

Univerza v Ljubljani

Pravna fakulteta

Ustreznost pravne ureditve varstva osebnih podatkov v digitalni dobi

(magistrsko diplomsko delo)

Avtorica: Tina Pavlović

Mentorica: izr. prof., doc. dr. Ana Vlahek, univ. dipl. prav.

Ljubljana, september 2018

Zahvala

Zahvaljujem se svoji mentorici izr. prof., doc. dr. Ani Vlahek za vso pomoč pri izdelavi tega magistrskega diplomskega dela.

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

Povzetek

Varstvo osebnih podatkov je pereča tema današnjega časa. Osebni podatki so postali dragocena surovina, ki podjetjem prinaša neprecenljivo prednost na trgu. Z razvojem digitalnih tehnologij je zbiranje osebnih podatkov postalo veliko lažje in obsežnejše, česar so se uporabniki komaj začeli zavedati. Pravica do varstva osebnih podatkov je v zadnjih letih, prav zaradi razvoja tehnologije, doživela kar nekaj sprememb in posodobitev. Veliko vlogo pri tem je imela Splošna uredba o varstvu podatkov, ki je prinesla kar nekaj ključnih sprememb na tem področju. Poudarek je bil predvsem na krepitevi pravic posameznikov. Z uredbo je bil prenovljen postopek privolitve, ki je sedaj veliko bolj prijazen uporabniku. Razširjena je bila tudi definicija pojma osebnega podatka, katera je bila prilagojena tako, da zajema tudi elemente moderne tehnologije. Hkrati je bilo z uredbo, v postopku pridobivanja osebnih podatkov, izraziteje poudarjeno načelo transparentnosti. V magistrskem diplomskem delu so predstavljene ključne novosti Splošne uredbe o varstvu podatkov in nekatere pomanjkljivosti njene ureditve, ki se kažejo na področju moderne tehnologije.

Ključne besede: varstvo osebnih podatkov, veliko podatkovje, internet stvari, GDPR, zasebnost, privolitev, anonimizacija, transparentnost

Summary

Personal data protection is a topical issue nowadays, as personal data has become an important input giving corporations a valuable advantage on the market. With the development of various digital technologies, collection of personal data became easier and broader. However, the general public is barely becoming conscious of the fact at matter. Based on the mentioned developments in the area of collecting personal data, the right to protection of personal data has experienced various amendments and updates recently. The General Data Protection Regulation specifically had an important part in the process, as it brought several crucial changes, primarily focusing on the reinforcement of individuals' rights. GDPR amended the process of consent, which is now friendlier to the individual. The definition of the term personal data has been widened in such a way that it now also incorporates elements of modern technologies. At the same time, the GDPR also emphasized the principle of transparency in the process of collecting personal data. The present Master's Degree presents crucial novelties and some deficiencies brought forward with the adoption of the GDPR in the area of modern (digital) technologies.

Key words: protection of personal data, big data, internet of things, GDPR, privacy, consent, anonymization, transparency

Vsebina

1. UVOD	6
2. TEORETIČNI DEL	8
2.1. Osební podatki	8
2.2. Pravica do zasebnosti	8
2.3. Pravica do varstva osebnih podatkov	10
3. PRAVNI OKVIR	12
3.1. Pravna ureditev v Evropski uniji	12
3.1.1. Direktiva 95/46/ES	12
3.1.2. Uredba 2016/679	12
3.2. Pravna ureditev v Republiki Sloveniji	16
3.2.1. Zakon o varstvu osebnih podatkov (ZVOP-1)	16
3.2.2. Predlog ZVOP-2	21
4. RAZPRAVNI DEL	23
4.1. Zbiranje podatkov	23
4.1.1. Big data	24
4.1.2. Internet stvari	25
4.2. Problematični vidiki Splošne uredbe o varstvu podatkov	26
4.2.1. Pravna podlaga	26
4.2.2. Transparentnost	28
4.2.3. Anonimizacija	30
5. SKLEPNE UGOTOVITVE	32
6. LITERATURA	34

1. UVOD

Hitrejši in dostopnejši razvoj znanosti in tehnologije se vedno bolj kaže na vsakem koraku posameznika. Naša življenja postajajo vedno bolj digitalizirana, uporabljamo vedno več naprav, ki jih lahko povežemo z internetom t.i. internet stvari (IoT). Predmetni izumi so bili ustvarjeni z namenom omogočanja bolj kakovostnega in produktivnega življenja, pri čemer pa ima slednje za posledico vedno večji »vpogled« zadevnih naprav v našo zasebnost. Po podatkih analize družbe Gartner bo do leta 2020 več kot 20 milijard naprav povezanih z internetom.¹ Varstvo osebnih podatkov v okviru interneta je tako postalo aktualna in pereča tema 21. stoletja.

Digitalizacija je v današnjem času prisotna na številnih področjih, pojavlja se tako na zasebnih področjih, kot tudi na javnem področju. Sama se bom v magistrskem delu osredotočila na varstvo osebnih podatkov v povezavi z digitalizacijo na zasebnih področjih.

V današnjem digitalnem svetu s pomočjo pametnih naprav nastajajo raznovrstne zbirke podatkov, kjer so shranjeni številni osebni podatki posameznikov. Naprave, kot so pametni telefoni, gospodinjski aparati in celotni pametni domovi, podatke ne le shranjujejo, temveč tudi ustvarjajo.² Zelo dolgo se ljudje zbiranja in ustvarjanja podatkov niso zavedali, vendar se stanje ozaveščenosti, tudi zaradi Splošne uredbe o varstvu podatkov v zadnjem času precej izboljšuje.

Pravica do varstva osebnih podatkov ni »nova« pravica, pojavila se je že v prejšnjem stoletju, postaja pa vedno bolj pomembna v dobi tehnologije, ker ljudje, zavedno ali nezavedno, s pomočjo pametnih naprav delimo vedno več svojih podatkov z ostalimi.

Svetovalna družba McKinsey je leta 2011 objavila pomembno poročilo na področju velikega podatkovja, v katerem so med drugim ugotovili, da je le to prisotno v vseh industrijskih panogah, in s tem poudarili pomen ter poslovne priložnosti ekonomije podatkov. S tem so opozorili tudi na možne posledice, ki jih te spremembe povzročajo v gospodarstvu na splošno, kako podjetja ščitijo te podatke in komu dopuščajo dostop do njih. Za nekatera največja in najuspešnejša svetovna podjetja, kot so Google, Facebook, Amazon in Microsoft, so podatki

¹ <www.gartner.com/newsroom/id/3598917>.

² J. Stušek, nav. delo, str. 218.

eno najvrednejših sredstev, njihova obdelava in prodaja pa središče modernih poslovnih modelov.³

Magistrsko delo je razdeljeno na tri glavne vsebinske sklope. V prvem sklopu, v katerem bo obravnavana teorija, bom v prvem poglavju najprej opredelila pravico do varstva osebnih podatkov in jo nekoliko razčlenila. Drugi sklop bo posvečen pravnemu okviru in ureditvi v Evropski uniji in v Sloveniji. Znotraj EU bom najprej na kratko predstavila dosedanjo ureditev v Direktivi 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 (Direktiva 95/46/ES)⁴, nato pa se bom osredotočila na Uredbo (EU) 2016/679 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 (GDPR)⁵ in predstavila vse novosti, ki jih prinaša. Predstavljena bo tudi trenutno aktualna ureditev v Sloveniji in novi predlog Zakona o varstvu osebnih podatkov (ZVOP-2). Zadnji sklop bo razdeljen na dve poglavji. V prvem bo tehnično predstavljeno »moderno« zbiranje podatkov, v drugem pa bom analizirala ureditev področij varstva osebnih podatkov, urejenih znotraj Splošne uredbe o varstvu podatkov, ki so po mojem mnenju najbolj problematična z vidika modernih tehnologij.

Raziskovalno vprašanje, ki bo vodilo nastajanje magistrskega dela, je, ali je na ravni EU in v Sloveniji zagotovljena ustrezna pravna ureditev varstva osebnih podatkov na področju sodobne tehnologije. Tu se bom osredotočila predvsem na novosti Splošne uredbe o varstvu podatkov. Moja hipoteza je, da je pravna ureditev varstva osebnih podatkov na področju sodobne tehnologije, kot sta veliko podatkovje in internet stvari, še vedno zastarela in na tem področju neustrezna.

³ H. Uršič, nav. delo, str. 358.

⁴ UL L 281.

⁵ UL L 119.

2. TEORETIČNI DEL

2.1. Osební podatki

Slovar slovenskega knjižnega jezika določa podatek kot dejstvo, ki o določeni stvari kaj pove ali se nanjo nanaša.⁶ Podatek je torej vsaka informacija o neki stvari, kar je zelo širok pojem in predstavlja veliko število dejstev.

Definicijo osebnega podatka, ki je veljala do 25.5.2018, je določal Zakon o varstvu osebnih podatkov (ZVOP-1)⁷ v 6. členu, ki je osebni podatek definiral kot katerikoli podatek, ki se nanaša na posameznika, ne glede na obliko, v kateri je izražen. Posameznika pa kot določeno ali določljivo fizično osebo, na katero se nanaša osebni podatek. Določljiva fizična oseba je oseba, ki 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.

Predlog novega Zakona o varstvu osebnih podatkov (ZVOP-2) je povzel ureditev iz trenutnega zakona, a ga je nadgradil z omembo podatka o lokaciji in spletnem identifikatorju, kar kaže na posodobitev predloga glede na digitalno dobo, v kateri živimo.

Pri presoji pojma osebnega podatka je informacijski pooblaščenec v enem izmed mnenj opozoril, da podatka, kot sta npr. ime in priimek, nista nujno varovana osebna podatka, če se z njima ne da določiti posameznika. Ko pa tema dvema podatkoma dodamo še kakšno značilnost posameznika (naslov, starost, itd.), posameznik postane določljiv in vsi njegovi podatki varovani z zakonom.⁸

2.2. Pravica do zasebnosti

Pravica do zasebnosti je bila prvič omenjena že leta 1948 v 12. členu Splošne deklaracije človekovih pravic A/RES/217A (III), ki določa, da se nikogar ne sme nadlegovati s samovoljnim vmešavanjem v njegovo zasebno življenje, v njegovo družino, v njegovo stanovanje ali njegovo dopisovanje in tudi ne z napadi na njegovo čast in ugled. Določa tudi,

⁶ <<https://sskj.si/?s=podatek>>.

⁷ Uradni list RS, št. 94/07.

⁸ Mnenje št. 0712-1/2014/3443 z dne 7. 11. 2014.

da ima vsakdo pravico do zakonskega varstva pred takšnim vmešavanjem ali takšnimi napadi. Čeprav takrat informacijska tehnologije še ni v tolikšni meri ogrožala človekove zasebnosti, dobiva predmetna določba z razvojem sodobnih informacijskih tehnologij vedno večji pomen saj služi kot podlaga za vse nadaljnje pravne akte.

Nekateri avtorji navajajo tri sestavine zasebnosti. Zasebnost v prostoru, ki se nanaša na željo posameznika, da ima možnost biti sam, torej ločen od fizične prisotnosti drugih ljudi, zasebnost osebnosti se nanaša npr. na svobodo misli, opredelitve in izražanja ter informacijska zasebnost, ki jo največkrat zanemarimo. Njeno bistvo je želja posameznika, da obdrži informacije o sebi, ker noče, da bi bili z njimi seznanjeni drugi. Ko govorimo o varstvu osebnih podatkov, je najpomembnejša prav ta sestavina zasebnosti.⁹

Problem definicije zasebnosti in pravice do zasebnosti je v tem, da je zasebnost relativna in subjektivna. Vsak ima nekoliko drugačna pričakovanja glede pomena zasebnosti, ki se spreminjajo tudi glede na čas in družbeni kontekst. Prav to je tudi razlog, da se pravna teorija izogiba natančnemu definiranju pravice do zasebnosti.¹⁰

Za enega prvih mejnikov obravnavanja pravice do zasebnosti štejemo članek *The right to privacy*, ki sta ga leta 1890 napisala Samuel D. Warren in Louis D. Brandeis. V članku sta pojasnila potrebo po uveljavitvi pravice do zasebnosti in prilagajanju pravne ureditve novim razmeram. Posebej sta izpostavila tudi vpliv tehnološkega razvoja na pravico do zasebnosti oziroma njeno zožitev zaradi novih izumov in naprav, kot je bil takrat fotoaparat in naprave za slikovno ter zvočno snemanje. S primeri iz prakse sta jasno nakazala vpliv tehnologije na pravico do zasebnosti, stališče za katero lahko rečemo, da velja še danes, vendar celo v širši obliki.¹¹

Tehnologija počasi odstranjuje meje privatnosti, s čimer je zasebnost postala nedotakljiva in enako pomembna pravica kot pravica do življenja in svobode v današnjem svetu. Tako po svetu, kot tudi v Evropski uniji, je splošno sprejet koncept pričakovane zasebnosti, ki ga je leta 2010 uporabilo tudi Ustavno sodišče RS v eni od sodb.¹² Po tem konceptu je potrebno pretehtati dva elementa, pričakovanje zasebnosti in upravičenost takega pričakovanja v družbi. Če

⁹ J. Čebulj, nav. delo, str. 7.

¹⁰ M. Kovačič, nav. delo, str. 12.

¹¹ S. Warren in L. Brandeis, nav. delo, str. 193-220.

¹² US RS Up-3381/07 z dne 4.3.2010.

ugotovimo, da je posameznik na nekem področju izrazil pričakovanje zasebnosti in je to pričakovanje družbeno upravičeno, v takem primeru ne moremo oporekati zasebnosti.

Zasebnost je nujen instrument za vzpostavitev javne podobe posameznika. Vsak lahko sam izbira, katere informacije o sebi bo izdal javnosti in komu bo te informacije izdal. V kolikor posameznik ne more samovoljno razpolagati s svojimi podatki, bo težko prevzel podobo »nedoločenega abstraktnega človeka«, ki je nujno potreben za delovanje demokratične družbe.¹³

2.3. Pravica do varstva osebnih podatkov

Varstvo osebnih podatkov je v Sloveniji ustavno zagotovljena človekova pravica. Pravica do varstva osebnih podatkov je zapisana v 38. členu Ustave RS, ki 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.«

Ustavodajalec se je odločil za obdelovalni model, saj je določil predvsem pravila za urejanje dopustne obdelave osebnih podatkov, ki jo lahko le izjemoma omejimo z zakonom. To pomeni, da je na področju obdelovanja osebnih podatkov prepovedano vse, razen tistega, kar je izrecno dovoljeno z zakonom. Vsaka obdelava pomeni poseg v Ustavo, zato mora biti z zakonom določeno kateri osebni podatki se lahko obdelujejo, namen obdelave mora biti jasno določen in zagotovljeno ustrezno zavarovanje.¹⁴

Iz 1. člena ZVOP-1, ki ga skoraj v popolnosti povzema tudi predlog ZVOP-2, izhaja, da je varstvo osebnih podatkov del širšega področja varstva zasebnosti oziroma tako imenovane informacijske ali podatkovne zasebnosti. Bistvo varstva osebnih podatkov oziroma podatkovne zasebnosti posameznika primarno ni v »kvazilastniškem konceptu osebnih podatkov«, ko posameznik nastopa kot lastnik svojih osebnih podatkov, temveč v varstvu in nadzoru obdelave osebnih podatkov, za katero povprečni posameznik verjetno niti ne ve, da poteka.¹⁵

Varstvo osebnih podatkov in varstvo zasebnosti sta sicer različni pravici, ki pa sta med seboj tesno povezani. Danes se obe poudarjata kot temeljni človekovi pravici v Evropski uniji, kar pa bi ni bil vedno prevladujoč pogled. Evropski zakonodajalec je bil v začetnem obdobju EU

¹³ S. Dolenc, nav. delo, str. 125.

¹⁴ J. Bogataj, nav. delo, str. 19.

¹⁵ N. Pirc Musar, nav. delo, str. 40.

osredotočen predvsem na ekonomsko integracijo in spodbujanje razvoja enotnega trga. Ena izmed posledic vzpostavljanja štirih glavnih svoboščin na evropskem trgu je bil tudi dogovor o prostem pretoku podatkov. Pravica do varstva osebnih podatkov je bila urejena v Splošni deklaraciji človekovih pravic, Evropski konvenciji o varstvu človekovih pravic in temeljnih svoboščin ter v Konvenciji 108 o varstvu posameznika glede na avtomatsko obdelavo osebnih podatkov, vendar pa je šele leta 1995 sprejeta Direktiva 95/46/ES področje uredila bolj natančno in celostno.¹⁶

Prek prakse Sodišča EU, zlasti pa s sprejetjem Lizbonske pogodbe in Listine EU o temeljnih pravicah, je pravica do varstva osebnih podatkov pridobila tudi temeljni status.¹⁷ Pravica do varstva osebnih podatkov pa ni absolutna pravica, saj jo je skladno z načelom sorazmernosti treba obravnavati glede na vlogo, ki jo ima v družbi in jo uravnotežiti z drugimi temeljnimi pravicami, kar določa tudi GDPR v uvodnih določbah.

Pri varovanju osebnih podatkov se srečata dve nasprotujoči pravici oziroma dva nasprotna interesa, želja do neomejenega dostopa do osebnih podatkov in posameznikova želja po varovanju svojih osebnih podatkov. V vsakem primeru je potrebno pretehtati kateri interes prevlada.

¹⁶ H. Uršič, nav. delo, str. 360-361.

¹⁷ Prav tam, str. 361.

3. PRAVNI OKVIR

3.1. Pravna ureditev v Evropski uniji

Pravno podlago za ureditev varstva osebnih podatkov na ravni Evropske unije določa 16. člen Pogodbe o delovanju Evropske unije (PDEU)¹⁸, ki pravi, da ima vsakdo pravico do varstva osebnih podatkov, ki se nanašajo nanj. Enako določbo vsebuje tudi Listina Evropske unije o temeljnih pravicah (Listina)¹⁹ v 8. členu. Podrobneje pa področje varstva osebnih podatkov urejajo sekundarni viri Evropske unije. Do začetka uporabe Splošne uredbe o varstvu podatkov je to področje urejala Direktiva 95/46/ES, ki je bila prenesena v trenutno še veljavni ZVOP-1.

3.1.1. Direktiva 95/46/ES

Direktiva 95/46/ES je bila sprejeta leta 1995 s strani Evropskega parlamenta in Sveta z namenom ureditve varstva posameznika pri obdelavi osebnih podatkov in prostem pretoku teh podatkov. Do začetka uporabe GDPR je bila Direktiva 95/46/ES osrednji evropski pravni akt na področju varovanja zasebnosti. Razlogov za sprejetje je bilo več (vsi so navedeni v uvodnih določbah), eden od ključnih pa je zagotovo ta, da je prišlo do vedno pogostejših obdelav osebnih podatkov na različnih področjih gospodarske in družbene dejavnosti ter do napredka v informacijski tehnologiji, saj se je Direktiva 95/46/ES uporabljala predvsem za osebne podatke, ki so bili v celoti ali delno obdelani z avtomatskimi sredstvi.

V uvodnih določbah GDPR je določeno, da cilji in načela Direktive 95/46/ES še vedno veljajo, zato se ne bom spuščala v samo ureditev, še posebej zato, ker GDPR v večji meri povzema in nadgrajuje ureditev iz Direktive 95/46/ES. Od 25. 5. 2018 naprej Direktiva 95/46/ES tako ne velja več, saj jo je skladno s 94. členom razveljavila in nadomestila Splošna uredba o varstvu podatkov.

3.1.2. Uredba 2016/679

Eden izmed razlogov za sprejetje GDPR, kot izhaja že iz uvodnih določb, je hiter tehnološki razvoj, ki je prinesel nove izzive za varstvo osebnih podatkov. Zaradi tega razvoja je potreben trden in skladnejši okvir varstva osebnih podatkov, ki bo podprt z doslednim izvrševanjem.

Nadalje GDPR določa, da bi za zagotovitev dosledne in visoke ravni varstva posameznikovih pravic ter odstranitev ovir za prenos osebnih podatkov, morala biti raven varstva pravic in

¹⁸ UL C 202.

¹⁹ UL C 202.

svoboščin pri obdelavi osebnih podatkov enaka v vseh državah članicah. Države članice so v povezavi s splošnim in horizontalnim pravom o varstvu osebnih podatkov, sprejele več področnih zakonov, kjer so potrebne podrobnejše določbe. Verjetno je ravno to razlog, da so se tokrat odločili za ureditev področja z uredbo, saj slednja predstavlja pravni akt EU, ki je neposredno uporabljiv v vseh državah članicah Evropske unije.

Ravno temu je veliko držav članic nasprotovalo, med njimi tudi Republika Slovenije, ki so predlagale naj se GDPR preoblikuje v direktivo. Skrbelo jih je tudi, da ne bi prišlo do neutemeljenega znižanja standardov varstva osebnih podatkov, ki so bili v Slovenije pred uvedbo GDPR visoki.

Splošna uredba o varstvu podatkov je, verjetno tudi zaradi tega razloga, ena izmed bolj lobiranih uredb, saj je bilo v postopku pogajanj vloženi več kot 7.000 amandmajev.²⁰

V nadaljevanju tega podpoglavja se bom osredotočila predvsem na pomembne novosti GDPR in razlike z Direktivo 95/46/ES.

3.1.2.1. Splošne določbe

Kot je to razvidno iz 1. člena uredbe, GDPR določa pravila o varstvu posameznikov pri obdelavi osebnih podatkov in pravila o prostem pretoku osebnih podatkov.

V 2. členu je določeno, da se GDPR uporablja za obdelavo osebnih podatkov v celoti ali delno z avtomatiziranimi sredstvi in za drugačno obdelavo za osebne podatke, ki so del zbirke ali so namenjeni oblikovanju dela zbirke. GDPR se uporablja zgolj za dejavnosti znotraj področja EU in se ne uporablja s strani fizičnih oseb med potekom osebne ali domače dejavnosti.

3.1.2.2. Krajevna veljavnost

V 3. členu je opredeljena razširjena ozemeljska veljavnost, kjer je navedeno, da se GDPR uporablja za obdelavo osebnih podatkov v okviru dejavnosti sedeža upravljavca ali obdelovalca v Evropski uniji. Prav tako se uporablja za obdelavo osebnih podatkov s strani upravljavca ali obdelovalca, ki nima sedeža v Evropski uniji, kadar so dejavnosti obdelave povezane z nudenjem blaga ali storitev takim posameznikom v Evropski uniji ali s spremljanjem njihovega vedenja, kolikor to poteka v Evropski uniji.

²⁰ <<https://svetkapitala.delo.si/ikonomija/se-zc-pripravljate-na-novo-uredbo-o-varstvu-osebni-podatkov-3293>>.

3.1.2.3. *Opredelitev pojmov*

Sledi opredelitev pojmov, kjer je potrebno omeniti predvsem razširjeni definiciji osebnih podatkov in obdelave, novo definicijo privolitve ter kar nekaj novih pojmov, ki so jih uvrstili v GDPR. V definicijo osebnih podatkov so dodali primeroma naštetih identifikatorje, med katerimi so tudi spletni identifikatorji, kot so ID piškotkov, IP naslovi, RFID oznake, itd.

Nov pojem, ki se pojavi je tudi »oblikovanje profilov«, ki pomeni vsako obliko avtomatizirane obdelave osebnih podatkov, ki vključuje uporabo osebnih podatkov za ocenjevanje nekaterih osebnih vidikov v zvezi s posameznikom. Definicijo privolitve posameznika so spremenili tako, da so dodali, da mora iti za izrecno in nedvoumno izjavo volje, kar izključuje, do sedaj največkrat uporabljeni, opt-out oziroma avtomatsko privolitev. Nova pojma sta tudi genetski in biometrični podatki, kateri so s 25. 5. 2018 postali osebni podatki, ki so varovani z GDPR.

3.1.2.4. *Načela*

Načela, ki jih zasleduje GDPR so zelo podobna tistim, ki jih je določila že Direktiva 95/46/ES z eno izjemo. Ta načela so naštetih v 5. členu in določajo zakonitost, pravičnost in preglednost, omejitve namena podatkov skupaj z najmanjšim obsegom podatkov, načelo točnosti, omejitve shranjevanja ter načelo odgovornosti upravljavca. Novo načelo, ki ga Direktiva 95/46/ES ni vsebovala je načelo celovitosti in zaupnosti, ki upravljavcem nalaga dolžnost zagotavljanja varnosti osebnih podatkov, vključno z zaščito pred nedovoljeno in nezakonito obdelavo ter pred izgubo ali uničenjem podatkov.

3.1.2.5. *Obdelava osebnih podatkov*

Pravni temelji za obdelavo osebnih podatkov, določeni v 6. členu GDPR, ostajajo enaki, kot jih je določila že Direktiva 95/46/ES. Novost, ki je določena v GDPR, je možnost obdelave podatkov za drug namen, kot za tistega, za katerega so bili izbrani, pod določenimi pogoji in v kolikor obdelava ne temelji na privolitvi posameznika.

V 7. členu so določeni pogoji, ki so potrebni za privolitev posameznika v obdelavo osebnih podatkov, ki jih Direktiva 95/46/ES ni urejala:

1. Privolitev mora biti dana na tak način, da je upravljavec zmožen dokazati, da je posameznik privolil v obdelavo.
2. Če je privolitev dana v pisni izjavi, ki se nanaša tudi na druge zadeve, mora biti privolitveni obrazec ločen od ostalega teksta, v razumljivi in dostopni obliki ter v jasnem in preprostem jeziku.

3. Posameznik mora imeti vedno možnost svojo izjavo preklicati na enak oziroma podoben enostaven način kot jo je dal.

4. V primeru, da gre za izvajanje pogodbe, vključno z zagotavljanjem storitev, ne sme biti pogojena s privolitvijo v obdelavo osebnih podatkov, ki niso potrebni za izvedbo zadevne pogodbe.

Še ena novost, ki jo je prinesla GDPR in je posledica vedno večje razpoložljivosti tehnologije, je obvezna privolitev ali odobritev privolitve nosilcev starševske odgovornosti pri otrocih, ki še niso dopolnili 16 let. Pri tem je GDPR dopustila diskrecijo državam članicam, da lahko starost otrok znižajo, pri čemer je najnižja dovoljena starost 13 let.

3.1.2.6. Pravice posameznika

Tretje poglavje GDPR ureja pravice posameznika, na katerega se nanašajo osebni podatki. Poleg tistih pravic, ki jih je določala že Direktiva 95/46/ES, kot so pravica do dostopa, do ugovora in do popravka, so dodali tudi pravico posameznika do informacije o tem, koliko časa se hranijo njegovi osebni podatki.

V 17. členu so dodali še pravico do izbrisa oziroma do pozabe, na podlagi katere lahko posameznik doseže izbris svojih osebnih podatkov, pod določenimi pogoji in pravico do prenosljivosti podatkov, ki jo ureja 20. člen, ki posamezniku omogoča, da se podatki neposredno prenesejo od enega upravljavca k drugemu.

3.1.2.7. Upravljavec in obdelovalec

Tako kot je to uredila že Direktiva 95/46/ES, tudi GDPR ureja dolžnosti upravljavca in obdelovalca, s tem, da jim nalaga še več obveznosti in odgovornosti. V 25. členu je določeno tudi vgrajeno in privzeto varstvo podatkov, katerega morajo zasledovati upravljavci. Ponovno je poudarjeno načelo najmanjšega obsega podatkov, psevdonimizacija ter zaščitni ukrepi za varstvo podatkov.

Prav tako je podrobneje urejen odnos med upravljavcem in obdelovalcem, definiran pa je tudi odnos med obdelovalcem in podobdelovalcem, za katerega mora upravljavec dati soglasje.

Kot novo evidenco, ki jo mora voditi vsak upravljavec, ki ima najmanj 250 zaposlenih in obdeluje podatke, ki lahko predstavljajo tveganje za pravice in svoboščine oziroma jih ne obdeluje le občasno ali obdeluje posebne vrste podatkov, GDPR v 30. členu ureja evidenco dejavnosti obdelave. Ta evidenca naj bi zajemala podatke upravljavca, namen obdelave, opis

kategorij posameznikov, kategorije uporabnikov, roke za izbris podatkov in tehnične ter organizacijske varnostne ukrepe.

3.1.2.8. Ocena učinka

GDPR je uvedla še en predhodni mehanizem za zagotovitev večjega varstva osebnih podatkov predvsem zaradi uporabe novih tehnologij, ki ga ureja v 35. členu, kot oceno učinka. Ta ocena je potrebna v primeru sistematičnega in obsežnega vrednotenja osebnih vidikov v zvezi s posamezniki, ki temelji na avtomatizirani obdelavi, v primeru obsežne obdelave posebnih vrst podatkov in obsežnega sistematičnega spremljanja javno dostopnega območja. Ocena mora zajemati opis predvidenih dejanj in namenov obdelave, oceno potrebnosti in sorazmernosti, oceno tveganj za pravice, svoboščine, ukrepe za obravnavanje tveganj skupaj z zaščitnimi in varnostnimi ukrepi ter mehanizme za zagotovitev varstva osebnih podatkov in za dokazovanje skladnosti z GDPR.

3.1.2.9. Pooblaščen oseb za varstvo podatkov

Za javne organe in upravljavce, katerih temeljne dejavnosti zajemajo redno in sistematično spremljanje podatkov ali obsežno obdelavo posebnih vrst podatkov, je obvezno imenovanje pooblaščen oseb za varstvo podatkov, kot to določa 37. člen. Pooblaščen oseb svetuje upravljavcu oziroma obdelovalcu o njihovih obveznostih, spremlja skladnosti z GDPR in drugimi določbami prava EU in prava države članice, svetuje glede ocene učinkov, sodeluje z nadzornim organom ter deluje kot kontaktna točka zanj.

3.2. Pravna ureditev v Republiki Sloveniji

Prvi zakon s področja varstva osebnih podatkov v Republiki Sloveniji je začel veljati marca 1990, katerega je leta 1999 zaradi približevanja Evropski uniji in zaradi sprejetja Direktive 95/46/ES nadomestil novi Zakon o varstvu osebnih podatkov. Nov zakon je bil zaradi nepopolne usklajenosti z Direktivo 95/46/ES noveliran leta 2001. Tri leta kasneje je bil zaradi ponovne uskladitve z Direktivo 95/46/ES na podlagi vstopa Slovenije v EU sprejet nov Zakon o varstvu osebnih podatkov, ki je bil leta 2007 noveliran in v določbah, ki jih GDPR ni nadomestila, velja še danes.

3.2.1. Zakon o varstvu osebnih podatkov (ZVOP-1)

Koncept varstva osebnih podatkov je skozi zgodovinski razvoj ostal praktično enak kot ga uvaja ZVOP-1, z nekaterimi novostmi. ZVOP-1 ni zgolj sistemski zakon, kot so bili zakoni do tedaj, temveč je v svojem VI. delu tudi področni zakon, ki z natančno določitvijo pravic, obveznosti, načel in ukrepov upravljavcem osebnih podatkov daje neposredno zakonsko

podlago za obdelavo osebnih podatkov na področju neposrednega trženja, videonadzora, biometrije, evidentiranja vstopov in izstopov iz prostora ter strokovnega nadzora.²¹ Za vse tiste primere, ko specialnega zakona ni, pa ZVOP-1 postavlja smernice, pravila, osnovna načela za kakršnokoli obdelavo osebnih podatkov in hkrati tudi smernice za urejanje tega področja v specialnih oziroma področnih zakonih.²²

3.2.1.1. Načela

V začetnih členih so zapisana glavna načela. V 2. členu je zapisano načelo zakonitosti in poštenosti, ki pomeni, da morajo biti splošna pravila obdelave osebnih podatkov predpisana z zakonom, hkrati pa morajo vsi, ki obdelujejo podatke, ravnati pošteno. V ta člen je bila implementirana določba Direktive 95/46/ES, ki je določila, da morajo biti vsi osebni podatki pošteno in zakonito obdelani.²³

Drugo načelo, določeno v 3. členu zakona, ki ga je prav tako vsebovano v Direktivi 95/46/ES, je načelo sorazmernosti, ki določa, da morajo biti osebni podatki, ki se obdelujejo, ustrezni in po obsegu primerni glede na namene, za katere se zbirajo in nadalje obdelujejo. Ustavno sodišče RS je v odločbi leta 2003 opozorilo, da se mora za omejitev varstva osebnih podatkov uporabljati tako imenovani strogi test sorazmernosti.²⁴

V 4. členu ZVOP-1 je definirana prepoved diskriminacije, s katero je vsakemu posamezniku zagotovljeno varstvo osebnih podatkov, ne glede na narodnost, raso, barvo, veroizpoved, etnično pripadnost, spol, jezik, politično in drugo prepričanje, spolno usmerjenost, premoženjsko stanje, rojstvo, izobrazbo, družbeni položaj, državljanstvo, kraj oziroma vrsto prebivališča ali katerokoli drugo okoliščino. Takšna določba je splošna antidiskriminacijska klavzula, ki jo poznajo tudi temeljni predpisi s področja varstva temeljnih človekovih pravic.²⁵

3.2.1.2. Krajevna veljavnost

ZVOP-1 velja za upravljavce, ki so ustanovljeni, imajo sedež ali so registrirani oziroma je njihova podružnica registrirana v Republiki Sloveniji. Uporabi se tudi v primeru, če upravljavec ni ustanovljen, nima sedeža oziroma ni registriran v državi članici Evropske unije in za obdelavo osebnih podatkov uporablja avtomatsko ali drugo opremo, ki se nahaja v Republiki Sloveniji, v kolikor se ta ne uporablja zgolj za prenos podatkov, kar določa 5. člen.

²¹ J. Bogataj, nav. delo, str. 23.

²² N. Pirc Musar, nav. delo, str. 40.

²³ Prav tam, str. 42.

²⁴ Odločba US RS, št. U-I-60/03 z dne 4. 12. 2003.

²⁵ N. Pirc Musar, nav. delo, str. 49.

3.2.1.3. Pomen izrazov

V 6. členu zakon določa pomen izrazov, ki se pojavijo v zakonu.

Pomembna je predvsem razlaga pojma obdelave osebnih podatkov, ki določa, da obdelava pomeni kakršnokoli delovanje ali niz delovanj, ki se izvaja v zvezi z osebnimi podatki, ki so avtomatizirano obdelani, 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, vpogled, uporaba, razkritje s prenosom, sporočanje, širjenje ali drugo dajanje na razpolago, razvrstitev ali povezovanje, blokiranje, anonimiziranje, izbris ali uničenje. Zakon ne določa numerus clausus dejanj temveč z besedo »zlasti« le primeroma našteva možne oblike obdelovanja, tako da lahko tudi kakršnokoli drugo ravnanje pomeni njihovo obdelovanje.²⁶

Nadalje sta določeni tudi definiciji upravljavca in pogodbenega obdelovalca, ki se razlikujeta v tem, da upravljavec kot fizična ali pravna oseba javnega ali zasebnega sektorja sam ali skupaj z drugimi določa namene in sredstva obdelave osebnih podatkov, medtem ko pogodbeni obdelovalec obdeluje osebne podatke v imenu in na račun upravljavca.

V 14. točki je opisan pojem osebne privolitve posameznika, ki je prostovoljna izjava volje posameznika, da se lahko njegovi osebni podatki obdelujejo za določen namen, in je dana na podlagi informacij, ki mu jih mora zagotoviti upravljavec po tem zakonu. Osebna privolitev posameznika je lahko pisna, ustna ali druga ustrezna privolitev posameznika. ZVOP-1 je glede privolitve posameznika bistveno manj strog, kot so bili zakoni o varstvu osebnih podatkov pred njim, saj so dovoljevali le obdelavo na podlagi pisne privolitve, medtem ko ZVOP-1 dovoljuje tudi ustno ali drugo ustrezno privolitev, iz katere je mogoče nedvomno sklepati na posameznikovo privolitev.²⁷

ZVOP-1 jasno določa tudi pojma blokiranje in anonimiziranje. Blokiranje je takšna označitev osebnih podatkov, da se omeji ali prepreči njihova nadaljnja obdelava, medtem ko anonimiziranje pomeni takšno spremembo oblike osebnih podatkov, da jih ni več mogoče povezati s posameznikom ali je to mogoče le z nesorazmerno velikimi napori, stroški ali porabo časa.

V 19. točki je določena definicija občutljivih osebnih podatkov, ki pravi, da so to podatki o rasnem, narodnem ali narodnostnem poreklu, političnem, verskem ali filozofskem prepričanju,

²⁶ N. Pirc Musar in J. Bogataj, nav. delo, str. 60.

²⁷ Prav tam, str. 66.

članstvu v sindikatu, zdravstvenem stanju, spolnem življenju, vpisu ali izbrisu v ali iz kazenske evidence ali evidenc, ki se vodijo na podlagi zakona, ki ureja prekrške. Občutljivi osebni podatki pa so tudi biometrične značilnosti, če je z njihovo uporabo mogoče določiti posameznika v zvezi s kakšno od prej navedenih okoliščin.

3.2.1.4. Obdelava osebnih podatkov

Drugi del zakona vsebuje določbe, ki urejajo obdelavo osebnih podatkov in v 8. členu določa splošno opredelitev pravne podlage za obdelavo osebnih podatkov, kateri se lahko obdelujejo le, če obdelavo določa zakon ali če je za obdelavo podana osebna privolitev posameznika. Ker gre zgolj za splošno opredelitev pravne podlage, so v 9. in 10. členu natančneje razdelane ostale pravne podlage in izjeme od splošnih pravnih podlag. V drugem odstavku pa je vsebovana zahteva, da mora biti namen obdelave osebnih podatkov določen v zakonu, v primeru osebne privolitve pa mora biti posameznik predhodno pisno ali na drug ustrezen način seznanjen z namenom obdelave.

V 9. členu so določene pravne podlage v javnem sektorju, ki jih ne bom povzemala, saj se v magistrskem delu osredotočam predvsem na zasebni sektor.

Glede na določbo prvega odstavka 10. člena ZVOP-1 se osebni podatki v zasebnem sektorju lahko obdelujejo, če obdelavo osebnih podatkov in osebne podatke, ki se obdelujejo, dopušča zakon. Z zakonom pa se lahko določi, da se določeni osebni podatki obdelujejo le na podlagi osebne privolitve posameznika. Poleg zakona in privolitve posameznika, se lahko osebni podatki obdelujejo tudi na podlagi sklenjene pogodbe oziroma že v fazi pogajanj za sklenitev pogodbe, če je obdelava potrebna in primerna za izvedbo pogajanj ali za izpolnjevanje pogodbe. Zadnjo pravno podlago v zasebnem sektorju pa predstavljajo zakoniti interesi zasebnega sektorja, v kolikor prevladajo nad interesi posameznika.

V 11. členu zakon določa možnost upravljavca, da posamezna opravila v zvezi z obdelavo osebnih podatkov, s pogodbo zaupa pogodbenemu obdelovalcu, ki je registriran za opravljanje takšne dejavnosti in hkrati zagotavlja ustrezne varnostne postopke in ukrepe. Pogodbeni obdelovalec sme posamezna opravila opravljati v okviru naročnikovih pooblastil in podatkov ne sme obdelovati za noben drug namen. Vse pravice in obveznosti uredita s pogodbo o obdelavi, ki mora biti sklenjena v pisni obliki in mora vsebovati tudi dogovor o potrebnih varnostnih ukrepih.

Obdelavo občutljivih osebnih podatkov opredeljuje 13. člen zakona, ki taksativno določa kdaj se lahko takšni podatki sploh obdelujejo. In sicer, na podlagi privolitve, za obdelavo podatkov

na področju zaposlovanja, za potrebe varovanja življenja, za namene zakonitih dejavnosti, če jih je posameznik sam javno objavil, za zdravstvene namene, za potrebe pravnih zahtevkov ali če tako določa drug zakon. Zaradi svoje narave jih je potrebno še bolj skrbno varovati kot ostale vrste osebnih podatkov, kar določa 14. člen zakona.

ZVOP-1 v 15. členu varuje posameznika pred avtomatiziranim odločanjem, ki se v digitalni dobi uporablja vedno pogosteje. Odločitev na podlagi avtomatizacije, ki ima za posledico pravne učinke v zvezi s posameznikom ali nanj znatno vpliva in je namenjena ovrednotenju nekaterih osebnih vidikov v zvezi z njim, je dovoljena le v dveh primerih: 1. če je odločitev sprejeta med sklepanjem ali izvajanjem pogodbe, pod pogojem, da je pobuda za sklenitev ali izvajanje pogodbe, ki jo je vložil posameznik, na katerega se osebni podatki nanašajo, izpolnjena ali da obstajajo primerni ukrepi za varstvo njegovih zakonitih interesov, kakršni so zlasti dogovori, ki mu omogočajo ugovarjati takšni odločitvi ali izraziti njegovo stališče in 2. če je določena z zakonom, ki določa tudi ukrepe za varstvo zakonitih interesov posameznika, na katerega se nanašajo osebni podatki, zlasti možnost pravnega sredstva zoper takšno odločitev.

Upravljavca je na podlagi 19. člena dolžan posamezniku, katerega podatke zbira, sporočiti svoje kontaktne informacije, namen obdelave osebnih podatkov ter informacije o pravicah, ki mu pripadajo.

Podatki se lahko hranijo le toliko časa, dokler je to potrebno za dosego namena za katerega so bili zbrani, kar določa 21. člen. Po izpolnitvi namena obdelave se podatki zbrisajo, uničijo, blokirajo ali anonimizirajo, v kolikor zakon ne določa drugače.

Zakon v 24. in 25. členu določa organizacijske, tehnične in logično-tehnične postopke in ukrepe, ki jih morajo zagotoviti upravljavci in pogodbeni obdelovalci, da se prepreči slučajno ali namerno nepooblaščen uničevanje podatkov, njihova sprememba ali izguba ter nepooblaščen obdelava. Ti ukrepi zajemajo varovanje prostorov, opreme in sistemsko programske opreme, varovanje aplikativne programske opreme, preprečevanje nepooblaščenega dostopa do osebnih podatkov pri prenosu, učinkovito blokiranje, uničevanje, izbris ali anonimizacijo ter poznejše ugotavljanje, kdaj so bili podatki vneseni v zbirko osebnih podatkov, uporabljeni ali drugače obdelani in kdo je to storil.

3.2.1.5. Pravice posameznika

V tretjem delu zakon ureja pravice posameznikov katerih podatki se obdelujejo.

Pravica posameznika do seznanitve je določena v 30. členu in določa, da mora upravljavec na zahtevo posameznika opredeliti, ali se obdelujejo podatki v zvezi z njim, mu omogočiti vpogled v osebne podatke, mu posredovati izpis podatkov iz zbirke, mu posredovati seznam uporabnikov, katerim so bili podatki posredovani, dati informacijo o virih, na katerih temeljijo zapisi, dati informacije o namenu obdelave in pojasniti tehnične postopke odločanja v primeru avtomatiziranega odločanja. V 31. členu je določen postopek seznanitve oziroma postopek vložitve zahteve posameznika.

Ostale pravice posameznikov, ki zagotavljajo transparentnost obdelave osebnih podatkov so urejene v 32. členu. Upravljavec mora na zahtevo posameznika, na katerega se nanašajo osebni podatki, dopolniti, popraviti, blokirati ali izbrisati osebne podatke, za katere posameznik dokaže, da so nepopolni, netočni ali neažurni ali da so bili zbrani ali obdelani v nasprotju z zakonom. Prav tako mora na zahtevo o tem obvestiti vse uporabnike in pogodbene obdelovalce. Posameznik ima kadarkoli z ugovorom pravico zahtevati prenehanje obdelave podatkov na podlagi zakonitega interesa upravljavca.

3.2.2. Predlog ZVOP-2

Predlog Zakona o varstvu osebnih podatkov (ZVOP-2) bi sicer moral biti sprejet najkasneje do 25. 5. 2018, ko se je začela uporabljati GDPR, vendar do zaključka priprave magistrske naloge predlog še ni bil potrjen s strani državnega zbora, zato bom v nadaljevanju predstavila zadnjo verzijo predloga, ki je bil predložen na sejo državnega zbora dne 4. 4. 2018.

Predlog naj bi zasledoval dva cilja, ki sta omenjena tudi v samem spremnem besedilu zakona. Prvi je zagotovitev izvrševanja določb GDPR na način, da bi bil zakon čimbolj sistematski in bi bilo čim več vprašanj urejeno na enem mestu. Drugi cilj pa je omogočiti ljudem, javnim organom in poslovnim subjektom čimbolj povezane in pojasnjevalno predpisane sistemske norme, ki bodo omogočile koherenten pristop k uresničevanju in varstvu pravic.

Predlog ZVOP-2 v večini povzema določbe GDPR skoraj do popolnosti in jih nadgrajuje, kjer je to potrebno. Zato bom v tem poglavju opisala zgolj novosti in morebitne nadgradnje, ki jih določa predlog.

3.2.2.1. *Temeljne določbe*

Glede na zadnjo verzijo predloga je v 2. členu določena pravica do varstva osebnih podatkov, ki jo, kot omenjeno, sicer ureja že 38. člen URS. Poleg pravice, ta člen povzema tudi načela, na katerih sloni GDPR. Gre torej za nek uveden člen, ki bo nadomestil 1. člen ZVOP-1.

V 11. členu je Slovenija izkoristila diskrecijsko pravico in znižala starost otrok, za katere morajo privolitev dati oziroma odobriti starši, na 15 let. Pri tem so sledili 146. členu Družinskega zakonika,²⁸ skladno s katerimi, ima otrok pri petnajstih letih sposobnost sam sklepati pravne posle.

V predlogu zakona so v 12. členu povzeli obdelavo posebnih vrst osebnih podatkov iz GDPR, v tretjem odstavku pa so dodali še posebne zaščitne ukrepe, ki jih mora zagotoviti tisti, ki te podatke obdeluje.

3.2.2.2. Pravice posameznikov

Členov GDPR od 13. do 20. predlog ni povzel ampak se nanje zgolj sklicuje v 14. členu, ki ureja odgovornost upravljavca, kar je nenavadno, saj so v teh členih določene vse pravice posameznikov. To ni problematično z vidika veljavnosti, saj je GDPR neposredno uporabljiv pravni vir, temveč z vidika informiranosti posameznika in glede na dejstvo, da so večji del ostalih členov skoraj dobesedno prenesli v predlog zakona.

Predlog zakona opisuje zgolj postopek vložitve zahteve posameznika, postopek odločanja in možnost pritožbe.

3.2.2.3. Upravljavec in obdelovalec

Tudi določbe o upravljavcu in obdelovalcu so v večini povzete iz GDPR, pri določbi 34. člena predloga, ki ureja varnost osebnih podatkov pa sta dodana dva ukrepa, ki naj bi ju zagotovila upravljavec in obdelovalec podatkov. Prvi je zagotovitev programske opreme, da obdelava osebnih podatkov v zbirkah poteka v mejah pooblastil uporabnika takšnega sredstva. Drugi pa določa ukrepe, ki omogočajo poznejše ugotavljanje, kdaj so bili podatki vneseni v zbirko, uporabljeni ali kako drugače obdelani in kdo je to storil, za obdobje petih let od zaključka leta, v katerem je potekala obdelava. Zadnji ukrep je v neki meri predhodno določal že ZVOP-1 v 30. členu.

3.2.2.4. Pooblaščen oseba za varstvo osebnih podatkov

Predlog zakona je v 46. členu določil pogoje, ki jih mora pooblaščen oseba izpolnjevati pred imenovanjem. Glede ostalih določb je povzel določbe GDPR in jih bolj podrobno uredil.

²⁸ Uradni list RS, št. 15/17 in 21/18 – ZNOrg.

4. RAZPRAVNI DEL

4.1. Zbiranje podatkov

Obdelava osebnih podatkov, pod katero spada tudi samo zbiranje podatkov, je v GDPR definirana kot vsako dejanje ali niz dejanj, ki se izvaja v zvezi z osebnimi podatki ali nizi osebnih podatkov z avtomatiziranimi sredstvi ali brez njih. Pred vsakim zbiranjem oziroma obdelavo podatkov je potrebno preveriti ali imamo ustrezno pravno podlago. Na voljo je 6 pravnih temeljev, ki jih določa 6. člen GDPR: privolitev, izvajanje pogodbe, izpolnitev zakonske obveznosti, zaščita življenjskih interesov posameznika, opravljanje naloge v javnem interesu in zakoniti interes. Vsi temelji so enakovredni, kar je, glede na prakso, v nasprotju s splošnim prepričanjem ljudi, da je privolitev primarni in najbolj pomemben pravni temelj. Slednjega tako izberemo glede na samo naravo osebnih podatkov in glede na namen.

Velika količina podatkov ne nastaja več samo na podlagi naše zavestne aktivne dejavnosti, kot je snemanje, slikanje, pisanje, temveč jih vedno več pasivno ustvarijo tudi naprave, kot so telefoni, računalniki. Ti podatki so preprosto dostopni in na voljo za analize, saj se shranjujejo v digitalni obliki. Ravno ta tehnologija analiziranja novih uporabnih informacij iz posameznih zbirk podatkov in oblikovanje novih zbirk je ključnega pomena v današnjem času.²⁹ Prav analiza je tista točka, ki pokaže resnično moč teh obsežnih zbirk podatkov, t.i. velikega podatkovja, ki vodi do vzpostavitve novih, presenetljivih in nepričakovanih rezultatov.³⁰

Samo s pomočjo interneta je mogoče o posamezniku zbrati številne osebne podatke. A internet uporabnikom a priori ne zagotavlja zasebnosti ampak si jo morajo zagotoviti uporabniki sami. Po ugotovitvah Odbora za varstvo osebnih podatkov, je internet odprt javni sistem, ki deluje po tehnično znanih protokolih in je usmerjen v izmenjavo informacij, ne v zagotavljanje tajnosti informacij.³¹ Torej mora v prvi vrsti posameznik sam poskrbeti za varno prenašanje in shranjevanje svojih osebnih podatkov na internetu.

Pri zbiranju podatkov je potrebno zasledovati tudi načelo najmanjšega obsega podatkov in zbirati samo tiste podatke, ki so res potrebni za dosego zastavljenega namena. Vsak upravljavec mora pred vsakim zbiranjem narediti analizo in oceniti katere osebne podatke posameznika potrebuje in katera pravna podlaga bi bila za zbiranje le-teh najbolj primerna.

²⁹ S. Dolenc, nav. delo, str. 112.

³⁰ H. Uršič, nav. delo, str. 358.

³¹ M. Brezovšek in D. Črnc, nav. delo, str. 202.

V zvezi z zbiranjem osebnih podatkov na spletu mora upravljavec premisliti o sorazmernosti zbiranja teh podatkov. V kolikor posameznik v obdelavo ni privolil, mora biti le-ta upravičena in minimalna.³²

4.1.1. Big data

Moderna informacijska tehnologija je omogočila povezovanje in združevanje različnih vrst podatkov iz različnih virov, s pomočjo katerih ustvarja nove dodane vrednosti osebnih podatkov pod imenom veliko podatkovje oziroma »big data«.

Enotne definicije velikega podatkovja ni. Razumemo ga kot novo orodje, ki obsega tako velike količine podatkov kot tudi načine in metode iskanja novih pomenov s pomočjo algoritmov.³³ Razlog za pojav tega novega orodja je verjetno ravno v tem, da smo samo v letu 2016 proizvedli toliko podatkov kot prej v celotni zgodovini človeštva skupaj.³⁴

Z novimi načini ustvarjanje podatkov oziroma podatkovnih zbirk, veliko podatkovje prinaša ustvarjalcem novo družbeno moč in družbeni nadzor.³⁵ Osmišljanje podatkov s pomočjo algoritmov prinaša posameznikom, podjetjem in državam številne prednosti na različnih področjih. To orodje je zanimivo predvsem za organe pregona, ker jim pomaga pri namigih, kje se bo, po vsej verjetnosti, zgodilo novo kaznivo dejanje, veliko vrednost ima tudi za družbena omrežja, pri povezovanju ljudi, pripomoglo pa je tudi k večji avtomatizaciji transakcij na borzah.³⁶

Veliko podatkovje pa ne pomeni le množičnega zbiranja podatkov, ampak podatke osmišlja in ustvarja novo vrednost podatkov, predvsem z analizo teh podatkov.³⁷ Da pa bo analiza podatkov pravilna in predstavljala realne podatke, morajo biti podatki, ki jih uporabijo natančni, kakovostni, raznoliki, dovolj poglobljeni in objektivni.³⁸ Algoritmi lahko vsebujejo tudi predsodke ali nedovoljene parametre odločanja, bodisi zaradi napak pri oblikovanju bodisi zaradi njihove izrecne izključitve in posrednega računanja nekaterih parametrov iz drugih značilnosti.³⁹

³² M. Brkan, nav. delo, str. 68.

³³ A. Završnik in L. Selinšek, nav. delo, str. 11.

³⁴ A. Završnik, nav. delo, str.46

³⁵ A. Završnik in L. Selinšek, nav. delo, str. 11-12.

³⁶ A. Završnik, nav. delo, str. 36.

³⁷ Prav tam, str. 49.

³⁸ Prav tam, str. 41.

³⁹ Prav tam, str. 41.

Tehnologije velikega podatkovja na podlagi množice izbranih podatkov omogočajo dokaj zanesljivo napoved prihodnosti, kar predstavlja veliko prednost, tistega, ki lahko dostopa do takšnih informacij. Ravno zato veliko podjetij in držav vlaga veliko sredstev in energije v to tehnologijo, saj je, kot sem že omenila, dostop do takšnih informacij velika prednost pred ostalimi, ki teh podatkov ne posedujejo.⁴⁰

Pri velikem podatkovju gre predvsem za povezovanje podatkov iz različnih virov, ki sami zase ne nosijo velike vrednosti, v neko celoto, ki pridobi močan vsebinski pomen. Delci informacij so sami zase nekoristni, ko pa se jih poveže v celoto postane ta neprecenljiva. Ta pojav se imenuje mozaična teorija in se je prvič pojavila v sodni praksi Združenih državah Amerike.⁴¹ Mozaična teorija je povezana s konceptom pričakovane zasebnosti, ki je bil omenjen že v teoretičnem delu magistrskega dela.

Osebni podatki so vedno pomembnejši in v 21. stoletju predstavljajo pravo bogastvo oziroma novodobno nafto.

4.1.2. Internet stvari

Internet stvari temelji na povezovanju ogromne količine naprav z vgrajenimi senzorji oziroma tipali, ki jim omogočajo povezovanje in komuniciranje med seboj in z najrazličnejšimi aplikacijami. 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.⁴²

Pametne naprave so bile namenoma oblikovane tako, da so uporabniku čim manj opazne in niso vsiljive, kar se na področju varstva osebnih podatkov kaže kot pomanjkljivost. Prednost teh naprav je tudi brezžična povezava z internetom, ki pa je problematična z vidika varstva osebnih podatkov, saj so naprave tako bolj izpostavljene napadom in prisluškovanjem s strani drugih. Namen interneta stvari, za razliko od velikega podatkovja, ni množično zbiranje podatkov, temveč olajšanje in zagotavljanje večje kvalitete življenja posameznikov.

Sestavljen je iz komunikacijskega, energetskega in transportnega interneta, ki skupaj delujejo kot en sam operacijski sistem, pri čemer vsak od treh internetov podpira drugega.⁴³ Pojavlja se v vseh industrijskih in komercialnih sektorjih, uporablja pa se tudi za ustvarjanje pametnih

⁴⁰ S. Dolenc, nav. delo, str. 113.

⁴¹ P. Križnar, nav. delo, str. 114.

⁴² <<https://iprom.si/slovar/internet-stvari/>>.

⁴³ J. Rifkin, nav. delo, str. 22.

mest. V komercialnem sektorju se uporabljajo predvsem za spremljanje pretoka blaga in storitev, tipala v skladiščih beležijo razpoložljivost zalog in obveščajo glavno pisarno o okvarah, v trgovinah pa s pomočjo tipal spremljajo povpraševanje po določenih izdelkih.⁴⁴

Da je internet stvari pomemben tehnološki napredek, govorijo podatki o izboljšanju termodinamičnega izkoristka, povečanju produktivnosti, zmanjšanju stroškov proizvodnje, ki so celoten obseg blaga in storitev v gospodarstvu pripeljali na skoraj ničelne mejne stroške.⁴⁵ Senzorji nameščeni v cestni infrastrukturi, pametnih domovih, pametnih avtomobilih itd. naj bi na letni ravni do leta 2025 dosegli 11,1 trilijona ameriških dolarjev ekonomskih učinkov.⁴⁶ Internet stvari je kljub nevarnostim, ki jih prinaša, tehnološki napredek družbe, ki ga je potrebno obdržati oziroma razvijati naprej.

4.2. Problematični vidiki Splošne uredbe o varstvu podatkov

V tem poglavju se bom osredotočila na tri elemente, ki se meni zdijo najbolj problematični oziroma potrebni sprememb, kadar gre za področje velikega podatkovja in interneta stvari.

4.2.1. Pravna podlaga

Največji problem pri zbiranju podatkov za potrebe velikega podatkovja in interneta stvari je pomanjkanje seznanjenosti uporabnika z dejstvom, da se njegovi podatki pravzaprav zbirajo oziroma obdelujejo in uporabljajo v različne namene. Ideja velikega podatkovja in interneta stvari temelji namreč na načelu maksimizacije zbiranja podatkov. Kar pomeni, da se zbira ogromne količine podatkov, ki se hranijo za nedoločen čas in uporabljajo za nedoločene namene, kar je v popolnem nasprotju z načeloma minimizacije in omejitve obsega podatkov, na katerih temelji GDPR in vsa ostala zakonodaja s področja varstva osebnih podatkov.

Kot sem omenila že v tretjem poglavju, obstaja 6 pravnih temeljev za obdelavo osebnih podatkov. Za področje velikega podatkovja in interneta stvari pridejo najbolj v poštev sledeči: privolitve, pogodba in zakoniti interes upravljavca.

Problem pri privolitvi v obdelavo osebnih podatkov za potrebe velikega podatkovja je v nepredvidljivih in nenapovedljivih rabah teh podatkov, saj je privolitev, skladno z GDPR, mogoča le za specifične namene, ki jih je potrebno določiti vnaprej.⁴⁷ Zato privolitev v obliki, ki jo določa GDPR v te namene izgubi pomen in jo je praktično nemogoče pravilno zagotoviti

⁴⁴ J. Rifkin, nav. delo, str. 19.

⁴⁵ J. Rifkin, nav. delo, str. 18.

⁴⁶ A. Završnik, nav. delo, str. 47.

⁴⁷ H. Uršič, nav. delo, str. 364.

oziroma bi bila brezpredmetna. S tem, ko bi posameznik vnaprej privolil v nedoločeno obdelavo podatkov, bi pristal na vsakršno obdelavo in s tem tudi, da se uporabijo v njegovo škodo.⁴⁸ Kar absolutno nasprotuje vsem načelom, na katerih sloni GDPR.

Ravno zaradi teh težav nekateri menijo, da bi bilo, na področju velikega podatkovju, smiselno opustiti sistem privolitve posameznika v obdelavo njegovih osebnih podatkov, saj niso zmožni razumeti procesov in namenov obdelave, v katero so privolili, ker ne posedujejo zadostnega tehničnega znanja za to.⁴⁹ Nekateri avtorji predlagajo vrnitev pravne ureditve, ki je obstajala v devetdesetih letih ob pojavih moderne tehnologije, ko uporabniki prav tako niso razpolagali s potrebnim znanjem za razumevajočo odločitev oziroma privolitev. V takšnih primerih naj bi omejili vlogo posameznikov in okrepili vlogo upravljavcev, ki s takšnim znanjem razpolagajo.⁵⁰

Drug problem, ki se pojavi pri privolitvi, je kdo je pravzaprav uporabnik pametne naprave oziroma kdo bi moral privoliti v obdelavo podatkov na napravi. Tukaj se pojavi dilema, ali bi moral v obdelavo privoliti le lastnik naprave, ali bi to morali storiti vsi uporabniki naprave, in kako bi takšne privolitve sploh lahko zagotovili.

Pri internetu stvari bi, kot pravna podlaga za zbiranje osebnih podatkov, pogojno lahko prišla v poštevpogodba, saj gre za nakup naprave, katera potem zbira podatke. Na tej podlagi se lahko zbirajo le tisti podatki, ki so nujno potrebni za izvedbo pogodbe. Tukaj je torej potrebno oceniti, ali je uporabnost naprave, ki deluje na podlagi zbranih podatkov lahko del pogodbe, kot je določeno v GDPR ali ne. V kolikor bi ugotovili, da je to nujno potrebno za izvedbo pogodbe, pa je še vedno potrebno premisliti o uporabi varnostnih ukrepov za zavarovanje osebnih podatkov, še posebej pri internetu stvari, kjer se zbirajo predvsem posebne vrste podatkov, ki so še dodatno zaščiteni. Eden od takih ukrepov je psevdonomizacija, ki omogoča nadaljnje spremljanje in zbiranje podatkov, ki so potrebni, s tem, da se zaščiti identiteta posameznika.

Delovna skupina iz člena 29 je v mnenju št. 06/2014 dodatno pojasnila ureditev in izbiro pravnih podlag, predvsem zakoniti interes upravljavca. V njem je opozorila na to, da legitimnega interesa ne smejo uporabljati kot zadnje možnosti, v primeru, ko nobena druga podlaga ne bi prišla v poštev. Pred uporabo te pravne podlage je potrebno pretehtati kateri

⁴⁸ L. Selinšek, nav. delo, str. 177.

⁴⁹ A. Mantelaro, nav. delo, str. 659.

⁵⁰ A. Mantelaro, nav. delo, str. 655.

interes prevlada, interes upravljavca ali posameznika. Upravljavec mora v tem primeru, za razliko od ostalih podlag, opraviti poseben test in presoditi ali ima potreben legitimen interes za zbiranje določenih podatkov.⁵¹

V tem mnenju je Delovna skupina iz člena 29 tudi bolj podrobno navedla korake, ki bodo upravljavce pripeljali do pravilne odločitve. Prvi korak je, kot sem omenila že zgoraj, utemeljitev legitimnega interesa, kateri mora slediti objektivna presoja vplivov na posameznika. Nato se s pomočjo ravnotežnega testa presodi, kateri interesi oziroma pravice prevladajo. Na koncu sledi še preučitev potrebnih varnostnih ukrepov in varovalk za zaščito posameznika, še posebej, če gre za obdelavo posebnih vrst osebnih podatkov.⁵² Pri tem je potrebno poudariti, da psevdonomiziranje podatkov ne pomeni avtomatične spremembe nelegitimnega interesa v legitimnega, lahko pa v določenih primerih zmanjša poseg upravljavca v pravice posameznika.⁵³

Na vprašanje kaj lahko spada pod zakoniti interes upravljavca, je delno odgovorilo Sodišče Evropske unije v zadevi Google Španija in Google Inc. proti Agenciji za varstvo podatkov⁵⁴, kjer je zavzelo stališče, da obdelava podatkov, zbranih preko interneta stvari, ki se nanašajo na zdravstveno stanje posameznika, dom, zasebnost, lokacijo ali zasebno življenje, ne more biti opravičena zaradi ekonomskih interesov upravljavca. Ekonomski interes je namreč potrebno primerjati s temeljnimi svoboščinami posameznika, na katerega se ti podatki nanašajo.⁵⁵ Upravljavec ima dolžnost presojati legitimni interes za vsak posamičen primer posebej in obdržati dokaz o postopku presoje in ugotovljenih dejstvih.

4.2.2. Transparentnost

Čeprav je načelo transparentnosti oziroma preglednosti v GDPR omenjeno le bežno v 5. členu in ni izrecno opredeljeno, je eno izmed vodil GDPR, ki je opisano tudi v uvodnih določbah. V 39. odstavku uvodnih določb je namreč določeno, da morajo biti načini zbiranja, uporabe, pregledovanja in obseg obdelave pregledni.

⁵¹ Delovna skupina 29 člena, mnenje št. 06/2014, str. 9.

⁵² Prav tam, str. 50-51.

⁵³ Prav tam, str. 42.

⁵⁴ C-131/12.

⁵⁵ Prav tam, str. 15.

Načelo se nanaša na tri področja, in sicer na zagotavljanje informacij posameznikom v zvezi s pravično obdelavo podatkov, komuniciranje upravljavcev s posamezniki in uresničevanje pravic posameznikov.⁵⁶

Vsebuje zahtevo, da so vse informacije in sporočila, ki se nanašajo na obdelavo osebnih podatkov, lahko dostopni in razumljivi ter izraženi v jasnem in preprostem jeziku. To načelo zadeva predvsem informacije za posameznike, katerih osebni podatki se obdelujejo, o istovetnosti upravljavca in o namenih obdelave ter dodatne informacije, ki jih mora upravljavec zagotoviti posamezniku. Upravljavec mora posameznike opozoriti na tveganja, pravila, zaščitne ukrepe in pravice, ki jim pripadajo ter način za uresničevanje teh pravic.⁵⁷

Bistvo načela preglednosti je predhodna seznanitev posameznikov z obsegom in posledicami obdelave osebnih podatkov in izogibanje kasnejšim presenečenjem s strani posameznikov glede same obdelave podatkov.⁵⁸

Pri velikemu podatkovju in internetu stvari je verjetno najbolj problematično posamezniku predstaviti informacije v jasnem in preprostem jeziku. Upravljavec ima dolžnost, da posameznikom na razumljiv način razloži namen, za katerega se podatki zbirajo in se s tem izogne nerazumljivim tehničnim izrazom in terminologiji.

V (h) točki prvega odstavka 15. člena GDPR je določena pravica posameznika do dostopa podatka o obstoju avtomatiziranega sprejemanja odločitev, ki vključuje oblikovanje profilov, in o pomenu ter predvidenih posledicah. Pri zagotavljanju teh informacij bodo imeli upravljavci zelo velike težave glede jasnosti in razumljivosti s strani posameznikov. Še posebno pazljivi morajo biti pri zagotavljanju jasnih informacij otrokom oziroma mlajši populaciji, kjer mora biti jezik še bolj preprost.

Transparentnost upravljavca osebnih podatkov s posamezniki ima tako dobro kot tudi slabo stran. Dobra stran je predvsem večje zaupanje posameznikov oziroma uporabnikov naprav v primeru interneta stvari, slabost pa se lahko kaže v obliki sabotaže z lažnimi podatki, ko posamezniki ugotovijo, da se ti podatki zbirajo za oblikovanje profilov. Pojavi se lahko tudi zastraševalni učinek (ang. chilling effect) v primeru zbiranja podatkov za potrebe osebnega

⁵⁶ Delovna skupina 29 člena, Smernice o preglednosti, str. 4.

⁵⁷ UL L 119.

⁵⁸ Delovna skupina člena 29, Smernice o preglednosti, str. 7.

oziroma ciljnega trženja, ki posameznike odvrne od internetnega iskanja, nakupovanja in uporabe posebnih potrošniških storitev.⁵⁹

4.2.3. Anonimizacija

Na področju anonimizacije osebnih podatkov je potrebno ločiti več različnih pojmov. Prvi je vsesplošni pojem de-identifikacije, ki obsega različne tehnike, s katerimi je mogoče odstraniti osebno določljive podatke iz zbirke podatkov. Po de-identifikaciji posameznika tako preko teh podatkov ni več mogoče identificirati. Anonimizacija je ena izmed tehnik de-identifikacije, ki odstranjuje neposredne identifikacijske znake, kot so ime, naslov, telefonska številka itd. Pseudonomizacija pa nadalje predstavlja podskupino anonimizacije in označuje odstranitev osebno določljivih podatkov s sistematičnim nadomeščanjem s pomočjo psevdonomov in omogoča obratni proces, zato ga ne smemo enačiti z anonimizacijo, ki ni povraten proces.

Anonimizirani podatki so samo tisti, ki jih nihče, ne le upravljavec, ne more več povezati z določljivim posameznikom oziroma bi takšno povezovanje zahtevalo nesorazmerno velike stroške, napore ali veliko porabljenega časa.⁶⁰ Pri presoji o določljivosti posameznika upravljavec ne upošteva le svojih zmožnosti temveč tudi zmožnosti ostalih subjektov, glede na vse zbirke osebnih podatkov.⁶¹

Pravo varstva osebnih podatkov zajema le podatke o določenem ali določljivem posamezniku, torej podatke na podlagi katerih je mogoče osebo identificirati. Ostali podatki spadajo med neosebne podatke, ki ne uživajo enakega varstva, med katere spadajo tudi anonimizirani podatki.⁶² Anonimizira se lahko nize podatkov, tabele in baze podatkov, posameznih podatkov pa se praktično ne da anonimizirati, lahko se jih zgolj psevdonomizira oziroma zamaskira.⁶³

Kljub uporabi naprednih postopkov anonimizacije osebnih podatkov, s katerimi se pobrišejo imena, naslovi in ostali identifikacijski podatki, slednje danes ne zadošča več, saj lahko kljub temu, nekdo iz zbirke medsebojno povezanih podatkov razbere identiteto konkretnih posameznikov.⁶⁴ Težava pri velikem podatkovju je namreč v tem, da je anonimizacija mogoča le do neke mere, saj je anonimizirane podatke še vedno mogoče povezati s konkretnim posameznikom, čemur pravimo re-identifikacija.

⁵⁹ A. Donovan, R. Finn in K. Wadhwa, nav. delo, str. 67-68.

⁶⁰ A. Tomšič, nav. delo, str. 22.

⁶¹ Mnenje št. 0712-1/2017/2497 z dne 19. 12. 2017.

⁶² L. Selinšek, nav. delo, str. 177.

⁶³ Mnenje št. 0712-1/2017/2497 z dne 19. 12. 2017.

⁶⁴ S. Dolenc, nav. delo, str. 118.

Namen velikega podatkovja je zbiranje ogromnih količin podatkov in povezovanje baz, ki vse te podatke vsebujejo. Prav to povezovanje baz podatkov oteži anonimizacijo, saj je o posamezniku na voljo veliko osebnih podatkov, ki jih je posledično lažje povezati z določenim ali določljivim posameznikom, s čimer anonimizacija izgubi svoj pomen. Anonimizacija pa je še veliko težja v zbirkah podatkov, kjer se posameznik od drugih loči le na podlagi lastnosti, ki jih zberejo senzorji, ki so nameščeni v pametnih napravah, saj je vsaka takšna zbirka unikatna zaradi količine podatkov, ki jih zbirajo.

5. SKLEPNE UGOTOVITVE

Varstvo osebnih podatkov je v zadnjem času postala zelo pereča tema, o kateri so veliko pisali tudi mediji, še posebej v mesecih pred začetkom uporabe GDPR. Zbiranje in obdelovanje osebnih podatkov postaja vedno bolj kompleksno in zahtevno za razumevanje povprečnega uporabnika informacijskih tehnologij. S tem se je posledično zmanjšal tudi posameznikov nadzor nad osebnimi podatki in z njim tudi njihova varnost.

Revolucijo na področju osebnih podatkov je prinesla Splošna uredba o varstvu podatkov, ki je modernizirala ureditev tega področja z uvedbo pomembnih novosti, predvsem pa s poudarkom na varstvu posameznikovih pravic. Pozornost s strani javnosti pa je pridobila zaradi relativno visokih kazni, ki lahko doletijo upravljavce in obdelovalce osebnih podatkov v primeru kršitve njenih določb.

Evropski zakonodajalec je nekoliko posodobil načela, na katerih temelji GDPR in na katerih so pred njo temeljili predhodni sekundarni pravni akti. Glavna novost GDPR so nove pravice posameznikov, s katerimi imajo posamezniki več nadzora nad obdelavo osebnih podatkov. Z vidika digitalnih tehnologij je pomembna razširitev definicije osebnih podatkov, ki od uveljavitve GDPR naprej vsebujejo tudi genetske in biometrične podatke, ki se zbirajo predvsem za potrebe interneta stvari in imenovanje pooblaščenih oseb za varstvo podatkov v primeru, ko gre za redno in sistematično spremljanje podatkov, kar velja za področje velikega podatkovja. GDPR zahteva tudi preventivno varovanje podatkov; upravljavec mora, v kolikor obstaja možnost velikega tveganja za pravice posameznikov, pred obdelavo podatkov z uporabo novih tehnologij opraviti oceno učinkov.

Razvoj tehnologije je vedno hitrejši, pravo pa se razvija in napreduje zelo počasi, saj stremi k urejeni in stabilni ureditvi. Zato je pomembno, da ureditev varstva osebnih podatkov ni preveč določna, ampak mora ostati prilagodljiva, da ne bo po nepotrebnem zavirala napredka tehnologije. Sprememba zakonodaje namreč zahteva veliko časa, predvsem pa so zanjo potrebna zadostna finančna sredstva.

V trenutni ureditvi se prvi problem pojavi pri pravni podlagi za zbiranje osebnih podatkov na področju interneta stvari in velikega podatkovja. GDPR namreč taksativno določa 6 pravnih temeljev, od katerih noben ni v popolnosti ustrezen za področje (sodobnih) digitalnih tehnologij. Rešitve problema, ki jih zagovarjajo nekateri avtorji, bi terjale temeljite spremembe trenutne zakonodaje, ki je bila pravzaprav komaj sprejeta oziroma je začela veljati letos. Drug

problem, ki sem ga izpostavila, je pomanjkljivo zagotavljanje transparentnosti in s tem povezanih pravic posameznikov, predvsem zaradi nerazumevanja tehnologije s strani povprečnih uporabnikov. Zadnji problem pa predstavlja nezmožnost zagotovitve pravilne anonimizacije podatkov, ki so bili zbrani s pomočjo senzorjev pametnih naprav ali za potrebe velikega podatkovja.

V magistrskem delu sem potrdila svojo hipotezo, da je trenutna ureditev varstva osebnih podatkov na področju sodobne tehnologije na določenih področjih zastarela in neustrezna, kar ogroža varstvo posameznikov, katerih podatki se obdelujejo.

Čeprav sem mnenja, da je trenutna ureditev še vedno v zaostanku z moderno tehnologijo, je Splošna uredba o varstvu podatkov naredila velik korak naprej in pripomogla k večji ozaveščenosti varstva osebnih podatkov, ki je v današnjem času zelo pomembna tema. Njen glavni cilj, tj. zagotovitev večjega varstva posameznikom in ozaveščanje ljudi o pomembnosti varstva osebnih podatkov, je bil kljub temu dosežen. Eden večjih izzivov na tem področju v prihodnosti bo najti ravnovesje med pravicami posameznikov in potrebnim razvojem in tehnološkim napredkom družbe.

6. LITERATURA

Monografije:

- Marjan Brezovšek in Damir Črnc: Demokratična uprava in tajnost podatkov. Fakulteta za družbene vede, Ljubljana 2007, str. 202.
- Maja Brkan: Varstvo osebnih podatkov v spletnem okolju, v: Meta Ahtik in drugi; Matija Damjan(ur.): Pravo v informacijski družbi. GV založba, Ljubljana 2014, str. 68.
- Janez Čebulj: Varstvo informacijske zasebnosti v Evropi in v Sloveniji. Inštitut za javno pravo pri Pravni fakulteti, Ljubljana 1992, str. 7.
- Sašo Dolenc: Veliko podatkovje in avtonomni subjekt svobodne volje, v: Aleš Završnik (ur.), Liljana Selinšek (ur.) in drugi: Pravo in nadzor v dobi velikega podatkovja. Inštitut za kriminologijo pri Pravni fakulteti, Ljubljana 2018, str. 112-125.
- Matej Kovačič: Nadzor in zasebnost v informacijski družbi: Filozofski, sociološki, pravni in tehnični vidiki nadzora in zasebnosti na internetu. Znanstvena knjižnica - Fakulteta za družbene vede, Ljubljana 2006, str. 12.
- Primož Križnar: Varstvo lokacijske zasebnosti s pomočjo mozaične teorije podatkov, v: Zbornik znanstvenih razprav, 76 (2016), str. 114.
- Jeremy Rifkin: Družba ničelnih mejnih stroškov. Prevod Urške Pajer, Modrijan, Ljubljana 2015, str. 18-22.
- Janez Stušek: Potencial velikega podatkovja z vidika obrambe obdolženca, v: Aleš Završnik (ur.), Liljana Selinšek (ur.) in drugi: Pravo in nadzor v dobi velikega podatkovja. Inštitut za kriminologijo pri Pravni fakulteti, Ljubljana 2018, str. 218.
- Helena Uršič: Je v dobi velikega podatkovja še prostor za mikro pravice posameznika?, v: Aleš Završnik (ur.), Liljana Selinšek (ur.) in drugi: Pravo in nadzor v dobi velikega podatkovja. Inštitut za kriminologijo pri Pravni fakulteti, Ljubljana 2018, str. 358.
- Aleš Završnik: Algokracija: od vladavine prava do vladavine algoritmov, v: Aleš Završnik (ur.), Liljana Selinšek (ur.) in drugi: Pravo in nadzor v dobi velikega podatkovja. Inštitut za kriminologijo pri Pravni fakulteti, Ljubljana 2018, str. 36-49.
- Aleš Završnik in Liljana Selinšek: Uvodna beseda: Zakaj je veliko podatkovje pomembno za pravo, kriminologijo in družbeni nadzor?, v: Aleš Završnik (ur.), Liljana Selinšek (ur.) in drugi: Pravo in nadzor v dobi velikega podatkovja. Inštitut za kriminologijo pri Pravni fakulteti, Ljubljana 2018, str. 11-12.

Članki:

- Anna Donovan, Rachel Finn in Kush Wadhwa (ur.): Deliverable D2.1: Report on legal, economic, social, ethical and political issues, 2014.
- Alessandro Mantelero: The future of consumer data protection in the E.U.: Re-thinking the “notice and consent” paradigm in the new era of predictive analytics, v: Computer Law & Security Review, 30 (2014) 6, str. 655-659.
- Liljana Selinšek: Veliko podatkovje v pravu in ekonomiji: veliki izzivi ali velike težave?, v: Lexonomica, 7 (2015) št. 2, str. 177.
- Andrej Tomšič: Varstvo osebnih podatkov v dobi podatkovnega izobilja, v: Smartdoc, (2014), str. 22.
- Samuel D. Warren in Louis D. Brandis: The right to privacy, v: Harvard Law Review, 4 (1890) 5, str. 193-220.

Pravni predpisi:

- Article 29 Working Party: Guidelines on transparency under Regulation 2016/679, 2018.
- Jože Bogataj: Uvodna pojasnila, v Nataša Pirc Musar (ur.) in drugi: Zakon o varstvu osebnih podatkov (ZVOP-1): s komentarjem. GV založba, Ljubljana 2006, str. 19-60.
- Delovna skupina za varstvo podatkov iz člena 29: Mnenje št. 6/2014 o pojmu zakonitih interesov upravljavca podatkov iz člena 7 Direktive 95/46/ES, 2014.
- Delovna skupina za varstvo podatkov iz člena 29: Mnenje št. 6/2014 o pojmu zakonitih interesov upravljavca podatkov iz člena 7 Direktive 95/46/ES, 2014.
- Delovna skupina za varstvo podatkov iz člena 29: Mnenje 8/2014 o nedavnem razvoju dogodkov glede interneta stvari, 2014.
- 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.
- Družinski zakonik. Uradni list RS, št. 15/17 in 21/18 – ZNOrg.
- Listina EU o temeljnih pravicah. UL C 202, 7. 6. 2016.
- Mnenje Informacijskega pooblaščenca št. 0712-1/2014/3443 z dne 7. 11. 2014.
- Mnenje Informacijskega pooblaščenca št. 0712-1/2017/2497 t dne 19. 12. 2017.
- Nataša Pirc Musar (ur.) in drugi: Zakon o varstvu osebnih podatkov (ZVOP-1): s komentarjem. GV založba, Ljubljana 2006, str. 40-60.

- Pogodba o delovanju Evropske unije. UL C 326, 26. 10. 2012.
- Predlog Zakona o varstvu osebnih podatkov (ZVOP-2) z dne 6. 4. 2018.
- Splošna deklaracija človekovih pravic A/RES/217A (III), 1948.
- 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).
- Ustava Republike Slovenije. Uradni list RS, št. 33/91-I, 42/97 – UZS68, 66/00 – UZ80, 24/03 – UZ3a, 47, 68, 69/04 – UZ14, 69/04 – UZ43, 69/04 – UZ50, 68/06 – UZ121,140,143, 47/13 – UZ148, 47/13 – UZ90,97,99 in 75/16 – UZ70a.
- Zakon o varstvu osebnih podatkov. Uradni list RS, št. 94/07 – uradno prečiščeno besedilo.

Sodna praksa:

- Odločba US RS, št. U-I-60/03 z dne 4. 12. 2003.
- US RS Up-3381/07 z dne 4. 3. 2010.
- Sodba Sodišča EU, C-131/12 z dne 13. 5. 2014.

Spletni viri:

- <Iprom.si/slovar/internet-stvari> (13. 7. 2018).
- <www.gartner.com/newsroom/id/3598917> (29. 6. 2018).
- <<https://svetkapitala.delo.si/ikonomija/se-ze-pripravljate-na-novo-uredbo-o-varstvu-osebni-podatkov-3293>> (13. 6. 2018).
- <<https://sskj.si/?s=podatek>> (15. 5. 2018).