Univerza v Ljubljani

Pravna fakulteta

OSEBNI PODATKI V PAMETNIH MESTIH

(magistrsko diplomsko delo)

Avtorica: Katarina Rojc

Mentor: Prof. dr. Aleš Završnik

ZAHVALA

Za pomoč in nasvete pri nastajanju magistrskega diplomskega dela se iskreno zahvaljujem mentorju prof. dr. Alešu Završniku.

Hvala družini in mojim najbližjim, ki so mi ves čas študija stali ob strani in verjeli vame. Hvala fantu Eriku za potrpežljivost in motivacijo ter prijateljicam za spodbudo, podporo in pomoč.

KAZALO

POVZETEK

Informacije so najbolj dragocena surovina današnjega časa. Tega se zavedajo tudi snovalci mest. Od informacij, ki bi jih pridobili s pomočjo mestne infrastrukture si obetajo izboljšati kakovost življenja in energijsko učinkovitost mest. Pri pametnem mestu gre za sistematično uporabo informacijske in komunikacijske tehnologije (IKT) z namenom ekološkega in družbenega napredka. Ker takšna uporaba IKT močno posega v zasebnost posameznika se naloga opredeli do posameznih digitalnih pravic in predlaga možne načine, ki bi uporabniku zagotovili večjo stopnjo zasebnosti. Pri tem glavno vlogo zavzamejo izobraževalne dejavnosti ter postopki anonimizacije in psevdonimizacije podatkov. V osrednjem delu naloga predstavi nacionalno in evropsko zakonodajo na področju varstva osebnih podatkov. Ker zbiranje podatkov v pametnih mestih v večjem delu poteka preko povezanih naprav, se osredotoča na zakonske rešitve, ki zadevajo: privolitev uporabnika v zbiranje podatkov, postopek obdelave podatkov, transparentnost postopka ter zahtevo po najmanjšem obsegu zbranih podatkov, glede na namen zbiranja. Obenem ponudi tudi alternativne rešitve zagotavljanja zasebnosti, kot je načelo vgrajene zasebnosti in lepljiva zasebnost. Zadnji del naloge predstavlja vlogo ter način dela organov pregona kaznivih dejanj pri sistematični uporabi IKT v pametnih mestih. Sklepno ugotavlja, da je Evropska unija s sprejetjem Splošne uredbe o varstvu osebnih podatkov določneje uredila privolitev in posameznikom zagotovila dodatne digitalne pravice, a bo zaradi razvoja IKT potrebno razmišljati o novih pristopih pri dajanju privolitve in določanju meja zasebnosti.

Ključne besede: osebni podatek, pametno mesto, veliko podatkovje, internet stvari, informirana privolitev, obdelava podatkov, masovni nadzor, načelo vgrajene zasebnosti, psevdonimizacija, anonimizacija

ABSTRACT

The fact that information is the most valuable commodity is very important to urban planners. They anticipate great results from information collected through the city infrastructure to ensure a better life quality and energetic sustainability of the cities. Smart cities systematically take use of the information and communications technology (ICT) with the purpose of social and ecological progress. Due to the significant affect of the ICT on the privacy of an individual this thesis focuses mostly on identifying the digital rights of an individual and proposes possible ways to ensure a higher standard of privacy for the users. Educational activities and the procedure of anonymisation and pseudonimisation have the main role in this process. In the main part of this work the national and European legislation in the field of data protection are presented. As data collecting in Smart cities is mostly through smart devices, the focus is on legal solutions that concern the consent of the user in collecting data, processing data, transparency of the process and data minimization. Alternative solutions to provide privacy, such as Privacy by design and Sticky policy, are presented. The final part of the work presents the role and working methods of law enforcement for systematically using ICT in Smart cities. In conclusion, with passing the General Data Protection Regulation, the European Union began to specifically regulate the institution of consent and gave more digital rights to individuals. However, with the development of ICT it will be necessary to think about new approaches in giving consent and setting the boundary for privacy.

Kay words: personal data, Smart city, Big data, Internet of things, informed consent, data processing, mass surveillance, Privacy by design, anonymization, pseudonimization

1. UVOD

Varne mestne četrti. Dobre šole. Dostopna stanovanja. Tekoči promet. Vse to je možno!

S tem sloganom IBM na francoski spletni strani oglašuje posebno mrežno rešitev za pametna mesta.

S takšnimi obljubami nastopajo veliki koncerni v tej smeri. V zadnjih letih je koncept pametnega mesta pridobil pomen na skoraj vseh kontinentih. Vsako leto po celem svetu nastanejo projekti, ki nosijo nalepko »Smart City«.

Digitalna revolucija se razprostira na vse sektorje našega gospodarstva (vključno z javnim sektorjem) in s tem tudi na upravljanje z mesti. Trenutno živi v mestih 51,6 % svetovnega prebivalstva, napovedujejo pa, da naj bi se ta številka povzpela na 66,4 % do leta 2050.[1]

Urbanizacija predstavlja trend današnjega časa, s seboj pa prinaša številne težave, s katerimi se soočajo načrtovalci mest, tako se v gosto poseljenih mestih soočajo s težavami zagotavljanja dostopa do osnovne infrastrukture. Cilj oblikovalcev pametnih mest je zagotoviti trajnostni razvoj mest s pomočjo informacijskih in komunikacijskih tehnologij. Prav informacijska tehnologija načrtovalcem mest omogoča vzpostavitev pametnih rešitev na obstoječi infrastrukturi. Narediti pametno mesto iz nič, kjer so urbanisti postavljeni v vlogo bogov, ne predstavlja težave, saj niso omejeni z že obstoječimi strukturami. Primer takšnega pametnega mesta, ki je bilo ustvarjeno iz nič, je Lavasa[2], prvo indijsko zasebno načrtovano mesto, ki ga gradijo v bližini Pune, ki slogovno temelji na italijanskem mestu Portofino ter ima vse karakteristike pametnega mesta.

Čeprav pametna mesta v zvezi z načrtovanjem in možnostjo participacije obetajo zelo veliko, koncept s seboj prinaša kar nekaj nevarnosti. Naloge, ki pripadajo javnemu sektorju, v pametnih mestih padejo v roke zasebnikov. Tehnologija pametnih mest po večini izvira iz velikih koncernov IBM, Siemens in Cisco, ki bi skozi mrežno prepletenost mest prišli do ogromnih količin podatkov. Varnost podatkov je negotova. Mesto in njegova infrastruktura že

[1] F. Miller, B. Niesing, Die Zukunft der Stadt, v: Fraunhofer Magazin, 4(2012), str. 9.
[2] M. Kennart, C. Provost, Inside Lavasa, v: The guardian, (19.11.2015), URL: https://www.theguardian.com/cities/2015/nov/19/inside-lavasa-indian-city-built-private-corporation, (12.8.2016)

sama po sebi tvorita najkompleksnejšo strukturo, ki jo je človek kadarkoli ustvaril. Če si zamislimo, da ta infrastruktura postane prepletena z enako kompleksnimi informacijskimi obdelovalnimi procesi, to pripelje do raznovrstnih možnosti za napake in nepredvidljive učinke zamenjave.

Prav zaradi hitrega tehnološkega razvoja in globalizacije je na področju varstva osebnih podatkov prišlo do novih izzivov. Obseg zbiranja in izmenjave osebnih podatkov se je bistveno povečal. Tehnologija zasebnim podjetjem in javnim organom omogoča, da osebne podatke uporabljajo za dosego svojih ciljev v obsegu, kakršnega še ni bilo, pri čemer posamezniki svoje osebne podatke posredujejo preko različnih komunikacijskih tokov. Tehnologija je spremenila tako gospodarsko kot družbeno življenje. Za zagotovitev sožitja med interesi posameznikov in interesi gospodarstva bo treba sprejeti soglasje, ki bo vsem interesom omogočilo sobivanje.

Struktura magistrskega diplomskega dela je sestavljena tako, da najprej predstavi pomen pametnega mesta, saj do danes ne obstaja enotna definicija pametnega mesta, obstajajo pa posamične značilnosti, ki so prepoznavne v vsakem pametnem mestu. Splošnemu opisu pametnega mesta sledi ključni del magistrskega dela. Začne se s širšim pogledom na nadzor in pravico do zasebnosti, kjer predstavim idejo o pametni zasebnosti, ki bi ustrezala zahtevam pametnega mesta. V četrtem in petem poglavju obravnavam ključne pravne podlage na področju varstva osebnih podatkov, tako na nacionalni kot na evropski ravni, pri tem pa se osredotočam na oddelke v zakonu, ki so najbolj pomembni za posameznika, ki se sooča z dejavniki pametnega mesta. Kako zbrani osebni podatki pomagajo organom pregona pri odkrivanju kaznivih dejanj in predvidevanju nastanka kaznivega dejanja, je predstavljeno v šestem poglavju, kjer se tudi s pomočjo dveh sodb Evropskega sodišča za človekove pravice opredelim do masovnega zbiranja osebnih podatkov v pametnih mestih.

2. Pojem pametno mesto

2.1 Razvoj in definicija pametnega mesta

Pojem pametnega mesta (ang. Smart city) se je razvil v sredini devetdesetih let, v tem času je bila v ospredju predvsem vloga informacijske in komunikacijske tehnologije (v nadaljevanju: IKT). Izhodiščna ideja je temeljila na predpostavki, da učinkovitost mest ne temelji le na »trdi« infrastrukturi, temveč tudi na razpoložljivosti in kvaliteti komunikacijske in socialne infrastrukture. Pomemben predmet takratne diskusije je bila predvsem tematika e-uprave, ki poudarja večjo vključenost državljanov v postopek odločanja s pomočjo informacijskih tehnologij.[3] Pojem pametno mesto se dinamično razvija. V literaturi se koncept pametno mesto velikokrat povezuje s pojmi, kot so: znanje (ang. knowledge), digitalno (ang. digital), kibernetsko (ang. cyber), ekološko mesto (ang. Eco-City) ali zeleno mesto (ang. Green City).

»Z izrazom pametna mesta, v povezavi z IKT, označujemo mesta in družbene skupnosti oziroma zaokrožena življenjska okolja, ki z uporabo informacijskih tehnologij dosegajo večjo učinkovitost rabe virov, omogočajo boljše počutje in višjo kakovost bivanja, zmanjšujejo stroške ter se aktivno odzivajo na potrebe prebivalcev, obiskovalcev, širše skupnosti, javnih služb in podjetij. Rešitve pametnih mest in skupnosti temeljijo na soodvisnosti okolja, infrastrukture in družbe. Soodvisnost različnih podsistemov in pozitivni učinki integriranega pristopa se kažejo na raznih področjih, od prometa in logistike, učinkovite rabe energije, varnosti, poslovnega in industrijskega okolja, pa vse do javnih storitev, osebnega počutja in zdravja.«[4]

Raziskava za evropsko iniciativo pametnih mest (ang. European Smart Cities Initiative),[5] ki je bila opravljena na pobudo Strateškega energijskega tehnološkega plana (ang. SET-Plan), je poimenovala tri značilnosti, ki opredeljujejo pametno mesto:

- okolju prijazen pristop,

[3] A.Coe, G.Paquet, J. Roy, E-governance and smart communities: a social learning challenge, v: Social Science Computer Review, 19 (2001), str. 80–93.
[4] M. Mohorčič, A. Robnik, D. Baškovič, Delavnica«Pametna mesta in skupnost kot razvojna priložnost Slovenije«, v: Zbornik 18. mednarodne multikonference Informacijska družba, H (2015), str. 3.
[5] E. de Oliveria Fernandes, Smart City Initiative: How to Foster a Quick Transition Towards Local Sustainable Energy Systems, v: THINK, (2011), dostopno na: http://think.eui.eu

- uporaba informacijske in komunikacijske tehnologije kot ključ do pametnega upravljanja,
- trajnostni razvoj kot končni cilj.

Evropska iniciativa pametnih mest se osredotoča na energetske sisteme mest. Pametno mesto definirajo kot mesto, ki izboljšuje kvaliteto življenja in lokalne ekonomije s ciljem preiti v nizko-ogljično prihodnost. Investicije v energetsko učinkovitost in lokalno obnovljivo energijo z dosledno redukcijo uporabe fosilnih goriv in CO_2 emisij razumejo kot ključ za dosego trajnostnega in kvalitetnega življenja v mestu.

Kot perspektivno pametno mesto je obravnavano mesto, ki se loti inovativnih ukrepov na področju energijskih potreb, s ciljem izpolniti zahteve, opredeljene v EU 2020. V primeru te definicije se pojem »smart« enači s pojmi nizko-ogljično in trajnostno mesto.

2.1.2 Predlog definicije pametnega mesta

Na podlagi opisanih značilnosti, ki izkazujejo pametna mesta, bi le-to lahko definirali kot mesto, v katerem se sistematično uporablja informacijska in komunikacijska tehnologija kot tudi tehnologija za varovanje virov z namenom prehoda v postfosilno družbo, zmanjšanja porabe virov, zvišanja življenjske kvalitete prebivalstva in izboljšanja konkurenčnosti obstoječega gospodarstva. Pri tem je treba upoštevati področja energije, transporta, urbanizma in lokalne oblasti. Osnovni značilnosti pametnih mest sta integracija in prepletenost teh področij z namenom izpolnitve ekološkega in socialnega napredka.[6]

2.3 Infrastruktura pametnih mest

Infrastruktura mesta je sestavljena med drugim iz stanovanj, sistema oskrbe z vodo, kanalizacijskega sistema, električne oskrbe in distribucije, transporta, komunalnih storitev in telekomunikacij.

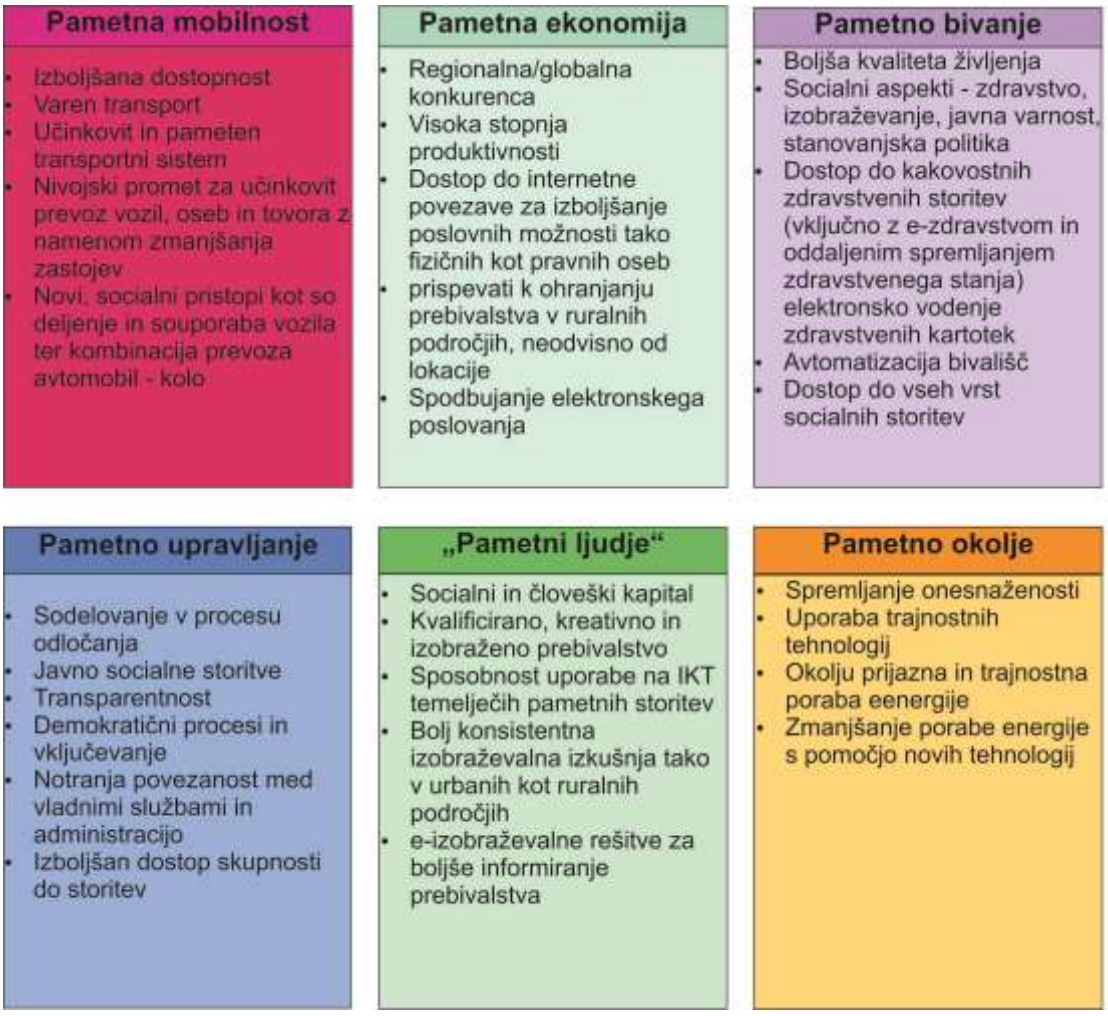
Infrastruktura pametnih mest[7] se razlikuje od tradicionalnih urbanih infrastruktur zaradi svojih zmožnosti pametnega odzivanja na spremembe v okolju, vključno z upoštevanjem potreb uporabnikov in druge infrastrukture za doseganje učinkovitejšega izvajanja. Infrastruktura

[6] I. Kossina, Smart City: Begriff, Charakteristika und Beispiele, v: Wiener Stadtwerke zur nachhaltigen Entwicklung, 7 (2011), str. 19.
[7] UNCTAD secretariad, United Nations Commission on Science and Technology for Development Intersessional Panel 2015–2016, v: Issues Paper On Smart Cities and Infrastructure, (2016), str. 15-33.

pametnih mest zagotavlja temelj vsem šestim področjem, ki jim je v pametnih mestih dana posebna pozornost: pameten transport, pametna ekonomija, pametno življenje, pametno upravljanje, pametni ljudje in pametno okolje. Treba je opozoriti, da so gradniki pametne infrastrukture visoko specifični in so v svoji naravi določeni v skladu s stopnjo razvoja.

Infrastruktura predstavlja temelj razvoja pametnega mesta. Pametno infrastrukturo delimo na dve kategoriji: fizično in digitalno. Pametna mesta potrebujejo skupno obravnavanje obeh vrst pametne infrastrukture.

Fizična infrastruktura v pametnih mestih je sestavljena iz: pametnih zgradb, pametnega transporta, pametne energije, pametnega upravljanja z vodo in komunalnimi odpadki ter pametnega zdravstva.



SLIKA 1: Temeljni gradniki pametnega mesta in njihove karakteristike[8]

[8] M. Jaekel, Smart City wird Realität Wegweiser für neue Urbanitäten in der Digitalmoderne, v: Springer Fachmedien Wiesbaden (2015), str. 29.

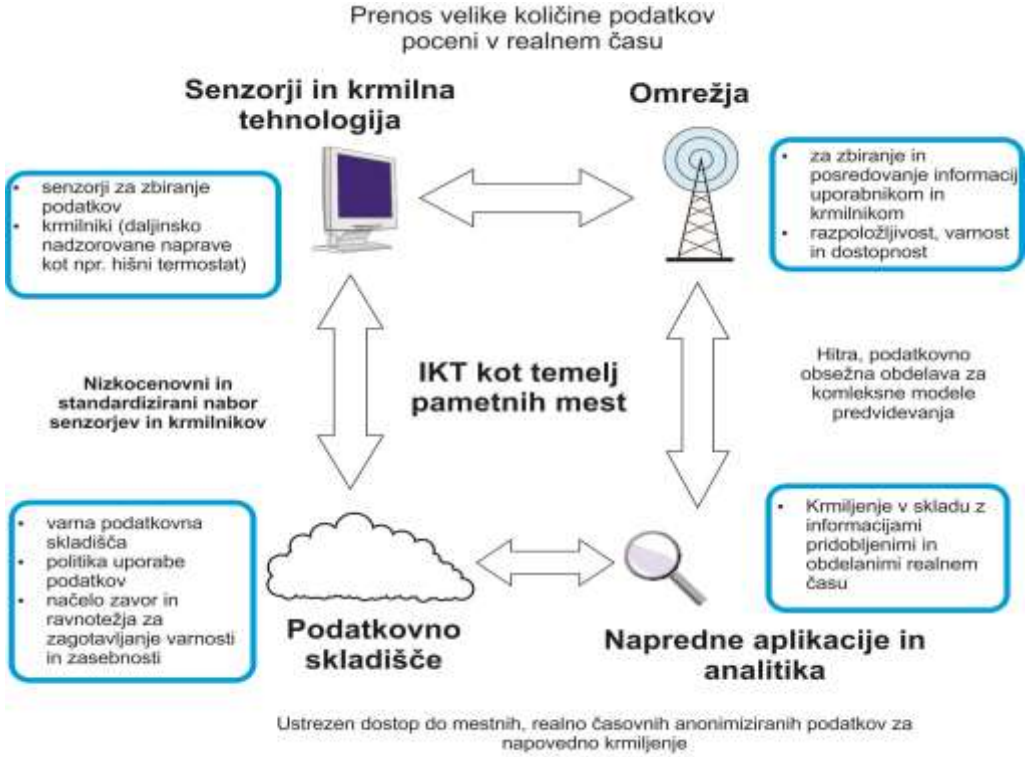
V sklop digitalne infrastrukture pa je umeščeno področje IKT ter podatkovna infrastruktura.

2.3.1 Pametna digitalna infrastruktura[9]

2.3.1.1 Vloga informacijske in komunikacijske tehnologije v pametnih mestih

Pametno mesto uporablja vse medsebojno povezane informacije, ki so na razpolago z namenom boljšega razumevanja in nadzora poslovanja ter optimalne rabe omejenih virov. IKT igra pomembno vlogo v tem procesu, saj zagotavlja digitalno platformo, s katero se lahko vzpostavi mreža znanja in informacij. Namen take platforme ni le zbiranje podatkov v mestu, podatki služijo tudi boljšemu razumevanju delovanja mesta.

Ključna vrednost IKT v pametnem mestu je sposobnost pravočasnega zajemanja in posredovanja podatkov. Če je informacija zagotovljena v realnem času in je natančna, to mestu omogoča ukrepati, še preden se problem zaostri. Pametno mesto lahko zato razumemo kot predvidljivo mesto, kjer se določeni dogodki in izgredi lahko predvidijo, to pa se kaže v izboljšani kvaliteti življenja ter omogoča odločitve, ki temeljijo na boljši informiranosti.



SLIKA 2: Tokokrog digitalne infrastrukture[10]

[9] UNCTAD secretariad, United Nations Commission on Science and Technology for Development Intersessional Panel 2015–2016, v: Issues Paper On Smart Cities and Infrastructure, (2016), str. 28–30.

Zbiranje in shranjevanje podatkov v pametnih mestih poteka preko interneta stvari (ang. Internet of Things), velikega podatkovja (ang. Big data) ter računalništva v oblaku (ang. Cloud computing).

2.3.1.2 Internet stvari

Internet stvari temelji na povezovanju ogromne količine naprav z vgrajenimi senzorji, ki jim omogočajo povezovanje in komuniciranje med seboj in z najrazličnejšimi aplikacijami. Leta 2008 je bilo z internetom povezanih 7 milijard naprav, 2015 je ta številka poskočila na 25 milijard, do leta 2050 pa se pričakuje povezanost več kot 50 milijard naprav in stvari.[11] Internet stvari predstavlja enega izmed stebrov interneta prihodnosti, ki bo z uporabo standardiziranih komunikacijskih protokolov in omrežne infrastrukture, sposobne samostojne konfiguracije, razširil internet na fizične predmete, ki nas obdajajo v vsakdanjem življenju.

Pričakovati je, da bodo stvari, povezane v internet stvari, generirale in pridobivale velike količine podatkovnih zbirk iz različnih lokacij, s tem pa povečale potrebo po njihovem učinkovitem shranjevanju in obdelavi. Zbiranje podatkov znotraj interneta stvari poteka neprestano in neodvisno od ljudi.[12]

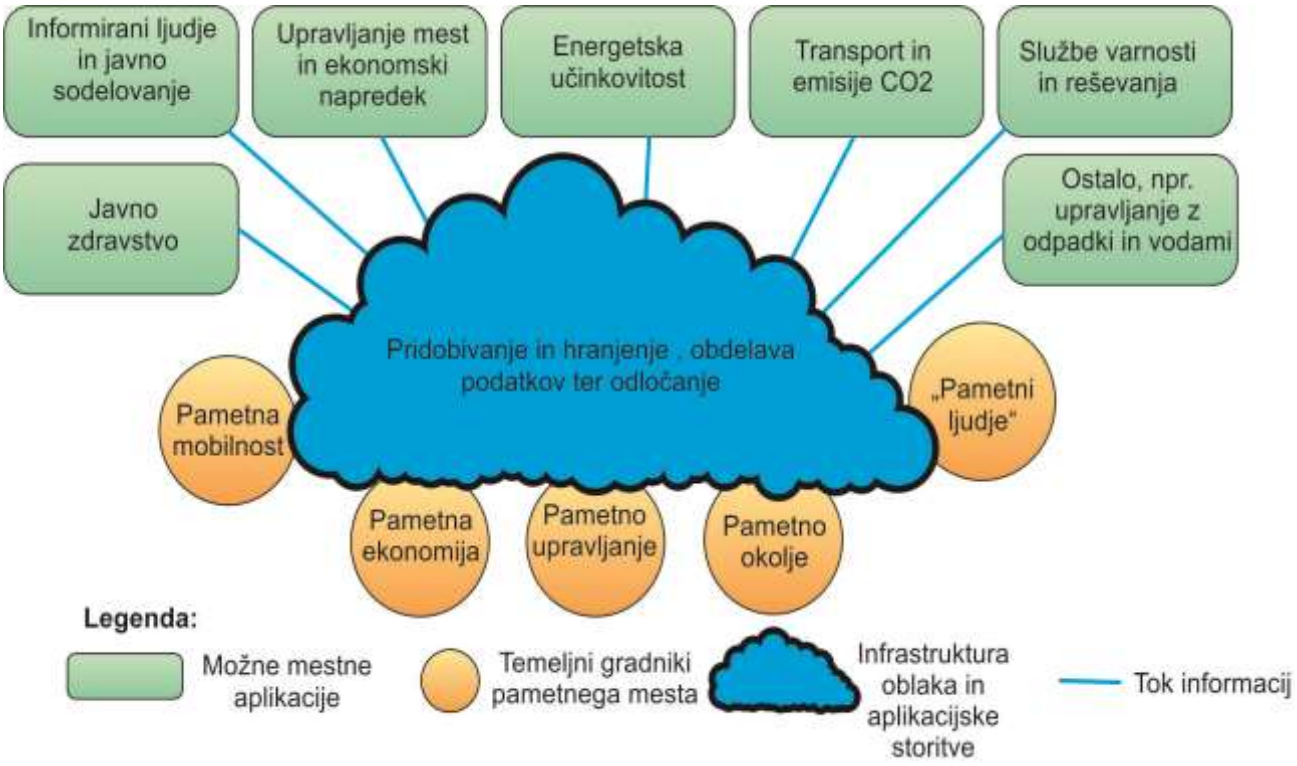
SLIKA 3: Področja uporabe interneta stvari[13]

[10] UNCTAD secretariad, United Nations Commission on Science and Technology for Development Intersessional Panel 2015–2016, v: Issues Paper On Smart Cities and Infrastructure, (2016), str. 29.
[11] H. Frei, Effizient – aber überhaupt nicht städtisch, Vom Internet der Dinge zur Smart City?, v: NZZ, (12. 7. 2015), URL: http://www.nzz.ch/feuilleton/effizient--aber-nicht-staedtisch-1.18577769, (15. 8. 2016).
[12] IPROM, Internet stvari, URL: https://iprom.si/slovar/internet-stvari/, (20. 8. 2016).
[13] N. Mitton, V. Loscari, R. Petrolo, Towards a smart city based on cloud of things, a survey on the smart city vision and paradigms, v:Transactions on Emerging Telecommunications Technologies, (2015), str. 4.

2.3.1.3 Veliko podatkovje

Do danes ni poenotene definicije velikega podatkovja. Na splošno lahko veliko podatkovje opredelimo kot podatkovno enoto, ki presega meje in zmožnosti konvencionalne informacijske tehnologije. Veliko podatkovje obsega predvsem evidentiranje podatkovnih količin, shranjevanje, pregled, razporeditev, analizo in virtualizacijo velikega podatkovnega volumna, ki ga običajne tehnologije zaradi količine niso sposobne obravnavati.[14]

Tehnologija, ki omogoča zbiranje in obdelavo ogromne količine podatkov, je zelo raznolika in se nenehno razvija, temelji pa na tem, da z analitičnimi orodji in procesi preverimo, ali med podatki obstajajo pomenske korelacije in povezave. Dodana vrednost nastane, kadar analiza pokaže neki nov, uporaben vpogled.



SLIKA 4: Tok informacij in obdelava zbranih podatkov[15]

[14] M. Gottwald, Big data: Was ist Big Data? - Big Data Analytics, Software, Tools + Trends, v: SoftSelect glossar, URL: http://www.softselect.de/wissenspool/big-data (20. 8. 2016).

[15] Z. Khan, A. Anjum, K. Soomro, M. Atif Tahir , Towards cloud based big data analytics for smart future cities, v: Journal of Cloud computing, (2015), str. 3.

2.3.1.4 Računalništvo v oblaku

(Trenutno) osrednja infrastruktura, ki omogoča razmah velikega podatkovja, je računalništvo v oblaku (ang. cloud computing), ki tvori pomemben del t. i. digitalnega vesolja (ang. digital universe).[16]

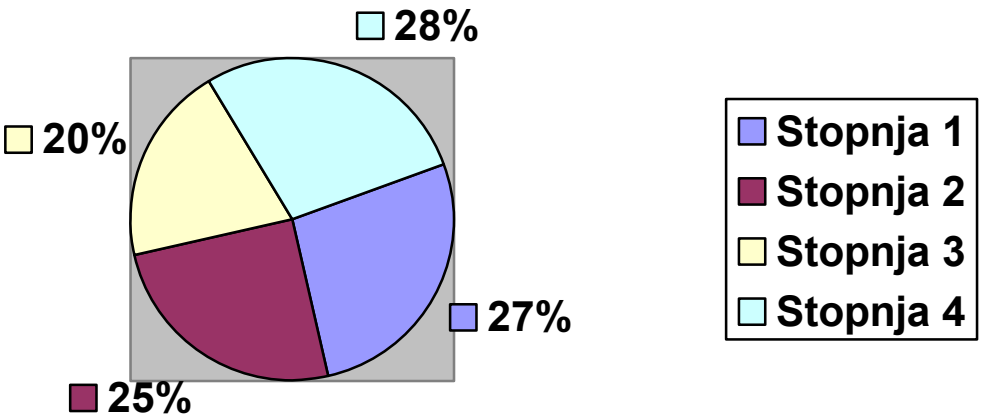
»Je računalništvo, ki temelji na medmrežni povezljivosti, kjer so deljeni računalniški viri, programska oprema ter informacije, ponujene računalnikom in ostalim napravam na zahtevo.«[17]

2.4 Stopnje razvoja pametnih mest v Evropi

V reprezentativni študiji[18] Evropskega parlamenta, z naslovom Analiza pametnih mest v Evropi, so izbrali mesta Evropske unije in preverili njihovo stopnjo razvitosti v smeri pametnega mesta. Izmed 469 mest Evropske unije s številom prebivalstva nad 100.000 so bile v 240 mestih zaznane aktivnosti, značilne za pametna mesta. Delovanje v smeri pametnega mesta je v večini 240 mest bolj majhnega obsega. Poleg tega študija prihaja do zaključka, da se večina projektov pametnih mest nahaja v fazi zgodnjega razvoja, pri čemer večja mesta na podlagi sredstev, s katerimi razpolagajo, in zaradi politične podpore izkazujejo najvišjo stopnjo razvoja. Na podlagi modela razvitosti (ang. Maturity Model) mesta lahko razdelimo na štiri stopnje[19]:

- Stopnja 1: strategija pametnega mesta.
- Stopnja 2: poleg strategije ima mesto že razvit projektni plan, a še nobenih pilotnih projektov oz. implementacij projektov.
- Stopnja 3: poleg projektnih planov se že izvajajo pilotni projekti pametnih mest.
- Stopnja 4: pametno mesto z vsaj eno razvito iniciativo pametnega mesta.

[16] L. Selinšek, Veliko podatkovje v pravu in ekonomiji: veliki izzivi ali velike težave?, v: LEXONOMICA, 2 (2015), str. 165–166.
[17] Računalništvo v oblaku- zgodovina, definicija, URL: http://www.geministyle.si/print/racunalnistvo/splosno/racunalnistvo-v-oblaku-2.html, (20.8.2016).
[18] Directorate for Internal Policies/Policy Department A: Economic and Scientific Policy, Mapping smart cities in the EU, (2014).
[19] M. Jaekel, Smart City wird Realität Wegweiser für neue Urbanitäten in der Digitalmoderne, v: Springer Fachmedien Wiesbaden (2015), str. 206–210.



Z modela razvitosti je razvidno, da več kot 70 % analiziranih mest v Evropski uniji ne preseže faze izvajanja pilotnega projekta pametnega mesta. 50 % mest ni speljalo oziroma implementiralo nikakršnega pilotnega projekta pametnega mesta. Večina analiziranih mest EU uporablja koncept pametnega mesta v namen oglaševanja mesta, pri čemer se nahajajo v zgodnji fazi razvoja pametnega mesta.

Evropska komisija je leta 2010 predstavila program Evropa 2020.[20] Evropa 2020 je evropska strategija za zagon gospodarstva in zaposlovanja v regijah, z namenom ustvariti pametno, trajnostno in vključujočo ekonomijo. Digitalna agenda je ena izmed sedmih vodilnih pobud strategije Evropa 2020 in je namenjena določitvi ključne vloge, ki jo bo igrala uporaba IKT, če želi Evropa doseči svoje cilje za leto 2020. Cilj Digitalne agende za Evropo je poskrbeti, da bo enotni evropski digitalni trg, ki se opira na hitre in ultrahitre internetne povezave ter interoperabilne aplikacije, prinesel trajne gospodarske in družbene koristi.

[20] Evropska komisija, Evropa 2020, Cilji strategije Evropa 2020, URL: https://ec.europa.eu/info/strategy/european-semester/framework/europe-2020-strategy_en

2.5 Primer pametnega mesta: BARCELONA

Barcelona je v letu 2015 pridobila naziv »Global Smart City« in s tem prevladala nad mesti, kot so New York, London, Nica in Singapur. Ocenjeno je bilo, da je špansko mesto prevladalo predvsem zaradi razvoja na področju pametne energije (ang. Smart Grid) in pametnega transporta. Na področju pametne energije se Barcelona ponaša z obnovljivim pridobivanjem energije – s sedmimi urami sonca na dan Barcelona proizvede zadostno količino sončne energije za potrebe samooskrbe. V letu 2006 je Barcelona postala prvo mesto, ki je zahtevalo uporabo solarnih ogrevalnikov vode. Na področju ogrevanja in klimatizacije je vzpostavljen sistem elektrarne Districlima, ki za ogrevanje do zdaj 78 sodelujočih zgradb uporablja paro, ki nastane pri izgorevanju smeti, za hlajenje pa uporablja morsko vodo.

Na področju transporta je vzpostavljeno pravokotno avtobusno omrežje (t. i. orthogonal bus network), ki omogoča hitrejše potovanje, pogostejše linije in enostavnejšo uporabo. V omrežje so vključeni avtobusi, ki delujejo na hibridni pogon. Poskrbljeno je tudi za individualno mobilnost. Za individualni transport je poskrbljeno s projektom Bicing, ki zagotavlja 6000 koles uporabnikom, ki potrebujejo prevoz na krajših relacijah. Lažje parkiranje omogočajo senzorji, ki vozniku preko pametnega telefona z aplikacijo ApparkB sporočajo stanje zasedenosti parkirnih mest.

Barcelona stremi tudi k trajnostnemu okoljskemu razvoju, s tem namenom je razvit pameten namakalni sistem. Senzorji sporočajo vlago tal, na podlagi teh informacij in podatkov o vremenu se analizira potrebna količina vode za optimalno namakanje. Za javno razsvetljavo mesto uporablja LED-tehnologijo, ki aktivira osvetlitev le ob zaznavi gibanja, prav tako pa mesto razpolaga z najboljšo prekritostjo z WLAN-omrežjem.[21]

[21] J. Ancheta ,Ten Reasons why Barcelona is a Smart City, v: Vilaweb, (26. 2. 2014), URL: http://www.vilaweb.cat/noticia/4175829/20140226/ten-reasons-why-barcelona-is-smart-city.html, (25. 8. 2016).

3. Nadzor in zasebnost v pametnih mestih

»V zadnjih nekaj desetletjih smo priča prodoru novih digitalnih in omrežnih tehnologij, ki v svojem delovanju omogočajo vsesplošno prisotnost državnega in korporativnega nadzora. Te tehnologije imajo sposobnost, da zajamejo in posredujejo podatke o uporabi naprav; hkrati je razvita sofisticirana programska oprema, ki obdeluje in interpretira pomen podatkov na avtomatiziran, avtonomni in avtomatski način. Pri tem uporablja vgrajene GPS-naprave, senzorje in digitalne fotoaparate, kar omogoča obširni geonadzor ljudi in krajev«.[22]

Podatki predstavljajo stranski produkt informacijske družbe. Vsaka interakcija, ki jo imamo z računalnikom ali drugo napravo, ki je povezana z internetom, ustvari zapisnik o podatkih, ki so bili pridobljeni. Vse, kar počnemo, pusti za nami podatkovno senco, ki je pod stalnim nadzorom. Prav tako je vzpon velikega podatkovja posledica informacijske družbene socializacije. Socializacija in tehnološki napredek posameznika podzavestno silita v neprestano potrebo po izboljšanju svojega vsakdanjika s pomočjo pametnih naprav, s tem sami omogočamo in gradimo svet vsesplošnega nadzora.

Velja, da je nadzor tesno povezan s tehnologijo, predvsem z informacijsko tehnologijo, ki je namenjena zbiranju in obdelavi vseh vrst podatkov in informacij. Računalnik oziroma informacijsko-komunikacijska tehnologija se vzpostavljata kot osrednja tehnologija nadzora, saj se ta tehnologija nadzorovanja poglablja in krepi. Ne samo, da ga omogoča, temveč ga tudi olajšuje, saj je že v osnovi zasnovana za zbiranje in hranjenje podatkov. Nastanek interneta je problem nadzorovanja in zasebnosti še okrepil.

Benthamov načrt Panoptikona iz leta 1791 je predvideval optični nadzor, v informacijski družbi pa vidnost ni več samo optična. Zbirke podatkov so ena poglavitnih orodij množičnega nadzora. James Rule ugotavlja,[23] da predstavljajo omejitev sodobnih sistemov nadzora štirje dejavniki: velikost datotek, ki jih sistem lahko shranjuje, stopnja, do katere so lahko ti sistemi centralizirani, hitrost pretoka podatkov in informacij med točkami v sistemu ter število stičnih točk med sistemom in subjektom.

[22] M. Kovačič, Nadzor in zasebnost v informacijski družbi: filozofski, sociološki, pravni in tehnični vidiki nadzora in zasebnosti na internetu, (2006), str. 22.
[23] J. B. Rule, Social control and modern social structures, v: Surveillance studies reader, (2007), str. 26–28.

Beniger[24] v svoji knjigi Revolucija nadzora postavi tezo, da se revolucija nadzora vzdržuje sama po sebi. Razlog za porast nadzora so po Benigerju trije dejavniki: izraba energije, hitrost obdelovanja informacij in tehnologije nadzora, pri tem napredek enega dejavnika povzroči napredek preostalih dveh.

Takšno pozitivno spiralo opazimo tudi v primeru nadzora v pametnih mestih. S porastom naprav, ki so povezani z internetom (leta 2008 je bilo z internetom povezanih 7 milijard naprav in stvari, 2015 je ta številka poskočila na 25 milijard, do leta 2050 pa se pričakuje povezanost več kot 50 milijard naprav),[25] raste količina zbranih podatkov. V letu 2011 je bila na svetovni ravni presežena količina podatkovnega volumna zetabajtov in rasti podatkov ni videti konca. Predvideva se, da naj bi podatkovni volumen do leta 2020 obsegal 35 zetabajtov in več podatkov, kot jih imamo, lažje nadzorujemo in predvidevamo dogodke.

3.1 Digitalne pravice posameznikov

Zgodovinsko gledano smo stremeli k temu, da varujemo območje svoje zasebnosti, ki se začne z našim telesom, vključuje naš dom in se razširja na področje zasebne komunikacije. Na to kaže tudi Evropska konvencija o človekovih pravicah, ki v 8. členu zahteva spoštovanje pravice do zasebnega in družinskega življenja. Nasprotno mesta simbolizirajo tipični javni prostor, kjer je bilo pričakovanje zasebnosti že od nekdaj nizko oziroma ničelno.

V času pametnih mest pa je opaziti nasprotno paradigmo – kar je bilo zgodovinsko sprejeto kot javno, (mestni trgi, ceste, transport ter zdravstveni sistem), je danes dano v upravljanje zasebnemu sektorju oziroma so senzorji in ostale naprave, ki zbirajo podatke v podatkovne baze, last zasebnikov. Ti deli mesta so postali psevdo-zasebni prostori.[26]

Osebni podatki, ki bi včasih ostali varno znotraj štirih sten, so danes posredovani oziroma shranjeni – po večini brez naše vednosti zunaj našega dosega. Zbirajo se preko pametnih telefonov, prenosnih naprav, so shranjeni na strežnikih ali v oblaku. Poleg tega so podatki, ki so bili nekoč znani le nam, danes dostopni celemu svetu.

[24] J. R. Beniger, The control revolution, (1989), str. 427–434.
[25] H. Frei, Effizient – aber überhaupt nicht städtisch, Vom Internet der Dinge zur Smart City?, v: NZZ, (12. 7. 2015), URL: http://www.nzz.ch/feuilleton/effizient--aber-nicht-staedtisch-1.18577769, (15. 8. 2016).
[26] L. Edwards, Privacy, Security and Data Protection in Smart Cities: a Critical EU Law Perspective, v: CREATe Working Paper , 11 (2015), str. 13.

Tudi v javnih prostorih, kjer so se ljudje nekoč zanesli na praktično anonimnost, je prisotnost nadzora s sistemi, kot so sistem televizijskih kamer zaprtega kroga (ang. closed circuit television cameras), avtomatsko prepoznavanje registrskih tablic, globalni sistem pozicioniranja (ang. GPS), brezžični internet in programi za prepoznavanje obrazov, postala vseprisotna. Kombinacija tako imenovanih prepustnih domov in splošno prisotnega nadzora kaže, da smo prešli v čas informacijske družbe, v kateri je povsod razširjena obdelava podatkov in kjer ločnica med javnim in zasebnim ne obstaja več. Bistven problem v javnosti pametnih mest je, da ni mogoče preprečiti zbiranja podatkov prebivalcev pametnih mest.[27]

Številne iniciative[28] se že desetletja zavzemajo za vzpostavitev Listine o temeljnih pravicah na internetu. Evropska unija je na področju varovanja osebnih podatkov v letu 2016, s sprejetjem Splošne uredbe o varovanju podatkov 2016/679, naredila velik korak k zagotavljanju enakih digitalnih pravic vsakomur, ki živi na območji EU. Splošna uredba vzpostavlja naslednje pravice, predstavljene v nadaljevanju.

3.1.1 Pravica do dostopa do podatkov, na katerega se nanašajo osebni podatki

Pravica do dostopa do podatkov posameznikom omogoča dostop do informacij. Predvsem je pravica pomembna za posameznike, ki menijo, da o njih krožijo nepravilni ali nezakonito obdelani podatki. Pravica do dostopa do podatkov ne poda ocene o pridobljenih informacijah, kar pomeni, da s samim zahtevkom za pridobitev informacij posameznik proti podjetju ali organizaciji ne vzpostavlja nobenih očitkov. Pravica do dostopa se nanaša na avtomatizirano obdelavo podatkov kot tudi ročno obdelane podatke.[29]

3.1.2 Pravica do popravka

Posameznik uporabi pravico do popravka v primeru, ko so shranjeni podatki pomanjkljivi, zastareli ali na kakšen drug način napačni. Upravljavec podatkov pa se ne sme zanašati na

[27] L. Edwards, Privacy, Security and Data Protection in Smart Cities: a Critical EU Law Perspective, v: CREATe Working Paper, 11(2015), str. 13, 14.
[28] APC Internet Rights Charter (https://www.apc.org/node/5677), Svetovni vrh o informacijski družbi (http://www.itu.int/net/wsis/), Global Network Initiative (https://www.globalnetworkinitiative.org/)
[29] Uredba 2016/679/ES Evropskega parlamenta in Sveta z dne 27. aprila 2016 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), 15. člen.

posameznike, da ga bodo opozorili na pomanjkljivosti. Dolžnost upravljavca je, da zagotavlja ažurnost podatkov.[30]

3.1.3 Pravica do izbrisa (»pravica do pozabe«)

Pravica do izbrisa zagotavlja, da digitalne informacije, ki se nanašajo na posameznike, niso dostopne za vedno. Splošna uredba določa predvsem pravice in obveznosti v zvezi z izbrisom. Le 2. odstavek 17. člena Splošne uredbe vsebuje idejo pravice do pozabe, ki preprečuje posredovanje osebnih podatkov: »Kadar upravljavec objavi osebne podatke in je v skladu s 1. odstavkom osebne podatke obvezan izbrisati, ob upoštevanju razpoložljive tehnologije in stroškov izvajanja sprejme razumne ukrepe, vključno s tehničnimi, da upravljavce, ki obdelujejo osebne podatke, obvesti, da posameznik, na katerega se nanašajo osebni podatki, od njih zahteva, naj izbrišejo morebitne povezave do teh osebnih podatkov ali njihove kopije.«

Pravica do izbrisa pa se lahko omeji v primerih, ko je posameznik, na katerega se nanašajo osebni podatki, oseba javnega življenja in ima javnost interes na teh podatkih.[31]

3.1.4 Pravica do omejitve obdelave

Posameznik lahko v določenih primerih zahteva omejitev obdelave osebnih podatkov. To se lahko zgodi v primerih, kadar posameznik, na katerega se nanašajo osebni podatki, oporeka točnost podatkov ali želi v primeru nezakonite obdelave namesto izbrisa uveljavljati omejitev njihove uporabe. Poleg tega tudi v primeru, ko upravljavec osebnih podatkov ne potrebuje več za namene obdelave, temveč jih posameznik, na katerega se nanašajo osebni podatki, potrebuje za uveljavljanje, izvajanje ali obrambo pravnih zahtevkov, ali ko je posameznik, na katerega se nanašajo osebni podatki, vložil ugovor v zvezi z obdelavo, dokler se ne preveri, ali zakoniti razlogi upravljavca prevladajo nad razlogi posameznika, na katerega se nanašajo osebni podatki.[32]

[30] Uredba 2016/679/ES Evropskega parlamenta in Sveta z dne 27. aprila 2016 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), 16. člen.
[31] Uredba 2016/679/ES Evropskega parlamenta in Sveta z dne 27. aprila 2016 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), 17. člen.
[32] Uredba 2016/679/ES Evropskega parlamenta in Sveta z dne 27. aprila 2016 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), 18. člen.

3.1.5 Pravica do prenosljivosti podatkov

Posameznik je upravičen, da podatke, ki jih je dal na razpolago za avtomatizirano obdelavo, na primer družabnemu omrežju, prenese na drugega upravljavca. S to pravico se posamezniku zagotovi lažji prehod med upravljavci, brez strahu pred izgubo podatkov.[33]

3.1.6 Pravica do ugovora

Posameznik ima pravico, da kadarkoli ugovarja obdelavi osebnih podatkov, ki je potrebna za naloge v javnem interesu ali pri izvajanju javne oblasti, dodeljene upravljavcu, ali je obdelava potrebna zaradi zakonitih interesov, za katere si prizadeva upravljavec ali tretja oseba (1. odst. 6. člena tč. e, f). Upravljavec lahko podatke obdeluje le takrat, kadar nad takimi interesi prevladajo interesi ali temeljne pravice in svoboščine posameznika, na katerega se nanašajo osebni podatki, ki zahtevajo varstvo osebnih podatkov.

Kadar se osebni podatki obdelujejo za namene neposrednega trženja, ima posameznik, na katerega se nanašajo osebni podatki, pravico, da kadar koli ugovarja obdelavi osebnih podatkov v zvezi z njim za namene takega trženja, vključno z oblikovanjem profilov, kolikor je povezano s takim neposrednim trženjem.[34]

3.1.7 Avtomatizirano sprejemanje odločitev, vključno z oblikovanjem profilov

Posameznik, na katerega se nanašajo osebni podatki, ima pravico, da zanj ne velja odločitev, ki temelji zgolj na avtomatizirani obdelavi, vključno z oblikovanjem profilov.

To ne velja, če je odločitev nujna za sklenitev ali izvajanje pogodbe med posameznikom, na katerega se nanašajo osebni podatki, in upravljavcem, če je utemeljena z izrecno utemeljitvijo posameznika, na katerega se nanašajo osebni podatki, ali v primeru, da je odločitev dovoljena po pravu Unije ali pravu države članice, ki velja za upravljavca in določa tudi ustrezne ukrepe

[33] Uredba 2016/679/ES Evropskega parlamenta in Sveta z dne 27. aprila 2016 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), 20. člen.
[34] Uredba 2016/679/ES Evropskega parlamenta in Sveta z dne 27. aprila 2016 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), 21. člen.

za zaščito pravic in svoboščin ter zakonitih interesov posameznika, na katerega se nanašajo osebni podatki.[35]

3.2 Pametna zasebnost za pametna mesta

Stopnja, na kateri se zbirajo, analizirajo in uporabljajo podatki o prebivalcih v pametnih mestih, se razlikuje od vsakršnega mehanizma nadzora v preteklosti. Odločitve v pametnih mestih se sprejemajo na podlagi specifičnih osebnih podatkov milijonov posameznikov, pri tem se uporabljajo podatki od obraznih odtisov do vzorcev nakupovanja, geolokacije in vse do porabe energije. Čeprav se je toleranca do vladnega nadzora v vsej svoji zgodovini spremenila, še vedno ostajajo pomisleki v povezavi z zasebnostjo v pametnih mestih. Prizadevanja pri iskanju razumnega ravnovesja med javno koristjo, ki jo prinaša veliko podatkovje, in izgubo individualne zasebnosti so sprožila silovite razprave in predloge reform. Pogled na prihodnost futurističnih mest pogosto vzbuja občutke nezaupanja in strah pred nenehnim računalniškim nadzorom. Tehnologija pametnih mest je kontradiktorna in skrivnostna, čeprav temu ne bi bilo treba biti tako. Cilj lokalne uprave, razvijalcev interneta stvari in urbanistov bi moral biti spodbujanje in vključevanje prebivalstva v tehnološke novitete. Za dosego cilja je treba graditi na naslednjih korakih, ki bodo predstavljeni v nadaljevanju.

3.2.1 Dostop

Vse bolj, ko javnost postane domača s tem, kako, kje in zakaj se zbirajo podatki s tehnologijami v pametnih mestih, bolj bodo ljudje zaupali takšnim operacijam. Posameznikova pravica do dostopa je ključna za vzpostavitev zaupanja in sprejemanja novih povezanih tehnologij, vključno s pametnim mestom. Ta pravica bi omogočila, da nadzor v pametnem mestu ne bi bil več kontradiktoren in skrivnosten, saj bi uporabniki z vpogledom v podatke, ki se zbirajo o njih, vzpostavili odnos zaupanja in transparentnosti.

Na uveljavljajočem trgu interneta stvari podjetja že spodbujajo posameznike, da dostopajo do podatkov, ki se stekajo v podatkovne baze podjetij iz povezanih naprav, ki se nahajajo v domovih, avtomobilih in pisarnah posameznikov. V velikem podatkovnem svetu to pomeni, da posameznikom ponudimo dostop do njihovih podatkov na način, ki bo za njih uporaben. S pomočjo dostopnosti in analize podatkov bo uporabnik prišel do koristnih zaključkov o

[35] Uredba 2016/679/ES Evropskega parlamenta in Sveta z dne 27. aprila 2016 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), 22. člen.

lastnem vedenju (npr. informacije o prehrani, gibanju in možnostih za investicije v sklade). Zagotavljanje dostopa do uporabnih osebnih podatkov prinaša koristi tako za potrošnika kot tudi za organizacijo. Ne le, da bi uporabniki imeli vpogled v zbrane podatke, tak dostop bi dodatno spodbujal oblikovanja bolj inovativnih tehnologij za omilitev trenj, ki se pojavljajo ob vzpostavljanju infrastrukture pametnega mesta.

Poleg tega, da osebne informacije usmerimo v uporabno skupno sredstvo, katerega korist imajo tako razvijalci tehnologije v pametnih mestih kot tudi prebivalci, dostop omogoča še pomembno funkcijo odgovornosti. Posebno v okolju hiperpovezane mestne birokracije pravica do dostopa ustvarja funkcijo institucionalne transparentnosti; če prebivalci lahko dostopajo do lastnih podatkov, bodo tako imeli boljši občutek, katere službe so zadolžene za nadzor in varnost. Poleg tega bo dostop omogočil posameznikom, da bodo sprožili pregled organizacij v zvezi z informacijskimi praksami ali pa razkrinkali potencialno zlorabo uporabe podatkov.[36]

3.2.2 Podatkovna uporabnost

Podatkovna uporabnost opisuje ravnanje, s katerim bi uporabnik na podlagi pridobljenih podatkov pridobil koristne rezultate oziroma storitve – na primer fitnes merilnik, ki zbira podatke uporabnika o srčnem utripu, porabi kalorij in kakovosti spanca. Poleg tega, da zbrane podatke posreduje proizvajalcu, je njegov izvirni pomen korist uporabnika, da s pomočjo naprave izboljša svoje počutje. Ta pristop zagovarja, naj posameznik nima le koristi od dostopa do zbranih podatkov, temveč tudi od uporabe analiziranih podatkov za lastne potrebe. Omogočiti prebivalstvu uporabo zbranih podatkov in imeti koristi od njih je ključni korak za pridobitev javnega zaupanja in podpore za implementacijo pametnih mest.[37]

3.2.3 De-identifikacija

De-identifikacija je postopek odstranitve informacij, zbranih in shranjenih s strani organizacij, ki omogočajo identifikacijo posameznika.

Pri de-identifikaciji ne gre za posamezno tehniko, temveč za vsesplošni pojem, ki zaobsega različne pristope, katerih namen je odstraniti osebno določljive podatke iz zbranih podatkov z

[36] K. Finch, O. Tene, Welcome to the Metropticon: Protecting privacy in a hyperconnected town, v: Fordham Urban Law Journal, 5 (2015), str. 1608.
[37] K. Finch, O. Tene, Welcome to the Metropticon: Protecting privacy in a hyperconnected town, v: Fordham Urban Law Journal, 5 (2015), str. 1609.

namenom, da posameznik ne more biti več identificiran. Metoda de-identifikacije mora biti prikrojena glede na vsebino in kontekst podatkov, hkrati pa je treba upoštevati dejavnike, kot sta vrsta in pomen informacij.

Ker ni podane splošne definicije pojma, se je oblikoval splošni pristop razumevanja pojava[38]: De-identifikacija je krovni pojem za vsakršni postopek odstranitve povezave med zbranim podatkom in posameznikom. Anonimizacija je posamezni pristop de-identifikacije, ki označuje odstranitev neposrednih identifikacijskih znakov, kot so ime, naslov in telefonska številka, in odstranitev oziroma zameglitev indirektnih identifikacijskih znakov z namenom ohranitve anonimnosti. Psevdonimizacija je podskupina anonimizacije, ki označuje odstranitev osebno določljivih podatkov s sistematičnim nadomeščanjem s psevdonimi, kot je ponarejeno ime ali številka. Ta tehnika uporablja psevdonimizacijski algoritemski ključ, ki včasih omogoča obratni proces. Zaupnost predvideva postopek v dveh korakih – podatki so sprva de-identificirani z odstranitvijo neposrednih identifikacijskih znakov, temu pa sledi ovrednotenje in upravljanje s tveganjem indirektnih identifikacijskih znakov. Ta pristop se pojavlja predvsem v povezavi z varnostjo in statistiko.

Nov, de-identificiran nabor podatkov se lahko uporabi za tri temeljne namene:
- izmenjava informacij z zunanjimi organizacijami, brez potrebe po odobritvi s strani pristojnega organa oziroma soglasja posameznika,
- interna uporaba, ki nudi alternativo originalnemu naboru podatkov in obenem zmanjša tveganje kršitve zasebnosti,
- objava v publikacijah za namen raziskav in transparentnosti.

Koristi de-identifikacije:
- de-identificirane informacije se ne obravnavajo kot osebni podatki in ne padejo v pravne okvire varovanja osebnih podatkov,
- po de-identifikaciji se informacije lahko uporabijo v sekundarne namene in se posredujejo brez potrebe po pridobitvi soglasja ali odobritve pristojnega organa,
- de-identifikacija ponuja kompromis pri iskanju ravnotežja posameznikove pravice do podatkovne zasebnosti,

[38] Commisioner for Privacy and Data Protection: Background Paper: De-Identification, URL: https://www.cpdp.vic.gov.au/images/content/pdf/privacy_week/De-identification_Background_Paper.pdf, str. 1-3.

– tehnike de-identifikacije se lahko izvedejo na različnih stopnjah informacijskega toka.

Evropska direktiva o varstvu podatkov uporablja pojem anonimizacije. Anonimizacija je v direktivi definirana negativno. Uvodna izjava 26 Direktive 95/45 Evropskega parlamenta in Sveta[39] določa: »Načela varstva se ne uporabljajo za podatke, ki so spremenjeni v anonimne tako, da posameznik, na katerega se osebni podatki nanašajo, ni več določljiv.«

V 2. členu Direktive je določljiva oseba definirana kot »tista, ki se lahko neposredno ali posredno identificira, predvsem s sklicevanjem na identifikacijsko številko ali na enega ali več dejavnikov, ki so značilni za njeno fizično, fiziološko, duševno, ekonomsko, kulturno ali socialno identiteto«.

Direktiva o varstvu podatkov psevdonimizacije ne predvideva. Vendar je v 42. členu pojasnjevalnega poročila h Konvenciji št. 108 navedeno, da »zahteva […] v zvezi s časovnimi omejitvami hrambe osebnih podatkov v poimenski obliki ne pomeni, da bi bilo treba podatke po določenem času nepreklicno ločiti od imena osebe, na katero se nanašajo, temveč samo, da podatkov in identifikatorjev ne bi bilo mogoče zlahka povezati«.[40] To je mogoče doseči s psevdonimizacijo osebnih podatkov. Splošna uredba 2016/679 ES41 v točki (e), 4. odst., 6. člena predvideva postopek psevdonimizacije kot zaščitni ukrep v primeru, ko obdelava podatkov poteka za drug namen, kot so bili zbrani, in to brez privolitve posameznika.

Psevdonimizirane podatke je mogoče razvozlati samo z uporabo ključa za dešifriranje, zato je identifikacija brez ključa možna le s težavo. Ker pa povezava z identiteto še vedno obstaja v obliki psevdonima in ključa za dešifriranje, je ponovna identifikacija zlahka mogoča za vse, ki imajo pravico uporabljati takšen ključ. Zlasti je treba preprečiti, da bi šifrirne ključe uporabljale nepooblaščene osebe.

Primer psevdonimizacije:

»Stavek „Charles Spencer, rojen 3. aprila 1967, je oče štirih otrok, dveh dečkov in dveh deklic“ je na primer mogoče psevdonimizirati tako:

[39] Direktiva 95/46/ES z dne 24. oktobra 1995 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov, uvodna izjava 26.

[40] Konvencija št. 108 Sveta Evrope z dne 28. januarja 1981 o varstvu posameznikov glede na avtomatsko obdelavo osebnih podatkov, 42. člen.

[41] Uredba 2016/679/ES Evropskega parlamenta in Sveta z dne 27. aprila 2016 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), 6. člen.

„C. S., 1967, je oče štirih otrok, dveh dečkov in dveh deklic“ ali
„324 je oče štirih otrok, dveh dečkov in dveh deklic“ ali
„YESz320l je oče štirih otrok, dveh dečkov in dveh deklic“.

Psevdonimizacija osebnih podatkov je eden od najpomembnejših načinov za zagotovitev varstva osebnih podatkov v velikem obsegu; če se uporabi osebnih podatkov ni mogoče v celoti odreči. Na učinkovitost varstva osebnih podatkov vpliva metoda psevdonimizacije«[42].

[42] Agencija Evropske unije za temeljne pravice (FRA), Svet Evrope: Priročnik o evropskem pravu varstva osebnih podatkov, (2014), str. 43, 44.

4. Slovenske določbe varovanja osebnih podatkov

»Varstvo osebnih podatkov je v Republiki Sloveniji ena izmed ustavno zagotovljenih človekovih pravic in temeljnih svoboščin in spada v okvir pravic s področja zasebnosti. Ustavna ureditev varstva osebnih podatkov se opira zlasti na načela varstva osebnih podatkov, ki so vsebovana v Konvenciji o varstvu posameznika glede na avtomatsko obdelavo podatkov, ki je bila sprejeta v okviru Sveta Evrope. Konvencija pomeni izvedbo tiste določbe Konvencije o varstvu človekovih pravic in temeljnih svoboščin - EKČP, po kateri ima vsak pravico do spoštovanja svojega zasebnega in družinskega življenja, svojega doma in korespondence (prvi odstavek 8. člena).«[43]

4.1 Ustavno pravna ureditev

Ustava RS v 38. členu določa:

Zagotovljeno je varstvo osebnih podatkov. Prepovedana je uporaba osebnih podatkov v nasprotju z namenom njihovega zbiranja. Zbiranje, obdelovanje, namen uporabe, nadzor in varstvo tajnosti osebnih podatkov določa zakon. Vsakdo ima pravico seznaniti se z zbranimi osebnimi podatki, ki se nanašajo nanj, in pravico do sodnega varstva ob njihovi zlorabi.

»Iz besedila 38. člena Ustave RS izhajajo štiri načela: načelo zakonitosti, načelo namenskosti (oziroma načelo predhodne določitve namena), načelo seznanjenosti in načelo sodnega varstva. Ustavodajalec se je pri urejanju področja odločil za tako imenovani »obdelovalni model« in ne za tako imenovani »model zlorabe«, saj je določil predvsem pravila za urejanje dopustne obdelave osebnih podatkov na zakonski ravni in ne načelne svobode obdelave podatkov, ki je lahko le izjemoma izrecno omejena z zakonom. Takšen model pomeni, da je na področju obdelave osebnih podatkov prepovedano vse, razen tistega, kar je z zakonom izrecno dovoljeno. Vsaka obdelava osebnih podatkov namreč pomeni poseg v z Ustavo varovano človekovo pravico do varstva osebnih podatkov, zaradi česar je takšen poseg dopusten, če je v zakonu določno opredeljeno, kateri osebni podatki se smejo obdelovati, jasno pa mora biti razviden tudi namen obdelave osebnih podatkov ter zagotovljeno ustrezno zavarovanje. Namen obdelave osebnih podatkov mora biti ustavno dopusten, obdelovati pa se smejo le tiste vrste osebnih podatkov, ki so primerne in nujno potrebne za uresničitev zakonsko opredeljenega namena. Določba drugega odstavka 38. člena Ustave RS določa

[43] J. Čebulj, Varstvo osebnih podatkov in informacije javnega značaja, (2005), str. 19.

obveznost, da se zbiranje, obdelovanje, namen uporabe, nadzor ter varstvo tajnosti osebnih podatkov uredijo z zakonom.«[44]

4.2 Zakon o varstvu osebnih podatkov

Prvi zakon s področja varstva osebnih podatkov v Republiki Sloveniji je začel veljati leta 1990. Leta 1999 je bil zaradi približevanja k Evropski uniji in zahtev Direktive 95/46/ES Evropskega parlamenta in Sveta o zaščiti posameznikov pri obdelavi osebnih podatkov in o prostem gibanju takih podatkov sprejet nov Zakon o varstvu osebnih podatkov (Uradni list RS, št. 94/07, uradno prečiščeno besedilo, v nadaljevanju ZVOP-1).[45] ZVOP-1 določa pravice, obveznosti, načela in ukrepe, s katerimi se preprečujejo neustavni, nezakoniti in neupravičeni posegi v zasebnost in dostojanstvo posameznika pri obdelavi osebnih podatkov.

4.2.1 Razčlenitev pojmov

Za razumevanje določb ZVOP-1 ter za določanje obsega uporabe zakona je nedvomno bistvenega pomena razlaga izraza osebni podatek. »Izraz je v ZVOP-1 definiran kot katerikoli podatek, ki se nanaša na posameznika, ne glede na obliko, v kateri je izražen. Posameznik je v 2. točki ZVOP-1 definiran kot določena ali določljiva fizična oseba, na katero se nanaša osebni podatek; fizična oseba je določljiva, če jo lahko neposredno ali posredno identificiramo, predvsem s sklicevanjem na identifikacijsko številko ali na enega ali več dejavnikov, ki so značilni za njeno fizično, fiziološko, duševno, ekonomsko, kulturno ali družbeno identiteto, pri čemer način identifikacije ne povzroča velikih stroškov, nesorazmerno velikega napora ali ne zahteva veliko časa.«[46] Vse opisane karakteristike so značilne za delovanje pametne infrastrukture in pametnih naprav, ki nenehno beležijo podatke o posamezniku.

Za kasnejše razumevanje procesov velikega podatkovja je odločilen pojem obdelava osebnih podatkov. »Iz prvega člena zakona namreč izhaja, da se določbe ZVOP-1 uporabljajo le, kadar gre za obdelavo osebnih podatkov. Po definiciji iz 3. točke prvega odstavka 6. člena ZVOP-1 obdelava osebnih podatkov pomeni kakršno koli delovanje ali niz delovanj, ki se izvaja v zvezi z osebnimi podatki, ki so avtomatizirano obdelani ali ki so pri ročni obdelavi del zbirke osebnih podatkov ali so namenjeni vključitvi v zbirko osebnih podatkov, zlasti zbiranje, pridobivanje, vpis, urejanje, shranjevanje, prilagajanje ali spreminjanje, priklicanje,

[44] N. Pirc Musar, Zakon o varstvu osebnih podatkov (ZVOP-1) s komentarjem, (2006), str. 19, 20.
[45] N. Pirc Musar, Zakon o varstvu osebnih podatkov (ZVOP-1) s komentarjem, (2006), str. 21.
[46] N. Pirc Musar, Zakon o varstvu osebnih podatkov (ZVOP-1) s komentarjem, (2006), str. 58.

vpogled, uporaba, razkritje s prenosom, sporočanje, širjenje ali drugo dejanje na razpolago, razvrstitev ali povezovanje, blokiranje, anonimizacija, izbris ali uničenje. Obdelava je lahko ročna ali avtomatizirana.

Namen tako široke definicije obdelave osebnih podatkov je nedvomno v tem, da bi bilo področje uporabe ZVOP-1 zasnovano čim širše, saj definicija zajema praktično vsa ravnanja, ki jih je mogoče izvajati z osebnimi podatki.«[47] Pri tem je treba poudariti, da podatek ni isto kot informacija. »Podatek je znano dejstvo o določeni stvari, predmetu, pojavu, ki je temelj za sklepanje. Informacija pa je podatek, obdelan in prikazan na način, ki je uporabniku razumljiv in povečuje prejemnikovo znanje. Informacija je torej podatek, ki ima uporabno vrednost.«[48]

4.2.2 Privolitev

»Osebne podatke je možno in dopustno obdelovati, kadar je to določeno z zakonom ali na podlagi osebne privolitve posameznika. Osebna privolitev je lahko pisna, ustna ali druga ustrezna posameznikova privolitev. V določbi 8. člena ZVOP-1 je zajeta tudi določba točke (a) 7. člena Direktive 95/46/ES, po kateri države članice določijo, da se lahko osebni podatki obdelujejo samo, če je posameznik, na katerega se osebni podatki nanašajo, nedvoumno dal svojo privolitev. Direktiva postulira načelo, da je za vsako obdelavo osebnih podatkov potrebno posebno soglasje posameznika. Privolitev pa mora biti dana brez kakršnega koli dvoma. Če upravljavec ne razpolaga z izjavo volje posameznika, na katerega se osebni podatki nanašajo, domneva o privolitvi ni možna. Gre torej za tako imenovano prepoved s pridržkom dovolitve, ki velja za vsako obdelavo osebnih podatkov. Privolitev temelji na samostojni in prostovoljni odločitvi posameznika in je najpomembnejši element obdelave osebnih podatkov.«[49]

4.2.3 Pravna podlaga legitimnih interesov

Na področju interneta stvari in velikega podatkovja prihaja do zbiranja in obdelave osebnih podatkov predvsem s strani zasebnega sektorja. Pravno podlago za obdelavo osebnih podatkov v zasebnem sektorju nudi 10. člen ZVOP-1. Zasebni sektor ima večjo svobodo glede dopustnosti obdelave osebnih podatkov, kot pa jo pri obdelavi osebnih podatkov zakon dopušča javnemu sektorju.

[47] N. Pirc Musar, Zakon o varstvu osebnih podatkov (ZVOP-1) s komentarjem, 2006, str. 59, 60.
[48] N. Pirc Musar, Zakon o varstvu osebnih podatkov (ZVOP-1) s komentarjem, (2006), str. 60, 61, 62.
[49] N. Pirc Musar, Zakon o varstvu osebnih podatkov (ZVOP-1) s komentarjem, (2006), str. 75, 76, 80.

»V zasebnem sektorju velja načelo izenačenosti, saj je obdelava osebnih podatkov možna tako na podlagi zakona kot s posameznikovo osebno privolitvijo, pri čemer sta obe pravni podlagi izenačeni.

Privolitev kot pravno podlago po 1. odstavku 10. člena ZVOP-1 je v svetu podatkovnega izobilja pogosto težko ali pa vsaj neekonomično zagotoviti. Marsikatera koristna aplikacija, sistem, storitev ne bi mogla zaživeti, če bi se za njeno delovanje zahtevalo vnaprejšnjo informirano privolitev, pa čeprav bi bila ta posamezniku omogočena na čim bolj enostaven način (npr. s klikom na povezavo, odgovorom na SMS-sporočilo ipd.).« [50]

»Določba 3. odst. 10. člena ZVOP-1 konkretizira točko (f) 7. člena Direktive 95/46/ES, ki določa, da se osebni podatki obdelujejo, če je obdelava potrebna zaradi zakonitih interesov, za katere si prizadeva upravljavec ali tretja stranka ali stranke, ki so jim osebni podatki posredovani, razen kadar nad takimi interesi prevladajo temeljne pravice in svoboščine posameznika, na katerega se osebni podatki nanašajo, ki se varujejo na podlagi člena 1(1). Direktiva predvideva izčrpno tehtanje med interesi upravljavcev osebnih podatkov in interesi posameznikov na drugi strani. Obdelava osebnih podatkov pa mora biti vedno tudi potrebna in primerna (načelo sorazmernosti). Pri tem je treba upoštevati naslednje elemente:

- naravo in izvor legitimnih interesov upravljavcev in upravičenost njihovih pričakovanj;
- vpliv na posameznika in ogroženost interesov in pravic posameznika v smislu tega, kaj se bo zgodilo z njihovimi osebnimi podatki in kakšne posledice bo to imelo na posameznika ter
- varovalke, s katerimi je mogoče zmanjšati ali omejiti možne negativne posledice na zagotavljanja pravic posameznika, kot so minimizacija obdelave podatkov, anonimizacijske tehnike, povečana transparentnost, pravica do preklica obdelave podatkov in pravica do prenosljivosti podatkov.«[51]

4.2.4 Avtomatizirano odločanje

Celotna ideja pametnih mest, ki temelji na optimizaciji procesov tako na področju javne infrastrukture kot tudi v zasebnem življenju, pa ima lahko za posledico posredno

[50] A. Tomšič, Varstvo osebnih podatkov v dobi podatkovnega izobilja, (2014), str. 16.
[51] A. Tomšič, Varstvo osebnih podatkov v dobi podatkovnega izobilja, (2014), str. 17.

diskriminacijo in negativno selekcijo posameznikov na podlagi analize zbranih osebnih podatkov.

»ZVOP-1 ščiti posameznika, ki v obdobju modernih informacijskih tehnologij postaja vse prevečkrat objekt obdelave, zavedati pa se je treba, da je nevarnost zlorabe informatike pri oblikovanju odločitev ena glavnih nevarnosti, ki nam preti v prihodnosti. Rezultat, do katerega pride stroj in ki temelji na vedno bolj razviti programski opremi, ima zgolj na videz objektiven in nesporen značaj. Človek kot odločevalec mu zato lahko brez tehtnega premisleka pripisuje pretiran pomen in se na takšne rezultate celo preveč zanese. ZVOP-1 v 15. členu posameznika varuje pred takšnim avtomatiziranim odločanjem tako, da mu zagotavlja, da noben postopek ne bo zaključen zgolj na podlagi dejstev, pridobljenih z avtomatizirano obdelavo njegovih osebnih podatkov. Da bi obdelovalec osebnih podatkov storil kršitev določbe 15. člena, morajo biti izpolnjeni trije pogoji:

1. Posameznik mora biti podvržen odločitvi, ki ima zanj neugodne posledice, kot je avtomatizirano sprejeta zavrnitev prošnje za določeno storitev oziroma dostop do določenih luksuznih dobrin.
2. Odločitev, ki jo sprejme obdelovalec osebnih podatkov, se mora opirati izključno na avtomatizirano obdelavo. Programska oprema je lahko zgolj pripomoček za odločanje, v nobenem primeru pa ne sme biti edina podlaga za odločitev, ki povzroči posamezniku določene posledice. Vedno mora obstajati prostor za človeško presojo.
3. Obdelovalec osebnih podatkov mora s pomočjo avtomatizirane obdelave dobiti takšne podatke, ki posamezniku samodejno določijo neki osebnostni profil.

Da bi se posamezniku omogočilo uspešno ugovarjanje odločitvi, ki je sprejeta s pomočjo avtomatizirane obdelave njegovih osebnih podatkov, ter se mu s tem zagotovilo ustrezno varstvo njegovih zakonitih interesov, je v 7. točki prvega odstavka 30. člena ZVOP-1 še dodatno določeno, da mora upravljavec osebnih podatkov posamezniku na njegovo zahtevo pojasniti tehnične oziroma logično-tehnične postopke odločanja, če avtomatizirano odločanje izvaja z obdelavo osebnih podatkov posameznika. Kdor avtomatizirano obdeluje osebne podatke v nasprotju s 15. členom zakona, stori prekršek po 91. členu ZVOP-1.«[52]

[52] N. Pirc Musar, Zakon o varstvu osebnih podatkov (ZVOP-1) s komentarjem, (2006), str. 143–146.

4.2.5 Transparentnost

»Osnovni namen ZVOP-1 je zagotoviti čim večjo transparentnost na področju zbiranja osebnih podatkov. S tem namenom je v 19. členu ZVOP-1 določena dolžnost upravljavca, da posameznika obvešča o obdelavi osebnih podatkov. Upravljavec mora svoje dolžnosti informiranja izpolniti, četudi posameznik tega od njega ne zahteva.

Ta določba se razlikuje od določbe 30. člena ZVOP-1, ki določa, da mora za seznanitev posameznik postaviti ustrezno zahtevo, medtem ko je obveščanje posameznika ob zbiranju osebnih podatkov neposredno od njega ali od tretjih dolžnost upravljavca osebnih podatkov in pravica posameznika, ki je ni dolžan posebej uveljavljati.«[53]

[53] N. Pirc Musar, Zakon o varstvu osebnih podatkov (ZVOP-1) s komentarjem, (2006), str. 160.

5. Pogled evropskega prava na digitalizacijo mest

Temelj pametnega mesta predstavlja informacijska tehnologija. V tem poglavju obravnavam tri gradnike pametnega mesta (internet stvari, veliko podatkov in računalništvo v oblaku), ki poleg napredka pri zagotavljanju trajnostnega razvoja mest predstavljajo tehnološko grožnjo zasebnosti.

5.1 Glavni zakonodajni instrumenti varstva podatkov

»Varstvo osebnih podatkov in spoštovanje zasebnega življenja sta pomembni temeljni pravici. Evropski parlament že od nekdaj vztraja, da je treba najti ravnotežje med večjo varnostjo ter zaščito človekovih pravic, kamor sodi tudi varstvo podatkov in zasebnosti. Pravica do varstva osebnih podatkov ni absolutna pravica; v skladu z načelom sorazmernosti jo je treba obravnavati glede na vlogo, ki jo ima v družbi, in jo uravnotežiti z drugimi temeljnimi pravicami.

Pravno podlago varstva osebnih podatkov predstavljata Člen 16 Pogodbe o delovanju Evropske unije (nadalje: PDEU) ter Člena 7 in 8 Listine Evropske unije o temeljnih pravicah. Člen 16 PDEU določa, da Evropski parlament in Svet določita pravila o varstvu fizičnih oseb pri obdelavi osebnih podatkov s strani institucij, organov, uradov in agencij Unije ter držav članic pri dejavnostih s področja, za katere se uporablja pravo Unije.

Listina EU o temeljnih pravicah, ki je postala pravno zavezujoča 1. decembra 2009, pa v členih 7 in 8 priznava spoštovanje zasebnega življenja in varstvo osebnih podatkov kot tesno povezani, vendar ločeni temeljni pravici.

Prvi pravno zavezujoč mednarodni instrument predstavlja Konvencija št. 108 Sveta Evrope z dne 28. januarja 1981 o varstvu posameznikov glede na avtomatsko obdelavo osebnih podatkov, ki je bila sprejeta na področju varstva podatkov. Njen cilj je „zagotoviti [...] vsakemu posamezniku [...] spoštovanje njegovih pravic in temeljnih svoboščin in v tem okviru še posebej spoštovanje pravice do zasebnosti glede na avtomatsko obdelavo osebnih podatkov“.

Pred začetkom veljavnosti Lizbonske pogodbe je bila zakonodaja o varstvu podatkov na področju svobode, varnosti in pravice razdeljena med prvi steber (varstvo podatkov v zasebne

in poslovne namene, sprejemanje zakonodaje z uporabo metode Skupnosti) in tretji steber (varstvo podatkov za namene kazenskega pregona, sprejemanje na medvladni ravni). Stebrna struktura je bila odpravljena z Lizbonsko pogodbo, ki nudi trdnejšo podlago za razvoj jasnejšega in učinkovitejšega sistema varstva podatkov. Bistvene zakonodajne instrumente za obravnavanje interneta stvari, velikega podatkovja ter računalništva v oblaku predstavljata Direktiva 95/46/EC z dne 24. oktobra 1995 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter Direktiva 2002/58/ES, spremenjena leta 2009, o e-zasebnosti.

Direktiva 95/46/EC predstavlja osrednji del zakonodaje o varstvu osebnih podatkov v Evropski uniji. V njej so določena splošna pravila o zakonitosti obdelave osebnih podatkov in pravice posameznikov, na katere se osebni podatki nanašajo, predvideni pa so tudi neodvisni nacionalni nadzorni organi. V skladu s to direktivo mora posameznik dati izrecno privolitev in biti vnaprej obveščen, preden se njegovi podatki obdelujejo. Direktiva 95/46/EC bo razveljavljena maja 2018.

Ključni organ na področju zakonodaje varstva osebnih podatkov predstavlja Delovna skupina člena 29, ustanovljena na podlagi člena 29 Direktive o varstvu podatkov.«[54] Delovna skupina izdaja priporočila, mnenja in delovne dokumente, hkrati pa je odigrala ključno vlogo pri predlogu splošne uredbe o varstvu podatkov, Uredba (EU) 2016/679 Evropskega parlamenta in Sveta, z dne 27. aprila 2016, katere cilj je posodobitev in prenova določb iz Direktive o varstvu podatkov iz leta 1995. Uredba je začela veljati 25. 5. 2016, njene določbe pa se bodo morale neposredno uporabljati v vseh državah članicah v dveh letih. Splošna uredba 2016/679 naj bi zagotovila večje poenotenje pravil o varstvu osebnih podatkov v državah članicah EU. Poenotenje pravil bo omogočilo učinkovitejšo in enako zaščito posameznikov na ravni EU. Poenotenje pravil bo poleg dodatnih pravic, ki bodo omogočile boljšo zaščito informacijske zasebnosti in bodo natančneje opredeljene, privedlo tudi do enotnega razlagalca, ki bo skozi odločitve bolj prilagodljiv za hitre spremembe na področju informacijske tehnologije in njihovega posega v informacijsko zasebnost.

[54] K. Milt, Kratki vodič po Evropski uniji, Varstvo osebnih podatkov, (2016), URL: http://www.europarl.europa.eu/atyourservice/sl/displayFtu.html?ftuId=FTU_5.12.8.html, (1.10. 2016)

5.1.1 Katero pravo se uporabi?

Vprašanje, katero pravo uporabiti, ko gre za obdelavo osebnih podatkov, ki se zbirajo s pomočjo pametnih naprav, je zapleteno, kajti upravljavci podatkov lahko svojo dejavnost obdelave podatkov izvajajo v različnih državah. Prenos osebnih podatkov v države zunaj Evropske unije je problematičen, tako v primeru Direktive in tako bo tudi ostalo z začetkom veljavnosti Splošne uredbe. Razlog za to temelji na predvidevanju, da v državah zunaj EU področje varovanja podatkov ni urejeno v zadostni meri. Izjemo za določeno državo lahko naredi evropska Komisija, če prepozna standard varovanja podatkov kot dovolj visok.

Trenutna Direktiva o varstvu podatkov se uporabi v primeru, ko ima družba, ki v okviru svoje dejavnosti opravlja obdelavo osebnih podatkov, sedež znotraj Evropske unije. Direktiva se poleg tega uporabi tudi takrat, kadar ima družba sedež zunaj Evropske unije, posega pa po sredstvih, ki se nahajajo v državah Evropske unije. Direktiva s pojmom sredstva zaobsega vse povezane naprave, ki so namenjene pridobivanju ali nadaljnji obdelavi osebnih podatkov. Uporaba Direktive tako ni odvisna od lastništva naprave, temveč od obdelave podatkov.

5.2 Internet stvari (ang. Internet of Things)

Internet stvari, poznane tudi kot ubiquitous computing, sistem okoljske inteligence ali razširjena računalniška obdelava, imajo dolgo tradicijo v informacijski znanosti, razmeroma pozno pa je na njih postala pozorna pravna stroka. Opaziti je porast literature na temo potencialne grožnje, ki jo internet stvari predstavljajo za zasebnost posameznikov, in dvig javne zavesti o internetu stvari, predvsem v kontekstu pametnih mest kot orodja vsesplošnega nadzora.

Ključni problem interneta stvari v povezavi z varovanjem zasebnosti je, da so bile naprave z namenom oblikovane na način, da so uporabniku nevsiljive in neopazne. Vse to z željo, da vstopijo v naš vsakdanjik do trenutka, ko postanejo nenadomestljive in si življenja brez njih ne moremo predstavljati. Sistemi interneta stvari, kot sta na primer pametna osvetlitev dnevne sobe in pametni termostat (kot je učilni termostat NEST), so ustvarjeni z namenom nenehnega spremljanja potreb in želj uporabnika. Pri vstopu v določeno internetno stran oziroma družabno omrežje imamo možnost seznaniti se in odločiti, ali se strinjamo z zbiranjem podatkov. Pri internetu stvari je takšna notifikacija in možnost seznanitve pomanjkljiva.

Tudi v primerih, ko nevsiljivost in neopaznost naprave ni značilnost delovanja, naprave, povezane z internetom stvari, ne predvidevajo možnosti za prikaz obvestila o zasebnosti oziroma ne omogočajo izražanja jasnega in nedvoumnega soglasja. Uporabniki bi morali imeti vsaj teoretično možnost privoliti v politiko zasebnosti pred vstopom v storitev oziroma podpisom pogodbe za uporabo različnih pametnih naprav. Opaziti je, da v takšnih sistemih ustaljeni varnostni ukrepi soglasja v evropskem pravu varovanja osebnih podatkov ne delujejo. Zbiranje podatkov brez privolitve posega v pravico do informacijske samoodločbe posameznika, še posebej, ko gre za občutljive podatke, kot so na primer zdravstveni podatki.

Poseg v interese posameznika je urejen tako v nacionalni zakonodaji kot v direktivi EU. Potrebna pa je pravna ureditev posega v podatke v primeru novih tehnologij, kot je internet stvari. Delovna skupina člena 29, ki predstavlja neodvisen svetovalni organ Evropske komisije na področju varstva podatkov in zasebnosti, je v okviru svoje pristojnosti dajanja priporočil in mnenj že zavzelo stališče v zvezi z internetom stvari.

5.2.1 Internet stvari in evropsko pravo varstva osebnih podatkov

Internet stvari postavlja pravo varstva podatkov pred nove izzive. Klasični pristop varovanja osebnih podatkov je treba prilagoditi delovanju interneta stvari. Pri tem pa velja slediti štirim temeljnim načelom pridobivanja osebnih podatkov:

1. informiranju o obdelavi podatkov,
2. informiranju privolitve,
3. zahtevi po transparentnosti,
4. podatkovnim minimalizmom.

5.2.1.1 Obdelava podatkov

Uredba 2016/679 v uvodni izjavi 39 določa, da bi »način zbiranja, uporabe, pregledovanja ali drug način obdelave ter obseg obdelave ali prihodnje obdelave osebnih podatkov, ki se nanašajo na posameznike, moral biti pregleden za posameznika. Načelo preglednosti zahteva, da so vse informacije in sporočila, ki se nanašajo na obdelavo teh osebnih podatkov, lahko dostopne in razumljive ter izražene v jasnem in preprostem jeziku. [...]Posameznike bi bilo treba opozoriti na tveganja, pravila, zaščitne ukrepe in pravice v zvezi z obdelavo njihovih osebnih podatkov ter na to, kako lahko uresničujejo njihove pravice v zvezi s tako obdelavo. Zlasti posebni nameni, za katere se osebni podatki obdelujejo, bi morali biti izrecni in zakoniti ter določeni v času zbiranja osebnih podatkov.« Načelo preglednosti je pomembno predvsem,

ko posameznik od upravljavca želi pridobiti potrditev, ali se v zvezi z njim obdelujejo osebni podatki (15. člen Uredbe 2016/679). Prav tako pa mora upravljavec posamezniku, na katerega se nanašajo osebni podatki, zagotoviti pregledno poročilo o osebnih podatkih, ki se obdelujejo. To velja tudi v primeru, ko so bili podatki pridobljeni od posameznika, na katerega se nanašajo (13. člen Uredbe 2016/679), kot v primeru, ko podatki niso bili pridobljeni od posameznika, na katerega se nanašajo (14. člen Uredbe 2016/679).

V Uredbi 2016/679 so podrobno opredeljene splošne obveznosti upravljavcev in oseb, ki osebne podatke obdelujejo v njihovem imenu (obdelovalci). Uredba 2016/679 določa obveznost izvajanja ustreznih varnostnih ukrepov in obveznost uradnega obveščanja o kršitvah varstva osebnih podatkov**.** Tako 32. člen Uredbe 2016/679 od obdelovalcev zahteva sistemsko ureditev, ki ob upoštevanju tehničnih in organizacijskih ukrepov zagotavlja ustrezno raven varnosti. Pri tem Uredba 2016/679 uzakonja ukrep psevdonimizacije, ki ga Direktiva 95/46 ES ni predvidevala. Poleg tega 32. člen Uredbe 2016/679 predvideva številne ukrepe za zagotavljanje varnosti obdelave: šifriranje podatkov, zagotavljanje stalne zaupnosti in odpornost sistemov za obdelavo, pravočasno razpoložljivost in dostop do osebnih podatkov v primeru tehničnega incidenta ter redno testiranje, ocenjevanje in vrednotenje učinkovitosti tehničnih in organizacijskih ukrepov. S temi ukrepi se zlasti zagotovi, da osebni podatki niso samodejno dostopni nedoločenemu številu posameznikov.

Poleg preventivnih ukrepov za preprečitev vdora v zasebnost podatkov posameznika Uredba 2016/679 v 34. členu določa postopek v primeru kršitve varstva osebnih podatkov. Upravljavec je dolžan brez nepotrebnega odlašanja in najpozneje v 72 urah uradno obvestiti pristojni nadzorni organ (1. odst. 33. člena Uredbe 2016/679). Če kršitev varovanja osebnih podatkov pomeni veliko tveganje za pravice in svoboščine posameznikov, upravljavec brez nepotrebnega odlašanja sporoči posamezniku, na katerega se nanašajo osebni podatki, da je prišlo do kršitve varstva osebnih podatkov. V sporočilu je upravljavec dolžan jasno opredeliti vrsto kršitve ter informacije in ukrepe iz točk (b), (c) in (d) 3. odst. 33. člena Uredbe 2016/679.

5.2.2. Pravice posameznikov

5.2.2.1 Privolitev

V 2. členu Direktive za varstvo podatkov je opredeljena privolitev posameznika, na katerega se nanašajo osebni podatki. Kot privolitev se razume: »[…] vsaka prostovoljno dana posebna in informirana izjava volje, s katero posameznik, na katerega se osebni podatki nanašajo, izrazi soglasje, da se osebni podatki o njem obdelujejo.« Uporaba definicije iz 2. člena Direktive za varstvo podatkov v primeru interneta stvari naleti na težavo zaradi značilnosti delovanja naprav, ki se povežejo v sistem interneta stvari.

Delovna skupina člena 29 je poudarila številne težave v zvezi s privolitvijo in s samim dajanjem privolitve. Hkrati pa je opozorila na pomanjkljivo transparentnost v delovanju interneta stvari, saj se podatki v sistemu prenašajo med napravami avtomatično, brez vednosti uporabnika. Kot bistvo so poudarili, da je: »[…] možnost za odklonitev posredovanja podatkov internetu stvari zgolj teoretični koncept kot prava alternativa; taka situacija privede do vprašanja ali je uporabnikova privolitev v obdelavo podatkov lahko videna kot prostovoljna in veljavna na podlagi Evropskega prava.«[55]

Kot je že določala Direktiva 95/46ES, mora biti privolitev prostovoljna, specifična in ozaveščena. »Veljalo je, da je privolitev izjava volje, ta pa je lahko bila skladno s splošnimi pravili civilnega prava izjavljena tudi konkludentno, na primer z nadaljnjo uporabo spletne strani.«[56]

Uredba 2016/679 pa v 11. točki 4. člena opredeljuje nov pojem »informirane privolitve«, posameznika v obdelavo podatkov, ki od upravljavcev zahteva nedvoumno izjavo posameznika, ki temelji na predhodni ozaveščenosti. V Uredbi 2016/679 je tako predvideno, da je privolitev oblični pravni posel po vzoru oziroma v skladu z Direktivo o pravicah potrošnikov 93/13 EGS, ki od upravljavca zahteva vnaprej pripravljeno pisno izjavo o privolitvi, ki bi morala biti v razumljivi in lahko dostopni obliki ter jasnem in preprostem jeziku in ne bi smela vsebovati nedovoljenih pogojev.[57] Privolitev, ki bi temeljila na takšni

[55] Delovna skupina člena 29, Mnenje št. 8/2014 o najnovejšem razvoju na področju interneta stvari, (2014), str. 7.
[56] M. Podpečan, Prihodnost informacijske zasebnosti, v: Pravna praksa, 26(2015), str. 22.
[57] Uredba 2016/679/ES Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES, Uvodna izjava 42, str. 8.

pisni izjavi o privolitvi, bi izpolnila zahteve 7. člena Uredbe, ki določa, da mora biti privolitev dokazljiva, jasna ter dana prostovoljno.

Uredba 2016/679 v uvodni izjavi 171 ureja vprašanje veljavnosti pridobljenih privolitev na podlagi določb Direktive 95/46. Določa, da ni potrebe po ponovnem pridobivanju privolitve, če obdelava podatkov temelji na Direktivi 95/46 in ustreza pogojem za privolitev, kot so zapisani v Uredbi 2016/679. Hkrati pa Uredba 2016/679 v 3. odst. 7. člena dopušča posamezniku pravico do priklica privolitve v obdelavo osebnih podatkov. Pri tem preklic ne vpliva na zakonitost obdelave na podlagi privolitve pred njenim preklicem. Nejasno je, ali bodo pogodbe, ki prepovedujejo umik privolitve posameznika v času trajanja pogodbe, skladne z novo pravico do preklica privolitve, kot jo predvideva Uredba 2016/679. Postavlja se vprašanje, ali je teoretična pravica posameznika do preklica, ki jo zagotavlja Uredba, usklajena s tehnološkimi možnostmi?

Delovna skupina člena 29 je v svojem mnenju v zvezi z internetom stvari predlagala uvedbo pravice do prekinitve povezave oz. t. i. *right to be disconnected*.[58] Posameznik bi pravico uveljavljal na podlagi tehnične izbire, ki bi omogočala odjavo naprave s povezanega omrežja, pri čemer bi naprava nadalje delovala z razliko, da ni več povezana.

5.2.2.2 Zakonita obdelava

Za zagotavljanje zakonite obdelave osebnih podatkov mora biti podana privolitev posameznika ali pa je obdelava določena z zakonom. Pri tem pa je treba opozoriti, da v zakonu ni opredeljena prednost oziroma večja vrednost enega ali drugega temelja. Če je privolitev v skladu z evropskim pravom varstva podatkov nemogoča ali nesorazmerno draga, se ji upravljavci podatkov lahko v celoti »izognejo«.

Kjer se internet stvari uporablja v *namene preventive ali odkrivanja kriminala*, se podatki lahko pridobijo brez privolitve posameznika na podlagi 7(d). člena Direktive 95/46/ES. Prav tako lahko lokalne ali nacionalne agencije pridobijo podatke od e-upravnih sistemov, e-zdravstva, e-socialne podpore na *temelju javnega interesa*.

[58] Delovna skupina člena 29, Mnenje št. 8/2014 o najnovejšem razvoju na področju interneta stvari, (2014), str. 20.

Za večino komercialnih sistemov pa 7(f). člen Direktive 95/46/ES nudi široko polje interpretacije, saj določa, da se: »[…] osebni podatki lahko obdelujejo, če je obdelava potrebna zaradi zakonitih interesov, za katere si prizadeva upravljavec ali tretja stranka ali stranke, ki so jim osebni podatki posredovani, razen kadar nad takimi interesi prevladajo temeljne pravice in svoboščine posameznika, na katerega se osebni podatki nanašajo, ki se varujejo na podlagi člena 1(1).« Ta določba omogoča enostaven način, s katerim se upravljavec podatkov izogne nadzoru in privolitvi uporabnika.

Delovna skupina člena 29 je v mnenju 8/2014 poudarila sodbo v primeru *Google Španija in Google Inc. proti Agenciji za varstvo podatkov (Španija),* C-131/12, kjer je Sodišče Evropske unije odločilo, da obdelava podatkov, zbranih s pomočjo interneta stvari, ki se nanašajo na posameznikovo zdravstveno stanje, dom, zasebnost, lokacijo ali zasebno življenje, ne mora biti opravičena z razlogom ekonomskih interesov upravljavca storitve oz. naprave, ki se poveže z internetom stvari, saj je ekonomski interes treba gledati v primerjavi s temeljnimi svoboščinami lastnika podatkov.[59]

7. člen Direktive 95/46/ES se prekriva s 3. odst. 5. člena Direktive o zasebnosti in elektronskih komunikacijah (Direktiva 2002/58/ES), ki od objave revidirane verzije leta 2009 (Direktiva 2009/136/ES) zahteva, da je: »[…] shranjevanje podatkov ali pridobivanje dostopa do podatkov, shranjenih v terminalski opremi naročnika ali uporabnika, dovoljeno samo pod pogojem, da je zadevni naročnik ali uporabnik v to privolil po tem, ko je bil jasno in izčrpno obveščen v skladu z Direktivo 95/46/ES, med drugim o namenu obdelave. To ne prepreči nobenega tehničnega shranjevanja ali dostopa izključno za namen opravljanja prenosa sporočila prek elektronskega komunikacijskega omrežja.« S tem je privolitev edina možnost, ki omogoča legitimno shranjevanje podatkov, alternativa takšnemu pristopu ne obstaja. Pred privolitvijo, kot je opisana zgoraj, mora biti uporabnik *informiran* s predhodnim jasnim in izčrpnim obvestilom, ki pa ni treba, da je natančno. Ta določba je bila predvidena na začetku pojava e-trgovine, z namenom nadzora namestitve legitimnih piškotkov v računalnik uporabnika brez njegovega vedenja in privolitve. Do katere mere se ta določba uporablja v primeru zbiranja podatkov uporabnikov s pomočjo naprav povezanih z internetom stvari, ni znano.

[59] Delovna skupina člena 29, Mnenje št. 8/2014 o najnovejšem razvoju na področju interneta stvari, (2014), str. 15.

V času sprejemanja amandmajev k Direktivi 2002/58/ES o obdelavi osebnih podatkov in varstvu zasebnosti na področju elektronskih komunikacij leta 2009 so poizkušali dopolniti 3.odst. 5. člena Direktive 2002/58/ES v smeri razširitve in jasnejše uporabe še za druge vrste naprav, ne le za piškotke, zlasti za tako imenovane *rootkits*.[60]

Namera o razširitvi je rezultirala v uvodni izjavi 56 Direktive 2009/136/ES, ki je sedaj sledeča: »Če se take naprave priključi na javno dostopna elektronska komunikacijska omrežja ali če uporabljajo elektronske komunikacijske storitve kot osnovno infrastrukturo, bi se morale uporabljati ustrezne določbe Direktive 2002/58/ES, vključno z določbami o varnosti, podatkih o prometu in lokaciji ter o zaupnosti.«

Vprašanje je, ali je 3. odst. 5. člena Direktive 2002/58/ES uporaben za informacije, zbrane o uporabnikih s pomočjo naprav povezanih z internetom stvari, kot so na primer RFID-čipi. Vprašanje temelji na dveh predpostavkah:
1. ali so informacije shranjene v terminalski opremi,
2. ali je omrežje, v katerem se nahaja naprava, ki je povezana z internetom stvari, dovolj javno po določbi uvodne izjave 56, ki razširja domet 3. odst. 5 člena na »naprave, priključene na javno dostopna elektronska komunikacijska omrežja.

Delovna skupina člena 29 primeroma navede,[61] kdaj so podatki zbrani s pomočjo interneta stvari, shranjeni v terminalski opremi. V mnenju je naveden primer pametnega pedometra, ki ga uporabnik nosi na sebi, pri tem šteje korake, beleži lokacijo in se periodično sinhronizira z internetom. To delovanje verjetno kaže na to, da se informacije v času zbiranja shranijo v terminalski opremi uporabnika, četudi se kasneje naložijo v infrastrukturo oblaka, ki je v lasti proizvajalca pedometra. Privolitev na podlagi 3. odst. 5. člena Direktive 2002/58/ES bi bila zato potrebna.

Vprašanje, kdo je uporabnik, se postavi, ko naletimo na pametne naprave, za katere ne vemo, kdo je uporabnik, ali je to oseba, ki je na primer v pametnem vozilu brez voznika, prodajalec vozil brez voznika, ali pa je to operater/proizvajalec pametnega vozila. Delovna skupina meni, da bi tudi v takem primeru bilo potrebno privoljenje posameznika, ki uporablja tako vozilo.

[60] slovensko: korenski komplet, gre za programsko opremo, ki omogoča prikrit dostop do računalniškega sistema in uporabo skrbniških pravic, običajno zlonamerno.
[61] Delovna skupina člena 29, Mnenje št. 8/2014 o najnovejšem razvoju na področju interneta stvari, (2014), str. 14.

Druga točka, ki se pojavi v povezavi s 3. odst. 5. člena Direktive 2002/58/ES in razširitvijo učinkovanja privolitve, ki je opredeljen z uvodno izjavo 56 Direktive 2009/136/ES, je zbiranje informacij s pomočjo naprav, ki so povezane z »javno dostopnim elektronsko komunikacijskim omrežjem«. Če je pametno mesto vzpostavljeno s pomočjo zasebnih korporacij (npr. Cisco, Siemens) in sistemov, ki delujejo na zasebnih omrežjih, se postavi vprašanje, ali je pravica iz 3. odst. 5. člena Direktive 2002/58/ES uporabljiva.

Evropski nadzornik za varstvo podatkov je izrazil kritiko na dopolnitev Direktive 2002/58/ES, ki v uvodno izjavo 56 ni vključila dikcije, da se 3. odst. 5. člena Direktive 2002/58/ES uporabi za vsa » javno dostopna zasebna omrežja«. Področje Direktive 2002/58 ES, ki obravnava varstvo temeljnih pravic in svoboščin pri obdelavi osebnih podatkov je, po sprejetju Uredbe potrebno spremeniti v smeri, da bo skladno z novimi določbami Uredbe.

5.2.3. Transparentnost

Eno izmed vodil Uredbe 2016/679 je nadzor in preglednost nad obdelovanjem osebnih podatkov. Transparentnost posamezniku omogoči, da dobi vpogled v obdelovanje osebnih podatkov, in sicer tako, da je vsaka informacija, ki se nanaša na obdelovanje osebnih podatkov, preprosto dostopna in razumljiva ter da je uporabljen običajen jezik. Poleg novih pravic, ki jih prinaša Uredba 2016/679, ima posameznik za uresničitev namena transparentnosti na razpolago pravice, ki so bile vzpostavljene že z Direktivo 95/46, to je pravica dostopa do osebnih podatkov ter pravice do popravka in ugovora podatkov.

Uredba 2016/679, katere poglavitni cilj je povrnitev informacijske zasebnosti posameznikom, v svojih določbah predvideva dve novi pravici, in sicer pravico do pozabe oz. izbrisa (17. člen) in pravico do prenosljivosti podatkov (20. člen). »Pravica do pozabe izhaja iz znane sodbe *Google Španija in Google Inc. proti Agenciji za varstvo podatkov (Španija),* C-131/12 in omogoča posameznikom, da zahtevajo izbris osebnih podatkov pod določenimi pogoji. V 1. odstavku 17. člena so od točke a do f zapisani ti primeri. Gre npr. zato:

- da podatki niso več potrebni za namen, zaradi katerega so bili zbrani ali obdelani,
- da posameznik prekliče privolitev in ne obstaja druga podlaga,
- da so podatki obdelani nezakonito itn.

Druga pravica iz 20. člena pa zagotavlja, da je posameznik upravičen pridobiti podatke, za katere zaprosi, v strukturirani, splošno uporabljani in strojno berljivi obliki, in pravico, da te

podatke posreduje drugemu upravljavcu, ne da bi ga upravljavec, ki so mu bili osebni podatki zagotovljeni, pri tem oviral (prvi del te pravice dejansko omogoča prenos podatkov k drugemu upravljavcu).«[62]

5.2.4. Podatkovni minimalizem

Splošna uredba v točki (c) 1. odst. 5. člena opredeljuje načelo najmanjšega obsega podatkov, ki zahteva, da se obdelujejo le podatki, ki zadostujejo, so odločilni in po obsegu ne pretirani glede na način obdelovanja podatkov. »Načelo se nanaša na katero koli dejavnost, katere cilj je zmanjšanje obsega zbranih osebnih podatkov do obsega, ki je relevanten in potreben za dosego namena zbiranja. To načelo se lahko uresniči s pomočjo pesevdonimizacije ali nadaljnje obdelave, ki ne omogoča identifikacije posameznikov, na katere se nanašajo podatki.«[63]

5.2.5 Alternativa soglasju

5.2.5.1 Načelo vgrajene zasebnosti (ang. Privacy by design)

Alternativo tradicionalni privolitvi gre iskati v načelu vgrajene zasebnosti. To načelo pomeni, da se varstvo zasebnosti vgradi že v fazi oblikovanja značilnosti tehnike, poslovnih praks in fizične infrastrukture. Načelo vgrajene zasebnosti vključuje naslednje rešitve: omejevanje količine podatkovnih aplikacij na minimum, privzeto šifriranje podatkovnih tokov, anonimizacijo osebnih podatkov, vgradnjo obvestila o zasebnosti v sistem na način, ki je uporabniku prijazen, omejitev obdobja hrambe podatkov, zagotovitev nastavitve zasebnosti v meniju na način, ki je jasen in uporabniku prijazen.[64]

25. člen Uredbe 2016/679 opredeljuje zahteve, ki jih morajo upoštevati ponudniki programske opreme že v stopnji razvoja oziroma zahteve, ki jih morajo upoštevati tisti, ki obdelujejo osebne podatke: »[…] upravljavec tako v času določanja sredstev obdelave kot tudi v času same obdelave izvaja ustrezne tehnične in organizacijske ukrepe, kot je psevdonimizacija, ki so oblikovani za učinkovito izvajanje načel varstva podatkov, kot je načelo najmanjšega obsega podatkov, ter v obdelavo vključi potrebne zaščitne ukrepe, da se izpolnijo zahteve te uredbe in zaščitijo pravice posameznikov, na katere se nanašajo osebni podatki. Upravljavec

[62] M. Jesenko, GDPR, General Data Protection Regulation-Splošna uredba o varstvu podatkov, 26(2016),URL: http://www.insolvinfo.si/DnevneVsebine/Aktualno.aspx?id=169812
[63] M. Podpečan, Prihodnost informacijske zasebnosti, v: Pravna praksa, 26(2015), str. 6 priloga.
[64] L. Edwards, Privacy, Security and Data Protection in Smart Cities: a Critical EU Law Perspective, v: CREATe Working Paper, 11(2015), str. 27.

izvede ustrezne tehnične in organizacijske ukrepe, s katerimi zagotovi, da se privzeto obdelajo samo osebni podatki, ki so potrebni za vsak poseben namen obdelave. […] S takšnimi ukrepi se zagotovi zlasti, da osebni podatki niso samodejno dostopni nedoločenemu številu posameznikov brez posredovanja zadevnega posameznika.

Sedem vodil načela vgrajene zasebnosti:

1. Namen je preventiva.
2. Varstvo podatkov kot standardna storitev (»Privacy by Default«).[65]
3. Varstvo podatkov je predvideno pri oblikovanju.
4. Celostna funkcionalnost.
5. Neprekinjena varnost skozi celoten življenjski ciklus.
6. Vidnost in transparentnost.
7. Ohranitev zasebnosti uporabnikov – skrb za oblikovanje osredotočenosti na uporabnika.

V kolikšni meri bodo ta temeljna vodila pripomogla k tehnični implementaciji varstva podatkov v naprave, bo treba še počakati.

5.2.5.2 Lepljiva zasebnost (ang. Sticky policy)

Lepljiva zasebnost predstavlja smernice, ki po eni strani definirajo, kdo lahko dostopa do podatkov in v kakšne namene se podatki lahko uporabljajo, po drugi strani pa stalno spremlja podatke posameznika in nastopa vedno skupaj s podatki v sistemu. Ideja je, da odločitve v zvezi z zasebnostjo, ki jih uporabnik enkrat sklene, ostanejo v spominu pametnega sistema in stopijo v veljavo v trenutku, ko se sistem sooča z dejavniki zasebnosti. Razvoj lepljive zasebnosti gre v smeri, ki bi omogočala, da ko uporabnik v eni napravi določi zasebnost, se ta nastavitev prinese na novo pridobljene pametne naprave uporabnika. Zaradi stalnega spremljanja nastavitev zasebnosti podatkov posameznika bi bil pristop zanimiv za ohranitev zahtev po privolitvi kot pravni podlagi za obdelavo osebnih podatkov.[66]

[65] Načelo privzete zasebnosti (ang. Privacy by Default) določa, da so v zvezi s pametnimi napravami in aplikacijami privzete take nastavitve, ki od začetka uporabe zagotavljajo najširši obseg varstva osebnih podatkov, zlasti pa minimizirajo potrebo po obdelovanju osebnih podatkov.

[66] L. Edwards, Privacy, Security and Data Protection in Smart Cities: a Critical EU Law Perspective, v: CREATe Working Paper, 11(2015), str. 33.

5.2.5.3 Izboljšani načini tradicionalnega obveščanja in izbire

Tradicionalno obveščanje in izbire lahko dosežemo na naslednje načine:

- s preusmeritvijo uporabnika k video programu za pomoč pri vodenju skozi nastavitve zasebnosti;
- dom ali druge lokacije bi bile opremljene z detajlnim nadzorom »portali upravljanja«, kjer bi uporabniki lahko ponovno pregledali, kateri podatki so bili izbrani za nadaljnje posredovanje različnim aplikacijam preko različnih naprav;
- z vključitvijo QR-kod v IoT-naprave, pri čemer bi uporabnik s pomočjo pametne naprave skeniral kodo in s tem enostavno dostopal do politik zasebnosti ali drugih karakteristik varstva podatkov;
- zagotoviti je treba ikone, ki bi uporabnika opozorile na posredovanje informacij, ki se nanašajo na osebne podatke, ali prikaz svetlobnega signala, ko se IoT naprava poveže z internetom;
- omogočiti je treba uporabnikom, da so sprotno obveščeni o nastavitvah zasebnosti in varnosti, ti podatki so jim lahko posredovani preko SMS-obvestila ali e-maila.[67]

5.3 Veliko podatkovje (ang. Big Data)

Veliko podatkovje kot tudi pametno mesto sta moderni besedi, ki se velikokrat omenjata, a nimata jasnega pomena. Pogosto jih povezujemo z besedami, kot so: volumen, hitrost in raznolikost, s poudarkom na volumnu. Veliko podatkovje je prišlo v ospredje zaradi treh razlogov: stroški shranjevanja in obdelave so močno upadli, algoritmi za analizo velikih količin podatkov so izboljšani in (najpomembnejše) spletna podatkovna industrija in kasneje IoT-industrija sta ustvarili neverjetno velik zbir podatkov.

Pametna mesta ustvarjajo veliko podatkovje in delujejo s pomočjo njihove obdelave. V obeh primerih ni nujno, da veliko podatkovje vsebuje osebne podatke, čeprav bo temu skoraj vedno tako. Tudi v primeru, ko se podatki zbirajo v navidezni anonimnosti, kot na primer zvok koraka na trgu, se relativno enostavni dogodek poveže z dvema velikima bazama podatkov – baza podatkov, ki meri zvok koraka, in baza podatkov sistema televizije zaprtega kroga, ki omogoča identifikacijo posameznikov. Izkopavanje podatkov iz več kot enega niza podatkov iz različnih virov omogoča vzpostavitev identitete iskane osebe tudi v primeru, da so bili narejeni poskusi de-identifikacije. Razlog za to je učinek mozaika.

[67] L. Edwards, Privacy, Security and Data Protection in Smart Cities: a Critical EU Law Perspective, v: CREATe Working Paper, 11(2015), str. 31.

Ključne skrbi pri velikem podatkovju v povezavi z varovanjem osebnih podatkov so naslednje:

- možnost za reidentifikacijo domnevno anonimiziranih ali psevdonimiziranih podatkov,
- uporaba zbranih podatkovnih zbirk v namen, ki se razlikuje od osnovnega,
- pomanjkanje transparentnosti, predvsem težava v zvezi s pridobljenimi rezultati na podlagi obdelanih podatkov,
- masovno zbiranje podatkov.

Poleg tega obstaja posebna skrb v povezavi s posredno in netransparentno diskriminacijo, ki temelji ta na analizi podatkov in lahko pripelje do razvrščanja oseb na razrede glede na njihovo podatkovno analizo. Ta posredna diskriminacija lahko vodi v to, da posamezniki z značilnim profilom velikega podatkovja ne bi imeli dostopa do določenih storitev oziroma objektov.

5.3.1 Veliko podatkovje in evropsko pravo

Pravo varstva podatkov s tematiko velikega podatkovja pride v navzkriž v treh točkah: omejitev namena zbiranja podatkov, algoritmična transparentnost ter zmanjšanje obsega zbiranja podatkov. Pravo varstva podatkov temelji na ideji, da morajo biti podatki pridobljeni za *določne, izrecne in zakonite namene* in ne z namenom nadaljnje obdelave, ki je nezdružljiva s prvotnim namenom. Načelo omejitve namena se uporabi v primeru, ko obdelava ni bila odobrena na podlagi privolitve, temveč na nekem drugem temelju. Veliko podatkovje deluje v nasprotju s tem načelom.

Mayer-Schoenberger in Cukier[68] v svoji knjigi Big data poudarjata, da kljub kršenju načela omejenega namena obstajajo številne druge zakonite strategije, ki bi velikemu podatkovju lahko omogočile nadaljnjo obdelavo podatkov. Kot primer navajata privolitev v »verjetno« ponovno uporabo na začetku in v primeru potrebe po nadaljnji obdelavi pridobitev celostne privolitve. Kot možnost navedeta tudi temelj legitimnega interesa. Oba predloga se zdita navidezna. Blanketna privolitev v nadaljnjo uporabo podatkov bi bila nedoločna do te mere, da ne bi prestala testa zakonite obdelave osebnih podatkov. Kar je bolj problematično, je to, da podatkovno rudarjenje daje odgovore na vprašanja, na katere ob iskanju sploh nismo

[68] V. Mayer-Schoenberger, K. Cukier, Big Data: A Revolution That Will Transform How We Live, Work and Think , (2013), str. 15.

pomislili. Pri tem ne bi šlo le za iskanje odgovorov iz znanega na neznano, temveč iz neznanega na neznano.

Drug pomemben dejavnik je transparentnost obdelave in predstavlja temelj prava varovanja podatkov. Transparentnost je težava velikega podatkovja, saj le-to deluje kot črna omarica; podatki vstopajo, izstopi obdelan podatek, vmes je algoritem, ki ustvari rezultat. Algoritmi se nadgrajujejo in spreminjajo, zaradi česar jih je težko dokumentirati. Poleg tega algoritmi predstavljajo tržno skrivnost. Netransparentni algoritmi velikega podatkovja so nevarni, saj diskriminacija, ki bi bila drugače prepovedana (podatki o rasi in o spolni orientaciji), ostane nevidna za tančico algoritmov.

Pravica, ki je opredeljena v 3. odstavku 38. člena Ustave RS in določa, da ima vsakdo pravico seznaniti se z zbranimi osebnimi podatki, ki se nanašajo nanj, je obveščeni javnosti dobro znana, le redkim pa je znana pravica, zagotovljena na podlagi Direktive 95/46/ES.

Direktiva v 12.(a) členu posamezniku omogoča pridobitev informacij o logiki, zajeti v avtomatizirani obdelavi podatkov. Poimenovali bi jo lahko *algoritmična transparentnost*. Kako se ta pravica uveljavi in uporabi za varovanje uporabnika, je težko reči. Četudi upravljavec ve, po kakšnem ključu algoritem deluje, je vprašanje, kako naj to informacijo sporoči v razumljivi obliki. Mayer-Schoenbeger in Cukier predlagata, da se uvede nov poklic »algoritmista«, ki bi deloval neodvisno od upravljavca in katerega naloga bi bila interpretacija rezultatov povprečnemu uporabniku.

Tretji dejavnik velikega podatkovja, ki nasprotuje principom prava varstva podatkov, je, da mora biti zbiranje osebnih podatkov ustrezno, relevantno in omejeno na to, kar je potrebno za namene, za katere se obdelujejo. To načelo najmanjšega obsega podatkov je na novo urejeno v 5.(c) členu Uredbe 2016/679.

Minimizacija podatkov predstavlja omejevanje informacijske znanosti, saj je razvoj velikega podatkovja pripeljal do tega, da je cenejše, enostavnejše in bolj uporabno, da se zberejo vsi podatki z namenom, da bodo prišli v poštev v prihodnosti.

»Delovna skupina priznava, da izzivi velikega podatkovja zahtevajo inovativno razmišljanje glede uporabe ključnih načel varovanja podatkov v praksi. Kljub temu v tem trenutku ni

razloga za skrb, da načela evropskega prava varovanja podatkov, kot so zastavljena danes v Direktivi 95/46/ES, ne bi bila veljavna in primerna za razvoj velikega podatkovja«.[69]

5.4 Računalništvo v oblaku (ang. Cloud)

Končni člen v verigi množičnega zbiranja in shranjevanja podatkov predstavlja računalništvo v oblaku. Računalništvo v oblaku temelji na ideji, ki je v telekomunikacijah že dolgo poznan kot abstrakcija infrastrukture, platforme in storitev. Pomembna razloga za njegov razmah sta vedno večja razširjenost širokopasovnih povezav ter napredek na področju virtualizacije strojne opreme, ki danes omogoča popolno avtomatizacijo in optimizacijo delovanja velikih strežniških farm.

Inštitut NIST (National Institute of Standards and Technology) računalništvo v oblaku opredeljuje kot »model za zagotavljanje omrežnega dostopa do deljenega nabora računalniških virov (kamor sodijo omrežja, strežniki, diskovni prostor, aplikacije in storitve), ki jih je mogoče hitro pripraviti za uporabo in hitro sprostiti, oboje z minimalnim trudom in z minimalno interakcijo ponudnika storitve«.[70]

Ključna zahteva za preživetje takšnega sistema v širšem IKT-ekosistemu je širokopasovna omrežna povezava od uporabnika do infrastrukture v oblaku, kar je eden od razlogov za dokaj pozen razmah koncepta računalništva v oblaku. Podatki, ki se nahajajo v oblaku, imajo po navadi neznano in spremenljivo mesto shranjevanja in obdelave, pogosto pa so podatki posredovani v obdelavo v številne pravne rede. Mogoče je pogodbeno določiti, da se podatki shranijo in obdelajo na območju EU, a takšna vrsta pogodbenega urejanja je na uporabniškem trgu izjema. Poleg tega pa obstajajo razlogi, ki onemogočajo pogodbeno urejanje npr. logistika, saj na trgu prevladujejo ameriške korporacije, hkrati pa na območju EU primanjkuje razvoj industrije računalništva v oblaku. Razširjenost računalništva v oblaku za shranjevanje in obdelavo podatkov odpira veliko vprašanj v zvezi s tem, katero pravo naj uporabimo.

[69] Mnenje, na mnenje delovne skupine člena 29 o vplivu razvoja velikega podatkovja na varstvo zasebnosti posameznikov glede na obdelavo njihovih osebnih podatkov v EU, (16. 9. 2014), str. 2, URL: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp221_en.pdf

[70] E. Brown, Final Version of NIST Cloud Computing Definition Published, (24. 10. 2011), URL: https://www.nist.gov/news-events/news/2011/10/final-version-nist-cloud-computing-definition-published

5.4.1 Računalništvo v oblaku in evropsko pravo

Direktiva varovanja zasebnosti zagotavlja prost pretok osebnih podatkov v države zunaj Evropskega gospodarskega prostora pod pogojem, če država oziroma prejemnik zagotavlja ustrezno stopnjo varstva podatkov. Vse to z namenom omejitve čezmejnega prenosa podatkov.

Ustrezna raven varstva je opredeljena v 2. odst. 25. člena Direktive 95/46/ES in se oceni glede na vse okoliščine, ki so povezane s postopkom prenosa ali z nizom postopkov prenosa podatkov; predvsem je treba upoštevati značaj podatkov, namen in trajanje predlaganega postopka ali postopkov obdelave, državo izvora in ciljno državo, pravno ureditev – bodisi splošno ali sektorsko – ki je v veljavi v tretji državi ter strokovne predpise in varnostne ukrepe, ki se uporabljajo v tej državi.

Odstop od tega načela predstavlja 26. člen Direktive 95/46/ES, ki odstop dovoljuje na temelju privolitve osebe, na katero se podatki nanašajo, standardnih pogodbenih klavzul, zavezujočih poslovnih pravil ter na podlagi Direktive o varnem pristanu. Ta je podjetjem dovoljevala izvoz osebnih podatkov o evropskih uporabnikih v Združene države Amerike.

Shema »varnega pristana« se je uporabljala do jeseni 2015, ko je Sodišče Evropske unije dogovor razveljavilo. ZDA torej trenutno niso vključene na seznam tistih držav iz 66. člena ZVOP-1, za katere je ugotovljeno, da delno zagotavljajo ustrezno raven varstva osebnih podatkov. To pa pomeni, da mora vsaka organizacija pred iznosom podatkov pridobiti dovoljenje pooblaščenca (razen v primeru pravnih podlag iz 1. odstavka 70. člena ZVOP-1). Evropska podjetja, ki izvažajo osebne podatke, se morajo zavedati, da sama nosijo odgovornost za oceno zakonitosti iznosa in nadaljnje obdelave ter da morajo poskrbeti, da so pri vsakokratnem iznosu osebnih podatkov zajeta in spoštovana vsa načela evropskega varstva osebnih podatkov, kot jih opredeljuje Listina EU o temeljnih pravicah, pogodbe in Direktiva 95/46/ES.

Možna rešitev za evropska pametna mesta bi bila izgradnja evropskega oblaka, tudi šengenskega oblaka. Evropsko partnerstvo računalništva v oblaku (tudi: European Cloud Partnership, ECP) je bilo ustanovljeno leta 2012 na podlagi Evropske strategije za računalništvo v oblaku in predstavlja eno od 16 iniciativ Strategije enotnega digitalnega trga.

»Cilj ECP do leta 2016 je vzpostavitev evropskega oblaka za odprto znanost, ki je namenjen evropskim raziskovalcem in njihovim znanstvenim sodelavcem po vsem svetu. Evropski oblak za odprto znanost in evropska podatkovna infrastruktura ne bosta dostopna le skupnosti evropskih raziskovalcev, ampak tudi vrsti drugih uporabnikov, ki bodo tako lahko izkoristili njune prednosti:

- Podjetjem bo omogočen cenovno ugoden in lahek dostop do vrhunskih podatkov in računalniške infrastrukture, pa tudi do bogate zakladnice znanstvenih podatkov, ki bodo odprli pot do podatkovno vodenih inovacij. To bo še posebej koristilo malim in srednjim podjetjem, ki jim taki viri po navadi niso na razpolago.
- Industriji bo koristil obsežen ekosistem v oblaku, saj bo njegov nastanek pripomogel k razvoju novih evropskih tehnologij, kot so energijsko varčni čipi za visoko zmogljivo računalništvo.
- Javnim službam bo koristil zanesljiv dostop do zmogljivih računalniških virov in vzpostavitev platforme, na kateri bodo lahko odprle svoje podatke in storitve. Tako bodo javne službe lahko cenejše in boljše, povezava med njimi pa hitrejša. Tudi raziskovalci bodo lahko izkoristili spletni dostop do bogate zakladnice podatkov, ki jih ustvarjajo javne službe«.[71]

71 Evropska komisija, European Cloud Initiative to give Europe a global lead in the data-driven economy, (19. 4. 2016), URL: http://europa.eu/rapid/press-release_IP-16-1408_sl.htm

6. Položaj organov pregona v pametnih mestih

Želja po sodelovanju organov pregona z zasebnimi podjetji ni nova. Osebni podatki, zbrani s strani zasebnih podjetij, so lahko nujni za preprečitev, odkrivanje, preiskovanje in pregon kaznivega dejanja. Število naprav, ki so povezane z internetom, je vsak dan večje, kar organom pregona omogoča, da uporabijo te naprave z namenom razrešitve kaznivih dejanj. Brezžične kamere in mikrofoni, ki so vgrajeni v naprave, lahko omogočijo snemanje glasu ali zaznajo gibanje lastnika oziroma osumljenca.

6.1 Načini dostopa do podatkov

Zasebna podjetja lahko na različne načine posredujejo podatke javnim oblastem, vključno organom pregona. V večini evropskih pravnih redov si organi pregona pridobijo odločbo sodišča za pridobitev želenih podatkov s strani zasebnih podjetij. Poleg ustaljene pravne prakse pa se uveljavljajo tudi drugi načini, s katerimi je organom pregona omogočen dostop do podatkov, zbranih s strani zasebnih podjetij. Tako je posredovanje podatkov lahko prostovoljno ali zavezujoče, temelječe na pogojih, ki jih določa nacionalno pravo ali na podlagi multi-ali bilateralnih dogovorov. Posredovanje tako lahko temelji tudi na pogodbi, sklenjeni med organom pregona ter zasebnim podjetjem.

Posebno področje predstavljajo podatki odprtega dostopa, ki ne zahtevajo posredovanja podatkov. Organi pregona do teh podatkov dostopajo, ne da bi prišlo do realnega prenosa podatkov. Gre za podatke, ki niso omejeni na točno določen krog oseb, prav tako pa ni nujno, da so ti podatki natančni in zanesljivi.

Podatki izvirajo od zasebnih podjetij in vključujejo sivo literaturo, časopisne članke in socialne medije. Odprti podatki ne predstavljajo novega koncepta, razlog, da so odprti podatki pridobili pomen, je poplava informacij, ki so rezultat socialnih medijev in drugih virov na internetu. Pri tem pa je treba opozoriti, da odprti podatki vključujejo podatke, ki onemogočajo identifikacijo osebnih podatkov, saj tudi za odprte podatke velja Direktiva 95/46/ ES.[72]

Vse te različne pravne podlage, ki omogočajo prenos podatkov, se izražajo v vrsti razmerja med strankama, ki vpliva sam način prenosa podatkov in uporabnosti podatkov po prenosu.

[72] E. de Busser, Private companies and the transfer of data to law enforcement authorities: Challanges Data Protection, v: Maastricht Journal, 3(2016), str. 481–483.

6.2 Analitika velikih podatkov in organi pregona

6.2.1 Prevencija

Digitalna revolucija vpliva tudi na način delovanja policije. Znanstveno fantastični triler »Minority Report« v filmu prikazuje metodo, ki jo bodo v prihodnje uporabljali tudi organi pregona. Z modelom napovedovanja zločina (ang. Predictive Policing) bodo oblasti v prihodnje nadzorovale in identificirale socialna žarišča. Model napovedovanja zločina je oblika predvidljive analitike (ang. Predictive Analytics), ki na podlagi podatkovnih modelov predvideva, kako se bo oziroma se lahko določena situacija v prihodnosti razvije.

S pomočjo te tehnologije organi pregona ugotavljajo, kdaj in kje se bo zgodilo kaznivo dejanje, z namenom preventivnega delovanja. Vse to se naredi s pomočjo programske opreme, ki analizira veliko količino podatkov in statistik, jih primerja, išče vzorce in identificira možne kraje in čas kaznivega dejanja. Četudi se ves postopek sliši zelo avtomatiziran, je model napovedovanja zločinov odvisen od ljudi. Organi pregona morajo program neprestano osveževati z novimi podatki, z namenom zagotavljanja ažurnosti, poleg tega pa mora biti policija prisotna na analiziranem kraju kaznivega dejanja.

Pilotni projekt modela napovedovanja zločina se je izvedel leta 2010, v kalifornijskem mestu Santa Cruz. Od takrat program razporeja delovanje 100 policistov v 15 območij, ki izkazujejo visok potencial za nastanek kaznivih dejanj. Programska oprema napovedovanja zločina je bila zasnovana s strani matematika George Mohlerja in antropologa Jeffreyja Brantinghama. Pri tem uporaba temelji na matematični formuli za ugotavljanje popotresnih sunkov. Mohler je izhajal iz teorije, da se kriminalec, ki je uspešno izvedel kaznivo dejanje, vrne na kraj kaznivega dejanja z namenom ponovitve, kar je identično z nastankom popotresnih sunkov, ki sledijo po predvidljivih prelomnih črtah in intervalih.[73]

6.2.2 Preiskovanje kaznivih dejanj

Dejstvo je, da naprave, ki so povezane z internetom stvari, prestrežejo veliko osebnih podatkov in jih kasneje nezavarovano posredujejo s pomočjo interneta. Ta način delovanja je vzbudil zanimanje tudi pri organih pregona. Za zbrane podatke se že dolgo ne zanimajo samo proizvajalci in upravljavci, temveč tudi tretje osebe.

[73] Dem Verbrechen auf der Spur, v: Zukunfts Institut, URL: https://www.zukunftsinstitut.de/artikel/big-data/predictive-policing/

Zadnji odmevni primer, ko je policija želela uporabiti podatke, zbrane z napravo, ki je povezana z internetom stvari, je primer umora v zvezni državi Arkanses. Policija je želela pridobiti podatke, ki se nanašajo na uporabo zvočnika ECHO, katerega proizvajalec je Amazon. Zvočnik ima vgrajen mikrofon, ki se vklopi, ko uporabnik izreče ukaz »Alexa«. Policija si je s pomočjo možnih zvokov, ki jih je prestregel zvočnik, obetala, da bo v tem primeru pridobila dokaze. Zadeva je še v teku, Amazon pa še ni posredoval glasovnega gradiva, saj čaka na pravnomočnost sodne odredbe. Čeprav obstaja majhna verjetnost, da je naprava zabeležila želene dokaze, primer nakazuje, kako internet stvari, povezane naprave in pametni domovi vedno bolj prihajajo v središče zanimanja organov pregona.[74]

6.3 Odločitve Evropskega sodišča človekovih pravic v zvezi z masovnim nadzorom

Primera Zakharov proti Rusiji, št. 47143/06 z dne 4. 12. 2015 ter Szabo in Vissy proti Madžarski, št. 37138/14 z dne 12. 1. 2016 sta pomembni odločitvi Evropskega sodišča človekovih pravic (v nadaljevanju: ECHR) v zvezi z masovnim nadzorom.

»Sodišče ECHR je v zadevi Zakharov proti Rusiji, v kateri se je ruski novinar in publicist Roman Andrejevič Zakharova pritožil zoper dejstvo, da je varnostno-obveščevalna služba FSB v prostore vseh ruskih mobilnih operaterjev namestila svojo prisluškovalno opremo, tako da je lahko samostojno – brez pomoči ali celo vedenja operaterja – prisluškovala kateremu koli telefonskemu pogovoru v državi. Menil je, da sta SFB oz. država Rusija s tem nedopustno posegla v pravico državljanov do spoštovanja njihove zasebnosti, saj bi takšno ravnanje pri državljanih lahko – če citiramo naše Ustavne sodišče v predlanski sodbi o razveljavitvi obvezne hrambe prometnih podatkov – »ustvarilo neoprijemljivi občutek stalnega nadzora, ki lahko vpliva na izvrševanje drugih pravic, predvsem pravice do svobodnega izražanja in obveščanja«.

S to sodbo je ECHR vzpostavil: »[…] evropski standard za masovni nadzor telekomunikacij za obveščevalne in državnovarnostne namene.« Ta standard zdaj zahteva, da države oblikujejo svojo zakonodajo tako, da bodo varnostno obveščevalne službe v zaprosilih za izvajanje prisluhov morale določno navesti, na katere osebe, prostore oz. priključke naj se prisluhi nanašajo (kar pomembno omejuje možnost odredb za »strateški nadzor

[74] A. Selyukh, As we leave more tracks, Amazon ECHO factors in murder investigation, v: npr. URL: http://www.npr.org/sections/alltechconsidered/2016/12/28/507230487/as-we-leave-more-digital-tracks-amazon-echo-factors-in-murder-investigation

komunikacij«), zaprosila bodo morala skozi dejansko in vsebinsko (sodno ali drugo primerno) presojo, nadzor pa bo treba izvajati čez posrednika, ker v primeru neposrednega nadzora varnostno-obveščevalnih služb do komunikacijskih vodov ni mogoče zagotoviti primernega nadzora oz. preprečiti zlorab.

V zadevi Szabo in Vissy proti Madžarski je bil razlog za tožbo ustanovitev posebne protiteroristične enote, ki je s spremembo zakonodaje dobila široka pooblastila za nadzor nad komunikacijami posameznikov. Pritožnika, zaposlena pri nevladni organizaciji, kritični do vlade, sta vložila pritožbo zaradi kršitve pravice do zasebnosti, pravice do sodnega varstva in učinkovitega pravnega sredstva.

ESČP je ugotovilo, da je bila madžarska zakonodaja sicer dovolj jasna in predvidljiva, da so posamezniki lahko razumeli, v kakšnih okoliščinah lahko pride do nadzora nad komunikacijami (v primeru nevarnosti terorizma in reševalnih operacij v tujini). ESČP pa je ugotovilo, da omenjena zakonodaja ne zagotavlja ustreznih varovalk, ki bi preprečevale zlorabo pravice do zasebnosti. Zakonodaja namreč ni določila kategorij posameznikov, ki jih lahko komunikacije prikrito nadzorujejo, kar je pomenilo, da je lahko ukrepov deležen prav vsak posameznik na Madžarskem, pristojnim organom pa ni bilo treba izkazati dejanske ali domnevne povezave s terorističnimi grožnjami. Prav tako pristojnim organom ni bilo treba utemeljiti in predložiti kakršnih koli dokazov za utemeljitev nujnosti nadzora nad konkretnimi posamezniki. Predvsem pa zakonodaja ni omogočala sodnega nadzora nad ukrepi; ESČP je jasno zapisalo, da nadzor s strani izvršne oblasti ni ustrezen mehanizem za varovanje pravic posameznikov. Ne nazadnje pa madžarska zakonodaja posameznikom ni zagotavljala niti učinkovitega pravnega sredstva, posamezniki pa niso bili nikoli (niti po prenehanju ukrepov) obveščeni o prikritem nadzoru«.[75]

Uporaba smernic teh odločitve za delovanje sistema pametnih mest je potrebna, saj sistem nadzora v pametnih mestih še bolj ekstenzivno. Količina zbranih podatkov v sklopu delovanja pametnega mesta kar nekajkrat presega količino zbranih podatkov, ki se zberejo v sklopu tajnega delovanja.

[75] Informacijski pooblaščenec, Povzetki sodb: Sodbe Evropskega sodišča za človekove pravice, URL: https://www.ip-rs.si/varstvo-osebnih-podatkov/iskalnik-po-odlocbah-in-mnenjih/sodbe-mednarodnih-sodisc/povzetki-sodb/

Če podatki, zbrani za namene pametnega mesta, ne služijo le osnovni funkciji – optimizaciji procesov trajnostnega delovanja in upravljanja z infrastrukturo mest – temveč preidejo v roke organov pregona, ti razpolagajo z velikim naborom osebnih podatkov, do katerih so prišli brez sodne odločbe. Pri tem gre za nesorazmeren poseg v pravice posameznika, ki ne prestane testa nujnosti. Treba je razumeti, da so podatki, ki jih ustvarja posameznik, last posameznika, na katerega se nanašajo, ne glede na to, kdo te podatke zbira, se pravi, da ima posameznik absolutno pravico nad temi podatki, enako kot ima absolutno pravico nad svojim telesom in denarjem. V tem konceptu je bistvena transparentnost glede vseh okoliščin v zvezi z zbiranjem podatkov.

7. ZAKLJUČEK

S strategijo Evropa 2020 želi Evropska komisija stopiti v korak s časom in informacijsko tehnologijo. S pomočjo informacijske in komunikacijske tehnologije želi mestom pomagati pri razvoju v smeri nizko-ogljičnega in učinkovitega okolja. Pri tem je izredno pomembna drža evropske politike za uveljavitev ideje pametnih mest. Evropska mesta so po večini v zgodnji stopnji razvoja v pametno mesto, kar pomeni, da imajo razvito strategijo. Le 25 % je pametnih mest z vsaj eno razvito iniciativo pametnega mesta. Z zornega kota trajnostnega razvoja in učinkovitosti mest so te številke skrb vzbujajoče. Implementacija informacijskih tehnologij v obstoječo mestno infrastrukturo zahteva veliko volje tako družbe kot tudi mestnih oblasti, hkrati pa takšno predrugačenje mest v pametna mesta zahteva veliko investicij in posegov v ustaljeno mestno infrastrukturo. Politika mest mora delovati v smeri izobraževanja občanov mest, ki se bodo soočali z novimi pristopi, ki bodo na eni strani prispevali k učinkovitosti delovanja mest, po drugi strani pa bodo z željo po učinkovitosti posegali v zasebnost posameznikov in njihovo pravico do informacijske samoodločbe. Pogodba o Evropski uniji v 2. členu namreč določa, da EU temelji na vrednotah človekovega dostojanstva, svobode, demokracije, enakosti, pravne države in spoštovanja človekovih pravic, vključno s pravicami pripadnikov manjšin.

Največji izziv pri razvoju pametnih mest je soočanje informacijske tehnologije z varstvom temeljnih pravic. Listina EU o temeljnih pravicah v 7. in 8. členu določa spoštovanje zasebnega življenja in varstvo osebnih podatkov kot tesno povezani, vendar ločeni pravici. Glavna naloga snovalcev pametnih naprav je poiskati pravo razmerje med posegom v zasebnost in doseganjem učinkovitega delovanja naprave. Če temu izzivu ne bodo zadostili v zadostni meri, lahko pride do preobrata na strani uporabnikov naprav. V primeru, da precejšen del uporabnikov naprav, ki gradijo pametno mesto, začne zavračati njihovo uporabo, lahko to pripelje do oblikovanja marginalne skupine, ki zavrača digitalni razvoj. To bi lahko imelo za posledico množično izključitev na področjih javnega življenja kot tudi participativnega odločanja.

Evropska unija je s sprejetjem Splošne uredbe želela poenotiti zakonodajo na področju varovanja podatkov. Poleg harmonizacije je cilj Splošne uredbe modernizacija področja varstva podatkov, v smeri prilagoditve novemu tehnološkemu razvoju. Cilj poenotenja in

modernizacije ni bil dosežen v zadostni meri. Razlog, da želja po poenotenju prava varstva podatkov ni bila izpolnjena, je možnost različnih interpretacij abstraktnih določil varstva podatkov s strani držav članic. Pravico do interpretacije ima tudi organ na ravni evropske unije, a ta obrazložitev ni obvezujoča za odločanje sodišč, gre le za priporočilo. Modernizacija področja varstva podatkov s Splošno uredbo je bila izpolnjena delno. Napredek je viden na področju uporabe prava, saj ni več merodajen kraj, kjer se podatki obdelujejo, temveč se upošteva, ali so bili podatki pridobljeni od posameznikov, ki se nahajajo na področju Evropske unije. Šibka točka modernizacije varstva podatkov je še vedno pravica do posredovanja osebnih podatkov na temelju utemeljenega interesa tretjih, npr. podjetja, z namenom obdelave podatkov. Največja pomanjkljivost modernizacije varstva podatkov pa je dejstvo, da Uredba ne vsebuje posebnih določil, ki se tičejo velikih izzivov informacijske tehnike, ki so: veliko podatkovje, internet stvari in računalništvo v oblaku.

Vse to pripelje do zaključka, da bo treba v prihodnje spremeniti način pristopa pri soočanju informacijske tehnologije in zagotavljanju varstva podatkov. Zakonodaja na tem področju bo potrebovala bolj prožne rešitve, ki bodo posameznikom omogočale čim večjo svobodo pri odločanju, koliko osebnih podatkov za voljo učinkovitejšega obvladovanja svojega vsakdana, bodo pripravljeni deliti. V ta namen sem predstavila alternative soglasju. Nekatere na trgu že obstajajo, druge so bolj teoretične, a menim, da bo v prihodnosti prevladovala ideja o vgrajeni zasebnosti, saj bo le-ta kos hitrim tehnološkim napredkom.

Vseh teh nalog pa ni možno narediti le s sprejemanjem prožne zakonodaje, pomembna je tudi informiranost posameznikov, tako o pravicah, ki jim jih pravo že ponuja, kot s samimi možnostmi, ki jih ponujajo naprave pri zagotavljanju zasebnosti. Trajnostni razvoj mest s pomočjo informacijskih tehnologij je neizogiben in napredek na področju tehnologije je treba usmeriti v dobro ohranjanja zemlje, hkrati pa morajo posamezniki, ki so ali bodo vpeti v ta omrežni svet, postati bolj angažirani in zahtevati pojasnila in zagotovila, da bodo pravice na področju zasebnosti, ki si jih je človeštvo priborilo skozi zgodovino, ostale ohranjene in ne bodo podlegle želji po večji varnosti skozi nadzor. Naj zaključim svoje delo s citatom Benjamina Franklina: »Kdor se odreče znatnemu delu svobode, da bi pridobil začasno varnost, ne zasluži ne svobode niti varnosti.«

8. BIBLIOGRAFIJA

8.1 Strokovne monografije

- Beniger, James R., The control revolution, Harvard University Press, Cambridge, Messachusetts and London, England 1989.
- Čebulj, Janez Varstvo osebnih podatkov in informacije javnega značaja, (2005), str. 19.
- Kovačič, Matej, Nadzor in zasebnost v informacijski družbi: filozofski, sociološki, pravni in tehnični vidiki nadzora in zasebnosti na internetu, Ljubljana, 2006.

8.2 Zborniki in članki

- Agencija Evropske unije za temeljne pravice (FRA), Svet Evrope: Priročnik o evropskem pravu varstva osebnih podatkov, (2014), str. 43, 44.
- Ancheta, Justine, Ten Reasons why Barcelona is a Smart City, v: Vilaweb, (26. 2. 2014), URL: http://www.vilaweb.cat/noticia/4175829/20140226/ten-reasons-why-barcelona-is-smart-city.html (25. 8. 2016).
- Brown, Eveline A., Final Version of NIST Cloud Computing Definition Published, (24. 10. 2011), URL: https://www.nist.gov/news-events/news/2011/10/final-version-nist-cloud-computing-definition-published
- Coe, Amanda, Paquet, Gilles, Roy, Jeffrey, E-governance and smart communities: a social learning challenge, v: Social Science Computer Review, 19 (2001), str. 80–93.
- Commisioner for Privacy and Data Protection: Background Paper: De-Identification, URL: https://www.cpdp.vic.gov.au/images/content/pdf/privacy_week/De-identification_Background_Paper.pdf
- de Busser, Els, Private companies and the transfer of data to law enforcement authorities: Challanges Data Protection, v: Maastricht Journal, 3(2016), str. 481–483.
- Dem Verbrechen auf der Spur, v: Zukunfts Institut, URL: https://www.zukunftsinstitut.de/artikel/big-data/predictive-policing/ (13. 1. 2017)
- de Oliveria Fernandes, Eduardo, Smart City Initiative: How to Foster a Quick Transition Towards Local Sustainable Energy Systems, v: THINK, (2011).
- Directorate for Internal Policies/Policy Department A: Economic and Scientific Policy, Mapping smart cities in the EU, (2014).

- Evropska komisija, Evropa 2020, Cilji strategije Evropa 2020, URL: https://ec.europa.eu/info/strategy/european-semester/framework/europe-2020-strategy_en (25. 8. 2016).
- Evropska komisija, European Cloud Initiative to give Europe a global lead in the data-driven economy, (19. 4. 2016), URL: http://europa.eu/rapid/press-release_IP-16-1408_sl.htm
- Edwards, Lilian, Privacy, Security and Data Protection in Smart Cities: a Critical EU Law Perspective, v: CREATe Working Paper , 11 (2015), str. 13.
- Frei, Hans, Effizient – aber überhaupt nicht städtisch, Vom Internet der Dinge zur Smart City?, v: NZZ, (12.7.2015), URL: http://www.nzz.ch/feuilleton/effizient--aber-nicht-staedtisch-1.18577769, (15. 8. 2016).
- Finch, Kelsey, Tene, Omer, Welcome to the Metropticon: Protecting privacy in a hyperconnected town, v: Fordham Urban Law Journal, 5 (2015), str. 1608, 1609.
- Gottwald, Michael, Big data: Was ist Big Data? - Big Data Analytics, Software, Tools + Trends, v: SoftSelect glossar, URL: http://www.softselect.de/wissenspool/big-data (20. 8. 2016).
- IPROM, Internet stvari, URL: https://iprom.si/slovar/internet-stvari/, (20. 8. 2016).
- Informacijski pooblaščenec, Povzetki sodb: Sodbe Evropskega sodišča za človekove pravice, URL: https://www.ip-rs.si/varstvo-osebnih-podatkov/iskalnik-po-odlocbah-in-mnenjih/sodbe-mednarodnih-sodisc/povzetki-sodb/
- Jaekel, Michael, Smart City wird Realität Wegweiser für neue Urbanitäten in der Digitalmoderne, v: Springer Fachmedien Wiesbaden (2015), str. 206–210.
- Jesenko, Miha, GDPR, General Data Protection Regulation-Splošna uredba o varstvu podatkov, (2016), URL: http://www.insolvinfo.si/DnevneVsebine/Aktualno.aspx?id=169812
- Kennart, Matt, Provost, Claire, Inside Lavasa, v: The guardian, (19.11.2015), URL: https://www.theguardian.com/cities/2015/nov/19/inside-lavasa-indian-city-built-private-corporation, (12.8.2016)
- Khan, Zaheer, Anjum, Ashiq, Soomro, Kamran, Atif Tahir, Muhammadv, Towards cloud based big data analytics for smart future cities, v: Journal of Cloud computing, (2015), str. 3
- Kossina, Issabela, Smart City: Begriff, Charakteristika und Beispiele, v: Wiener Stadtwerke zur nachhaltigen Entwicklung, 7 (2011), str. 19.

- Miller, Franz, Niesing, Birgit, Die Zukunft der Stadt, v: Fraunhofer Magazin, 4(2012), str. 9.
- Mitton, Nathalie, Loscari, Valeria, Petrolo, Riccardo, Towards a smart city based on cloud of things, a survey on the smart city vision and paradigms, v:Transactions on Emerging Telecommunications Technologies, (2015), str. 4.
- Mayer-Schoenberger, Viktor, Cukier, Kenneth, Big Data: A Revolution That Will Transform How We Live, Work and Think , (2013), str. 15.
- Mohorčič, Mihael, Robnik, Ana, Baškovič, Dalibor, Delavnica «Pametna mesta in skupnost kot razvojna priložnost Slovenije«, v: Zbornik 18. mednarodne multikonference Informacijska družba, H (2015), str. 3.
- Podpečan, Mitja, Prihodnost informacijske zasebnosti, Pravna praksa, 26 (2015), str. 22.
- Rule, James B., Social control and modern social structures, v: Surveillance studies reader, (2007), str. 26–28.
- Selinšek, Liljana, Veliko podatkovje v pravu in ekonomiji: veliki izzivi ali velike težave? v: LEXONOMICA, 2 (2015), str. 165–166.
- Selyukh, Alina, As we leave more tracks, Amazon ECHO factors in murder investigation, v: npr. URL: http://www.npr.org/sections/alltechconsidered/2016/12/28/507230487/as-we-leave-more-digital-tracks-amazon-echo-factors-in-murder-investigation
- Tomšič, Andrej, Varstvo osebnih podatkov v dobi podatkovnega izobilja, (2014), str.16, URL: http://media-doc.si/wordpress/wp-content/uploads/2016/11/13_Tomsic.pdf
- UNCTAD secretariad, United Nations Commission on Science and Technology for Development Intersessional Panel 2015–2016, v: Issues Paper On Smart Cities and Infrastructure, (2016), str. 28–30.

8.3 Nacionalna zakonodaja

- Ustava Republike Slovenije (Ur. l. RS, št. 33/1991, Uradni list RS, št. 42/1997 - UZS68, 66/2000 - UZ80, 24/2003 - UZ3a, 47, 68, 69/2004 - UZ14,69/2004 - UZ43, 69/2004 - UZ50, 68/2006 - UZ121,140,143, 47/2013, 47/2013).
- Zakon o varstvu osebnih podatkov (ZVOP-1), Uradni list RS, št. 86/2004, 113/2005 - ZInfP, 51/2007 - ZUstS-A, 67/2007.
- Pirc Musar, Nataša, Bien Sonja, Bogataj Jože, Prelesnik Mojca, Žaucer Alenka, Zakon o varstvu osebnihpodatkov s komentarjem, GV založba, (2006),

8.3 Zakonodaja EU

- Listina EU o temeljnih pravicah 2010/C 83/02, Uradni list EU C 83/389, z dne 30. 3. 2010; Uradni list EU C 202/2, z dne 7. 6. 2016.
- Pogodba o Evropski uniji, Uradni list EU, C115/15, z dne 9. 5. 2008; prečiščena različica objavljena v Uradnem listu EU C202, z dne 7. 6. 2016.
- Pogodba o delovanju Evropske unije, 2012/C 326/01, Uradni list EU C326, z dne 26. 10. 2012; prečiščena različica objavljena v Uradnem listu EU C202, z dne 7. 6. 2016.
- Direktiva Evropskega parlamenta in Sveta 95/46/ES z dne 24. oktobra 1995 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov, Uradni list EU št. 281, z dne 23. 11. 1995.
- Direktiva Evropskega parlamenta in Sveta 2002/58/ES z dne 12. julija 2002 o obdelavi osebnih podatkov in varstvu zasebnosti na področju elektronskih komunikacij, Uradni list EU št. 201, z dne 31. 7. 2002 (Direktiva o zasebnosti in elektronskih komunikacijah), revidirana z Direktivo 2009/136/ES.
- Uredba (EU) Evropskega parlamenta in Sveta 2016/679 z dne 27. 4. 2016 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), Uradni list EU, L 119/1, z dne 4. 5. 2016.

8.4 Mednarodne konvencije

- Evropska konvencija o človekovih pravicah in temeljnih svoboščinah s Protokoli, 1950.
- Konvencija o varstvu posameznika glede na avtomatsko obdelavo podatkov, Uradni list RS, Mednarodne pogodbe, št. 3/1994 (RS 11/1994), z dne 28. 2. 1994.

8.5 Sodna praksa Sodišča EU

- Zadeva C-131/12, Google Spain SL, Google Inc. proti AEDP, Mariu Costeji Gonzalezu, ECLI:EU:C:2014:317.
- Zakharov proti Rusiji, št. 47143/06 z dne 4. 12. 2015.
- Szabo in Vissy proti Madžarski, št. 37138/14 z dne 12. 1. 2016.

8.6 Druga literatura

- Article 29 Data protection party, Opinion 8/2014 on the recent developementson the Internet of Things, (16.9.2014), 14/EN, WP223, URL: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf

– Statement on Statement of the WP29 on the impact of the development of big data on the protection of individuals with regard to the processing of their personal data in the EU , (16. 9. 2014), str. 2, URL: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp221_en.pdf.
– Article 29 Data protection party, Opinion 5/2012 on Cloud Computing (1.7.1012), 01037/12EN, WP196, URL: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf.