakazuje na to, da bomo za zagotovitev zasebnosti v pametnih mestih potrebovali predvsem pametne ljudi, ki bodo željni zasebnosti in bodo za to pripravljeni tudi nekaj narediti (največ pa lahko storimo sami).

UPORABLJENI VIRI

Anthopoulos, L. (2017). Smart utopia VS smart reality: Learning by experience from 10 smart city cases. *Cities*, 63, 128–148. http://dx.doi.org/10.1016/j.cities.2016.10.005

Beretta, I. (2018). The social eff ects of eco-innovations in Italian smart cities. *Cities, 72*, 115–121. http://dx.doi.org/10.1016/j.cities.2017.07.010

Bernik, I. in Meško, G. (2011). Internet study of familiarity with cyber threats and fear of cybercrime. *Revija za kriminalistiko in kriminologijo*, *62*(3), 242–252.

Brandt, T., Bendler, J. in Neumann, D. (2016). Social media analytics and value creation in urban smart tourism ecosystems. *Information and Management*. http://dx.doi.org/10.1016/j.im.2017.01.004

Chan, J., Bateman, L. in Olafsson, G. (2016). A people & purpose approach to humanitarian data information security and privacy. *Procedia Engineering*, *159*, 3–5. https://doi.org/10.1016/j.proeng.2016.08.056

Elmaghraby, A. S. in Losavio, M. M. (2014). Cyber security challenges in smart cities: Safety, security and privacy. *Journal of Advanced Research*, *5*(4), 491–497. http://doi.org/10.1016/j.jare.2014.02.006

Gharaibeh, A., Salahuddin, M. A., Hussini, S. J., Khreishah, A., Khalil, I., Guizani, M. in Al-Fuqaha, A. (2017). Smart cities: A survey on data management, security and enabling technologies. *IEEE Communications Surveys & Tutorials, 19*(4), 2456–2501. http://doi.org/10.1109/COMST.2017.2736886

Haralambos, M. in Holborn, M. (2004). *Sociology: Themes and perspectives*. London: Harper Collins Publishers.

Kanduč, Z., Mihelj Plesničar, M., Kmet, S., Petrovec, D., Završnik, A. in Zgaga, S. (2012). *Nežnejši spol? : ženske, nasilje in kazenskopravni sistem.* Ljubljana: Inštitut za kriminologijo pri Pravni fakulteti. Pridobljeno na http://dirros.openscience.si/IzpisGradiva.php?lang=slv&id=871

Kim, T., Ramos, C. in Mohammed, S. (2017). Smart city and IoT. *Future Generation Computer Systems*, *76*, 159–162. http://doi.org/10.1016/j.future.2017.03.034

Lefèvre, T. (v tisku). Big data in forensic science and medicine. *Journal of Forensic and Legal Medicine*. http://doi.org/10.1016/j.jflm.2017.08.001

Lopez, J., Rios, R., Bao, F. in Wang, G. (2017). Evolving privacy: From sensors to the Internet of Things. *Future Generation Computer Systems*, *75*, 46–57. https://doi.org/10.1016/j.future.2017.04.045

Lueks, W., Alpár, G., Hoepman, J. H. in Vullers, P. (2017). Fast revocation of attribute-based credentials for both users and verifiers. *Computers and Security*, *67*, 308–323. http://doi.org/10.1016/j.cose.2016.11.018

Markelj, B. in Zgaga, S. (2016). Comprehension of cyber threats and their consequences in Slovenia. *Computer Law and Security Review, 32*(3), 513–525. http://doi.org/10.1016/j.clsr.2016.01.006

Rajkumar, R., Lee, I., Sha, L. in Stankovic, J. (2010). Cyber-physical systems: The next computing revolution. V *DAC '10, Proceedings of the 47th Design Automation Conference* (str. 731–736). New York: ACM New York. https://doi.org/10.1145/1837274.1837461

Resolucija o strategiji nacionalne varnosti Republike Slovenije (ReSNV-1). (2010). *Uradni list RS,* (27/10).

Sotlar, A. in Tominc, B. (2012). Zaznava deklarativnih virov ogrožanja nacionalne varnosti v slovenski družbi. *Varstvoslovje, 14*(3), 231–258.

Sotlar, A. in Trivunović, J. (2012). Detektivi in varstvo zasebnosti v Republiki Sloveniji. *Varstvoslovje*, *14*(3), 307–330.

Šifrer, J. in Bren, M. (2011). *SPSS – multivariatne metode v varstvoslovju*. Ljubljana: Fakulteta za varnostne vede.

Uredba (EU) 2016/679 Evropskega parlamenta in sveta o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES (Splošna uredba o varstvu podatkov). (2016). *Uradni list Evropske Unije*, (L 119/1).

Ustava Republike Slovenije [Ustava RS]. (1991,1997, 2000, 2003, 2004, 2006, 2013, 2016). *Uradni list RS*, (33/91-I, 42/97, 66/00, 24/03, 69/04, 69/04, 69/04, 68/0647/13, 47/13, 75/16).

van den Besselaar, P. (2005). The life and death of the great Amsterdam digital city. V P. van den Besselaar in S. Koizumi (ur.), *Digital Cities: III. information technologies for social capital: Cross-cultural perspectives*, (str. 66–96). Berlin: Springer. http://doi.org/10.1007/11407546_4

van Zoonen, L. (2016). Privacy concerns in smart cities. *Government Information Quarterly*, *33*(3), 472–480. http://doi.org/10.1016/j.giq.2016.06.004

Weber, R. H. (2015). The digital future – A challenge for privacy? *Computer Law and Security Review*, *31*(2), 234–242. http://doi.org/10.1016/j.clsr.2015.01.003

Williams, T. L. (2017). *A longitudinal study of privacy awareness in the digital age and the influence of knowledge* (Doktorska disertacija). Little Rock: University of Arkansas.

Završnik, A. (2010). Tehnično nadzorovanje vsakodnevnega življenja – postdisciplinske teoretične perspektive. *Revija za kriminalistiko in kriminologijo, 61*(2), 178–190.

Završnik, A. (2017). *Big data, crime and social control*. Abingdon: Routledge.

Završnik, A. in Levičnik, P. (2014). Zasebnost po Snowdnu: Novejša pojmovanja zasebnosti in odnos javnosti do le-te v Sloveniji. *Zbornik znanstvenih razprav*, *74*(1), 117–152.

Ziegeldorf, H. J., Morchon, G. O. in Wehrle, K. (2014). Security enhancement of authenticated RFID generation. *Security and communication networks*, *7*(12), 2728–2742. http://doi.org/10.1002/sec

O avtorjih:

Damjan Fujs, diplomirani varstvoslovec informacijske varnosti, študent magistrskega študijskega programa Varstvoslovje na Fakulteti za varnostne vede Univerze v Mariboru. E-pošta: damjan.fujs@student.um.si

Dr. Blaž Markelj, docent za področje informacijske varnosti na Fakulteti za varnostne vede Univerze v Mariboru. E-pošta: blaz.markelj@fvv.uni-mb.si