UNIVERZA V LJUBLJANI
FAKULTETA ZA DRUŽBENE VEDE

Damjan Mihelič

Varovanje zasebnosti v ZDA in EU v luči novih družbeno-tehnoloških fenomenov

Magistrsko delo

Ljubljana, 2016

UNIVERZA V LJUBLJANI
FAKULTETA ZA DRUŽBENE VEDE

Damjan Mihelič
Mentor: dr. Bogomil Ferfila

Varovanje zasebnosti v ZDA in EU v luči novih družbeno-tehnoloških fenomenov

Magistrsko delo

Ljubljana, 2016

Univerza
v Ljubljani
Fakulteta
za družbene vede

Kardeljeva ploščad 5
1000 Ljubljana, Slovenija
telefon 01 58 05 122
01 58 05 120

IZJAVA O AVTORSTVU
magistrskega dela

Podpisani/-a Damjan Mihelič, z vpisno številko 21051150, sem avtor/-ica magistrskega dela z naslovom: Varovanje zasebnosti v ZDA in EU v luči novih družbeno-tehnoloških fenomenov.

S svojim podpisom zagotavljam, da:

- je predloženo magistrsko delo izključno rezultat mojega lastnega raziskovalnega dela;
- sem poskrbel/-a, da so dela in mnenja drugih avtorjev oz. avtoric, ki jih uporabljam v predloženem delu, navedena oz. citirana v skladu s fakultetnimi navodili;
- sem poskrbel/-a, da so vsa dela in mnenja drugih avtorjev oz. avtoric navedena v seznamu virov, ki je sestavni element predloženega dela in je zapisan v skladu s fakultetnimi navodili;
- sem pridobil/-a vsa dovoljenja za uporabo avtorskih del, ki so v celoti prenesena v predloženo delo in sem to tudi jasno zapisal/-a v predloženem delu;
- se zavedam, da je plagiatorstvo – predstavljanje tujih del, bodisi v obliki citata bodisi v obliki skoraj dobesednega parafraziranja bodisi v grafični obliki, s katerim so tuje misli oz. ideje predstavljene kot moje lastne – kaznivo po zakonu (Zakon o avtorski in sorodnih pravicah (UL RS, št. 16/07-UPB3, 68/08, 85/10 Skl.US: U-I-191/09-7, Up-916/09-16)), prekršek pa podleže tudi ukrepom Fakultete za družbene vede v skladu z njenimi pravili;
- se zavedam posledic, ki jih dokazano plagiatorstvo lahko predstavlja za predloženo delo in za moj status na Fakulteti za družbene vede;
- je elektronska oblika identična s tiskano obliko magistrskega dela ter soglašam z objavo magistrskega dela v zbirki »Dela FDV«.

V Ljubljani, dne 12. 5. 2016 Podpis avtorja/-ice: _____

Varovanje zasebnosti v ZDA in EU
v luči novih družbeno-tehnoloških fenomenov

Zasebnost v informacijski družbi je koncept, do katerega imajo v ZDA drugačen odnos kot v EU. Zaradi različne zgodovine, pravne tradicije in drugačnih gospodarskih vrednot se je v ZDA razvil pristop, ki zasebnost obravnava manj kot pravico in bolj kot dobrino, s katero je mogoče trgovati po načelih prostega trga. Na drugi strani ima Evropa veliko izkušenj s totalitarnimi režimi, kar je eden od razlogov, da je v evropskih državah zasebnost razumljena kot neodtujljiva pravica, ki predstavlja enega od temeljev svobodnega delovanja in izražanja posameznikov v družbi ter jo je treba zato ustrezno zakonsko zaščititi. Posledično je zakonsko varovanje informacijske zasebnosti v EU mnogo bolj sistematično in celovito kot v ZDA, kjer je način varovanja zasebnosti sektorski.

Ogrožanje informacijske zasebnosti dobiva nove dimenzije z uveljavljanjem novih družbeno-tehnoloških fenomenov, s čimer so mišljene tehnologije masovnih podatkov, računalništva v oblaku ter interneta stvari, ki so v tem delu tudi podrobno predstavljene. Osrednja zamisel tega dela je, da omenjeni družbeno-tehnološki fenomeni prinašajo izzive na področje varovanja zasebnosti, na katere je obstoječa zakonodaja premalo pripravljena. Ti izzivi so posledica specifičnosti masovnih podatkov, ki se vse pogosteje obdelujejo preko storitev računalništva v oblaku, prihajajoči internet stvari pa bo njihovo količino še izdatno povečal. Med njih spadajo težave s potencialno ponovno identifikacijo anonimiziranih podatkov, neustreznost koncepta informacij, ki omogočajo identifikacijo posameznika, kot temelja osebnih podatkov, vprašanje lastništva nad podatki ter novih spoznanj, pridobljenih z njihovo pomočjo, neprimernost načela obveščanja in soglasja kot trenutno poglavitnega načina urejanja pridobivanja podatkov, problematika samodejnega profiliranja na podlagi obdelave podatkov, zajemanje podatkov iz vse bolj intimnih področij življenj uporabnikov itd.

Ker se regulatorne rešitve praviloma sprejemajo počasi in postopno, je v tem delu izražen argument, da bodo bodoče rešitve za varovanje informacijske zasebnosti morale vključevati tudi drugačne pristope, kot sta uporaba tehnologije in zaščita zasebnosti z mehanizmi tržnega gospodarstva. Nekateri primeri tovrstnih rešitev so denimo vgrajena zasebnost, storitve na podlagi osebnih podatkov, diferencialna zasebnost itd. S tem se odpira tudi vprašanje nadaljnjega pojmovanja zasebnosti, njenega vrednotenja s strani posameznikov in družbe ter načinov njenega varovanja v prihodnosti.

Ključne besede: masovni podatki, računalništvo v oblaku, internet stvari, zasebnost, anonimnost, osebni podatki, internet, ZDA, EU

Privacy protection in the US and the EU in the light of new socio-technological phenomena

Privacy in an information society is a concept that is treated differently in the US and the EU. Due to its history, legal tradition and differing economic values, the US developed an approach that treats privacy not so much as a right, but as a commodity that can be traded according to the free market principles. Europe, on the other hand, has a lot of experience with totalitarian regimes, which is one of the reasons why in European countries privacy is understood as an inalienable right that represents one of the pillars of the freedom of action and expression of individuals in a society and should be protected accordingly by law. Therefore, legal protection of information privacy in the EU is much more systematic and comprehensive than in the US, where the approach to safeguarding privacy is sectoral.

Threats to information privacy are gaining novel dimensions with the adoption of new socio-technological phenomena, which is a collective term for big data, cloud computing and the internet of things, all presented in detail in this thesis. The central idea of the thesis is that the aforementioned socio-technological phenomena bring new challenges to the area of privacy protection, which are insufficiently addressed by the existing legislature. These challenges arise from the specific nature of big data, which are increasingly being processed through the services of cloud computing, while the upcoming internet of things is likely to contribute immensely to their quantity. Among them are problems with potential re-identification of anonymized data, inadequacy of personally identifiable information as the basis of personal data, questions regarding the ownership of data and insights gathered from them, unsuitability of notice and consent as the principal way of regulating the gathering of data, dilemmas associated with automatic profiling based on the processing of data, collecting data from increasingly more intimate parts of users' lives, etc.

Since regulatory solutions are usually adopted slowly and gradually, the thesis argues that any future solutions will have to involve alternative approaches, such as using technology and market mechanisms to protect privacy. Some examples of such solutions include privacy by design, personal data services, differential privacy, etc. This is going to have an impact on further conceptions of privacy, its valuation by individuals and society, and means of its future protection.

Keywords: big data, cloud computing, internet of things, privacy, anonymity personal data, internet, USA, EU

Nekega dne bomo morda na to dobo gledali kot na čas, ko bi z racionalnimi kompromisi lahko okrepili tako varnost kot svobodo, a so bili ti kompromisi zavrnjeni, ker sta bili obe strani tako zaverovani v svoj prav.

David Brin, *The Transparent Society*

KAZALO

1 UVOD 8
2 METODOLOŠKO – HIPOTETIČNI OKVIR 13
2.1 Predmet in cilji preučevanja 13
2.2 Hipoteze 14
2.3 Metode preučevanja 15
2.4 Temeljni pojmi 16
2.4.1 Masovni podatki 16
2.4.2 Računalništvo v oblaku 16
2.4.3 Internet stvari 17
2.4.4 Zasebnost 17
2.5 Seznam kratic 17
3 ZASEBNOST V SODOBNI INFORMACIJSKI DRUŽBI 19
3.1 Pojmovanje zasebnosti 19
3.2 (Zelo) kratka zgodovina zasebnosti 24
3.3 Stanje zasebnosti danes 27
4 FORMALNO-PRAVNO UREJANJE VAROVANJA ZASEBNOSTI 30
4.1 Varovanje zasebnosti v informacijski družbi v Združenih državah Amerike 30
4.1.1 *Ustavno pravo* 30
4.1.2 *Zakonodaja* 33
4.1.3 *Odškodninsko pravo* 36
4.2 Varovanje zasebnosti v informacijski družbi v Evropski uniji 37
4.2.1 *Zgodnji nadnacionalni dokumenti* 37
4.2.2 *Urejanje zasebnosti v Evropski uniji* 38
5 NOVI DRUŽBENO-TEHNOLOŠKIH FENOMENI 42
5.1 Masovni podatki 43
5.1.1 *Potencial masovnih podatkov* 46
5.1.2 *Masovni podatki ter načelo obveščanja in soglasja* 48
5.1.3 *Masovni podatki in anonimnost* 49
5.1.4 *Masovni podatki in sklepanje* 51
5.1.5 *Masovni podatki ter avtomatsko odločanje in profiliranje* 52

5.2 Računalništvo v oblaku 54
5.2.1 *Potencial računalništva v oblaku* 57
5.2.2 *Računalništvo v oblaku in ogrožanje zasebnosti* 59
5.2.3 *Računalništvo v oblaku in zakonsko varovanje zasebnosti* 60
5.2.4 *Računalništvo v oblaku in tehnično varovanje zasebnosti* 63
5.3 Internet stvari 65
5.3.1 *Potencial interneta stvari* 69
5.3.2 *Internet stvari in zasebnost* 70
6 ISKANJE REŠITEV ZA VAROVANJE ZASEBNOSTI V LUČI NOVIH DRUŽBENO-TEHNOLOŠKIH FENOMENOV 75
6.1 Vgrajena zasebnost 75
6.2 Kontekstna integriteta 77
6.3 Diferencialna zasebnost 78
6.4 Storitve na podlagi osebnih podatkov 79
6.5 Prenovljeno načelo obveščanja in soglasja 81
7 ZAKLJUČEK 82
7.1 Verifikacija hipotez 82
7.2 Sklepna beseda 87
8 LITERATURA 88

1 UVOD

Informacijska tehnologija je z razmahom računalnikov in interneta poskrbela, da se je v pičlega četrt stoletja[1] naš način dela, ustvarjanja, sodelovanja, zabave, učenja, in življenja nasploh popolnoma spremenil, ta proces pa še zdaleč ni zaključen. Nasprotno, odvija se z vse večjo naglico, ki ga na eni strani zaznamuje eksponentno naraščanje zmogljivosti tehnologij, na drugi pa vse večja dostopnost teh tehnologij, ki v izjemno kratkem času prehajajo od razvojne faze do faze množične uporabe. Skokovit razvoj informacijskih tehnologij povzroča globoke spremembe v družbi, gospodarstvu in znanosti, ki so lahko izjemno koristne, a prinašajo s seboj tudi grožnje in nevarnosti. Ena od posledic tega razvoja je tudi, da ga je z obstoječimi sredstvi in metodami vse težje regulirati.

Vprašanje zasebnosti na internetu prav zaradi razvoja novih tehnologij postaja vse bolj pereče. Varovanje zasebnosti na spletu[2] je sicer koncept, ki ga tako stroka kot laična javnost obravnavata že od začetka komercialne uporabe interneta, vendar je bila zasebnost uporabnikov v prvotnih letih zaradi same "anarhične" narave zgodnjega interneta manj na udaru, kot je danes. S širitvijo interneta na vsa področja našega življenja ter z razmahom tehnologij za zajemanje in obdelavo podatkov pa se je drastično spremenilo tudi pojmovanje zasebnosti na internetu. Po eni strani je naša spletna zasebnost danes ogrožena bolj kot kdaj koli, po drugi strani pa se zdi, da je zasebnost kot pravica in vrednota med internetnimi uporabniki vse manj cenjena, celo do te mere, da so nekateri strokovnjaki in vplivne osebnosti, kot sta ustanovitelj Facebooka Mark Zuckerberg in eden od "očetov interneta" Vinton Cerf, zasebnost na internetu razglasili za mrtvo in preživeto (Kirkpatrick 2010, Ferenstein 2015). Tovrsten odnos do zasebnosti je še posebno značilen za mlade, t. i. digitalne domorodce[3], ki so postali uporabniki interneta v njegovi zreli fazi (tj. po uvedbi standardov

[1] Seveda so tako računalniki kot internet starejša iznajdba, vendar velja, da je komercialna in zasebna uporaba računalniške tehnologije in interneta zaživela na začetku 90. let prejšnjega stoletja. Leta 1989 je britanski informatik Tim Berners-Lee zasnoval svetovni splet, leto kasneje pa definiral ključne tehnologije, ki so še danes temelj svetovnega spleta (HTML, URI in HTTP), še leto za tem pa je svetovni splet postal odprt za vse uporabnike.

[2] Pojma *internet* (ang. *Internet*) in (svetovni) *splet* (ang. *World Wide Web*) nista sinonima. Internet predstavlja infrastrukturo, splet pa orodje za njegovo uporabo. Vendar se v praksi ta dva pojma pogosto uporabljata kot sopomenki, poleg tega pa se v slovenščini pridevnik *spletni* uporablja kot prevod angleškega izraza *online*, zato bosta oba pojma pogosto uporabljena tudi v tem delu.

[3] Ang. *digital natives*; izraz označuje skupino ljudi, ki so bili rojeni že po uvedbi določene tehnologije in so posledično v stiku z njo že od zgodnjih let. Večina raziskovalcev izraza *digitalni domorodci* sicer ne uporablja več, vendar v javnosti ostaja priljubljen (boyd 2014, 196).

Web 2.0[4]) in se jim zdi odsotnost pravice do zasebnosti pri uporabi spletnih storitev samoumevna in običajna.

Pojmovanje zasebnosti kot arhaičnega in celo preživetega koncepta ni omejeno le na mlade, saj je tovrstna obravnava zasebnosti značilna tudi za velik del tehnološkega in informacijskega sektorja industrije in odraža vrednote skupin in posameznikov, ki so najbolj dejavni pri razvoju novih tehnologij. Prav tako je pravica do zasebnosti trn v peti določenim subjektom tako zasebnega kot javnega sektorja. Zaradi naraščanja količine podatkov, ki jih je z novimi tehnologijami vse lažje in ceneje pridobiti od uporabnikov, postajajo podjetja, ki se ukvarjajo z informacijsko dejavnostjo, vse bolj odvisna od njihovega nemotenega pritoka, zato na vsakršno omejevanje njihove uporabe, kot ga predstavlja denimo pravica do zasebnosti, gledajo kot na oviro pri svojem poslovanju. Na drugi strani se tudi državne organizacije že od vsega začetka zavedajo izrednega pomena dostopa do čim večje količine podatkov za zagotavljanje nacionalne varnosti, delovanja obveščevalnih služb, nadzora državljanov in rizičnih skupin znotraj države ter ostalih dejavnikov. Pritiski na zbiranje in uporabo osebnih podatkov v poslovnem svetu in za potrebe organov pregona so vse večji, pri čemer so se tehnološka orodja, ki omogočajo obdelavo takšnih podatkov, izpopolnila brez ustreznih odločnih ukrepov za zaščito zasebnosti (Zittrain 2008, 202).

Pri tem obstajajo v obravnavi koncepta zasebnosti znatne razlike med ZDA na eni strani in Evropo na drugi. Ta razhajanja so odraz različne zgodovinske tradicije, podjetniške kulture, politične filozofije in tehnološkega razvoja. V grobem lahko rečemo, da je varovanje zasebnosti v evropskih državah ter v nekaterih državah, ki sledijo evropskemu zgledu, močnejše kot v ZDA, čeprav se tudi to z razvojem novih tehnologij vse bolj spreminja. Medtem ko v Evropi gledamo na pravico do zasebnosti kot na temeljno človekovo pravico, ima ta v ZDA značilnosti dobrine (Craig in Ludloff 2011, 26), s katero lahko posamezniki svobodno trgujejo in jo menjajo za storitve in ugodnosti. Posledično imata obe tradiciji, ameriška in evropska, svojstven pristop za uveljavljanje načel zasebnosti ter nadzor nad njihovim izvajanjem, vendar postajajo pritiski na evropski model vse močnejši. Smer, v katero se bo nagnila tehtnica v prihodnosti, bo imela odločilne in daljnosežne posledice za vse deležnike.

[4] Z izrazom Web 2.0 običajno označujemo selitev aplikacij, ki so se tradicionalno nahajale na osebnih računalnikih, na internet, lahko pa se nanaša tudi na pojav vse večje količine uporabniško generiranih vsebin na spletu (Zittrain 2008, 102).

Hipoteza, da zasebnost postaja vse večji trn v peti tako sodobnih tehnoloških podjetij kot tudi državnih organizacij, temelji na predpostavki, da količina podatkov, ki jo z današnjimi sredstvi lahko zajamemo, shranimo in obdelamo, občutno presega zmožnosti zajetja, hrambe in obdelave še zgolj nekaj let nazaj, podoben trend rasti pa lahko pričakujemo tudi v bodoče. Ogromne količine podatkov postajajo obvladljive zaradi naraščajočih kapacitet za njihovo shranjevanje in novih orodij za obdelavo, medtem ko miniaturizacija in padanje cen senzorske tehnologije omogočata, da so senzorji za zajemanje podatkov navzoči v vedno večjem številu naprav, ki so dostopne tudi komercialnim uporabnikom in povezane s svetovnim spletom, kar omogoča nemoten pretok podatkov od uporabnikov do ponudnikov tehnologij. Sposobnost obdelave, pregledovanja, urejanja in kategoriziranja informacij v bazah podatkov je povzročila gonjo, da se o uporabnikih zbere še več podatkov in preuči možnosti njihove rabe (Payton in Claypoole 2014, 1. pogl.).

Fenomena zbiranja, obdelave in uporabe velike količine podatkov se je prijelo marketinško poimenovanje *big data*, kar se v slovenščino največkrat prevaja kot *masovni podatki*[5]. Pridobivanje masovnih podatkov se danes izvaja praktično povsod – v astronomiji, fiziki osnovnih delcev, genetiki, računalništvu, družboslovju, medicini, klimatologiji, kmetijstvu, vojski, proizvodnji, prodaji, zavarovalništvu, oglaševanju, športu, državnih institucijah in drugje (Thomas in McSharry 2015). Težava z vidika zasebnosti nastane, ko se masovni podatki pridobivajo neposredno ali posredno od človeških uporabnikov, bodisi kot posledica zagotavljanja storitev bodisi kot element elektronskega nadzora. Če je včasih veljalo, da ima samo država dovolj sredstev in moči za zbiranje uporabne količine informacij o svojih subjektih, je to v času masovnih podatkov omogočeno vsakemu ponudniku tehnologij z zadostnimi kapacitetami in interesom, teh pa bo v prihodnje vse več. Potrebno bo najti ravnovesje med interesi vseh deležnikov v tem procesu, pri čemer lahko postavimo hipotezo, da zakonodaja (še posebno v ZDA) trenutno ne dohaja izzivov, ki jih predstavljajo masovni podatki, in da bo morda treba rešitve iskati tudi izven okvirja državnih in mednarodnih institucij.

To delo bo poleg pojma zasebnosti v luči masovnih podatkov obravnavalo tudi nekatere sorodne koncepte, ki izhajajo iz pojava masovnih podatkov oziroma še dodatno spodbujajo

[5] Kljub temu, da se *big data*, *data mining*, *cloud computing* in sorodni izrazi pogosto uporabljajo tudi v domači literaturi in medijih, bodo v tem delu uporabljeni njihovi slovenski prevodi, če bo to le mogoče. Prevodi in razlage najpogostejših izrazov se nahajajo v poglavju Temeljni pojmi.

njihov razmah. Takšen koncept je denimo *cloud computing*, ki ga prevajamo kot računalništvo v oblaku in predstavlja sistem za proizvodnjo, shranjevanje, analizo in distribucijo podatkov, informacij, aplikacij in storitev organizacijam in posameznikom (Mosco 2014, 6). Pojav storitev v oblaku je omogočil, marsikje pa celo vsilil, selitev ogromnih količin podatkov, ki so nekoč domovali v zaprtih sistemih organizacij in posameznikov, na strežnike in v podatkovne centre ponudnikov, ki obvladujejo trg digitalnih informacij in ki jim zasebnost njihovih uporabnikov pogosto ne predstavlja najvišje prioritete. Računalništvo v oblaku zaznamuje tako zasebni kot javni sektor, saj poleg podjetij pogosto uporabljajo storitve v oblaku, ki so sicer praviloma v zasebni lasti, tudi državne organizacije. Prav tako lahko med storitve v oblaku štejemo večino današnjih aplikacij, katerih končni uporabniki smo posamezniki – od odjemalcev spletne pošte do družbenih omrežij. Pri slednjih se z vidika zagotavljanja zasebnosti pojavlja še dodatna težava, ker se odnos do zasebnosti spreminja tudi med samimi uporabniki, ki podatke iz svojega življenja vse bolj brez zadržkov delijo z ostalimi uporabniki in posledično s ponudniki storitev.

Masovni podatki in storitve računalništva v oblaku že danes krojijo naš odnos do zasebnosti na internetu, prihodnost pa bo vsekakor prinesla še večje izzive za regulatorje in pisce zakonov, ki si prizadevajo za ohranitev pravice do zasebnosti. Prihaja namreč doba interneta stvari (*internet of things*), ki ga bodo sestavljali predmeti z lastnimi viri napajanja, vgrajenimi senzorji in spletnimi naslovi (Howard 2015, xi). Z internetom tako ne bodo povezani le naši računalniki, tablice, igralne konzole in pametni telefoni, temveč cela vrsta objektov, od gospodinjskih aparatov, vsakdanjih pripomočkov, vozil in celo predmetov, ki jih nosimo na sebi (kmalu pa tudi v sebi), do celotnih zgradb, domov in mest. Ker bodo vse te pametne naprave imele vdelane senzorje, ki jim bodo omogočali interakcijo z okolico, zbiranje podatkov in komunikacijo z uporabniki, z drugimi napravami ter z oddaljenimi podatkovnimi centri v realnem času, lahko sklepamo, da bo nadzor nad uporabo podatkov in spoštovanjem zasebnosti za več redov velikosti zahtevnejši, kot je zdaj.

V okviru povedanega je namen tega dela ponuditi celovit pregled današnjega stanja na področju zasebnosti in interneta, s posebnim poudarkom na vidikih, ki jih v to področje vnašajo uporaba masovnih podatkov, računalništvo v oblaku, prihajajoči internet stvari in sorodni koncepti. Pri tem bo podana primerjalna analiza ameriškega in evropskega pristopa k varovanju spletne zasebnosti z obravnavo zgodovine, tradicije, političnega in gospodarskega položaja ter pravne in zakonodajne ureditve obeh akterjev. Predstavljeni bodo sedanji in bodoči izzivi, s katerimi se soočajo (oziroma se še bodo soočali) deležniki, ki so tako ali

drugače vpleteni v koncept zasebnosti na internetu, in možne rešitve, ki se ponujajo. Na podlagi strokovne literature, dostopnih podatkov in znanih dejstev bo v delu obravnavana tudi prihodnost zasebnosti ob uvajanju novih tehnologij, z orisom najverjetnejših scenarijev na podlagi obstoječih trendov in kazalnikov, saj gre za pomembna vprašanja, ki imajo oziroma bodo imela velik vpliv na vse nas.

2 METODOLOŠKO-HIPOTETIČNI OKVIR

2.1 Predmet in cilji preučevanja

Kot je zapisano v uvodnem delu, bo to magistrsko delo obravnavalo pojem zasebnosti na internetu z vidika nekaterih družbeno-tehnoloških pojavov, ki v zadnjih letih že pomembno vplivajo na zasnovo in razvoj informacijskega sektorja, njihov pomen pa bo v bližnji prihodnosti le še skokovito naraščal. Natančneje povedano bodo v delu predstavljeni naslednji koncepti: masovni podatki (ang. *big data*), računalništvo v oblaku (ang. *cloud computing*) in internet stvari (ang. *internet of things*). Medtem ko sta prva dva že dobro uveljavljena, pa pravi razcvet zadnjega šele prihaja. Vsi trije koncepti so medsebojno povezani, zato lahko pričakujemo, da bo njihov pomen v bodoče vzajemno naraščal.

Osrednja tema magistrskega dela bo vpliv omenjene trojice novih fenomenov na zasebnost. Živimo v času, ko je zasebnost na internetu na vse večji preizkušnji, razvoju tehnologij pa zakonodaja le stežka sledi. Razmah uporabe masovnih podatkov, računalništva v oblaku ter interneta stvari bo na področje varovanja zasebnosti vnesel še dodatne izzive, s katerimi se bosta morala spopasti tako javni kot zasebni sektor in morda celo sami uporabniki novih tehnologij. Večdimenzionalnost problema bo razčlenjena v magistrskem delu, pri čemer gre poudariti, da vpliv preučevanih fenomenov na zasebnost ne bo zgolj kvantitativen, torej v smislu povečanja števila že obstoječih težav, temveč tudi kvalitativen, saj se s tovrstnimi izzivi v preteklosti naša informacijska družba še ni srečevala.

Glavna akterja, na katera se bom osredotočil v magistrskem delu, bosta ZDA in Evropska unija. Čeprav se v sodobni globalni informacijski družbi inovacije porajajo decentralizirano, ZDA še vedno veljajo za tehnološko velesilo in središče, kjer se rodi največje število novih tehnologij. Poleg tega je zaradi zgodovine, tradicije in drugačnega vrednotnega sistema dojemanje zasebnosti v ZDA drugačno kot v Evropi. Tako imamo na eni strani tehnologije, ki se bliskovito razširijo po vsem svetu, medtem ko na drugi strani njihovo uporabo (če sploh) urejajo lokalni zakoni in predpisi. Slovenija je kot del Evropske unije podvržena evropskemu pravnemu redu, ki sicer področje zasebnosti ureja strožje in bolj sistematično kot v ZDA, čeprav se zdi, da postaja vpliv ameriškega načina vse močnejši tudi na stari celini. Eno od ključnih vprašanj, ki se ob tem zastavljajo, je, ali lahko na nove izzive varovanju zasebnosti učinkovito odgovori zakonodaja oziroma politične institucije ali pa je ta pristop neučinkovit

in je treba iskati tehnične in sistemske rešitve v načelih delovanja prostega trga in samoregulacije vpletenih deležnikov.

Novi družbeno-tehnološki fenomeni se s pridom uporabljajo tako v javnem kot zasebnem sektorju, zato je treba ločevati med različnimi viri ogrožanja zasebnosti, čemur bo v delu prav tako posvečena pozornost. Ni pa namen dela sistematično preučevanje kratenja državljanskih pravic in svoboščin v imenu zagotavljanja nacionalne varnosti, ki se je (predvsem) v ZDA začelo izvajati takoj po 11. septembru 2001 in katerega razsežnosti so se zares pokazale šele več let kasneje, ko so v javnost prišli številni skrivni programi ameriške vlade za zbiranje podatkov o svojih in tujih državljanih. Gre za izredno obsežno tematiko, o kateri je bilo prelitega že mnogo črnila in ki ji je s pozicije raziskovalca brez dostopa do internih virov praktično nemogoče priti do dna, zato ne bo predmet preučevanja v tem delu. Prav tako namen magistrskega dela ni podajanje vrednostnih sodb o smotrnosti posegov novih tehnologij na področje zasebnosti, temveč zgolj nepristranska analiza trenutnega stanja in prikaz možnega razvoja dogodkov v prihodnosti.

2.2 Hipoteze

Na podlagi zgoraj omenjenih dejstev lahko izluščimo naslednje hipoteze, ki bodo usmerjale raziskovalni in analitični proces magistrskega dela:

H1: Družbeno-tehnološki fenomeni, kot so uporaba masovnih podatkov, računalništva v oblaku ter interneta stvari, ne prinašajo zgolj povečanega obsega ogrožanja zasebnosti v informacijski družbi, ampak tudi povsem nove izzive in težave, ki bodo zahtevali razvoj drugačnih rešitev oziroma pristopov, kot so v uporabi danes.

Prva hipoteza obravnava nove družbeno-tehnološke fenomene z vidika njihove funkcionalnosti, ki naj bi bila v tolikšni meri drugačna od že dalj časa uveljavljenih tehnologij, da prinaša na področje varovanja zasebnosti izzive, s katerimi se v preteklosti nismo srečevali oziroma so se pojavljali zgolj v osamljenih primerih. Na hipotezo se v celoti nanaša 5. poglavje. Preverjanje te hipoteze bo zahtevalo preučitev karakteristik teh fenomenov ter njihovo primerjavo s starejšimi tehnologijami.

H2: Z uveljavljanjem in razcvetom družbeno-tehnoloških fenomenov, kot so uporaba masovnih podatkov, računalništva v oblaku ter interneta stvari, formalno-pravni

pristop k varovanju zasebnosti v informacijski družbi ni dovolj učinkovit, zato bosta vse večjo vlogo prevzemala obravnava koncepta zasebnosti na internetu po načelih delovanja prostega trga ter iskanje tehnoloških rešitev.

Druga hipoteza se nanaša na regulacijo novih družbeno-tehnoloških fenomenov z namenom varovanja zasebnosti. Hipoteza predpostavlja, da je zakonodajni pristop k varovanju zasebnosti tog in ne dovolj odziven na hitre spremembe v tehnološkem sektorju, zato bodo v ospredje prihajale tudi rešitve in pobude s strani industrije, ki po načelih delovanja prostega trga ne bo smela zanemariti ekonomske vrednosti, ki jo uporabniki pripisujejo zasebnosti pri uporabi njihovih podatkov. Na hipotezo se nanašata 4. in 6. poglavje, povezana pa je tudi s spoznanji iz 5. poglavja. Preverjanje hipoteze bo vključevalo preučevanje učinkovitosti obstoječe zakonodaje in predpisov v ZDA in Evropski uniji ter pregled drugih rešitev za varovanje zasebnosti, ki se že uporabljajo ali pa se bodo uporabljale v bodoče.

H3: Zaradi ameriške prevlade v informacijskem sektorju, vpliva ameriških korporacij in pritiskov ameriške zunanje politike je evropski model varovanja zasebnosti v informacijski družbi ogrožen in se bo v prihodnosti, z razcvetom družbeno-tehnoloških fenomenov, kot so uporaba masovnih podatkov, računalništva v oblaku ter interneta stvari, približeval ameriškemu pristopu.

Zadnja hipoteza zajema politično in gospodarsko komponento razcveta obravnavanih družbeno-tehnoloških fenomenov. Gre tudi za spopad različnih vrednot, ki usmerjajo varovanje zasebnosti v ZDA in Evropski uniji, kjer igrajo pomembno vlogo vpliv industrije, političnih institucij in lobijev, ki jih je v interesu zagotoviti kar se da neoviran pretok podatkov. Preverjanje hipoteze bo narejeno na podlagi spoznanj iz 3., 4. in deloma 5. poglavja. Pri verifikaciji bo treba iz nedavnih dogodkov na področju sprejemanja zakonodaje ter razvoja in širjenja obravnavanih družbeno-tehnoloških fenomenov izluščiti trende, ki kažejo bodisi v smeri potrditve hipoteze bodisi v smeri njene zavrnitve.

2.3 Metode preučevanja

Preučevanje tematike bo temeljilo na primarnih in sekundarnih virih, ki bodo zajemali strokovno literaturo tehnične in teoretične narave, članke in prispevke v znanstvenih revijah, uradne vire, kot so zakoni, predpisi in dokumenti, ter poljudne vire z zadostno mero

verodostojnosti, če bodo nudili širši vpogled v problematiko. Podajanje dejstev in opisovanje predmetov raziskovanja bo slonelo na deskriptivni metodi. Primerjalna analiza bo razkrila podobnosti in razlike med glavnimi akterji ogrožanja in varovanja zasebnosti – med javnim in zasebnim sektorjem z družbeno-ekonomskega vidika ter med ZDA in Evropsko unijo s družbeno-političnega vidika. Pri preučevanju raziskovalnih vprašanj bo uporabljen deduktiven pristop, torej sklepanje na podlagi obstoječih dejstev, od splošnega k specifičnemu, medtem ko generalizacija in ustvarjanje zaključkov pri obravnavi hipotez vključujeta induktivno razmišljanje in sintezo dejstev iz predelane literature.

Zamišljena struktura magistrskega dela je sledeča: uvodni del, ki mu sledita metodološki okvir z razlago temeljnih pojmov in vsebinski del s štirimi velikimi sklopi (koncept zasebnosti, primerjava stanja v ZDA in Evropski uniji, opis novih družbeno-tehnoloških fenomenov ter možne rešitve za varovanje zasebnosti), sklepni del pa bo vseboval preverjanje hipotez, zaključek, vire in morebitne priloge. Podrobnejša struktura magistrskega dela je navedena spodaj.

2.4 Temeljni pojmi

2.4.1 *Masovni podatki*

Masovni podatki so skupno ime za podatke, ki so tako obsežni, raznovrstni, kompleksni in/ali hitro se spreminjajoči, da jih ni več mogoče shranjevati in obdelovati z ustaljenimi orodji oziroma pristopi.

Vir: Davis in Patteson 2012, 4

2.4.2 *Računalništvo v oblaku*

Računalništvo v oblaku je skupno ime za računalniške vire, ki so uporabnikom na voljo kot storitev preko omrežja in so prilagodljivi glede na potrebe uporabnikov. Ti računalniški viri so nadalje lahko na voljo kot infrastruktura, platforma ali programska oprema.

Vir: Hon in Millard v Millard 2013, 1. del, 1. pogl.

2.4.3 *Internet stvari*

Internet stvari je globalna omrežna infrastruktura, ki povezuje fizične in virtualne objekte s pomočjo tehnologij za zajemanje podatkov in komuniciranje. Ta infrastruktura zajema obstoječe in bodoče prvine interneta in drugih omrežij. Nudila bo možnost identifikacije objektov, senzorsko in komunikacijsko tehnologijo, ki bodo služile samostojnim in kooperativnim storitvam ter aplikacijam. Značilnost teh bo visoka stopnja samodejnega zbiranja podatkov, obveščanja o dogodkih, mrežne povezljivosti in medobratovalnosti.

Vir: "IoT Privacy, Data Protection, Information Security" 2013, 1

2.4.4 *Zasebnost*

V tradicionalnem smislu je zasebnost koncept, ki označuje dejanja in dogodke, ki se ne zgodijo v javnosti. Zasebnost je pogosto opisana kot odsotnost poseganja v osebni prostor oziroma pravica posameznika, da ga drugi "pustijo pri miru". V formalno-pravnem smislu zasebnost temelji na naboru zakonskih omejitev, ki preprečujejo vdor v zaščiteni prostor subjekta.

Vir: Lessig 2006, 201; Solove 2007, 7

2.5 Seznam kratic

BI & DW – business intelligence & data warehousing / poslovna inteligenca & skladiščenje podatkov

CCPA – Cable Communications Policy Act / Zakon o komunikacijski politiki kabelskih televizij

CFAA – Computer Fraud and Abuse Act / Zakon o računalniških prevarah in zlorabah

CIA – Central Intelligence Agency / Centralna obveščevalna agencija

COPPA – Children's Online Privacy Protection Act / Zakon o varovanju zasebnosti otrok na spletu

DPPA – Driver's Privacy Protection Act / Zakon o varovanju zasebnosti voznikov

ECHR / EKČP – European Convention on Human Rights / Evropska konvencija o varstvu človekovih pravic in temeljnih svoboščin

ECPA – Electronic Communications Privacy Act / Zakon o zasebnosti elektronskih komunikacij

EU – Evropska unija

EULA – end-user licence agreement / licenčna pogodba s končnim uporabnikom

FBI – Federal Bureau of Investigation / Zvezni preiskovalni urad

FCRA – Fair Credit Reporting Act / Zakon o poštenem poročanju o kreditni sposobnosti

FERPA – Family Educational Rights and Privacy Act / Zakon o družinskih pravicah do izobraževanja in zasebnosti

FISA – Foreign Intelligence Surveillance Act / Zakon o zunanji obveščevalni dejavnosti

FIPPs – Fair Information Practice Principles / Načela poštenih informacijskih praks

FTC – Federal Trade Commission / Zvezna komisija za trgovino

GDPR – General Data Protection Regulation / Splošna uredba o varstvu podatkov

GLBA – Gramm–Leach–Bliley Act / Zakon Gramm–Leach–Bliley

GPS – Global Positioning System / globalni sistem pozicioniranja

HIPAA – Health Insurance Portability and Accountability Act / Zakon o prenašanju in odgovornosti za podatke zdravstvenega zavarovanja

IaaS – Infrastructure as a Service / infrastruktura kot storitev

NSA – National Security Agency / Nacionalna varnostna agencija

OECD – Organisation for Economic Co-operation and Development / Organizacija za gospodarsko sodelovanje in razvoj

PaaS – Platform as a Service / platforma kot storitev

PBD – privacy by design / vgrajena zasebnost

PDS – personal data services / storitve na podlagi osebnih podatkov

PII – personally identifiable information / informacije, ki omogočajo osebno identifikacijo

RFID – radio-frequency identification / radiofrekvenčna identifikacija

SaaS – Software as a Service / programska oprema kot storitev

TCPA – Telephone Consumer Protection Act / Zakon o zaščiti telefonskih uporabnikov

TTIP – Transatlantic Trade and Investment Partnership / Transatlantsko trgovinsko in investicijsko partnerstvo

VPPA – Video Privacy Protection Act / Zakon o varovanju zasebnosti video posnetkov

ZDA – Združene države Amerike

3 ZASEBNOST V SODOBNI INFORMACIJSKI DRUŽBI

3.1 Pojmovanje zasebnosti

Zasebnost je koncept z bogato preteklostjo in različnim vrednotenjem v različnih zgodovinskih obdobjih in političnih sistemih. Obseg teoretičnih del s področja zasebnosti je velik in zajema discipline od filozofije do političnih ved, teorije prava, medijskih in informacijskih ved ter vse pogosteje tudi računalništva in inženirstva (Nissenbaum 2010, 67). Intuitivno zasebnost dojemamo kot pravico do nevmešavanja v različne vidike našega življenja, vsiljivci pa so lahko posamezni ljudje, organizacije ali celotne države. Gre torej za omejevanje dostopa do posameznika s strani drugih (Gavison 1980, 428) oziroma za svoboščino brez nepooblaščenih posegov (Angwin 2014, 1. pogl). Popolna zasebnost bi v tem smislu predstavljala situacijo, v kateri je posameznik v celoti nedosegljiv drugim, kar pomeni, da drugi o posamezniku nimajo nobenih informacij, mu ne posvečajo nobene pozornosti in nimajo fizičnega dostopa do njega (Gavison 1980, 428). Takšno stanje je seveda v praksi nemogoče, zato tudi sama zasebnost ni koncept, kjer gre za vse ali nič, saj je tudi popolna izguba zasebnosti, torej da so o posamezniku znane prav vse informacije in je dostop do njega omogočen vsakomur in ob vsakem času, malo verjetna.

Zasebnost lahko razdelimo v tri osnovne kategorije (Craig in Ludloff 2011, 14):

- fizična zasebnost, ki zajema posege v fizični prostor, materialne dobrine ali telo posameznika;
- informacijska zasebnost, ki se nanaša na zajemanje, shranjevanje, posredovanje in uporabo informacij v različnih kontekstih;
- organizacijska zasebnost, ki za razliko od posameznikov obravnava dejavnosti in zaupne informacije organizacij, institucij in podjetij.

Pri tem se takoj poraja vprašanje, kateri posegi v zasebnost so pooblaščeni in kdo jih določa. Tradicionalno so težave z varovanjem zasebnosti enačili s posegi v skriti svet posameznika. V tem smislu je zasebnost povezana s skrivanjem, do kršitev pa prihaja z opazovanjem in javnim razkrivanjem zaupnih informacij (Solove 2011, 42). Kot bomo videli, v svetu sodobnih tehnologij in masovnega pretoka podatkov definicija zasebnosti, ki se opira na skrivanje zaupnih informacij, ne zadostuje več. Nadalje, kot nujno komponento zasebnosti nekateri avtorji navajajo *intimnost*. Zasebnost se torej tiče intimnih informacij, pri čemer je

intimnost definirana kot nekaj, kar vključuje negovane in zaupne odnose (Solove 2004, 212). Tudi ta opredelitev zasebnosti je z današnjega vidika pomanjkljiva, saj podatkov o zdravju ali finančnem stanju posameznika na podlagi tega ne moremo šteti med intimne, a so kljub temu podatki zaupne narave.

V prejšnjem odstavku je bila pri opredeljevanju zasebnosti uporabljena beseda pravica, vendar se zasebnost ponekod še zdaleč ne smatra kot neodtujljiva pravica, torej del naravnega prava, oziroma vsaj ne kot pojem, ki je enakovreden tradicionalnim pravicam in svoboščinam, kot je denimo svoboda govora. Obravnavanje zasebnosti kot drugorazredne pravice ima za posledico, da je zasebnost postavljena v podrejeni položaj, kadar pride do konflikta med različnimi vrednotami. Tako zasebnost najpogosteje potegne krajši konec, kadar je postavljena nasproti konceptu varnosti, saj sta varnost in zasebnost običajno predstavljena kot nasprotujoča si in izključujoča se pojma, še posebno v areni političnega delovanja. Nekateri avtorji (Solove 2004 in 2011, Schneier 2006) menijo, da odnos med varnostjo in zasebnostjo ni igra ničelne vsote, temveč gre za lažno dihotomijo, ki jo predvsem vladajoče elite izkoriščajo v prid omejevanja zasebnosti zaradi zagotavljanja domnevno večje varnosti. Prava dilema po njihovem ni zasebnost proti varnosti, temveč svoboda proti nadzoru. Svoboda namreč kot predpogoj zahteva tako varnost kot zasebnost.

V zasebnem sektorju se zasebnost najpogosteje postavlja nasproti konceptu uporabnosti oziroma zagotavljanja storitev. Od uporabnikov izdelkov in storitev se pričakuje, da se v zameno za njihovo uporabo odpovedo določeni meri zasebnosti. Ta model je v informacijski panogi še posebno uveljavljen pri ponudnikih storitev, ki so sicer v osnovi brezplačne, vendar njihova raba ponudnikom omogoča dostop do velike količine osebnih podatkov uporabnikov ter vsebin, ki jih ustvarijo.

Preprosto povedano se evropski in ameriški pogled na zasebnost razlikujeta predvsem v tem, da prvi smatra zasebnost kot pravico, drugi pa kot dobrino (Craig in Ludloff 2011, 26), kar se odraža na pravni ureditvi varovanja zasebnosti obeh akterjev. V Evropi se je zato uveljavil celovit pristop do varovanja zasebnosti, kar v praksi pomeni urejanje s krovno zakonodajo na ravni Evropske unije, ki zajema širok spekter uporabe podatkov tako v javni kot zasebni sferi. Na drugi strani je zakonsko varovanje zasebnosti v ZDA pogosto opredeljeno kot "sektorsko", z velikim številom specializiranih predpisov, ki urejajo posamezna področja, kjer prihaja do izmenjave podatkov, denimo finance, zdravstvo itd., medtem ko je pravna ureditev nekaterih

drugih področij (še posebno v zasebni sferi) šibka oziroma je sploh ni (Ohm v Lane in drugi 2014, 1. del, 4. pogl.).

Drugačno vrednotenje zasebnosti v Evropi in ZDA postavlja pod vprašaj tezo, da je zasebnost človekova pravica, ki jo je treba brezpogojno zaščititi. Celo tisti, ki zasebnosti pripisujejo status pravice, se načeloma strinjajo, da njena vrednost leži predvsem v posrednem zagotavljanju t. i. prvorazrednih pravic, npr. pravice do svobodnega izražanja ali združevanja. Gre torej za konflikt med nevtralnim in normativnim pojmovanjem zasebnosti: prvi obravnava zasebnost brez predpostavljanja, da je ta sama po sebi dobra, medtem kot drugi izhaja iz stališča, da je zasebnost zaželena, cenjena in potrebna zaščite (Nissenbaum 2010, 68).

Nevtralno pojmovanje zasebnosti se omejuje na zasebnost kot družbeni fenomen, ki se je skozi zgodovino spreminjal v skladu z vrednotami časa, čemur smo priča tudi v sodobni družbi s pojavom novih tehnologij. Vrednost zasebnosti je torej takšna, kakršno ji v danem trenutku pripisujejo njeni uporabniki, in je odraz družbeno-političnega okolja ter zgodovinskih slučajnosti. Na drugi strani zagovorniki normativnega pojmovanja vidijo v zasebnosti nujno komponento družbe, brez katere bi bile ogrožene številne oblike demokratičnega delovanja in izražanja, saj bi odsotnost nemotenega prostora za refleksijo in razvoj idej lahko vodila v samocenzuro in samoomejevanje. Zasebnost v tem oziru torej ni sama sebi namen, temveč sredstvo za doseganje določenega ideala demokratične politike, kjer so državljani več kot le pasivni dobavitelji informacij vsemogočnim tehnokratom (Morozov, 2013). Ali kot je že pred leti zapisal nemški pravnik Spiros Simitis: "Kjer pride do razkroja zasebnosti, je priložnost za osebno presojo političnih in družbenih procesov ter priložnost za razvoj in ohranjanje svojstvenega življenjskega sloga vse manjša" (Simitis 1987, 734). Zasebnost kot oblika usmerjanja pretoka informacij vpliva na obseg spodbujanja ali zaviranja določenih dejanj in izražanj identitete (Solove 2004, 176). V situaciji, kjer smo opazovani na vsakem koraku in kjer nam povsod pretijo nadzor, obsojanje, kritika in celo posnemanje naše edinstvenosti, izgubimo svojo individualnost, ki jo potrebujemo za ohranjanje človeškega dostojanstva in spoštovanja (Schneier 2006). Tudi zato večina razvojnih psihologov pravi, da je zasebnost ključna za oblikovanje človeške samopodobe (Tapscott, 2012b).

Tipičen primer zaviranja lastnega izražanja in delovanja zaradi pomanjkanja zasebnosti so totalitarne družbe, kjer vlogo kršitelja zasebnosti igra država oziroma oblast. Tajne službe, kot sta bili sovjetska KGB in vzhodnonemška Stasi, so v času hladne vojne vršile tako intenziven

nadzor nad lastnimi državljani, da o možnostih osebnega izražanja, ki jih povezujemo z demokratično družbeno ureditvijo, ni bilo niti govora. Vdor v zasebnost posameznika v takšnem primeru lahko opišemo z orwellovsko metaforo (Solove 2004, 175), torej s totalitarističnim nadzorom "velikega brata" iz romana *1984*, ki skuša zatreti vsakršno individualnost in uporništvo v družbi. Vendar obstaja še druga vrsta posegov v zasebnost, ki se sicer zdi manj zlovešča, a je v današnjem času gotovo bolj pogosta, in jo zajema kafkovska metafora (prav tam). Gre za obliko poseganja v avtonomijo posameznika z zbiranjem informacij o njem z namenom vodenja procesov, ki posamezniku morda niti niso škodljivi, a nima nad njihovim izvajanjem nikakršnega nadzora in je kot protagonist novele *Proces* na milost in nemilost prepuščen entitetam, ki s pomočjo pridobljenih podatkov usmerjajo tok njegovega življenja. Takšno ogrožanje zasebnosti izvajajo tako podjetja kot državne ustanove. Kot je bilo državljanom Sovjetske zveze onemogočeno izražanje in oblikovanje lastne podobe zaradi vseprisotnega nadzora KGB, tako tudi možnost vseprisotnega nadzora v informacijski družbi krši pravico do avtonomije, čeprav je tehnologija v rokah tako privatnega sektorja kot države in čeprav platformo za nadzor zagotavljajo korporacije v zasebni lasti (Rosen v Rosen in Wittes 2011, 72).

Nadalje Daniel Solove razdela nevarnosti, ki jih prinašajo posegi v zasebnost, glede na obe metafori. Kršenje zasebnosti skozi prizmo orwellovske metafore na ta način lahko (1) vodi v totalitarizem, (2) ogroža demokracijo in samoodločanje, (3) zatira pravico do svobodnega združevanja in (4) onemogoča anonimnost v družbi. Na drugi strani lahko nevarnosti ogrožanja zasebnosti v luči kafkovske metafore povzamemo kot (5) izgubljanje in razkrivanje informacij ter posledično ranljivost, (6) avtomatizacijo družbenih procesov in profiliranje državljanov, (7) pretirane reakcije v času kriz in (8) spreminjanje namenov in uporabe, zaradi katerih so se prvotno zbirali podatki. Vzpon novih družbeno-tehnoloških fenomenov, ki so predmet preučevanja v tem delu, lahko zagotovo povežemo s točkami 4, 5, 6 in 8, medtem ko tuje ne zveni niti sklicevanje na točko 2.

Skrb, da bi demokratične družbe zaradi uporabe novih tehnologij zdrsnile v totalitarizem, je verjetno pretirana navkljub dejstvu, da so prav vladajoče strukture med največjimi uporabniki teh tehnologij za poseganje v zasebnost državljanov. Vendar imajo te države običajno tudi dolgo tradicijo vladavine prava ter vzvode, ki preko sodne veje oblasti in mehanizmov neposredne demokracije lahko (vsaj v teoriji) omejujejo pristojnosti državnih organov. Drugače je v družbah, ki imajo že v osnovi avtokratski sistem vodenja. V takšnih državah je nadzor nad izvršno vejo oblasti šibak ali pa ga sploh ni, zato lahko vladajoče elite brez

zadržkov izkoriščajo tehnologijo za poseganje v zasebnost posameznikov in druge nezakonite namene. Tehnologija sama po sebi tako ni sredstvo povečanega ogrožanja zasebnosti, je pa lahko njegov pospeševalnik v rokah tistih, ki imajo zadostno moč v družbi, da lahko uidejo nadzoru in omejitvam.

Na nivoju posameznika je zasebnost pogosto različno ovrednotena. Nekaterim predstavlja nadvse pomembno vrednoto, medtem ko imajo drugi do zasebnosti bolj brezbrižen ali celo odklonilen odnos. Zdi se, da je zasebnost pomembnejša starejšim kot mlajšim, čeprav je to zgolj površinska ocena, ki se v praksi izkaže za nenatančno (boyd 2014). Gotovo pa med posamezniki dejansko obstajajo razlike v dojemanju zasebnosti, ki so vezane na njihovo osebnost, vzgojo in družbeno okolje, predvsem pa situacijo, v kateri se v danem trenutku nahajajo. Večina ljudi v javnosti ne pričakuje enake stopnje zasebnosti, kot jo uživajo v intimnosti svojega doma. Prav tako so pričakovanja glede zasebnosti drugačna, ko obiščemo zdravnika, kot so denimo na delovnem mestu, čeprav v obeh primerih akterju na drugi strani (zdravniku, delodajalcu) razkrijemo določene osebne podatke in informacije o sebi. Tu pridejo do izraza tudi kulturne razlike med državami in narodi. V Evropi velja, da se običajno ne govori odkrito o tem, koliko kdo zasluži, medtem ko Američani tega podatka ne smatrajo za zelo zaupnega. Nasprotno so osebni odnosi znotraj družine v ZDA pogosto skrbno varovana tema, o kateri se ne govori vsepovprek, v Evropi pa smo glede tega bolj odprti, čeprav seveda obstajajo tudi razlike med posameznimi narodi.

Ker se pričakovanja glede zasebnosti tako razlikujejo od situacije do situacije in celo od posameznika do posameznika, je smiselno govoriti o zasebnosti v različnih kontekstih (Nissenbaum 2010, 2011). Takšen pristop k zasebnosti temelji na teoriji kontekstne integritete, ki dopušča, da ljudje ne zahtevamo popolne zasebnosti in prostovoljno delimo informacije, dokler je zadoščeno določenim družbenim normam ("The Logic of Privacy" 2007). Zasebnost na ta način izgubi status univerzalne vrednote ali celo pravice in postane zrelativizirana in podvržena prevladujočim vrednotam posamezne družbe, vendar s tem tudi manj rigidna, kar omogoča bolj prilagodljivo implementacijo mehanizmov varovanja zasebnosti v zakonskem ali tehnološkem smislu.

3.2 (Zelo) kratka zgodovina zasebnosti

Zasebnost, kot jo razumemo danes, je stara zgolj okoli 150 let (Ferenstein 2015). To sicer ne pomeni, da pred tem zasebnost ni obstajala ali da v starejših družbah ni igrala pomembne vloge, vendar v teh primerih še ni šlo za formaliziran pojem. Šele v 19. stoletju je zasebnost dobila formalno-pravno podlago in bila prepoznana kot koncept, do katerega imajo ljudje pravico. Toda pot do tega prelomnega trenutka je bila dolga in ovinkasta.

V predzgodovinskih časih so ljudje živeli v plemenskih ureditvah, kjer zasebnost, kot jo poznamo danes, preprosto ni obstajala, saj tudi niso obstajale fizične strukture, ki bi posameznikom omogočale učinkovito osamitev. Preživetje je bilo postavljeno na prvo mesto in je zahtevalo sodelovanje celotne skupnosti, v kateri ni bilo prostora za individualizem. Lov, nabiralništvo, prehranjevanje, spanje, vojskovanje, sobivanje, skrb za potomce, pripovedovanje zgodb ... vse to so bile dejavnosti, ki so jih naši davni predniki počeli skupaj, tako kot to še danes počnejo sicer vse bolj redka tradicionalna plemena, ki jim je uspelo ohraniti določeno mero distance do sodobne civilizacije. Antropolog Bronislaw Malinowski je na Trobriandskih otokih opazil, da je celo intimnost v plemenski ureditvi skorajda nepoznana, saj odrasli niso pretirano skrbeli, da jih otroci ne bi zalotili pri spolnosti (Ferenstein 2015). Kljub temu obstajajo dokazi, da je določena mera zasebnosti (ali vsaj intimnosti pri spolnih odnosih) tudi v plemenskih družbah instinktivno pričakovana. Raziskava vzorcev vedenja pri spolnosti iz leta 1951[6] je namreč pokazala, da v kulturah, kjer obstajajo domovi z ločenimi sobami, pari dajejo prednost spolnosti za štirimi stenami, medtem ko v skupnostih brez ločenih sob v domovih spolnost raje izvajajo na prostem (prav tam).

Zasebnost, povezana z možnostjo umika od preostale družbe oziroma izražena kot prostovoljna osamitev, je najverjetneje nastopila šele s pojavom mest. Stari Grki so znali graditi domove s takšno razporeditvijo prostorov, ki je onemogočala vpogled v prav vsak kotiček domovanja. Čeprav so jih kasnejši Rimljani v marsičem posnemali, je njihov odnos do zasebnosti vendarle bil nekoliko ohlapnejši, o čemer pričajo tudi dokazi, da spolni odnosi v javnosti niso predstavljali tabuja. Lahko rečemo, da je bila pri premožnejših Rimljanih potreba po zasebnosti v nasprotju z željo po razkazovanju bogastva in moči, kar se je odražalo

[6] Šlo je za raziskavo *Patterns of Sexual Behavior*, ki sta jo leta 1951 napisala ameriška antropolog Clellan S. Ford in etnolog Frank A. Beach, ki danes spada med klasična dela antropološke literature. V njen sta primerjala vedenje pri spolnosti v 191 človeških kulturah in celo vzorce obnašanja pri drugih vrstah, še posebno primatih.

tudi v njihovi gradnji stavb z velikimi odprtimi prostori, ki se niso trudili skrivati podrobnosti iz zasebnega življenja (prav tam). V zgodovini to ni bilo zadnjič, da je zasebnost potegnila kratko v konfliktu z udobjem in osebnim ugledom.

Samota oziroma prostovoljna osamitev je postala družbeno sprejemljiva šele v zgodnjem srednjem veku, za kar so bili zaslužni predvsem kristjani. Da bi se izognili vsem skušnjavam grešnega življenja, ki posameznika naposled pripelje v pogubo, so najbolj goreči pripadniki krščanstva sprejeli osamitev od družbe v meniških samostanih. Tako je način bivanja, ki drugim preprečuje dostop do vseh podrobnosti posameznega življenja, prvič dobil pridih kreposti in ne le čudaštva. Takrat se je razvila tudi navada branja v tišini, ki je bila v nasprotju z glasnim branjem izven samostanskih zidov, kjer so znali brati le redki in so zato redko literaturo na glas prebirali pred širšim občinstvom.

S krščanstvom je povezan še en izum, ki je pomembno vplival na kasnejši razvoj koncepta zasebnosti. Leta 1215 so na četrtem lateranskem koncilu pod vodstvom papeža Inocenca III. zapovedali sveto spoved[7] kot cerkveno institucijo, ki je namenjena vsem verujočim (Ferenstein 2015) in po kateri se mora vsak odrasli vernik vsaj enkrat na leto spovedati pred svojim duhovnikom. S tem je bila posameznikom *ipso facto* dana pravica do zasebnosti glede določene vrste informacij, ki jih mora tudi spovedujoči duhovnik obravnavati kot zaupne. Na ta način so krščanski duhovniki postali tudi eni prvih upravljavcev z zaupnimi podatki drugih.

Pri razvoju koncepta zasebnosti ni igrala vloge le človeška družba, temveč tudi narava. Izbruhi nalezljivih bolezni so med nemočnim prebivalstvom, stoletja pred razumevanjem higiene kot enega najpomembnejših dejavnikov pri ohranjanju zdravja, terjali visok davek. Največjega med vsemi je zahtevala epidemija kuge v 14. stoletju, ki je v Evropi pomorila kar tretjino vseh ljudi. Čeprav je bilo do sodobne higiene še daleč, so se že takrat pojavila spoznanja o pomenu osamitve bolnikov zaradi preprečevanja nadaljnjega širjenja bolezni. Do tedaj je bilo običajno, da so tako ljudje po domovih kot bolniki v bolnišnicah spali karseda skupaj (prav tam). Črna smrt je to spremenila in tudi zaradi nje so se kasneje pojavile prve ločene postelje, namenjene zgolj posamezniku ali paru. V ta čas spadajo tudi prvi zametki zakonodajne zaščite zasebnosti. Leta 1361 je v Angliji obveljal zakon, ki je predvideval kazen za ljudi, ki so skrivaj oprezali za drugimi in jim prisluškovali (Kovačič 2006, 49).

[7] Spovedovanje je sicer obstajalo tudi že prej, vendar je s koncilom dobilo obliko, kot jo v krščanstvu poznajo še danes.

Gutenbergov izum tiskanja s premičnimi kovinskimi črkami v 15. stoletju je pomenil novo prelomnico v družbi in tudi pri pojmovanju zasebnosti. Porast števila knjig v desetletjih, ki so sledila izumu, je pomenil, da knjige niso bile več dragocen plod dolgoletnega ročnega dela menihov in da niso bile več namenjene le najožjemu krogu uporabnikov. S širitvijo knjig se je pojavil tudi nov kulturni ideal, ki je umetnike in teologe spodbujal k zavračanju zunanjega sveta in poglabljanju v raziskovanje odnosa z Bogom preko branja. To je pripomoglo k postopnemu vzponu evropskega individualizma (Ferenstein 2015), enega od temeljev sodobnega sveta. Pri tem je zanimivo, da branje v tišini pri običajnih ni postalo družbeno sprejeto še vsaj dvesto let, dokler knjige niso postale dovolj poceni, da so si jih lahko privoščili tudi manj premožni, in dokler opismenjevanje ljudi ni doseglo zadostne stopnje.

V času pred industrijsko revolucijo so se začele pojavljati prve težnje po uzakonjenju določenih vidikov zasebnosti, ki so se nanašali na podrobnosti iz zasebnega življenja ljudi. Ena prvih prepovedi poseganja v zasebnost je zadevala ameriške poštne uslužbence, ki jim je bilo leta 1710 z zakonom prepovedano brskati po tuji pošti (prav tam). Z industrijsko revolucijo in naraščanjem materialnega bogastva v družbi pa so tudi oblasti začele prepoznavati zasebnost kot enega od temeljev človeškega življenja, vsaj pri premožnih, če že ne pri revežih, ki so praviloma še vedno živeli v natrpanih skupnostih in skorajda brez vsakršne zasebnosti. S filozofskega vidika je pomemben tudi prispevek angleškega pravnika Jeremyja Benthama, ki je leta 1791 predstavil idejo panoptikona, zaporniške strukture, ki s svojo geometrijo omogoča stalno opazovanje vseh subjektov iz centralnega vira, ki pa ostaja pred subjekti skrit (Kovačič 2003, 20). Pravzaprav prikriti opazovalec niti ni potreben; dovolj je le *možnost* njegove navzočnosti, da se subjekti uklonijo njegovi volji zaradi strahu (Solove 2004, 31). Bentham je torej v zasebnosti videl pogoj za svobodno in racionalno delovanje posameznika, brez pritiskov, ki bi jih nanj vršil zunanji opazovalec.

V takšnih političnih in gospodarskih razmerah sta ameriška odvetnika Louis Brandeis[8] in Samuel Warren leta 1890 objavila članek z naslovom "Pravica do zasebnosti". V članku sta avtorja opisala svoja opažanja, da obstoječe ameriško obče pravo ne zadostuje pri omejevanju poseganja v zasebnost posameznikov. Pri tem sta izpostavila, da ima vsak posameznik

[8] Louis Brandeis, ki ga nekateri imenujejo tudi oče zasebnosti, je kasneje postal sodnik na Vrhovnem sodišču Združenih držav Amerike.

splošno pravico, da ga drugi pustijo pri miru[9]. Predlagala sta, da bi moral vsak biti sposoben braniti to pravico z odškodninskimi tožbami zoper kršitelje njihove zasebnosti. S tem sta pokazala, da uveljavljanje novih pravnih sredstev, namenjenih posegom v zasebnost, ne terja korenite spremembe zakonodaje, ampak predstavlja le razširitev že obstoječih načel. Že leta 1903 so se sodišča in zakonodajalci odzvali na članek Warrena in Brandeisa tako, da so sprejeli vrsto odškodninskih zakonov kot odgovor na tveganja, opisana v članku (Solove 2004, 58).

Varovanje zasebnosti je na ta način dobilo formalno priznanje in trdno zakonsko podlago, odškodninsko pravo pa še danes igra zelo pomembno vlogo v ameriškem pravnem redu pri vprašanjih poseganja v zasebnost. Pri tem je zanimivo, da sta Warren in Brandeis svoj članek spisala kot odziv na grožnje, ki jih v družbo vnaša nova tehnologija. V tistem času je namreč prišlo do razmaha fotografske tehnike in aparatov, ki so postajali manjši in bolj prenosni. Avtorja v sami fotografiji nista videla nič slabega, sta pa prepoznala nevarnosti, ki jih ta prinaša v navezi s širitvijo rumenega tiska (Solove 2004, 58). Časopisi so z uporabo fotografij v obrekljivih prispevkih dobili veliko moč škodovati ugledu ljudi, ki so si jih izbrali za tarče. Warren in Brandeis sta se zato upravičeno zbala, da žrtve rumenega tiska nimajo na voljo dovolj možnosti, da odgovorijo na takšne klevete v okviru obstoječega prava. V svojih domnevah sta se izkazala za vizionarja, saj je v desetletjih, ki so sledila njunemu članku, prav tehnologija postala največji vir ogrožanja zasebnosti.

3.3 Stanje in odnos do zasebnosti danes

V 20. stoletju je tehnologija vstopila v fazo pospešenega razvoja, ki z vsakim naslednjim letom le še pridobiva na hitrosti. Elektronika je omogočila pojav novih oblik poseganja v zasebnost. Fotografije, ki so prestrašile Warrena in Brandeisa, so dopolnili sprva zvočni in video posnetki, kasneje pa še podatki z najrazličnejših senzorjev, ki si jih pionirja zasebnosti v svojem času nista mogla niti zamisliti. Razvoj računalništva je povzročil revolucijo na številnih področjih življenja in dela ter sprožil digitalizacijo, ki je tehnologijo potisnila v vse kotičke sodobnega življenja. In ne nazadnje se je svet s pojavom interneta povezal v globalno

[9] Nekateri viri zato napačno pripisujejo Warrenu in Brandeisu enačanje pravice do zasebnosti s pravico do tega, da te pustijo pri miru. V članku avtorjev je nakazano, da je prva zgolj poseben primer druge (Gavison 1980, 437).

celoto, kjer so informacije o vsem in vsakomur dostopne v takšnem obsegu kot še nikoli prek v zgodovini. Trend razvoja tehnologije lahko poenostavljeno strnemo v naslednji opis: *več naprav, več podatkov, več povezljivosti*.

Skupaj s tehnologijo se je spreminjal tudi naš odnos do zasebnosti. Spomnimo se, da je zasebnost v svoji zgodovini od plemenskih ureditev do danes tako ali tako vselej izgubila, ko so ji nasproti stale druge vrednote, od varnosti in transparentnosti do ugodja in užitka. Večina ljudi je rade volje zamenjala zasebnost za udobje, bogastvo ali slavo (Ferenstein 2015) in zdi se, da danes ni nič drugače. Nekateri zato menijo, da je zasebnost v bližnji prihodnosti obsojena na trivialno vlogo v družbi, če že ne na popoln propad. S tem se bo naša družba vrnila h koreninam, ko si naši predniki niso niti predstavljali, da sploh lahko obstaja svet, v katerem zasebnost igra kakršno koli vlogo. Če to drži, je zasebnost dejansko le tri tisoč let trajajoča anomalija v človeški zgodovini, ki bo kmalu odstopila mesto drugim vrednotam, ki bodo omogočile boljše, učinkovitejše in pravičnejše življenje v tehnokratski družbi prihodnosti. Vzvišene izjave vplivnih ljudi iz informacijskega sektorja, kot je bila leta 1999 izjava Scotta McNealyja, izvršnega direktorja podjetja Sun Microsystems (Sprenger 1999), da ljudje pravzaprav nimamo nobene zasebnosti in da moramo to sprejeti, je treba nemara jemati brez ironije in posmeha.

Toda zdi se, da ljudje zasebnosti še vedno (vsaj navzven) pripisujemo velik pomen. V anketi iz leta 2011 so anketiranci ogrožanje zasebnosti na spletu postavili na prvo mesto med vsemi grožnjami, ki se jih bojijo – celo pred teroristične napade, osebni stečaj in vlom v dom (Craig in Ludloff 2011, 26). Druge raziskave kažejo, da obstaja precejšen razkol med izraženim odnosom do zasebnosti ter dejanskim obnašanjem v praksi, saj je večina vprašanih bila navkljub načelnim stališčem pripravljena zasebnost zamenjati za razne oblike ugodnosti (Acquisti v Lane in drugi 2014, 1. del, 3. pogl.).

Zaupanje Evropejcev v sposobnost posameznih institucij, da uspešno zaščitijo zasebnost uporabnikov, je merila raziskava Evrobarometer iz leta 2011 (Elias v Lane in drugi 2014, 2. del, 8. pogl.). Z več kot 60 odstotki so največje nezaupanje anketiranci izrazili do spletnih podjetij, iskalnikov, družbenih omrežij in ponudnikov elektronske pošte ter do ponudnikov telefonije in interneta. Sledile so jim trgovine, institucije Evropske unije, banke in finančne ustanove, državne institucije, največ zaupanja na področju varovanja zasebnosti pa med Evropejci uživajo ponudniki zdravstvenih storitev.

Podobna stališča imamo tudi Slovenci. Anketa Inštituta za kriminologijo pri Pravni fakulteti v Ljubljani, izvedena v letih 2012, 2013 in 2014, ugotavlja, da je kar 70 odstotkov anketirancev delno ali zelo zaskrbljenih glede posegov v zasebnost na spletu, povečano zaskrbljenost pa so izrazili tudi pri uporabi brezžičnih omrežij (53 odstotkov) in mobilnih telefonov (45 odstotkov) (Završnik in Levičnik 2014, 130–131)[10]. Po mnenju slovenskih anketirancev zasebnost na spletu najbolj ogrožajo velika podjetja, kot sta Google in Facebook, sledijo jim telekomunikacijski operaterji in trgovine s programi zvestobe. Domači in tujim obveščevalnim službam anketiranci niso pripisali pretirano velikega pomena pri posegih v njihovo zasebnost na spletu, je pa ta delež znatno zrasel po razkritjih Edwarda Snowdna (Završnik in Levičnik 2014, 134). In prav tako, kot se je pokazalo v tujih anketah, so se tudi Slovenci brez večjih zadržkov pripravljeni odpovedati svoji zasebnosti v zameno za določene storitve in ugodnosti. Prednjačijo obljubljeni popusti pri nakupih letalskih kart in artiklov v spletnih trgovinah, najmanj anketirancev pa bi zaupne podatke odstopilo v zameno za sodelovanje v nagradni igri (Završnik in Levičnik 2014, 139), kar je pogost način pridobivanja osebnih podatkov tudi v našem spletnem medijskem prostoru.

Ambivalenca uporabnikov do vprašanj zasebnosti je torej očitna tako v tujini kot doma. Naš odnos do zasebnosti v času vseprisotnih sodobnih tehnologij je zapleten in ga ni mogoče preprosto zreducirati na sprejemanje ali zavračanje. Ljudje zasebnost tudi v današnjih časih dojemamo kot nekaj, kar ni trivialno, čeprav pogosto ne znamo ubesediti svojih prepričanj in pojasniti, zakaj razmišljamo tako. V času kriz in afer, ko v javnost pridejo zgodbe o zlorabah zasebnosti s strani državnih ali zasebnih akterjev, se tudi naše vrednotenje zasebnosti okrepi, vendar naša dejanja še vedno govorijo drugačno zgodbo. Vpetost v tehnologijo in storitve, ki nam nudijo udobje, prikladnost in zabavo, je prevelika, da bi se lahko odpovedali ugodnostim na račun več zasebnosti. Prav to pa omogoča današnjim in bodočim akterjem, da od nas pridobivajo vse večje količine podatkov iz virov, za katere morda sploh ne vemo, da obstajajo, in z njihovo pomočjo odkrivajo dejstva o nas in naši družbi, ki jih do nedavnega ni bil zmožen napovedati nihče.

[10] Ocena ogrožanja zasebnosti iz drugih virov, ki niso povezani z internetom ali mobilnimi omrežji, je bila precej nižja (Završnik in Levičnik 2014, 130–131)

4 FORMALNO-PRAVNO UREJANJE VAROVANJA ZASEBNOSTI

4.1 Varovanje zasebnosti v informacijski družbi v Združenih državah Amerike

Ameriški koncept pravice do zasebnosti je običajno opredeljen kot nadzor nad informacijami, ki se tičejo subjekta (Craig in Ludloff 2011, 16). Ameriški pravni red se razlikuje od pravnega reda, ki sloni na evropski kontinentalni tradiciji. V ameriškem sistemu občega prava (ang. *common law*) ne obstaja celovit pregled, ki bi zajemal vse zakone in predpise. Izjemno pomembno vlogo pri oblikovanju zakonskih usmeritev imajo sodišča oziroma sodniki, ki sami odločajo o precedensih v posameznih primerih. To se razlikuje od civilnega prava (ang. *civil law*) v državah kontinentalne Evrope[11], kjer so zakoni in prepisi natančno kodificirani oziroma uzakonjeni in kjer je vloga sodnikov, da glede na dejstva v primeru uveljavijo ustrezne ukrepe, navedene v zakoniku.

Zato je tudi pristop k varovanju zasebnosti v ZDA drugačen kot v Evropi. V ZDA namreč ne obstaja nek splošen zakon o varovanju zasebnosti, ki bi pokrival številna različna področja, kot to počne *Direktiva o varstvu podatkov* v Evropski uniji (Ohm v Lane in drugi 2014, 1. del, 4. pogl.). Ameriški pravni red zasebnost obravnava skozi filter svobode in načel prostega trga (Craig in Ludloff 2011, 17) ter obenem sektorsko, kar pomeni, da je urejanje vprašanj s področja zasebnosti odvisno od posameznih področij z lastnimi zakoni in predpisi, denimo zdravstva, šolstva in financ. Nad vsemi zakoni in predpisi je a Ustava Združenih držav Amerike, ki kot vrhovni zakon s svojimi amandmaji zadeva tudi nekatere vidike zasebnosti, čeprav ta v njej ni nikjer izrecno omenjena (Movius in Krup 2009, 174). Schneier (2006) meni, da si snovalci ameriške Ustave niso niti predstavljali, da bi v prihodnosti lahko zasebnost bila stalno na udaru, zato se jim ni zdelo potrebno zasebnost opredeliti kot izrecno pravico.

4.1.1 *Ustavno pravo*

V ameriškem sistemu prava ustava zagotavlja minimalno stopnjo varovanja zasebnosti, kar pomeni da posamezne države ali zvezni zakoni ne morejo znižati te stopnje (Solove 2011,

[11] Razlike med obema sistemoma se sicer zmanjšujejo, saj v ZDA zakonodaja pridobiva na pomenu, v Evropi pa imajo sodniki tudi več manevrskega prostora pri odločanju v sodbah, kot bi lahko sklepali iz zgoraj povedanega.

13). Čeprav zasebnost v njej ni specifično izpostavljena, ameriško Vrhovno sodišče kljub temu tolmači štiri njene amandmaje v luči pravice do zasebnosti: prvega, četrtega, petega in devetega (Craig in Ludloff 2011, 16). Večina določil amandmajev (*The Constitution of the United States of America* 1787) se nanaša na delovanje ameriške zvezne vlade[12] in ne akterjev zasebnega sektorja. Poleg tega je Vrhovno sodišče že leta 1965 v sodnem primeru *Griswold proti Connecticutu* priznalo obstoj ustavne pravice do zasebnosti (Kovačič 2006, 55).

Četrti amandma ustave ZDA predstavlja osnovo regulacije zbiranja informacij s strani vlade (Solove 2011, 12). Nanaša se na omejevanje preiskav in zasegov, ki predstavljajo posege v zasebnost posameznikov in organizacij. Zagotavlja, da vlada ne more zbirati podatkov o subjektih brez ustreznega pregleda in brez omejitev, saj zahteva od nje, da pred sodiščem upraviči svoje razloge za zbiranje informacij. Kljub temu četrti amandma nikakor ne zagotavlja varnosti pred vladnimi posegi v zaupne podatke, ki so v rokah zasebnih akterjev, saj za omogočanje dostopa do podatkov vladi zadostuje že sodni poziv (redkeje sodni nalog), ki ga ni težko pridobiti (Solove 2011, 93). Četrti amandma pri varovanju zasebnosti sloni na načelu upravičenega pričakovanja zasebnosti (ang. *reasonable expectation of privacy*), ki ločuje med zasebnostjo in lastninsko pravico (Kovačič 2006, 52), zasebnost subjektov pa ščiti le v primerih, ko je moč ugotoviti, da je subjekt dejanja ali podatke upravičeno smatral za zaupne. Sodišča pri tem zaupnost še vedno tolmačijo skozi paradigmo skrivanja (ang. *secrecy paradigm*), po kateri so podatki zaupni le, če predstavljajo takšno ali drugačno obliko skrivnosti. V kontekstu novih družbeno-tehnoloških fenomenov, kjer lahko akterji popolnoma vsakdanje in prosto dostopne podatke o posameznikih zajemajo iz številnih virov ter nato z združevanjem in statistično obdelavo iz njih pridobijo nove informacije, ki bi jih posameznik gotovo smatral za zaupne, takšna paradigma postane preživeta in ne nudi zadostne zaščite. V primerih, kjer četrti amandma ne nudi zaščite, praznino včasih zapolnijo zakoni, še bolj pogosto pa zaščite preprosto ni (Solove 2011, 96).

Preostali amandmaji se varovanja zasebnosti dotikajo posredno. Prvi amandma se nanaša na zagotavljanje pravice do veroizpovedi, svobodnega govora in združevanja. Zasebnost je v tem primeru razumljena kot predpogoj za zagotavljanje svobodnega izražanja, o čemer je tekla

[12] Z ameriško zvezno vlado so mišljene vse vladne organizacije in institucije, ki jim je v interesu pridobivanje podatkov o lastnih in tujih državljanih. V prvi vrsti gre za organe pregona (FBI), obveščevalne službe (CIA) in organe nacionalne varnosti (NSA), a celoten seznam organizacij, ki zbirajo informacije iz javnih in zasebnih virov, je še mnogo daljši.

beseda že v poglavju o pojmovanju zasebnosti, seveda pa je ta interpretacija odvisna od sodišča in posameznega primera. Peti amandma posameznikom zagotavlja pravico, da vlada od njih ne sme izsiliti obremenilnih informacij, ki bi jih inkriminirale. Pri varovanju zasebnosti se sodišča nanj pogosto sklicujejo v navezi s četrtim amandmajem, poglavitna omejitev obeh pa je, da ščitita le pred posegi vlade oziroma države in na noben način ne nadzirata zbiranja in uporabe informacij v zasebnih organizacijah (Solove 2004, 63–64). Deveti amandma ne omejuje pravic ljudstva zgolj na tiste, ki so zapisane v ustavi, in na ta način preprečuje morebitno širjenje moči države na račun pravic, ki jih ustava ne vsebuje. Ker zasebnost v ustavi ni izrecno omenjena, bi se lahko sodišča pri omejevanju vladnega poseganja v zasebnost lahko naslonila tudi na deveti amandma.

Kako se je tolmačenje ameriške ustave glede vprašanj kršenja zasebnosti spreminjalo skozi čas in v odnosu do novih tehnologij, pričajo sodni primeri iz ameriške zgodovine. Leta 1928 je Vrhovno sodišče ZDA v primeru *Olmstead proti Združenim državam* namreč razsodilo, da vladno prisluškovanje telefonskim pogovorom subjekta brez sodnega naloga ni bilo protizakonito, saj so agenti FBI prisluškovalno napravo namestili izven subjektovega doma in na ta način niso posegli v njegov intimni prostor (Kovačič 2006, 46–47; Solove 2004, 197; Solove 2011, 6). Louis Brandeis, takrat že v vlogi vrhovnega sodnika, je odločitvi ostro nasprotoval na podlagi ocene, da spremembe v tehnologiji zahtevajo drugačno razlago, kaj predstavlja zasebno in kaj sestavlja zaupne podatke. Vendar je trajalo še skoraj štirideset let, da je vrhovno sodišče naposled upoštevalo njegovo mnenje. V primeru *Katz proti Združenim državam* iz leta 1967 je šlo za prisluškovanje brez sodnega naloga subjektu v telefonski govorilnici. Vrhovno sodišče je odločilo, da je šlo za protizakonit poseg, ker so tudi podatki na javnih mestih zaupni, če jih subjekt smatra za zaupne, in na ta način upravičeni do ustavne zaščite (Solove 2004, 198). Vrhovno sodišče je svojo odločitev utemeljilo tako na načelu upravičenega pričakovanja zasebnosti kot na paradigmi skrivanja. Odločitev je pomenila, da četrti amandma varuje ljudi in ne prostorov (Kovačič 2006, 47). Pomenljivo je, da je sodna praksa potrebovala kar štiri desetletja, da je stopila v korak z razvojem tehnologije, ki jo je predstavljajo elektronsko prisluškovanje. To nazorno priča, da se danes, ko se tehnologija razvija še nekaj redov velikosti hitreje, pri urejanju varovanja zasebnosti nikakor ne bi smeli zanesti izključno na zakonodajo.

4.1.2 *Zakonodaja*

S primerom *Katz proti Združenim državam* je bilo lastninsko koncipiranje pravice do zasebnosti v ameriški pravni teoriji naposled preseženo, vendar ga je še vedno moč zaslediti predvsem v zasebnem sektorju (Kovačič 2006, 53). Če se zasebnost lahko smatra kot lastnina oziroma dobrina, to pomeni, da lahko posamezniki z njo tudi trgujejo in se odpovedo pravici do nje v zameno za druge dobrine. To s pridom izkoriščajo zbiralci in upravljavci osebnih podatkov, ki te lahko od uporabnikov zbirajo skorajda brez vsakršnih omejitev. Pri tem se je uveljavilo načelo obveščanja in soglasja (ang. *notice and consent*), preko katerega akterji uporabnike obvestijo o načinih prenosa informacij (najpogosteje v obliki zbiranja podatkov) in jim ponudijo možnost sprejetja ali zavrnitve (Nissenbaum, 2011, 34). Primer obveščanja in soglasja v informacijskem sektorju so vsem dobro znane licenčne pogodbe s končnim uporabnikom (EULA), ki jih v praksi ne prebira praktično nihče, z sprejetjem njihovih pogojev pa uporabnik lahko pristane tudi na zbiranje podatkov o njem.

Ko akter pridobi soglasje in zbere zasebne podatke uporabnikov, ti formalno postanejo njegova last in lahko z njimi počne praktično kar koli (Kovačič 2006, 63), kar vključuje tudi njihovo obdelavo, povezovanje s podatki iz drugih virov, ter posredovanje in prodajo tretjim osebam, tudi morebitnim državnim institucijam. Povedano preprosto, mnogi načini uporabe podatkov v zasebnem sektorju v ZDA so brez regulacije. Kjer je uporaba omejena, zakoni sledijo načelom poštene rabe informacij (načela FIPP[13]) (Ohm v Lane in drugi 2014, 1. del, 4. pogl.). Kljub temu so določene informacije v ZDA razmeroma dobro zakonsko zaščitene, nanašajo pa se na posamezna področja v javnem in zasebnem sektorju, medtem ko izven teh področij trgovanje s podatki poteka po načelih prostega trga (Tanner 2014, 5. pogl.). V nadaljevanju so predstavljeni zakoni in predpisi, ki urejajo varovanje osebnih podatkov znotraj teh področij (Solove 2004, 67–71; Solove 2011, 10–12, 73–75; Craig in Ludloff 2011, 29; Ohm v Lane in drugi 2014, 1. del, 4. pogl.):

[13] Načela izhajajo iz leta 1973 in se glasijo: (1) prepovedano je shranjevanje osebnih podatkov v tajnosti, (2) osebam mora biti omogočen vpogled v informacije, zbrane o njih, ter v načine njihove uporabe, (3) osebam mora biti omogočeno, da preprečijo uporabo informacij, zbranih o njih, v druge namene brez njihovega soglasja, (4) osebam mora biti omogočeno, da popravijo ali dopolnijo informacije, zbrane o njih, in (5) organizacije, ki ustvarjajo, vzdržujejo, uporabljajo ali razpošiljajo zbirke osebnih podatkov, morajo zagotoviti uporabo podatkov za predviden namen ter ukrepati, da se prepreči zlorabe podatkov. Načela so močno vplivala na kasnejše *Smernice za zaščito zasebnosti in čezmejni pretok osebnih podatkov*, ki jih je sprejela OECD (Ohm v Lane *et al* 2014, 1. del, 4. pogl.).

- *Zakon o zasebnosti* (1974): kljub splošnemu imenu ureja samo varovanje zasebnosti informacij, shranjenih v velikih državnih bazah podatkov;
- *Zakon o zunanji obveščevalni dejavnosti* (FISA, 1978): namen zakona je bil vzpostaviti formalno-pravni okvir, znotraj katerega bi izvršna veja oblasti lahko legitimno izvajala zunanjo obveščevalno dejavnost z namenom zagotavljanja nacionalne varnosti, in se kot tak nanaša izključno na delo obveščevalnih služb;
- *Zakon o računalniških prevarah in zlorabah* (CFAA, 1984): zakon je bil zasnovan z namenom kriminalizacije vdorov v računalnike državnih organizacij;
- *Zakon o zasebnosti elektronskih komunikacij* (ECPA, 1986): ureja področje "novih" tehnologij, kot so avdio, video in podatkovne komunikacije, vključno z elektronsko pošto in mobilno telefonijo, ter omejuje prestrezanje poslanih podatkov in iskanje po shranjenih podatkih, a je neustrezen pri nadzoru velikega dela zbiranja informacij s strani zasebnega sektorja; namen zakona je bila zaščita elektronske pošte, računalniških datotek in komunikacijskih zapisov pred dejavnostmi državnih organizacij (na tem področju zakon uvaja strožja pravila kot FISA), vendar se zakona v kasnejših letih ni veliko posodabljalo in je danes precej zastarel[14];
- *Zakon o poštenem poročanju o kreditni sposobnosti* (FCRA, 1970): ureja varovanje zasebnosti na področju finančnih podatkov, s katerimi razpolagajo agencije za poročanje o kreditni sposobnosti, vendar ne omejuje sekundarne uporabe ali razkrivanja teh informacij;
- *Zakon o družinskih pravicah do izobraževanja in zasebnosti* (FERPA, 1974): ureja dostop do podatkov o dijakih in študentih, razen podatkov, ki se tičejo varnosti ali zdravja, ter ima zelo ozko področje pristojnosti;
- *Zakon o komunikacijski politiki kabelskih televizij* (CCPA, 1984): kabelskim operaterjem zapoveduje, da uporabnike obveščajo o naravi in uporabi zbiranja podatkov o njih in jim prepoveduje razkrivanje vsebin, ki jih uporabniki gledajo, razen če se podatki nanašajo na "legitimno poslovno dejavnost";
- *Zakon o varovanju zasebnosti video posnetkov* (VPPA, 1988): prepoveduje ponudnikom video vsebin razkritje nakupovalnih ali izposojevalnih navad svojih uporabnikov in na ta način ureja zelo ozko področje zasebnosti;

[14] Leta 2011 sprejeti *Patriotski zakon* je uvedel spremembe tudi v zakona FISA in ECPA. Večinoma je državi omogočil večja pooblastila pri izvajanju nadzora (Solove 2011, 12).

- *Zakon o zaščiti telefonskih uporabnikov* (TCPA, 1991): omejuje vsiljive klice prodaje prek telefona in ureja le ozko področje zasebnosti;
- *Zakon o varovanju zasebnosti voznikov* (DPPA, 1994): zveznim državam prepoveduje posredovanje informacij o motornih vozilih zasebnemu sektorju brez dovoljenja voznikov, kar je kljub omejenim pristojnostim zakona eden redkih poskusov nadzora pretoka podatkov med javnim in zasebnim sektorjem;
- *Zakon o prenašanju in odgovornosti za podatke zdravstvenega zavarovanja* (HIPAA, 1996): ureja področje zdravstva in prepoveduje uporabo in razkrivanje podatkov brez soglasja, razen za potrebe zdravljenja, plačevanja ali delovanja zdravstvenega sistema;
- *Zakon o varovanju zasebnosti otrok na spletu* (COPPA, 1998): prvi zvezni zakon, ki ureja vprašanje zasebnosti na internetu, vendar se nanaša le na pridobivanje podatkov, ki ga izvajajo spletne strani, namenjene otrokom, oziroma če lastniki strani vedo, da so med njihovimi uporabniki zanesljivo tudi otroci;
- *Zakon Gramm–Leach–Bliley* (GLBA, 1999): dovoljuje finančnim ustanovam, da prek obvestila uporabnikom posredujejo njihove informacije, ki niso javnega značaja, drugim povezanim ustanovam, vendar omogoča uporabnikom možnost zavrnitve, če gre za razkritje podatkov tretjim osebam.

Skupno vsem naštetim zakonom je, da so stari že leta ali celo desetletja, in da pokrivajo zgolj majhen del geografije zbiranja podatkov, ki z uveljavljanjem novih družbeno-tehnoloških fenomenov pridobiva stalno nove dimenzije. Ker nimajo urejene celostne zakonske zaščite varovanja zasebnosti na področju osebnih podatkov, ZDA predstavljajo med industrijsko razvitimi demokracijami izjemo (Payton in Claypoole 2014, 14. pogl.). Takšen mozaični pristop k zakonodaji odraža tradicionalen strah Američanov pred vmešavanjem vlade v dejavnosti zasebnega sektorja, kar ima za rezultat razdrobljeno in nezadovoljivo reševanje posamičnih vprašanj varovanja zasebnosti (Solove 2004, 71). Poleg teh zakonov obstaja še več kot stotina zveznih in državnih zakonov, ki urejajo določene vidike zasebnosti znotraj svojih področij (Craig in Ludloff 2011, 29). Nekateri predlogi zakonov, ki bi urejali novejše vidike varovanja zasebnosti na področju zbiranja podatkov, vključujejo Zakon o prepovedi sledenja na spletu, Zakon o odgovornosti in zaupanju glede podatkov, Zakon o listini pravic glede komercialne zasebnosti ipd. (Craig in Ludloff 2011, 69–70).

Na področjih, ki jih ne ureja noben zakon ali predpis, je varovanje zasebnosti prepuščeno dobri volji akterjev. Edini nadzor nad izvrševanjem lastnih politik zasebnosti, ki jih sprejmejo

podjetja in organizacije, vrši Zvezna komisija za trgovino (FTC), ki lahko kršitelje prisili, da opustijo nepoštena in varljiva ravnanja do svojih uporabnikov. Njena vloga je podobna vlogi evropskih organov za varstvo osebnih podatkov (Kovačič 2006, 66). Uspešnost komisije omejuje pomanjkanje časa in sredstev ter dejstvo, da akterji, ki varovanja zasebnosti sploh ne vključijo v svoje dokumente, niso del njene pristojnosti (Solove 2004, 73).

4.1.3 *Odškodninsko pravo*

Pomembno vlogo pri zagotavljanju varovanja zasebnosti v ameriškem pravnem sistemu igra odškodninsko pravo, ki ima svoje temelje v že omenjenem članku Warrena in Brandeisa iz leta 1890. Avtorja članka v obstoječi zakonodaji nista videla zadostne zaščite zasebnosti posameznikov, zato sta predlagala nove načine varovanja zasebnosti, v prvi vrsti odškodninsko ukrepanje, ki bi posameznikom nudilo možnost tožbe v primerih vdora v njihovo zasebnost (Solove 2004, 58). Tako odškodninske tožbe v ZDA še danes predstavljajo glavno orožje posameznikov in organizacij, ki menijo, da je bila njihova zasebnost nezakonito kršena.

Leta 1960 je ameriški pravnik William Prosser kategoriziral pretekle primere odškodninskih tožb v štiri razrede, ki so postali znani kot štiri delikti kršenja zasebnosti (Craig in Ludloff 2011, 17; Kovačič 2006, 61; Solove 2004, 59–61; Strandburg v Lane in drugi 2014, 1. del, 1. pogl.):

1. vdor v oškodovančevo samoto oziroma osamitev,
2. javno razkritje sramotilnih zasebnih podatkov o oškodovancu,
3. publiciteta, ki oškodovanca v javnosti prikazuje v slabi luči in
4. prisvojitev oškodovančevega imena ali podobe z namenom pridobivanja koristi.

Ti štirje delikti predstavljajo standard, s katerim znotraj ameriškega sodnega sistema ugotavljajo kršitve zasebnosti. Mnogi pravni strokovnjaki so mnenja, da so v svojih definicijah preveč togi za uspešno spoprijemanje z vprašanji glede zasebnosti v času digitalnih tehnologij (Craig in Ludloff 2011, 17). Odškodninski ukrepi so omejeni na posamezne prestopke in kršitve, zoper katere morajo oškodovanci na lastno pobudo vložiti tožbo. Zbiranje in obdelava masovnih podatkov, njihovo shranjevanje v oblaku ter uporaba novih tehnologij za zajemanje podatkov pa nikakor ne predstavljajo osamljenih kršitev, temveč gre za sistemsko delovanje, ki ga omogočajo nove tehnologije in ki pogosto ne

vključuje samo enega kršitelja, ampak celo vrsto udeležencev, ki sami po sebi ne delujejo v nasprotju z zakonom, rezultat njihovega skupnega nastopa pa ima za posameznike vseeno lahko škodljive posledice.

4.2 Varovanje zasebnosti v informacijski družbi v Evropski uniji

Če ameriški sistem zakonodaje lahko opišemo kot pristop z dna proti vrhu, lahko za evropskega rečemo, da deluje z vrha proti dnu (Craig in Ludloff 2011). Med zagovorniki močne zakonske zaščite zasebnosti velja evropski model za zgled. Mnoge države imajo pravico do zasebnosti zapisane v svojo ustavo, tudi Slovenija, in sicer v 35. členu, posameznim vidikom zasebnosti pa so namenjeni še členi 36, 37 in 38[15] (*Ustava Republike Slovenije* 1991). Razloge, zakaj se evropski sistem tako razlikuje od ameriškega, lahko iščemo v drugačni tradiciji, podjetniški kulturi in zgodovini. Evropa ima za razliko od ZDA veliko izkušenj s totalitarnimi režimi, ki so s pridom izkoriščali tudi pridobivanje osebnih podatkov za izvajanje nadzora in represije nad lastnim in tujim prebivalstvom. Teh metod niso uporabljale le tajne policije in obveščevalne službe povojnih komunističnih držav, temveč tudi nacisti med drugo svetovno vojno, ki so si s pridobljenimi podatki pomagali tudi pri ločevanju Judov od Nejudov in vodenju koncentracijskih taborišč (Kovačič 2004, 72). Potreba po močni zaščiti zasebnosti posameznika in priznanje zasebnosti kot neodtujljive pravice, ki jo treba varovati, je zato globoko zasidrana v evropski zavesti.

4.2.1 *Zgodnji nadnacionalni dokumenti*

Na ravni nadnacionalnih institucij je Svet Evrope že leta 1948 sprejel Evropsko konvencijo o človekovih pravicah (EKČP), ki predstavlja osnovo za delovanje Evropskega sodišča za človekove pravice. EKČP v svojem 8. členu navaja, da ima vsak pravico do spoštovanja zasebnega in družinskega življenja, doma in občil (*European Convention on Human Rights* 1948), s čimer so danes mišljene tudi telefonske komunikacije, elektronska pošta, sporočila SMS in podobno (Kovačič 2004, 81). Z uveljavljanjem in decentralizacijo digitalnih tehnologij v naslednjih desetletjih se je poudarek premaknil od zaščite tehnoloških sistemov

[15] Gre za pravico do nedotakljivosti stanovanja oziroma doma, pravico do varstva tajnosti pisem in drugih občil ter pravico do varstva osebnih podatkov (Kovačič 2003, 34).

do zaščite uporabnikov. Že zelo zgodaj v razvoju je zato v Evropi prevladalo mnenje, da je treba izenačiti varovanje informacijske zasebnosti v javnem in zasebnem sektorju oziroma da je treba zaščitno zakonodajo razširiti tudi večja in manjša podjetja (Kovačič 2004, 75). Ta pristop je vplival na oblikovanje zakonov in predpisov za varovanje zasebnosti v vseh nadaljnjih letih, medtem ko v ZDA ni nikoli prišlo do enotne obravnave zasebnosti na ravni države in gospodarstva.

Organizacija za ekonomsko sodelovanje in razvoj je leta 1980 sprejela *Smernice za zaščito zasebnosti in čezmejni pretok podatkov*, ki so skušale uveljaviti načela za zakonito ravnanje z osebnimi podatki tako v javnem kot zasebnem sektorju (Kovačič 2004, 76). Smernice so opredelile osem načel: (1) omejitev zbiranja, (2) kakovost podatkov, (3) navedba namena, (4) omejitev uporabe, (5) varnostni ukrepi, (6) odprtost, (7) vključitev posameznikov in (8) odgovornost (Ohm v Lane in drugi 2014, 1. del. 4. pogl.). Z razvojem digitalnih kapacitet so številne evropske države sprejele svojo zakonodajo za zaščito zasebnosti, ki se je v veliki meri zgledovala po smernicah OECD. Iz smernic je neposredno izhajala tudi *Konvencija o varstvu posameznikov glede na avtomatsko obdelavo osebnih podatkov*, ki jo je Svet Evrope sprejel leta 1981 in ki je poleg poštenega, ustreznega in omejenega zbiranja podatkov določala tudi, da imajo posamezniki pravico do pregleda, popravljanja ali izbrisa podatkov, ki se nanašajo na njih (Kovačič 2004, 76).

4.2.2 *Urejanje zasebnosti v Evropski uniji*

Smernice OECD so bile sicer natančne v svojih določilih za zaščito zasebnosti, vendar neobvezujoče. Pred letom 1995 so se zato zakoni, namenjeni varovanju zasebnosti, po posameznih evropskih državah precej razlikovali. Tega leta pa je Evropska unija po dolgotrajnem usklajevanju med državami članicami sprejela *Direktivo o varstvu podatkov* 95/46/EC, ki je zajemala osem načel iz smernic. Namen direktive, ki ima 33 členov in osem poglavij, je bil vzpostaviti regulatorni okvir za varen in prost pretok osebnih podatkov preko meja držav članic Evropske unije, poleg zagotavljanja osnov varnosti osebnih podatkov pri njihovi hrambi, prenosu in obdelavi (Craig in Ludloff 2011, 32–33). Direktiva se tako ni nanašala le na zaščito subjektov in njihovih podatkov, temveč je vključevala tudi vzpostavitev mehanizmov za mednarodni prenos podatkov, ki je danes eden temeljev digitalnega gospodarstva in pogost povzročitelj trenj med ZDA in Evropsko unijo.

Direktiva je začela veljati leta 1998. Držav članic sicer ne zavezuje neposredno, ampak jim omogoča, da same poiščejo ustrezne načine, s katerimi bodo zagotovile izpolnjevanje predpisanih pogojev. Državljani Evropske unije, ki menijo, da je bila njihova zasebnost nezakonito kršena, zato tudi nimajo na voljo pravnega sredstva v okviru direktive, ki bi ga lahko uporabili za zaščito svojih pravic, razen če takšna pravna sredstva obstajajo v sklopu zakonodaje posamezne države (Elias v Lane in drugi 2014, 2. del, 8. pogl.). Mora pa zato tudi vsaka nova država članica Evropske unije poskrbeti, da izpolni cilje, zadane v direktivi.

Pomemben doprinos direktive je tudi njen 28. člen, ki zahteva ustanovitev neodvisnega nadzornega organa, ki skrbi za spoštovanje zakonodaje in zaščito zasebnosti (Kovačič 2004, 78). To je lahko informacijski pooblaščenec, kot je primer v Sloveniji, ali kakšna druga specializirana agencija, nadzor pa ponekod izvajajo tudi strokovnjaki za informacijsko varnost. Pravni red ZDA ne pozna takšne institucije, ki bi bdela nad kršitelji zasebnosti. Še najbližje ji je Zvezna trgovinska komisija, ki pa lahko ukrepa le proti podjetjem, ki ne spoštujejo lastnih pravil in predpisov.

Direktiva evropskim podjetjem prepoveduje prenos osebnih podatkov v države, ki na področju zaščite zasebnosti ne izpolnjujejo kriterijev, zastavljenih v direktivi. Med takšne države s svojim razdrobljenim načinom varovanja zasebnosti spadajo tudi ZDA. Ker bi omejevanje pretoka podatkov med Evropsko unijo in ZDA imelo škodljive posledice za gospodarstvo na obeh straneh Atlantika, sta ameriško Ministrstvo za trgovino in Zvezna trgovinska komisija v sodelovanju z Evropsko unijo pripravila sporazum *Varna hramba* (ang. *Safe Harbor*), ki je bil naposled sprejet leta 2000 (Craig in Ludloff 2011, 34). Ta določa sedem načel varovanja osebnih podatkov, ki so podobna načelom iz smernic OECD, katerim se prostovoljno zavežejo ameriška podjetja in si na ta način zagotovijo izmenjavo podatkov z državami članicami Evropske unije. Podjetja lahko svoje strinjanje z načeli izrazijo v svoji politiki zasebnosti ali s pridružitvijo programu samoregulacije, kakršen je denimo program TRUSTe (prav tam). Kritike sporazuma letijo predvsem na pomanjkanje ustreznega nadzora in sistematičnega pregleda, saj je spoštovanje načel prepuščeno samoregulaciji podjetij in podpornih programov (Kovačič 2004, 79).

V današnjem času *Direktiva o varstvu podatkov* 95/46/EC ni več dorasla izzivom, ki jih prinašajo globalizacija, nenehno širjenje tehnoloških zmogljivosti in sprememba načinov, kako posamezniki ustvarjajo, delijo in uporabljajo osebne podatke, saj je nastala že v času pred komercializacijo interneta oziroma svetovnega spleta, prenosnimi in mobilnimi

računalniki, GPS in RFID napravami, storitvami Web 2.0 in seveda masovnimi podatki (Rubinstein 2013, 2). Kljub velikemu vplivu, ki ga ima direktiva na zaščito zasebnosti v Evropi, je Evropska komisija sklenila, da ta zaradi številnih tehnoloških sprememb, ki so nastopile po uvedbi direktive, potrebuje reformo oziroma okrepitev z bolj neposredno umestitvijo v sistem evropske zakonodaje (Elias v Lane in drugi 2014, 2. del, 8. pogl.). Zato je sčasoma nastala *Splošna uredba o varstvu podatkov* (GDPR), ki ima cilj povečati in poenotiti zaščito zasebnosti na nivoju posameznikov v Evropski uniji in obenem urediti vprašanje izvoza podatkov v države nečlanice. Največje spremembe se bodo nanašale na (1) obseg zakonodaje, ki bo zajemala vse posameznike in organizacije, ki bodo obdelovali osebne podatke državljanov Evropske unije, (2) koordinacijo nacionalnih organov za varovanje podatkov s strani Evropskega odbora za varstvo podatkov, (3) pridobivanje izrecnega soglasja uporabnikov in (4) pravico do izbrisa, če uporabnik umakne soglasje (prav tam). Pomembna je tudi novost, ki jo uvaja načelo prenosljivosti podatkov, omenjeno v 18. členu uredbe, in uporabnikom omogoča prenos svojih podatkov med storitvami, česar danes v praksi ne ponuja praktično nobeno podjetje. Načelo je bilo zasnovano z mislijo na osebne podatke v družbenih omrežjih (Rubinstein 2013, 7), zato ne ponuja izrecnih rešitev za težave, ki jih na področju varovanja zasebnosti prinašajo masovni podatki.

15. decembra 2015 so Evropski parlament, Evropski svet in Evropska komisija dosegli soglasje glede novih pravil za zaščito zasebnosti in osebnih podatkov, ki bodo predstavljali temelj sodobnega in usklajenega pristopa znotraj celotne Evropske unije. Novo uredbo je Evropski svet sprejel 8. aprila 2016, Evropski parlament pa nekaj dni kasneje, 14. aprila 2016. V veljavo bo stopila v dvoletnem obdobju od datuma sprejetja.

Poleg *Direktive o varstvu podatkov* 95/46/EC in *Splošne uredbe o varstvu podatkov* je Evropska unija sprejela dodatne direktive, ki urejajo posamezna področja zaščite zasebnosti. Leta 1997 je bila s tem namenom sprejeta *Direktiva o zasebnosti telekomunikacij* 97/66/EC ter leta 2002 *Direktiva o zasebnosti in elektronskih komunikacijah* 2002/58/EC, ki med drugim urejata shranjevanje podatkov o komunikacijskem prometu, ki se (ob določenih izjemah) ne sme izvajati brez soglasja uporabnika (Kovačič 2004, 82). Ta pristop vključevanja (ang. *opt in*) se pogosto razlikuje od pristopa ameriških podjetij, ki podatke o uporabnikih zbirajo brez njihove privolitve, dokler ti izrecno ne izrazijo želje po izključitvi iz procesa zbiranja (ang. *opt out*). *Direktiva o zasebnosti in elektronskih komunikacijah* 2002/58/EC določa tudi pravila uporabe neželene elektronske pošte in piškotkov ter narekuje ponudnikom storitev, da po določenem času hrambe izbrišejo ali anonimizirajo podatke.

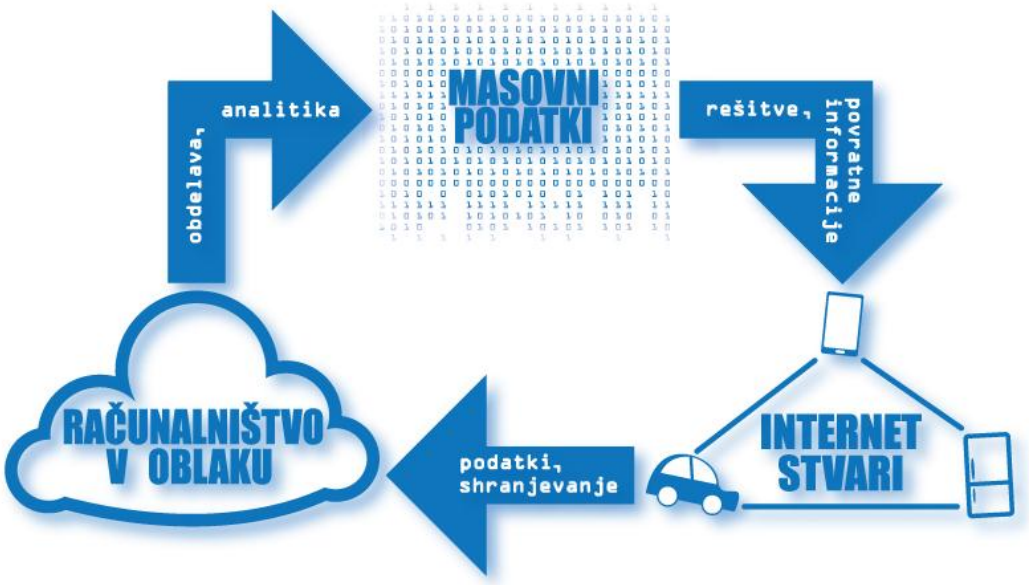
Leta 2006 je bila po številnih zapletih sprejeta tudi kontroverzna *Direktiva o hrambi podatkov* 2006/24/EC, v kateri so mnogi prepoznali resno ogrožanje zasebnosti. Nastala je po terorističnih napadih v Londonu in Madridu in ponudnikom telefonskih in internetnih storitev narekovala, da morajo v obdobju od šestih mesecev do dveh let obvezno hraniti podatke o uporabnikih in prometu za potrebe organov pregona in boja proti terorizmu (Craig in Ludloff 2011, 34). To je bilo povsem v nasprotju z direktivo iz leta 2002, saj za pridobivanje podatkov o prometu uporabnikov ni bilo več potrebno pridobiti njihovega soglasja. Leta 2014 je Evropsko sodišče sporno direktivo razveljavilo s pojasnilom, da je kršila osnovne človekove pravice (O'Brien 2014).

5 RAZCVET NOVIH DRUŽBENO-TEHNOLOŠKIH FENOMENOV

V tem delu z izrazom "novi družbeno-tehnološki fenomeni" označujemo tri tehnologije: masovne podatke, računalništvo v oblaku in internet stvari. Namen izraza je zajeti omenjene tehnologije z ustrezno nadpomenko zaradi preglednejšega opisovanja (in branja). V izrazu niso omenjeni zgolj tehnološki fenomeni, temveč jim je pripisana tudi družbena komponenta, s čimer želimo poudariti močno vpetost novih tehnologij v družbo oziroma različne družbene procese. Družba ni le uporabnica novih tehnologih, ampak te tehnologije vplivajo tudi na preoblikovanje družbe in usmerjajo njen razvoj. Povedano drugače, nove tehnologije uvajajo v družbo kvalitativne in kvantitativne spremembe, ki vplivajo in bodo tudi v prihodnosti vplivale na njen ustroj.

Pri tem je treba opozoriti, da "nove tehnologije" niso resnično nove, saj sta dve od omenjenih tehnologij (uporaba masovnih podatkov in računalništva v oblaku) že uveljavljeni, medtem ko je tretja (internet stvari) še v zgodnji fazi svojega razvoja. Kljub temu se bo uporaba masovnih podatkov in računalništva v oblaku v prihodnjih letih še povečevala, internet stvari pa bo še potenciral njun pomen in vpliv. Vse tri tehnologije namreč niso izolirane oziroma omejene vsaka na svoje področje, saj se njihova uporaba prepleta in daje rezultate, ki predstavljajo sinergijo vseh komponent. Povezavo med masovnimi podatki, računalništvom v oblaku ter internetom stvari v skupnem ekosistemu lahko ponazorimo s poenostavljeno shemo:

Slika 5.1: Poenostavljen prikaz soodvisnosti masovnih podatkov, računalništva v oblaku ter interneta stvari.



Prikazana povezava med novimi družbeno-tehnološkimi fenomeni seveda ni ekskluzivna. Masovni podatki se lahko zbirajo in obdelujejo iz najrazličnejših virov, denimo iz javno dostopnih baz podatkov, v katere se podatki stekajo že vrsto let ali celo desetletij. Prav tako se podatki lahko zbirajo in obdelujejo lokalno, torej brez posrednika v obliki storitev v oblaku. Nabor teh storitev je tudi sicer zelo širok in med njihove odjemalce spadajo tako posamezniki kot podjetja in državne ustanove. Poleg tega bo internet stvari omogočil vrsto novih funkcionalnosti, med katerimi bosta analitika in obdelava podatkov v oblaku predstavljala le en, čeprav zelo pomemben, del celote.

Večina sistemov za obdelavo masovnih podatkov ni uporabljala storitev računalništva v oblaku, vendar je pojav javnih oblakov[16], iskalnikov in družbenih omrežij povzročil, da so tudi ponudniki računalništva v oblaku, kot so Google, Amazon in Microsoft, razvili cenovno dostopne platforme za masovne podatke (Linthicum 2015). Z internetom stvari se bo dotok podatkov še povečeval, zato je smotrno pričakovati, da bo v te namene naraščala tudi uporaba računalništva v oblaku in masovnih podatkov. Že zdaj namreč skoraj 80 odstotkov razvijalcev aplikacij za internet stvari vsaj četrtino časa nameni analitiki in delu z bazami podatkov, medtem ko jih 42 odstotkov sodeluje pri naprednih analitičnih projektih, ki vključujejo masovne podatke; 55 odstotkov razvijalcev naprave v sklopu interneta stvari povezuje preko računalništva v oblaku (Columbus 2015). Uporaba tehnologije interneta stvari postaja cenovno dostopna prav zaradi javnih storitev računalništva v oblaku, ki omogočajo avtomatizacijo naprav s pomočjo pametnih omrežij, sistemov učenja, zbiranja in analize podatkov (Linthicum 2015).

5.1 Masovni podatki

Masovni podatki se nanašajo na nove načine, s katerimi organizacije, ki zajemajo od državnih institucij do podjetij, združujejo različne nabore digitalnih podatkov in nato s pomočjo statističnih metod in tehnik rudarjenja podatkov iz njih pridobivajo informacije, ki so bile pred tem nedostopne, in korelacije, do katerih ne bi mogli priti z uporabo ustaljenih metod

[16] Z izrazom "javni oblak" (ang. *public cloud*) je mišljena storitev računalništva v oblaku, ki je javno dostopna širšim množicam (v nasprotju z zaprtimi sistemi znotraj organizacij), čeprav storitve zagotavljajo praviloma podjetja v zasebni lasti.

(Rubinstein 2013, 1). Izraz "masovni podatki" najpogosteje opisuje podatke, ki so tako obsežni ali kompleksni, da za njihovo shranjevanje, urejanje in obdelavo tradicionalna orodja in metode ne zadostujejo več. Masovni podatki so preobsežni, da bi jih lahko urejali in analizirali z običajnimi protokoli za delo z bazami podatkov, kakršen je SQL[17], zato zahtevajo razvoj novih sistemov za shranjevanje in obdelavo, kot so gruče Hadoop[18], Bloomovi filtri in orodja za obdelavo podatkov R[19]. (Davis in Patterson 2012, 4).

Definicije masovnih podatkov pogosto navajajo tudi pravilo treh V-jev[20], ki predstavljajo količino (ang. *volume*), raznolikost (ang. *variety*) in hitrost (ang. *velocity*) (Mayer-Schönberger in Cukier 2013, 1. pogl), s katerimi želijo opozoriti, da je obseg le eden od sestavnih delov masovnih podatkov. Prav tako pomembna je raznolikost, saj se masovni podatki pridobivajo iz najrazličnejših virov, ki se bodo z razvojem interneta stvari še obogatili. Podatki iz mobilnih telefonov, avtomobilov, proizvodnih naprav, medicinskih pripomočkov, pametnih domov in gospodinjskih aparatov predstavljajo le del spektra vseh virov podatkov. Še bolj zgovorna je hitrost, s katero je mišljeno, kako hitro nastajajo novi podatki. S širjenjem virov podatkov in uvajanjem novih podatkovnih formatov tudi hitrost ustvarjanja podatkov narašča eksponentno. Po nekaterih ocenah se količina digitalnih podatkov podvoji vsake tri leta (prav tam) in 90 odstotkov vseh podatkov na svetu je bilo ustvarjenih v zadnjih dveh letih (Davis in Patterson 2012, 5), ta trend pa se bo nadaljeval tudi v bodoče.

Kljub temu je glavna značilnost masovnih podatkov njihov obseg. Kakšna naj bi bila količina podatkov, ki bi upravičevala oznako masovnosti, je predmet različnih definicij, spreminjala pa se je tudi s časom, saj so podatki, ki jih zajemamo danes, mnogo bolj zajetni, kot so bili še pred nekaj leti, prav tako pa bodo današnje količine podatkov zbledele v primerjavi s tistimi, s

[17] Structured Query Language (SQL) je programski jezik, zasnovan za obdelavo podatkov s pomočjo relacijskih sistemov za upravljanje podatkovnih baz. Za potrebe shranjevanja in obdelave masovnih podatkov se namesto SQL uporablja koncept NoSQL oziroma nerelacijske podatkovne baze.

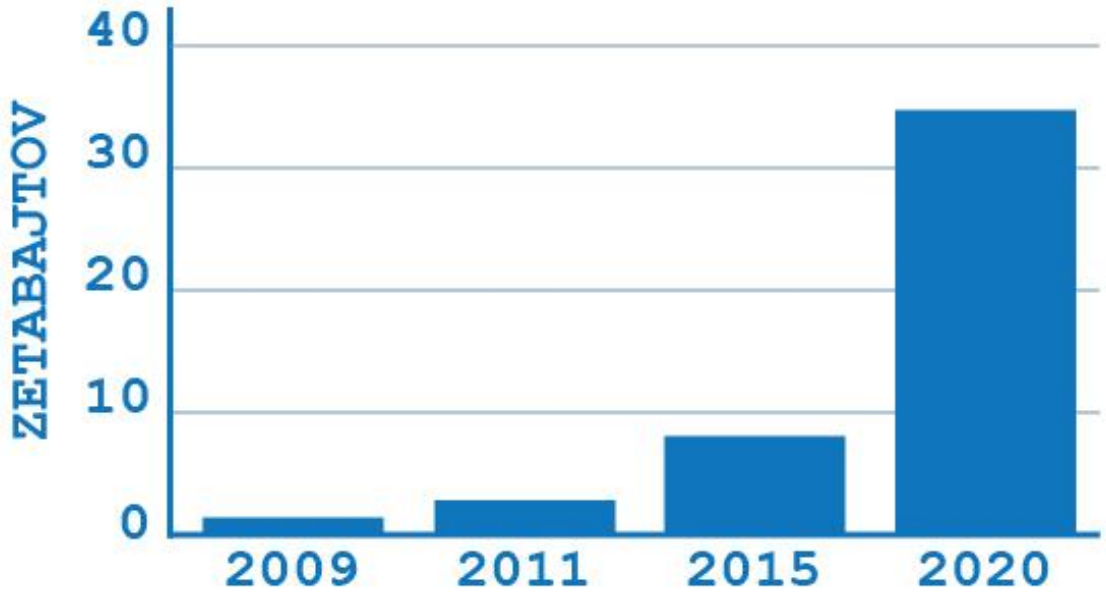
[18] Apache Hadoop je odprtokodno programsko ogrodje za distribuirano shranjevanje in obdelavo velikih količin podatkov, narejeno na osnovi Googlove programske opreme MapReduce.

[19] R je programski jezik oziroma programsko okolje, namenjeno statističnim obdelavam, analizi in rudarjenju podatkov.

[20] Občasno sta trem V-jem dodana še četrti in peti: pravilnost (ang. *veracity*) in vrednost (ang. *value*).

katerimi bomo imeli opravka že v bližnji prihodnosti. Pred nekaj leti je več deset terabajtov[21] podatkov zadostovalo, da je bilo moč govoriti o masovnih podatkih. Danes se je meja pomaknila vsaj tisočkrat višje, torej med petabajte. Količina podatkov, ki jo ustvarijo vse današnje naprave, je še mnogo večja. Raziskovalni center za fiziko osnovnih delcev CERN je že leta 2013 presegel mejo 100 petabajtov zbranih podatkov (Stodden v Lane in drugi 2014, 1. del, 5. pogl.), medtem ko Google *vsak dan* obdela 24 petabajtov podatkov (Mayer-Schönberger in Cukier 2013, 1. pogl.). Samo senzorji na napravah za črpanje nafte vsako leto pridobijo za eksabajt podatkov (Thomas in McSharry 2015, 6. pogl.). Za primerjavo: količina vseh besed, kar smo jih vsej človeški zgodovini izustili ljudje, naj ne bi presegala pet eksabajtov (Bunn 2012). Do leta 2013 naj bi bilo tako na svetu shranjenih za 1.200 eksabajtov informacij, od katerih je bilo manj kot 2 odstotka analognih podatkov (Mayer-Schönberger in Cukier 2013, 1. pogl.).

Slika 5.2: Količina ustvarjenih podatkov na svetovni ravni v zetabajtih.
Vir: "The Knowledge Effect" 2012



Z masovnimi podatki je povezan tudi koncept rudarjenja podatkov, ki se nanaša na iskanje vzorcev v naborih podatkov oziroma na pridobivanje predhodno neznanih in potencialno uporabnih informacij (Rubinstein 2013, 3), vendar ne nujno v sklopu masovnih podatkov.

[21] 1 terabajt je 10^{12} bajtov oziroma 1.000 gigabajtov, kar je kapaciteta cenovno dostopnega trdega diska. 1 petabajt je 10^{15} bajtov oziroma 1.000 terabajtov. 1 eksabajt je 10^{18} bajtov oziroma 1.000 petabajtov. 1 zetabajt je 10^{21} bajtov oziroma 1.000 eksabajtov oziroma 1.000.000 petabajtov.

Rudarjenje podatkov je že dalj časa predstavljajo vir ogrožanja zasebnosti, saj so se ga s pridom posluževale tudi državne institucije (Cate 2008, 438). Države rudarjenje podatkov izvajajo z namenom analize obsežnih informacij o ljudeh, ki lahko razkrijejo nenavadne vzorce ali obnašanje, pogosto tudi brez vnaprejšnjega utemeljenega suma (Solove 2011, 125). Masovni podatki dajejo rudarjenju podatkov dodaten zagon, saj omogočajo povezovanje podatkov iz različnih baz in posledično iskanje vzorcev ter korelacij, ki poprej niso bili dostopni. Odkrivanje takšnih vzorcev in korelacij se na tako zajetnih količinah podatkov izvaja tudi s tehnikami strojnega učenja in napovedne analitike. V poslovnem okolju se za obdelavo masovnih podatkov včasih uporablja izraz poslovna inteligenca (skupaj s skladiščenjem podatkov: BI & DW), ki vključuje tehnike in orodja za pretvorbo surovih podatkov v uporabne informacije za potrebe podjetij.

5.1.1 *Potencial masovnih podatkov*

Vse večja količina podatkov iz najrazličnejših področij našega življenja bo predstavljala izreden potencial za pridobivanje koristnih informacij, s katerimi lahko povečamo blagostanje, dvignemo kakovost življenja velikega dela svetovnega prebivalstva, pridemo do revolucionarnih novih spoznanj v znanosti in medicini in poiščemo rešitve za nekatere najbolj pereče probleme v sodobni družbi, od klimatskih sprememb do propadlih držav. Poleg tega lahko masovni podatki v prihodnjih letih postanejo eden glavnih virov inovacij in ustvarjanja novega gospodarskega kapitala. Na bolj vsakdanji ravni se pomena masovnih podatkov dobro zaveda vse večje število podjetij, ki z njihovo pomočjo ustvarjajo vrednost in konkurenčno prednost, ter političnih organizacij, ki iz masovnih podatkov črpajo družbeno in politično moč (Davis in Patterson 2012, 1). Spletna podjetja so bila med prvimi, ki so zaradi narave svojega dela začela zbirati velike količine podatkov in prepoznavati njihov pomen. Zato so razvila nove tehnologije in tehnike za obdelavo podatkov, s čimer so prehitela tradicionalna podjetja, ki so podatke zbirala sicer že dolgo pred tem, vendar v veliko manjšem obsegu. Raziskave kažejo, da naj bi rešitve, dosežene z obdelavo masovnih podatkov, dvignile produktivnost v podjetjih za 5 do 6 odstotkov, obstajajo pa tudi dokazi, da so masovni podatki pripomogli k prebojem v zdravstvu, pri učinkovitejšem zagotavljanju električne energije, pri odpravljanju težav v prometu in v logistiki (Rubinstein 2013, 3).

Če je potencial masovnih podatkov resnično velik, je realnost nekoliko drugačna, saj so brez ustreznih orodij in analitičnih tehnik takšni podatki zaradi svoje nepreglednosti in kaotičnosti

praktično neuporabni. Prav zato, ker se je treba do uporabnih informacij v podatkih še dokopati, govorimo o dobi masovnih podatkov in ne masovnih informacij. V povezavi s že omenjenimi tremi V-ji lahko ugotovimo, da obseg ogromne količine podatkov zahteva razširitev tehnik obdelave, ki bodo ustrezale sodobni strojni opremi, računalništvu v oblaku in sistemom za shranjevanje podatkov; hitrost podatkov narekuje razvoj algoritmov, ki omogočajo nenehno učenje in posodabljanje v navezi z ustrezno računalniško infrastrukturo; raznolikost podatkov pa potrebuje statistične metode, ki bodo omogočale lažje povezovanje različnih vrst podatkov, zbranih iz različnih virov (Kreuter in Peng v Lane in drugi 2014, 3. del, 12. pogl.).

Z ustreznim znanjem, pristopom in orodjem masovni podatki lahko postanejo prava zakladnica informacij, do katerih z metodami iz preteklosti ne bi mogli nikoli priti. Bistvo masovnih podatkov je namreč njihova napovedna moč (Mayer-Schönberger in Cukier 2013, 4. pogl). Zagovorniki uporabe masovnih podatkov pravijo, da podatki z uporabo pravih tehnik "govorijo zase", saj lahko preko njih pridemo do presunljivo natančnih napovedi. Pogosto se omenja primer Googla, ki je leta 2009 z analizo ključnih besed, ki jih ljudje vpisujejo v iskalnik, uspel predvideti izbruhe gripe v ZDA skorajda v realnem času, medtem ko so uradni podatki Centrov za nadzor bolezni prihajali vsaj teden ali dva kasneje[22] (Mayer-Schönberger in Cukier 2013, 1. pogl.). Googlova napoved izbruhov bolezni ni temeljila na zbiranju in analizi podatkov s terena, ampak na korelaciji med pogostostjo vpisovanja določenih ključnih besed, povezanih s sezonsko gripo, v iskalnik ter podatki o preteklih izbruhih gripe. Poleg velike natančnosti in hitrosti je bila Googlova metoda tudi poceni in nemoteča za udeležence.

Če je Googlovo napovedovanje izbruhov gripe znanilec prihodnosti, potem se bo za ceno iskanja korelacij v masovnih podatkih treba odpovedati tudi nekaterim ustaljenim pravilom, ki veljajo v statistiki, analitiki in znanosti nasploh. Treba bo sprejeti, da so podatki, na podlagi katerih se bodo iskale napovedi in sprejemale odločitve, zaradi svoje množičnosti, raznolikosti in kaotičnosti neurejeni in pogosto nenatančni. Natančnost zahteva skrbno izbiro podatkov, ki pride v poštev le, ko je količina teh še obvladljiva.

[22] Da napovedi na podlagi masovnih podatkov niso vsemogočne, se je pokazalo v sezonah 2011/2012 in 2012/2013, ko je bila Googlova napoved izbruhov gripe nenatančna. Leta 2013 je zgrešila vrhunec sezone gripe za kar 140 odstotkov (Lazer in Kennedy 2015). Google je kasneje tudi prenehal z izvajanjem programa. Eden od očitkov, ki so leteli na Google, je bil tudi, da je program postal nenatančen zaradi njegove netransparentnosti (Walsh 2014).

Pomanjkljivosti podatkov naj bi več kot odtehtala njihova količina, kjer nekateri avtorji govorijo celo o *vseh* možnih podatkih, ki jih je v določenem kontekstu mogoče pridobiti, in ne le o vzorcu, zbranem na podlagi širše populacije (v tem primeru postane $N = vse$) (Mayer-Schönberger in Cukier 2013, 2. pogl.). Uporaba masovnih podatkov torej narekuje tudi, da se v svojih prizadevanjih za pridobivanje novih informacij vsaj delno odpovemo vzorčenju in s tem povezanim statističnim metodam.

Poleg tega bomo morali sprejeti dejstvo, da včasih niti ne potrebujemo razkritja vzročne zveze med pojavom in posledico, ker nam zadostujejo že korelacije na osnovi masovnih podatkov. Vzročne povezave je namreč mnogo težje odkriti in potrditi kot korelacije. Korelacije nam ne razrivajo, *zakaj* se je nekaj zgodilo, temveč nas samo opozorijo na dogajanje (Mayer-Schönberger in Cukier 2013, 4. pogl.). V nasprotju s tem znanost že stoletja temelji na postavljanju hipotez ter iskanju vzročnih povezav s poskusi.

Naštete značilnosti masovnih podatkov bodo vplivale tudi na vprašanja varovanja zasebnosti. Uporaba masovnih podatkov namreč prinaša s seboj tudi nekatere povsem nove načine ogrožanja zasebnosti, med katere spada tudi odkrivanje korelacij na nepričakovanih mestih. Zastavlja se pomembno vprašanje, ali je zastarela zakonodaja, ki v ZDA in Evropi ureja zaščito zasebnosti v povezavi z obdelavo podatkov, sploh pripravljena na nove izzive, ki jih že danes prinašajo masovni podatki.

5.1.2 *Masovni podatki ter načelo obveščanja in soglasja*

Obstoječa zakonodaja za varovanje osebnih podatkov tako v ZDA kot v Evropski uniji temelji na načelu obveščanja in soglasja. Načelo naj bi zagotavljalo tržni mehanizem za spodbujanje samoregulacije in podatkovne zaščite s strani zasebnega sektorja, vendar je obveljalo splošno mnenje, da obveščanje in soglasje nista več ustrezna mehanizma za spoprijemanje z izzivi zasebnosti, ki jih je prinesel izbruh masovnih podatkov (Strandburg v Lane in drugi 2014, 1. del, 1. pogl.). Težava je že v tem, da načelo za uporabnike predpostavlja, da so sposobni trezno oceniti prednosti in pomanjkljivosti zbiranja podatkov in na podlagi tega sprejeti tehtne odločitve. V praksi velika večina uporabnikov tovrstnih obvestil ne prebere, niti jih ne razume (Barocas in Nissenbaum v Lane in drugi 2014, 1. del, 2. pogl.; Rubinstein 2013, 2), kaj šele da bi se spuščala v poglobljena razmišljanja o tem, kaj z osebnimi podatki počnejo organizacije, ki jih zbirajo. Če naj bi načelo obveščanja in soglasja ostalo temeljni kamen

informacijske zasebnosti tudi v bodoče, bi bilo treba politike zasebnosti ustrezno poenostaviti, skrajšati in standardizirati ter jih na ta način približati uporabnikom in spodbuditi njihov odziv. Na drugi strani kompleksnost zbiranja podatkov in stalno uvajanje novih tehnologij pomenita, da bi morale politike zasebnosti postati še bolj natančne in razčlenjene, če naj bi uporabniki zares želeli razumeti, kaj organizacije počnejo z njihovimi podatki (Strandburg v Lane in drugi 2014, 1. del, 1. pogl.). Problem načela obveščanja in soglasja je zato začaran krog, ki v kontekstu masovnih podatkov naleti na povsem nove ovire.

Kot je že bilo omenjeno, je poglavitni doprinos masovnih podatkov ta, da z združevanjem različnih baz podatkov in uporabo tehnik strojnega učenja in napovedne analitike omogoča pridobivanje povsem novih in nepredvidljivih informacij ter korelacij. Ker je izredno težko vnaprej predvideti, kakšne rezultate bo prinesla obdelava masovnih podatkov, načelo obveščanja in soglasja izgubi svoj smisel, saj ne more uporabnika seznaniti s posledicami uporabe njegovih podatkov. Poleg tega uporabniki ne morejo sprejeti tehtnih odločitev glede obdelave podatkov, če ne poznajo potencialnih korelacij, ki jih bo razkrilo rudarjenje njihovih podatkov. In ne nazadnje je tu še dilema lastništva nad informacijami, saj se zakoni o varovanju zasebnosti nanašajo na osebne podatke, vezane na posameznika, masovni podatki (ki so pogosto anonimizirani) pa razkrivajo informacije, ki poprej v teh podatkih niso bile razvidne (Rubinstein 2013, 5). Če lastništvo nad razkritimi informacijami ne pripada posameznikom, katerih podatki so bili uporabljeni, potem tudi načelo obveščanja in soglasja ne igra nobene vloge, ker obdelovalec masovnih podatkov ni kršil zasebnosti posameznikov. Da bi javnost dejansko lahko bila obveščena o tem, kaj se dogaja z njenimi podatki, in bi uporabniki poznali analitične lastnosti podatkov, potem bi bilo treba zagotoviti tudi sledenje lastništva nad podatki oziroma sledenje izvora podatkov. V jeziku matematike in računalništva lahko izvor informacij formalno predstavimo kot aciklični usmerjen graf, takšni grafi pa hitro postanejo zelo razvejani in zapleteni (Landwehr v Lane in drugi 2014, 10. pogl.). Z združevanjem masovnih podatkov iz različnih virov pa se običajno izgubijo tudi informacije o njihovem izvoru.

5.1.3 *Masovni podatki in anonimnost*

Eden od argumentov zagovornikov uporabe masovnih podatkov je, da ta v večini primerov sploh ne ogroža zasebnosti, saj so podatki, ki se obdelujejo, anonimni oziroma anonimizirani. Z anonimizacijo je mišljeno, da so bile podatkom odstranjene informacije, ki jih je mogoče

prepoznati v povezavi z določeno osebo (z ang. kratico: PII). V prvi vrsti gre za odstranjevanje osebnih identifikatorjev, kot sta ime in matična številka[23] ter nato še specifičnih indikatorjev, ki jih uporabljajo različne organizacije, kot so denimo bančni računi v finančnih institucijah (Ohm 2009, 1703). Namen obdelave masovnih podatkov je namreč iskanje korelacij v množici podatkov iz različnih virov in ne identifikacija posameznikov, ki so prispevali svoje podatke. Desetletja je veljalo, da lahko anonimizacija podatkov robustno zaščiti zasebnost njihovih lastnikov (Ohm 2009, 1706).

Masovni podatki so stvari obrnili na glavo. Izkazalo se je, da je pogosto mogoče brez večjih težav iz masovnih podatkov, ki naj bi bili anonimni, izluščiti informacije, s katerimi se lahko identificira posameznike, ki so prispevali podatke. Popolna anonimizacija namreč v praksi ni mogoča. Podatki so bodisi uporabni bodisi v celoti anonimni, a nikoli oboje hkrati. Leta 2008 sta raziskovalca na Univerzi v Teksasu prikazala, da je treba o posameznikih, katerih podatki so zajeti v podatkovni bazi, vedeti zelo malo, da se lahko uspešno razkrije njihova identiteta v naboru podatkov (Narayanan in Shmatikov 2008, 1). Združevanje masovnih podatkov iz različnih virov[24] izniči prizadevanja za odstranitev informacij tipa PII iz posameznega vira, ker so nekateri od teh anonimiziranih podatkov tako specifični, da v kombinaciji z ostalimi podatki hitro razkrijejo identiteto njihovega lastnika. Deanonimizacijski algoritmi delujejo tako, da skušajo povezati subjekte iz anonimiziranih naborov s podatki o celotni relevantni populaciji, ki jih je mogoče identificirati (Yakowitz Bambauer 2011, 21). Zato je bolje kot o anonimnosti podatkov govoriti o psevdonimnosti[25] in se pri tem zavedati, da anonimizacijski postopki niso jamstvo za varovanje zasebnosti (Barocas in Nissenbaum v Lane in drugi 2014, 1. del, 2. pogl.). Problematično je tudi, da podatki, ki so anonimizirani, ne uživajo več enake zakonske zaščite, kot bi jo sicer (Porter 2008, 3).

V primeru podatkov iz mobilnih naprav naj bi za potencialno ponovno identifikacijo milijonov uporabnikov zadoščale že štiri prostorsko-časovne točke (Pentland 2014, priloga 2). Še bolj problematično je, da na ponovno identifikacijo niso občutljivi le klasični podatki, ampak tudi grafi interakcij v družbenih omrežjih (Mayer-Schönberger in Cukier 2013, 8. pogl.), s čimer postane ogrožena zasebnost ne le enega posameznika, temveč vseh, s katerimi

[23] V ZDA številka socialnega zavarovanja.

[24] Google je denimo priznal, da združuje podatke o uporabnikih, pridobljene preko iskalnika, storitve YouTube in Gmail ter še več kot 50 drugih storitev, ki jih ponuja (Tapscott 2012c).

[25] Z drugim izrazom: o navidezni anonimnosti.

je ta v odnosu. Avtorja raziskave iz leta 2008 trdita, da je njun algoritem za ponovno identifikacijo dovolj robusten za uspešno uporabo na kakršnem koli naboru podatkov, ki vsebuje anomnimne zapise iz več različnih virov, kot so posamezne transakcije, preference in podobno (Narayanan in Shmatikov 2008, 14).

Ob pomanjkanju tehnoloških rešitev[26] za problem ponovne identifikacije bi morala po mnenju nekaterih strokovnjakov (Ohm 2009) odločno posredovati zakonodaja in vršiti strožji nadzor nad obdelavo masovnih podatkov. To bi obenem pomenilo, da se morali po dolgih letih posloviti od koncepta informacij tipa PII kot temelja za zakonsko varovanje zasebnosti. Na drugi strani nekateri avtorji (Yakowitz Bambauer 2011) menijo, da je strah pred ponovno identifikacijo pretiran in da večjo nevarnost predstavljajo druge oblike manipulacije masovnih podatkov, kot so računalniški vdori ali malomarno ravnanje s podatki.

5.1.4 *Masovni podatki in sklepanje*

Sklepanje (inferenca) predstavlja še en vidik ogrožanja zasebnosti, ki ga prinaša uporaba masovnih podatkov. Obdelovalcu masovnih podatkov niti ni treba uporabiti algoritmov za ponovno identifikacijo, ker se lahko o na podlagi analize dokoplje do določenih sklepov o lastnikih podatkov, ne da bi jih pri tem osebno identificiral (Barocas in Nissenbaum v Lane in drugi 2014, 1. del, 2. pogl.). Masovni podatki tako o posameznikih lahko razkrijejo nepričakovana dejstva, tudi če informacije tipa PII niso prisotne v naboru podatkov.

Odkrivanje doslej neznanih dejstev in korelacij je sicer ena od poglavitnih vrlin masovnih podatkov, ki lahko privede do dragocenih novih spoznanj in inovativnih rešitev. Na drugi strani lahko to lastnost podjetja izkoristijo v manj plemenite namene. Z obdelavo masovnih podatkov lahko pridejo do zelo nazornih podrobnosti iz življenj posameznikov, ki jih nato izrabijo v namene oglaševanja in prodaje izdelkov. Znan je primer Googla, ki zbira o uporabnikih najrazličnejše podatke, vendar ga identifikacija teh uporabnikov niti ne zanima, ker predstavlja le nepotreben šum, saj se lahko o posamezniku ogromno izve na posreden način (Hardy 2012). S tega vidika največjo grožnjo zasebnosti predstavljajo velike organizacije, kot so največja podjetja in državne institucije, ki imajo dostop do izjemno obsežnih podatkovnih baz. Več ko je na voljo podatkov iz različnih virov, bolj natančni in

[26] Ena od potencialnih opcij je diferencialna zasebnost, ki je podrobneje opisana kasneje.

pronicljivi so razkriti sklepi in korelacije. Morda bi lahko ugotovili, da gre v primeru oglaševanja in ponujanja storitev sicer za nadležne, a ne izrazito problematične kršitve zasebnosti, vendar ne gre pozabiti, da podjetja na podlagi pridobljenih dejstev lahko izvajajo diskriminacijsko obravnavo potrošnikov, s katero jim omejujejo izbiro, ovirajo gradnjo identitete ter ogrožajo njihovo avtonomijo in socialno pravičnost nasploh (Barocas in Nissenbaum v Lane in drugi 2014, 1. del, 2. pogl.).

To ustvarja zapleten pravni položaj, v kakršnem se lahko znajdejo posamezniki, o katerih obdelava masovnih podatkov razkrije praktično vse razen imena in priimka. Kršitve zasebnosti so se v preteklosti vedno povezovale z informacijami tipa PII, torej takšnimi, ki so razkrile identiteto posameznika, zato se ob tem zastavlja vprašanje, če sklepanje o posameznikih, ki neposredno ne razkriva njihove identitete, predstavlja vdor v zasebnost ali ne. Če je zasebnost razumljena kot sposobnost nadzora nad lastnimi informacijami (Craig in Ludloff 2011, 16), potem tudi odsotnost identifikacije ni dovolj, da pri iskanju sklepov v masovnih podatkih ni prišlo do njenega kršenja.

V kontekstu družbenih omrežij, za katere se zdi, da včasih o okusih in navadah uporabnikov vedo strašljivo veliko, so nekateri mlajši in tehnološko bolje podkovani uporabniki začeli uporabljati inovativne taktike, s katerimi želijo zmesti algoritme, ki delajo sklepe na podlagi njihovih objavljenih podatkov. Nadzor nad položajem želijo pridobiti z ukanami, ustvarjanjem in zapiranjem uporabniških računov, steganografijo[27] (Hardy 2012) in namenskim objavljanjem vsebin, ki niso povezane z njihovim značajem oziroma miselnimi procesi. S tem se želijo izogniti situaciji, ko jih lastniki družbenih omrežij pod krinko anonimnosti obravnavajo na načine, pred katerimi bi jih sicer anonimnost v tradicionalnem smislu morala varovati (Barocas in Nissenbaum v Lane in drugi 2014, 1. del, 2. pogl.).

5.1.5 *Masovni podatki ter avtomatsko odločanje in profiliranje*

Profiliranje je (pogosto avtomatiziran) proces uvrščanja posameznikov v predhodno definirane kategorije na podlagi dejstev, pridobljenih o njih z obdelavo podatkov. Gre za nadgradnjo sklepanja, ki ga omogočajo masovni podatki, in se najpogosteje omenja v povezavi z rudarjenjem podatkov, strojnim učenjem ter sklepno statistiko. Profiliranje

[27] Skrivanje pomena znotraj drugih elementov, ki sicer niso skriti očem javnosti.

izvajajo tako organizacije v zasebnem kot javnem sektorju, a pozornost javnosti je večkrat namenjena delu državnih institucij, še posebno ko profiliranje povezujejo z zagotavljanjem nacionalne varnosti.

Profili lahko predstavljajo poseg v zasebnost in avtonomijo posameznika, če vsebujejo nevarne predpostavke, skrite v arhitekturi programske opreme in algoritmov, ki se navzven kažejo kot nevtralne odločitve nepristranskih računalniških sistemov (Solove 2011, 191). Treba je poudariti, da je uporaba masovnih podatkov naredila proces profiliranja in avtomatskega odločanja bolj natančen in obsežen (Rubinstein 2013, 4), a nikakor ne nezmotljiv. Glavna težava pri tem je predvsem pomanjkanje transparentnosti takšnih procesov, ki se že zaradi svoje narave, sploh ko gre za vprašanja nacionalne varnosti, vršijo v tajnosti in brez vpogleda javnosti. Ko avtomatsko profiliranje izvajajo državne institucije, tveganja vključujejo kršenje zakonsko določenih pravic s področja zasebnosti, spodkopavanje nacionalne varnosti z obravnavanjem nedolžnih posameznikov, nezmožnost odkritja dejanskih osumljencev, nepotrebno zapravljanje proračunskih sredstev, vpletanje zasebnega sektorja zaradi izročitve podatkov državnim institucijam ter vmešavanje v mednarodni pretok podatkov (Solove 2001, 21–22).

Lažno pozitivni rezultati profiliranja so tisti, ki posameznike uvrstijo v napačno kategorijo. V primeru profiliranja zaradi zagotavljanja nacionalne varnosti to pomeni, da se nedolžna oseba lahko znajde na seznamu potencialnih teroristov, ker podatki, na podlagi katerih je bila sprejeta odločitev, niso popolni oziroma točni ali pa sistem preprosto ne more v vseh primerih uspešno ločiti vzorcev nedolžnega obnašanja od sumljivega (Solove 2001, 20). Zaradi pomanjkanja transparentnosti pri profiliranju, ki ga izvajajo državne institucije, je praktično nemogoče ovrednotiti pomisleke o zasebnosti napram zahtevam po varnosti, posamezniki pa pogosto nimajo nobene možnosti vpogleda v odločitve, ki jih zadevajo, niti možnosti pritožbe. Napake pri avtomatskem profiliranju ne vključujejo le sistemov nacionalne varnosti, ampak se lahko primerijo tudi drugje, denimo pri ocenah kreditne sposobnosti, poklicnih kvalifikacij in primernosti za sklenitev zavarovanja oziroma prejemanje socialne podpore (Rubinstein 2013, 4), kar ima lahko izjemno škodljive posledice za vpletene posameznike, ki jih je umetna inteligenca nehote napačno ocenila.

Ameriški Kongres je že davnega leta 1988 kot dodatek *Zakonu o zasebnosti* sprejel *Zakon o računalniških primerjavah in varovanju zasebnosti*, ki je urejal zgodnjo obliko rudarjenja podatkov, a je bilo to tudi zadnje, kar je na tem področju storil, saj so kasnejši zakoni državno

rudarjenje podatkov in profiliranje preprosto spregledali ali pa niso zagotovili ustrezne ureditve področja in varovanje zasebnosti (Cate 2008, 467). V Evropi bo bodoča *Splošna uredba o varstvu podatkov* z 20. členom zamenjala 15. člen obstoječe *Direktive o varstvu podatkov*, ki posameznikom zagotavlja, da ne bodo predmet avtomatskih odločitev, ki imajo pravne posledice ali pomembno vplivajo na njihovo življenje. 20. člen nove uredbe med drugim razširi področje avtomatskega odločanja, definira izjeme v primeru soglasja, prepoveduje avtomatsko obdelavo na podlagi izključno občutljivih[28] podatkov, daje pooblastila Evropski komisiji, da sprejme nadaljnje ukrepe za zaščito interesov posameznikov, sicer pa ohranja bistvo starega člena (Rubinstein 2013, 6). Kopja se lomijo tudi okoli člena, ki navaja, da profiliranje, ki temelji izključno na obdelavi psevdonimnih podatkov, ne predstavlja znatnega vpliva na interese, pravice in svoboščine posameznika (Barocas in Nissenbaum v Lane in drugi 2014, 1. del, 2. pogl.).

5.2 Računalništvo v oblaku

Računalništvo v oblaku je zrela tehnologija, ki ima svoje korenine v 20. stoletju, vendar je na komercialni ravni zaživelo šele ob prelomu tisočletja. Definiramo ga lahko kot ponujanje računalniških virov v obliki omrežnih storitev, najbolj pogosto preko interneta, ki se v obsegu prilagaja zahtevam različnih uporabnikov in kjer viri zajemajo širok nabor funkcionalnosti, od procesorske moči in shranjevanja podatkov do celovitih programskih aplikacij (Hon in Millard v Millard 2013, 1. del, 1. pogl.). Računalništvo v oblaku torej predstavlja distribucijo računalniških virov, ki deluje na zahtevo, je fleksibilna in ni odvisna od uporabnikove lokacije ali časa. Vsakemu uporabniku računalništva v oblaku je lahko dodeljeno okolje, ki se zdi kot dejanski računalnik, a ga v resnici simulira virtualna naprava, ki si z drugimi virtualnimi napravami deli skupno procesorsko moč in hrambo podatkov (Landwehr v Lane in drugi 2014, 10. pogl.).

Kdaj se je izraz "računalništvo v oblaku" prvič pojavil, ni povsem znano. Nekateri ga pripisujejo podjetju Compaq, ki je leta 1996 izrazilo upanje, da bodo bodoče aplikacije na

[28] Definicija "občutljivih podatkov" sicer ni rigorozna, a jih lahko opredelimo kot podatke, ki imajo potencial ogroziti zasebnost ali varnost, če pristanejo v napačnih rokah, oziroma lahko v primeru izgube prinesejo znatne pravne posledice, škodujejo ugledu posameznika ali organizacije ter povzročijo pravno, finančno ali poslovno škodo (Ohm 2015, 6).

temelju računalništva v oblaku povečale prodajo, medtem ko drugi menijo, da je izraz v splošno rabo prišel šele mnogo kasneje, ko je leta 2006 Eric Schmidt, izvršni direktor Googla, spregovoril o računalniških storitvah, ki domujejo v oblaku[29] (Mosco 2014, 15–16). Komercialne storitve, kot je denimo elektronska pošta, ki temelji na omrežni platformi[30], so bile sicer uporabnikom na voljo tudi že pred tem. V kolektivno zavest širših množic je računalništvo v oblaku stopilo leta 2011, ko je ameriško podjetje Salesforce v okviru finalnega obračuna moštev ameriškega nogometa lansiralo dva oglasa[31] za svojo spletno platformo, namenjeno poslovanju podjetij (Mosco 2014, 8).

Danes skorajda vsa največja podjetja v informacijskem sektorju ponujajo svoje storitve računalništva v oblaku v takšni ali drugačni obliki. Daleč največji tržni delež uživa Amazon, katerega primarna dejavnost že dolgo ni več spletna prodaja knjig. Amazon Web Services (AWS) je nabor spletnih storitev, ki je leta 2014 podjetju prinesel 4,6 milijarde, leta 2015 pa 6,2 milijarde dolarjev dobička ter raste s skoraj 50 odstotki letno (Golden 2015). Microsoft svoje storitve računalništva v oblaku ponuja preko platforme Azure, Google uporabnikom nudi široko paleto spletnih storitev in celo naprave, ki so v celoti odvisne od njegovih rešitev v oblaku (Mosco 2014, 52), Apple svoje spletne storitve trži pod imenom iCloud, IBM je svoj sistem na masovnih podatkih temelječe umetne inteligence Watson ponudil kot storitev v oblaku (Lohr 2015, 1. pogl.), itd. Ob boku velikim igralcem stoji ogromno manjših, a specializiranih podjetij, kot so že omenjeni Salesforce, Rackspace, Dropbox, VMware in mnogi drugi. Takšna podjetja se usmerjajo na različne ciljne skupine, denimo na poslovno javnost ali specifične uporabnike, in svojim strankam nudijo vse vrste storitev računalništva v oblaku, bodisi individualno bodisi v kombinaciji različnih storitev. Prav inovativnost je tista, s katero lahko manjša podjetja preživijo v konkurenci velikih ponudnikov računalništva v oblaku.

---

[29] Oblak je hitro postal uveljavljena metafora za distribuirane računalniške storitve, tako v vizualnem kot opisnem smislu. Večina ljudi danes oblak povezuje z Schmidtovo vizijo, torej kot nekakšen vseprisoten medij, v katerem domujejo računalniške storitve, kar je postalo tudi vodilo vseh, ki se ukvarjajo s trženjem računalništva v oblaku. Izraz je sicer bržkone sprva nastal kot opis diagrama v komunikacijsko mrežo povezanih naprav, ki je imel podobo oblaka (Mosco 2014, 77). Resnična podoba računalništva v oblaku je mnogo bolj prizemljena, kot bi lahko sklepali iz njegovega imena. Podatki in storitve, ki jih podjetja ponujajo v oblaku, se v resnici nahajajo v ogromnih računalniških centrih, ki so velik porabnik energije in močno obremenjujejo okolje.

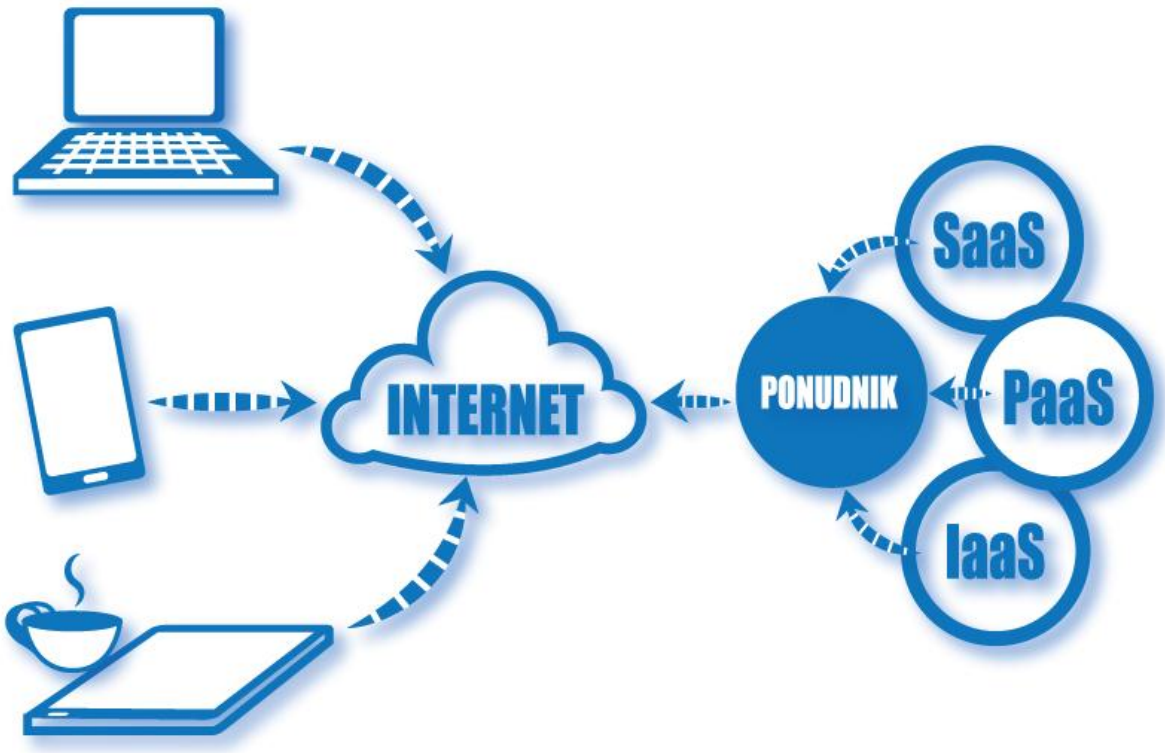
[30] Google je svojo spletno storitev elektronske pošte (ang. *webmail*) Gmail začel ponujati leta 2004, a že mnogo pred tem so bile (med drugimi) popularne storitve, kot sta Hotmail in RocketMail. Med Slovenci je bila v začetku tisočletja izjemno priljubljena spletna storitev Email.si.

[31] Eden od oglasov je dostopen prek: https://www.youtube.com/watch?v=zNCUS_9Xzu4.

Posebnosti računalništva v oblaku lahko strnemo v naslednje značilnosti (Mosco 2014, 38–39):

- avtomatizacija storitev na zahtevo: uporabniki računalništva v oblaku lahko naročajo storitve shranjevanja ali uporabe strežnikov brez neposredne interakcije s ponudnikom;
- širok spekter platform: uporabniki lahko do oblaka dostopajo prek katere koli platforme, na primer prek osebnih računalnikov, tablic ali pametnih telefonov;
- združevanje virov: ponudniki lahko združujejo vire, kot so hramba, procesorska moč, pasovna širina itd., iz različnih fizičnih lokacij in jih ponujajo različnim uporabnikom;
- odzivnost in prilagodljivost: storitve računalništva v oblaku se prilagajajo uporabnikom v skladu z njihovimi potrebami in odpravljajo potrebo po dragih tehnoloških investicijah v podjetjih;
- merljivost storitev: storitve računalništva v oblaku so merljive (denimo glede na količino shranjenih podatkov, pasovno širino itd.) in praviloma transparentne tako za ponudnika kot uporabnika.

Slika 5.3: Shematski prikaz delovanja računalništva v oblaku.



Na podlagi tega lahko storitve računalniška v oblaku razdelimo v tri velike kategorije[32], ki uporabnikom ponujajo različne stopnje nadzora, od največjega do najmanjšega (Hon in Millard v Millard 2013, 1. del, 1. pogl.; Mosco 2014, 39):

- infrastruktura kot storitev (IaaS): računalniški viri v svoji primarni obliki, torej procesorska moč in hramba podatkov, medtem ko je izbira programske opreme in aplikacij prepuščena uporabniku;
- platforma kot storitev (PaaS): platforma za razvijanje in uporabo programskih aplikacij s pomočjo orodij, ki jih zagotovi ponudnik;
- programska oprema kot storitev (SaaS): ponudnikove spletne aplikacije, namenjene končnim uporabnikom, kjer uporabniki ponudniku prepustijo izbiro vseh elementov storitve, vključno z operacijskim sistemom, omrežjem, strežniki in programsko opremo.

Nadalje lahko storitve računalništva v oblaku razdelimo na (Hon in Millard v Millard 2013, 1. del, 1. pogl.):

- zasebne, ki služijo organizacijam zaprtega tipa, kot so podjetja;
- javne, ki so na voljo širši javnosti, tudi individualnim uporabnikom;
- hibridne, ki predstavljajo storitve tako zasebnega kot javnega značaja; in
- skupne, kjer si infrastrukturo lastijo in delijo uporabniki s skupnim interesom, na primer državne institucije.

5.2.1 *Potencial računalništva v oblaku*

Prednosti, ki jih uporabnikom prinaša računalništvo v oblaku, so številne in očitne. Podjetja, ki uporabljajo storitve v oblaku, lahko prihranijo stroške in postanejo konkurenčnejša, ker lahko sredstva, namenjena lastni infrastrukturi, vložijo raje v razvoj izdelkov in iskanje novih rešitev. Poleg tega računalništvo v oblaku zagotavlja fleksibilnost poslovanja, ki je lastna infrastruktura ne dopušča, saj se obseg storitev prilagaja potrebam podjetij. Nezanemarljiv je

[32] Poleg naštetih kategorij (IaaS, PaaS, SaaS) se pojavlja tudi vse več izpeljanih kratic, kot so CaaS (ang. *Communication as a Service* ali *Content as a Service*), NaaS (ang. *Network as a Service*), MaaS (ang. *Monitoring as a Service*), LaaS (ang. *Location as a* Service ali *Licensing as a Service*), DBaS (ang. *Database as a Service*) ipd.

tudi vidik informacijske varnosti, ki jo predvsem manjša podjetja včasih s težavo zagotavljajo. Veliki ponudniki storitev v oblaku si lahko privoščijo najsodobnejše tehnološke rešitve s področja varnosti in najbolj izurjene računalniške strokovnjake. Zato so podatki, shranjeni v oblaku, pogosto varnejši od tistih, ki domujejo na lokalnih strežnikih podjetij. V ZDA storitve računalništva v oblaku uporablja že več kot polovica vseh podjetij, v Evropi pa naj bi do leta 2020 vpliv računalništva v oblaku na gospodarstvo znašal 940 milijard evrov in zagotavljal 3,8 milijona delovnih mest[33] (Hon in Millard v Millard 2013, 1. del, 1. pogl.). Na ravni posameznikov je že leta 2008 40 odstotkov ameriških spletnih uporabnikov koristilo storitve računalništva v oblaku v takšni ali drugačni obliki (Ozer in Conley 2010, 2).

Poleg tega računalništvo v oblaku storitvami SaaS podjetjem in posameznikom omogoča dostop do aplikacij s katere koli naprave in lokacije, če je na voljo dostop do spleta, in posledično lažjo sinhronizacijo dejavnosti na različnih napravah, deljenje podatkov z drugimi uporabniki in sodelovanje (Armbrust in drugi 2009, 4). Stalen dostop do orodij za delo postaja vse bolj pogosta praksa v organizacijah, zato se vse več podjetij in institucij odloča za selitev svojega dela v oblak[34]. S tega vidika ima računalništvo v oblaku potencial spremeniti velik del informacijskega sektorja, saj bo programska oprema kot storitev postajala vse bolj privlačna možnost, kar bo vplivalo na to, kako se bo v prihodnje razvijala in uporabljala tudi strojna oprema (Armbrust in drugi 2009, 1).

Pravzaprav je potencial računalništva v oblaku tako velik, da nekateri celo govorijo o oblaku kot rešitelju kapitalizma, ki ga bo popeljal do novih višav produktivnosti (Mosco 2014, 4–5). Napihnjene obljube so sestavni del vsake razvijajoče se tehnologije, zato jih je treba vzeti z veliko mero previdnosti, a kljub temu ne gre zanikati, da je računalništvo v oblaku fenomen, ki ima in bo še imel velik vpliv na informacijski sektor ter na gospodarstvo nasploh povsod po svetu. Njegova pomembnost namreč narašča v povezavi z ostalima družbeno-tehnološkima fenomenoma, obravnavanima v tem delu, namreč z masovnimi podatki in internetom stvari. Količina podatkov, ki jo bodo v bližnji prihodnosti ustvarjale naprave, povezane v internet

[33] Na drugi strani je treba omeniti tudi nezanemarljivo izgubo delovnih mest, ki je posledica krčenja IT oddelkov v podjetjih zaradi selitve procesov in orodij v oblak.

[34] Tudi avtor tega dela je bil v zadnjih nekaj letih v podjetju, kjer je zaposlen, priča menjavi ključnih platform za urejanje vsebin in delo s strankami, ki so jih nadomestile nove različice v oblaku, dostopne kjer koli in kadar koli. Začetno navdušenje nad prilagodljivostjo, ki jo prinašajo takšne aplikacije, je nekoliko uplahnelo ob ugotovitvi, da z oblakom obenem tudi ni več tehničnih ovir za delo od doma, ob koncu tedna in med dopustom.

stvari, bo postala tako velika, da mnoge organizacije preprosto ne bodo imele zadostnih lastnih sredstev za njihovo shranjevanje in obdelavo, zato bodo primorane uporabiti storitve v oblaku velikih ponudnikov. Tezo potrjuje dejstvo, da največji delež današnjih razvijalcev, ki se ukvarjajo z internetom stvari, povezuje to tehnologijo na prvem mestu z računalništvom v oblaku in na drugem mestu z masovnimi podatki (Columbus 2015). Nekateri so mnenja, da je prav računalništvo v oblaku tisti vezni člen, ki je omogočil razmah uporabe masovnih podatkov in bo v bodoče služil kot temeljni kamen interneta stvari (Linthicum 2015).

5.2.2 *Računalništvo v oblaku in ogrožanje zasebnosti*

Če odmislimo obdelavo masovnih podatkov v oblaku, ki na področje varovanja zasebnosti vnaša povsem nove grožnje, kot je bilo razloženo v prejšnjem poglavju, potem ogroženost zasebnosti v povezavi z uporabo storitev računalništva v oblaku lahko zreduciramo na koncept predaje lastnih podatkov v tuje roke in vse posledice, ki jih takšno ravnanje prinese za seboj. Povedano drugače in bolj neposredno – oblaka ni, so le računalniki drugih (Vesel in Bevc 2015). S tem je mišljeno, da se za izrazom "oblak" skriva običajna računalniška tehnologija, ki je v lasti tujih ljudi oziroma organizacij. Ko se odločimo za uporabo njihovih storitev, implicitno pristanemo na to, da jim zaupamo svoje podatke. To pomeni, da je ogrožanje zasebnosti s strani računalništva v oblaku v veliki meri problem zakonodaje, ki predpisuje (ali ne predpisuje), na kakšen način je urejeno lastništvo nad podatki, ki so v uporabi tretjih oseb, ter kakšne so pristojnosti in odgovornosti teh tretjih oseb glede varovanja zasebnosti svojih uporabnikov. Dodatno se zaplete tudi pri definiciji osebnih podatkov, kajti mnogi zakoni za varovanje zasebnosti se nanašajo zgolj na osebne podatke oziroma informacije tipa PII.

Na tehnični ravni lahko tveganja, povezana z zasebnostjo, ki jih prinaša računalništvo v oblaku, razdelimo v naslednje kategorije (De Capitani di Vimercati in drugi 2012, 3–8):

- tveganja za uporabnike: težave, ki jih predstavlja zaščita identitete uporabnikov, ki uporabljajo storitve in vire računalništva v oblaku;
- tveganja za podatke: težave z zagotavljanjem integritete in zaupnosti podatkov, ki so shranjeni v oblaku in nad katerimi njihovi lastniki običajno nimajo neposrednega nadzora;

- tveganja pri dostopanju do podatkov: težave z varovanjem zasebnosti tako uporabnikov kot podatkov, do katerih pride pri dostopanju do podatkov, ko lahko zasebnost kršijo zlonamerne tretje osebe ali ponudniki storitev sami.

Varovanje osebnih podatkov, na katerem temelji zaščita zasebnosti uporabnikov računalništva v oblaku, je predmet številnih akademskih, strokovnih in političnih razprav. Iščejo se rešitve tako na zakonskem kot tehničnem področju oziroma v kombinaciji obeh pristopov.

5.2.3 *Računalništvo v oblaku in zakonsko varovanje zasebnosti*

Kot je bilo opisano že v poglavju o zakonski ureditvi varovanja zasebnosti, obstoječa zakonodaja v ZDA, v manjši meri pa tudi v Evropski uniji, ne dohaja vseh izzivov, ki jih prinaša bliskovit napredek tehnologije. Zato danes ni povsem jasno, na kakšne oblike zakonske zaščite se lahko zanesejo uporabniki glede informacij, ki jih shranijo v oblaku (Ozer in Conley 2010, 4). Kljub temu, da pravni položaj računalništva v oblaku ni povsem urejen, pa so pričakovanja njegovih uporabnikov glede zasebnosti jasna in nedvoumna. Uporabniki storitve v oblaku, sploh ko gre za shranjevanje podatkov, običajno smatrajo kot vse druge oblike hrambe, tudi fizične, in posledično pričakujejo, da bodo njihove shranjene informacije ostale nerazkrite. Raziskava je pokazala (prav tam), da uporabnike računalništva v oblaku najbolj skrbi, da bi ponudniki prodali njihove podatke drugim akterjem (90 odstotkov), uporabili njihove podatke v namene oglaševanja (80 odstotkov), obdržali njihove podatke tudi potem, ko jih uporabniki izbrišejo (63 odstotkov), ali predali njihove podatke organom pregona (49 odstotkov).

V ZDA nepooblaščene preiskave in zasege s strani državnih organov omejuje četrti amandma, vendar ameriška sodišča še niso dala zadnje besede, če se ustavna zaščita nanaša tudi na dokumente, shranjene v oblaku. Gre za že znano dilemo načela upravičenega pričakovanja zasebnosti, ki velja samo v primeru, če subjekti informacij ne odstopijo prostovoljno tretjim osebam, kar je ob uporabi storitev v oblaku običajna praksa. Tako imenovana doktrina poslovnih zapisov oziroma doktrina tretjih oseb v ameriškem pravnem sistemu narekuje, da četrti amandma ne zagotavlja zaščite in ne zahteva naloga za preiskavo, če subjekt preda podatke tretji osebi (Ozer in Conley 2010, 6). Položaj je še bolj zapleten zaradi dejstva, da so podatki, shranjeni v oblaku, pogosto geografsko razpršeni po mnogih lokacijah, ki niso vse

nujno v isti državi. V tem primeru je lahko varovanje zasebnosti uporabnikov predmet zakonodaje držav, v katerih se nahajajo njihovi podatki.

V ZDA poleg ustave varovanje zasebnosti urejajo tudi posamezni zakoni in predpisi, vendar na tem področju ni zakona, ki bi se eksplicitno nanašal na računalništvo v oblaku. Še najbližje temu je *Zakon o zasebnosti elektronskih komunikacij*, ki pa je nastal že mnogo let pred razmahom komercialnega računalništva v oblaku. Zakon ščiti določene oblike elektronskih komunikacij, vendar ne navaja, če so dokumenti, ki jih hranijo ponudniki storitev v oblaku, tudi del te zaščite, saj se ne nanaša na nekatere funkcionalnosti računalništva v oblaku, ki v času nastanka zakona sploh še niso obstajale, na primer na sodelovanje več uporabnikov hkrati in deljenje dokumentov (Ozer in Conley 2010, 7). Drugi specifični zakoni, kot sta HIPAA in VPPA, sicer urejajo varovanje zasebnosti na svojem področju, a vključujejo praviloma le področne institucije (v primeru zakona HIPAA so to zdravstvene ustanove in zavarovalnice) in ne splošnih ponudnikov storitev v oblaku.

Zaradi tega je v ZDA varovanje zasebnosti v primeru uporabe storitev v oblaku v večini primerov prepuščeno ponudnikom in njihovim politikam zasebnosti (ter potencialno Zvezni komisiji za trgovino, ki naj bi izvajala nadzor nad izvrševanjem politik zasebnosti), ki s seboj prinašajo kopico že omenjenih težav in same po sebi niso nobeno jamstvo, da bodo ponudniki zasebnost uporabnikov tudi dejansko spoštovali. Pogosto se zgodi ravno nasprotno, namreč da si ponudniki s politiko zasebnosti izborijo široke pravice za zbiranje informacij o uporabnikih, shranjevanje podatkov za dolga časovna obdobja in njihovo uporabo v sekundarne namene (Ozer in Conley 2010, 8). S tem uporabnikom puščajo le malo možnosti za nadzor nad lastnimi informacijami.

Poleg tega so podatki, ki so shranjeni na strežnikih podjetij s sedežem v ZDA, podvrženi zakonom, ki v imenu zagotavljanja nacionalne varnosti omejujejo zasebnost, kakršen je *Patriotski zakon*. Ker ima podjetje Google sedež v ZDA, mora na zahtevo državnih organov predati podatke o svojih uporabnikih ne glede na to, kje so ti podatki fizično shranjeni, zaradi česar nekatere evropske države razmišljajo o zakonodaji, ki bi javnim uslužbencem prepovedala uporabo Googlovih storitev ter drugih podobnih storitev računalništva v oblaku (Deibert 2013, uvod).

V državah Evropske unije se pravice in obveznosti, ki izhajajo iz zakonov za varovanje zasebnosti, nanašajo samo na osebne podatke. Takšen "črno-bel" pristop pomeni, da je

posameznikova zasebnost zakonsko zaščitena samo, če je identiteta posameznika na podlagi njegovih podatkov mogoča. Poleg tega evropska zakonodaja ureja varovanje osebnih podatkov na podlagi lokacije, kjer se nahaja ponudnik storitev, kar pomeni da imajo nacionalni zakoni držav, ki temeljijo na *Direktivi o varstvu podatkov* 95/46/EC, globalen vpliv, če ponudniki, ki se sicer ne nahajajo v Evropi, uporabljajo opremo, ki je fizično locirana v državah Evropske unije (Hon, Millard in Walden v Millard 2013, 3. del).

Prihajajoča uredba, ki bo zamenjala obstoječo direktivo kot krovni pravni dokument na področju varovanja zasebnosti, bo odpravila fragmentacijo na področju implementacije evropske zakonodaje s strani posameznih držav članic ter razširila definicijo osebnih podatkov in na ta način dodatno zaščitila tudi uporabnike računalništva v oblaku, vendar bi to pomenilo, da bi v praksi tako ponudniki kot uporabniki računalništva v oblaku dobili še dodatne obveznosti glede upravljanja s podatki in njihovega prenosa, kar bi zelo verjetno upočasnilo gospodarsko dejavnost v informacijskem sektorju (prav tam). Razširitev definicije osebnih podatkov tudi v ničemer ne rešuje težave ponovne identifikacije na podlagi masovnih podatkov, ki bodo v prihodnje deležni vse večje uporabe v povezavi z računalništvom v oblaku. Kljub temu je načelo transparentnosti, ki ga predvideva uredba, dobrodošel doprinos k varovanju osebnih podatkov v oblaku, ker uporabniki pogosto niso jasno obveščeni o tem, kaj se dogaja z njihovimi podatki, katere tretje osebe so morebiti udeležene pri procesu obdelave in katere so pristojne institucije, na katere se lahko obrnejo v primeru kršitev (Reding 2011).

Direktiva o varstvu podatkov 95/46/EC tudi ločuje med konceptom upravljavca (ang. *controller*) in obdelovalca (ang. *processor*) podatkov. Prvi predstavlja osebo, podjetje ali institucijo, ki določa namen obdelave osebnih podatkov, medtem ko drugi predstavlja osebo, podjetje ali institucijo, ki podatke obdeluje v imenu nadzornika (*Direktiva o varstvu podatkov* 95/46/EC 1995, 1. pogl., 2. člen). Upravljavec je odgovoren za upoštevanje obveznosti, ki jih nalaga zakonodaja glede varstva osebnih podatkov, kar vključuje morebitno registracijo dejavnosti pri pristojnih nacionalnih organih, zagotavljanje osebnih podatkov na zahtevo uporabnikov ter pošteno in zakonito obdelavo osebnih podatkov, zato morebitne sankcije ob kršitvah prizadenejo upravljavca in ne obdelovalca[35] (Hon, Millard in Walden v Millard 2013, 8. del, 2. pogl.). Ločevanje med upravljavcem in obdelovalcem podatkov odpira nekatere dileme v okviru računalništva v oblaku. Storitve računalništva v oblaku so praviloma

[35] Države članice lahko sicer obveznosti naložijo tudi obdelovalcem, če se tako odločijo.

razdrobljene na številne fizično ločene računalniške centre, ki se lahko nahajajo tudi v različnih državah. Ponudniki takšnih storitev pogosto uporabljajo podizvajalce, ki lahko tudi svoje delo razdelijo med nove podizvajalce, nad katerimi prvotni ponudnik nima nadzora. V takšnih primerih je zelo težko izvajati nadzor nad spoštovanjem načel varnosti in zasebnosti osebnih podatkov in ponudnik uporabniku ne more vedno zagotoviti točnih informacij o fizični lokaciji njegovih podatkov, v kateri državi se podatki trenutno nahajajo in katera zakonodaja je pristojna za varovanje uporabnikove zasebnosti (Ozer in Conley 2010, 14). Obstoječa direktiva zato upravljavcem nalaga, da izberejo podizvajalce, ki nudijo zagotovila za izvajanje tehničnih in organizacijskih varnostnih ukrepov pri obdelavi podatkov (*Direktiva o varstvu podatkov* 95/46/EC 1995, 2. pogl., 8. oddelek, 17. člen), in da morajo tudi nadaljnji podizvajalci delovati v skladu z navodili upravljavca. Zaradi vse bolj zapletene in razdrobljene narave obdelave podatkov v oblaku se poskus ločevanja med upravljavcem in obdelovalcem podatkov sooča s številnimi težavami (Hon, Millard in Walden v Millard 2013, 8. del, 2. pogl.).

Navkljub trditvam Evropske komisije, da bo predlagana uredba rešila obstoječe probleme na področju varovanja osebnih podatkov v oblaku, zna imeti njeno sprejetje tudi nezanemarljive škodljive posledice za informacijski sektor v Evropi. Krepitev zaščite zasebnosti uporabnikov računalništva v oblaku na račun razširitve definicije osebnih podatkov in nalaganja dodatnih bremen ponudnikom storitev lahko povzroči, da bodo ponudniki primorani znatno dvigniti cene svojih storitev ali celo izključiti državljane Evropske unije iz njihove uporabe, kar lahko privede do diferenciacije ponudbe računalništva v oblaku, z različnimi cenami za različne nivoje varnosti in zasebnosti (Hon, Millard in Walden v Millard 2013, 8. del, 3. pogl.).

5.2.4 *Računalništvo v oblaku in tehnično varovanje zasebnosti*

Tehnične rešitve na področju varovanja zasebnosti poskušajo zaščititi identiteto uporabnikov računalništva v oblaku na eni strani ter integriteto podatkov v oblaku na drugi. Eden od poglavitnih pristop za varovanje identitete uporabnikov je že omenjen postopek anonimizacije, s katerim se pred obdelavo podatkov iz nabora odstranijo informacije tipa PII, ki lahko razkrijejo identiteto uporabnikov. Če so podatki anonimni, jih lahko ponudniki storitev računalništva v oblaku obdelujejo brez siceršnjih zakonskih omejitev (Hon, Millard in Walden v Millard 2013, 7. del, 3. pogl.). Najbolj pogoste metode anonimizacije so brisanje in izpuščanje identifikacijskih podrobnosti, kot so imena, zamenjava imen in drugih

identifikatorjev z ustreznimi kodami (psevdonimizacija) ter združevanje informacij v različne kategorije, kot so lokacija, leto rojstva ali starostne skupine (prav tam). Kot je bilo že omenjeno, je težava tega pristopa, da pri uporabi masovnih podatkov ni dovolj zanesljiv, saj je ponovna identifikacija na podlagi zgolj majhnega števila podatkov, zbranih iz različnih virov, relativno preprosta in hitra. V tem primeru bi morala vrzel zapolniti zakonodaja in razširiti definicijo osebnih podatkov tudi na anonimizirane podatke ter tako omejiti pristojnosti ponudnikov pri obdelavi takšnih podatkov, vendar tudi najnovejša prizadevanja na tem področju, kakršna je prihajajoča evropska *Splošna uredba o varstvu podatkov,* ne ponujajo zadovoljivih rešitev.

Za razliko od anonimizacije je šifriranje postopek, ki varuje tako identiteto uporabnikov kot varnost podatkov. Če je enosmerno[36] šifriranje uporabljeno le na informacijah tipa PII oziroma na identifikatorjih (tajnopis), medtem ko ostali podatki ostanejo nešifrirani (čistopis), potem gre efektivno za proces anonimizacije oziroma psevdonimizacije. Dvosmerno šifriranje lahko zajame celoten nabor podatkov, ki se lahko šifrirajo že na napravah uporabnikov pred prenosom v oblak, če je na njih nameščena ustrezna programska oprema. V takšnem primeru se poraja vprašanje, če šifrirani podatki še vedno predstavljajo osebne podatke in so kot takšni predmet zakonov in predpisov. Zdi se, da vsaj regulatorni organi v Evropi dejansko obravnavajo šifrirane podatke še vedno kot osebne podatke (prav tam). Varnost šifriranih podatkov je odvisna od več dejavnikov, denimo od uporabljene šifrirne metode, dolžine šifrirnega ključa in upravljanja s šifrirnimi ključi. Pomanjkljivost šifriranja je, da zahteva dodatne vire in vpliva na hitrost izvrševanja zahtev uporabnikov. Poleg tega so šifrirani podatki v večini primerov neuporabni za kakršno koli obdelavo, zato jih je treba pred tem dešifrirati in nato ponovno šifrirati. Če se občutljivi podatki v oblaku nahajajo v nešifrirani obliki tudi le kratek čas, so potencialno dostopni tako ponudniku kot morebitnim tretjim osebam. Alternativa je prenos šifriranih podatkov na lokalne naprave uporabnikov, čemur sledita dešifriranje in obdelava, vendar to v veliki meri zatre ves potencial računalništva v oblaku, torej uporabo storitev na oddaljenih napravah. Šifriranje je zato primerno predvsem za pasivno shranjevanje podatkov v oblaku (Hon, Millard in Walden v Millard 2013, 2. del, 2. pogl.). Rešitve, ki bi omogočale obdelavo šifriranih podatkov v oblaku, ne da bi bila pri tem posrednikom razkrita narava podatkov, spadajo pod homomorfno šifriranje, vendar še niso

[36] Enosmerno (simetrično) šifriranje uporablja isti ključ za šifriranje in dešifriranje, medtem ko dvosmerno (asimetrično) šifriranje uporablja za oba postopka različna ključa (Kovačič 2000, 1027). Ker je simetrično šifriranje cenejše od asimetričnega, mnogi predlogi rešitev temeljijo na tem pristopu (Samarati in De Capitani di Vimercati 2010, 4).

zadosti zmogljive za uporabo v praksi. Njihova uporaba v kontekstu računalništva v oblaku bi pomenila, da uporabniku ne bi bilo več treba zaupati v sposobnosti ponudnika, da bo ta uspešno zaščitil njegove podatke, saj bi ponudnik podatke obdeloval brez neposrednega dostopa do njihove nešifrirane oblike (Schneier 2009).

Pomanjkljivosti šifriranja, ki se kažejo predvsem v rigidnosti njegove uporabe in nujnosti pazljivega upravljanja s šifrirnimi ključi, so privedle k iskanju drugačnih tehničnih rešitev za zagotavljanje zasebnosti pri uporabi računalništva v oblaku. Ena takšnih je fragmentacija podatkov, ki se lahko uporablja bodisi v kombinaciji s šifriranjem bodisi samostojno. Fragmentacija je postopek, s katerim se loči občutljive podatke od podatkov, ki ne potrebujejo zaščite, ter se jih ločeno shrani kot fragmente, ki jih ni mogoče povezati (De Capitani di Vimercati in drugi 2012, 5). Uporabnik lahko podatke shrani kot fragmenta na dva ločena strežnika, ki ne komunicirata med seboj, in šifrira atribute, ki bi lahko razkrili prvotno povezavo. Fragmentacija brez šifriranja pa bi pomenila, da uporabnik fragment z občutljivi podatki shrani lokalno pri sebi, medtem ko je fragment s preostalimi podatki shranjen v oblaku, oba fragmenta pa lahko združijo le pooblaščeni uporabniki (Samarati in De Capitani di Vimercati 2010, 7–12; De Capitani di Vimercati in drugi 2012, 5). Fragmentacija je primernejša od šifriranja predvsem v primerih, kjer niso vsi podatki občutljive narave in bi njihovo šifriranje predstavljalo nepotrebno zapleten ukrep.

5.3 Internet stvari

Izmed novih družbeno-tehnoloških fenomenov, ki jih obravnava to delo, je internet stvari tisti, katerega čas šele prihaja, čeprav lahko brez slabe vesti zatrdimo, da tudi masovni podatki in računalništvo v oblaku še niso dosegli vsega svojega potenciala, na katerega bo v prihodnje v veliki meri vplival prav internet stvari. Pričakovati je, da bo količina zbranih podatkov zaradi interneta stvari eksponentno narasla, kar bo zahtevalo veliko računalniških virov za shranjevanje in obdelavo teh podatkov, pri čemer bo računalništvo v oblaku igralo ključno vlogo.

Internet stvari[37] je svoje nenavadno poimenovanje dobil zaradi dejstva, da bo v prihodnosti z internetom povezanih ogromno najrazličnejših naprav z vseh področij življenja, zaradi česar jih niti nima smisla podrobneje opredeljevati. Internet stvari bo torej vključeval naprave z lastnim IP naslovom[38] in pogosto z lastnim virom napajanja, ki bodo povezane v omrežje skupaj z drugimi podobnimi napravam ter računalniškimi centri za shranjevanje in obdelavo podatkov, kjer se bodo sprejemale odločitve in ukrepi na podlagi zbranih informacij (Miller 2015, 2. pogl.). Ime je sicer nekoliko zavajajoče, saj ni nujno, da bodo vse naprave povezane z internetom, kot ga poznamo danes, ampak bodo morda del drugih manjših oziroma v ta namen zgrajenih omrežij ali pa se bodo z internetom povezovale le občasno. Bolje kot o enem velikem omrežju je torej govoriti o omrežju več različnih omrežij.

Interneta stvari torej sestavljajo naslednje komponente (prav tam):

- v omrežje povezane naprave,
- senzorji v napravah, ki zbirajo podatke,
- brezžični oddajniki in sprejemniki za komunikacijo med napravami,
- omrežje, v katerega so povezane naprave (najpogosteje brezžično),
- programske aplikacije za analizo zbranih podatkov in sprejemanje ustreznih povratnih ukrepov.

K temu lahko dodamo naslednje značilnosti, ki bodo zaznamovale razvoj interneta stvari ("IoT Privacy, Data Protection, Information Security" 2013, 1):

- identifikacija uporabnikov, obdelovanje informacij, mreženje in zaznavanje s pomočjo senzorjev,
- komunikacija med napravami ter med napravam in ljudmi,
- naraščajoča količina zajetih podatkov,
- samodejna komunikacija in samodejno delovanje naprav brez vednosti uporabnikov,
- heterogenost naprav, ki bodo prisotne na vseh področjih.

---

[37] Ime se je prijelo kljub svojemu tržnemu prizvoku ali pa prav zaradi njega. Zaradi tehnologije senzorjev, ki bodo vgrajeni v veliko večino naprav, povezanih v internet stvari, nekateri za to novo obliko povezljivosti raje uporabljajo izraz "senzorska revolucija" (Miller 2015, 1. pogl.).

[38] IP naslov je unikatna numerična oznaka, ki je dodeljena vsaki napravi, povezani v računalniško omrežje, ki za komunikacijo uporablja internetni protokol.

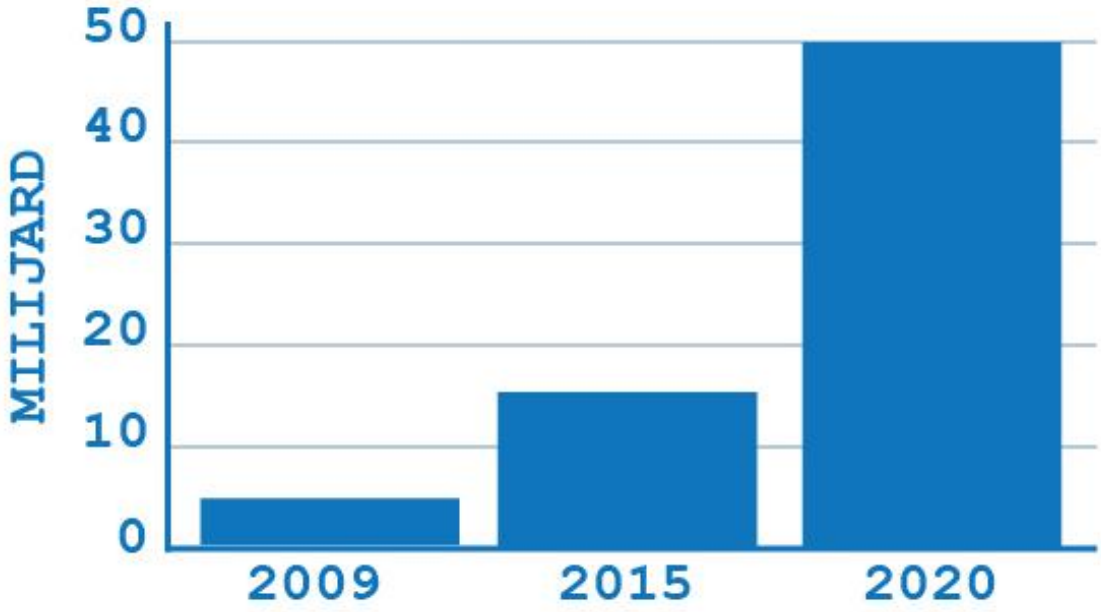
Ker bodo naprave, povezane v internet stvari, med seboj komunicirale in sodelovale, bo takšno omrežje predstavljalo več kot le vsoto posameznih sestavnih delov, čemur strokovnjaki pravijo ambientalna inteligenca (Miller 2015, 1. pogl.). Takšen sistem deluje samodejno in na podlagi zbranih informacij sprejema odločitve, s katerimi optimizira obstoječe stanje oziroma skrbi za izvrševanje nalog, denimo za nemoten potek proizvodnje ali za varčno porabo energije. Pomembno vlogo pri razvoju interneta stvari bo imela standardizacija na področju uporabljenih protokolov, arhitekture, varnosti in tudi zasebnosti. Brezžične komunikacije med napravami bodo slonele na današnjih tehnologijah WiFi, Bluetooth, NFC, RFID ter mobilni telefoniji naslednje generacije (5G), ki pa se stalno nadgrajujejo in dopolnjujejo.

Internet stvari bolj kot nadgradnjo današnjega interneta predstavlja njegovo dopolnitev. Danes so z internetom prek naprav, kot so računalniki in pametni telefoni, povezani predvsem ljudje, medtem ko bodo internet stvari sestavljale avtonomne naprave, ki bodo v veliki meri komunicirale med seboj (ang. *machine–to–machine* komunikacija oziroma M2M) in s človeškimi uporabniki interneta ne bodo imele veliko opravka. Napovedi kažejo, da bo internet stvari po številu priklopljenih naprav občutno presegel "internet oseb", v katerega je danes (leta 2016) vključenih vsaj 15 milijard[39] različnih naprav (Baxter 2014), od katerih jih že zdaj velik delež predstavljajo naprave interneta stvari. To je dvakrat več naprav, kot je na svetu ljudi, a bo ta številka v prihodnjih letih še strmo narasla. Napovedi o velikost interneta stvari se med seboj sicer zelo razlikujejo, saj naj bi bilo po nekaterih virih leta 2020 z internetom povezanih okoli 26 milijard naprav, po drugih pa več kot 200 milijard (Miller 2015, 2. pogl.) ali celo več kot 2.000 milijard, kar bi pomenilo približno tisoč povezanih stvari[40] na vsakega današnjega uporabnika interneta (Rifkin 2014, 5. pogl.). Podjetje Cisco, eden glavnih akterjev na področju razvoja interneta stvari, govori o 50 milijardah povezanih naprav do leta 2020 (Evans 2011, 3). Kakršna koli že bo ta številka, je jasno, da bo z internetom že v bližnji prihodnosti povezanih izjemno veliko število naprav, ki bodo ustvarjale ogromne količine podatkov.

[39] Po nekaterih napovedih celo 25 milijard naprav (Evans 2011, 3).

[40] Tisoč pametnih naprav na uporabnika se morda zdi veliko, a spomnimo naj, da internet stvari predvideva povezovanje skorajda *vseh* naprav, ki si jih je mogoče zamisliti, od zobnih ščetk in ključavnic do celotnih vozil in zgradb.

Slika 5.4: Število naprav, povezanih z internetom, v milijardah.
Vir: "Personal Data" 2011, 13



Iz povedanega sledi, da internet stvari ni nekaj, kar se bo zgodilo v prihodnosti, ampak se s polno paro gradi že precej časa, čeprav bo pravi potencial dosegel šele čez nekaj let. Ker bo vsaka naprava, ki bo povezana v omrežje, imela svoj IP naslov, je leta 2012 prišel v uporabo internetni protokol IPv6, ki bo zamenjal IPv4. IPv4 je uporabljal 32-bitne naslove in je omogočal 2^{32} oziroma okoli 4,3 milijarde unikatnih IP naslovov, kar je nezadovoljivo za razvoj interneta stvari. IPv6 zato uporablja 128-bitne naslove in v teoriji zagotavlja 2^{128} unikatnih IP naslovov. Današnje potrošniške naprave, ki imajo sposobnost povezave z internetom, pogosto označuje pridevnik "pameten". Toda pametni televizorji, hladilniki, avtomobili in celo domovi predstavljajo le majhen delež povezanih naprav. Večina takšnih naprav se nahaja v proizvodnji, podjetjih, zdravstvu in na drugih področjih, kjer tehnologijo uporabljajo za boljše upravljanje z viri, večjo učinkovitost in zniževanje stroškov. Pomembni uporabniki interneta stvari bodo tudi državne institucije, ker bodo s pomočjo podatkov, zbranih s povezanimi napravami, lažje skrbele za vzdrževanje infrastrukture, nadzor prometa, potrošnjo energije in podobno. Takšne pametne naprave bodo sposobne sporočati podatke o lokaciji, bližini predmetov, hitrosti, temperaturi, pretoku, pospešku, zvoku in sliki iz okolja, silah, obremenitvah, navoru, tlaku, interakcijah itd. (Goodman 2015, 12. pogl.).

Tovrstne naprave same po sebi zato ne predstavljajo grožnje zasebnosti, saj zbirajo podatke, ki so povezani s proizvodnim procesom, okoljem, vremenskimi pojavi, delovanjem naprav in

podobno. Vendar bodo na drugi strani vse bolj vsakdanje postajale tudi povezane naprave, ki pridobivajo podatke neposredno o njihovih človeških lastnikih in to na načine, ki so lahko zelo invazivni in intimni. Prve zametke takšnih naprav lahko že danes prepoznamo v pametnih telefonih, ki prek namenskih aplikacij beležijo biometrične podatke o uporabnikih in jih sporočajo v oddaljene centre v analizo. Povezane naprave prihodnosti bodo bržkone še mnogo bolj sofisticirane, zato se bo treba pripraviti na izzive, ki čakajo varovanje zasebnosti v zreli dobi interneta stvari.

5.3.1 *Potencial interneta stvari*

Zaradi svojega obsega in vseprisotnosti bo imel internet stvari velik vpliv na vsa področja življenja in dela ljudi. Če se bodo napovedi uresničile, bodo koristi za posameznike, podjetja in druge organizacije izjemne. Posameznim uporabnikom bo internet stvari olajšal bivanje, znižal življenjske stroške, skrbel za njihovo varnost doma in na cesti, nadziral njihovo zdravstveno stanje, omogočil več prostega časa, nudil zabavo ter rekreacijo in podobno. Podjetja bodo s pomočjo povezanih naprav in ustrezne analitike lahko postala učinkovitejša, varčnejša, okolju prijaznejša in cenejša do potrošnikov. Poleg tega jim bo internet stvari omogočil nove vire prihodkov na podlagi obstoječih izdelkov in storitev ter pomagal pri razvoju povsem novih procesov (Pretz 2014).

Vpliv, ki ga bo imel internet stvari na gospodarstvo v letu 2020, naj bi znašal skoraj dva bilijona (dva tisoč milijard) ameriških dolarjev, po nekaterih ocenah pa celo devet bilijonov ameriških dolarjev (Miller 2015, 2. pogl.). Izvršni direktor podjetja Cisco, John Chambers, je v zvezi s tem napovedal, da bo vpliv interneta stvari pet do desetkrat večji, kot ga ima internet danes (Goodman 2015, 12. pogl.). Analiza 770 podjetij po vsem svetu je pokazala, da jih tri četrtine že sedaj preučuje možnosti uporabe interneta stvari, kar 95 odstotkov podjetij pa bo internet stvari v takšnem ali drugačnem obsegu uporabljalo že v letu 2016 (Witchalis 2013).

Če internet stvari razumemo kot omrežje različnih omrežij, potem lahko govorimo tudi o prihajajočem internetu komunikacij, internetu energetike, internetu logistike itd., ki bodo skupaj v pametno omrežje povezali vse naprave, podjetja, domove in vozila ter tako omogočili ogromen dvig produktivnosti na svetovni ravni (Rifkin 2014, 5. pogl.). Če bo internet stvari dejansko izpolnil tovrstne smele napovedi, je drugo vprašanje, vendar ne gre zanikati, da bi s pomočjo pametnih in povezanih naprav ter analize masovnih podatkov, ki bi

jih takšne naprave omogočile, lahko že z relativno skromnimi prihranki pri porabi energije v industriji, goriva pri transportu in zdravil v zdravstvenem sistemu privarčevali velike vsote.

Lahko bi rekli, da je internet stvari pravzaprav nujno potrebna inovacija, če bomo želeli uspešno upravljati z naravnimi viri planeta, na katerem bo že čez nekaj desetletij sobivalo deset milijard ljudi. Učinkovit nadzor nad mesti, pridelavo in distribucijo hrane, uporabo energije, onesnaževanjem, infrastrukturo in ostalimi dejavniki sodobne civilizacije bo zahteval avtomatizacijo večine procesov zbiranja podatkov in analiziranja, v veliki meri pa tudi sprejemanja odločitev, ki bodo temeljile na spoznanjih, pridobljenih iz masovnih podatkov, in ne bodo več odvisne samo od človeške presoje.

Ne nazadnje ima internet stvari tudi potencial opolnomočiti ljudi, ki so tako ali drugače zatirani, neprivilegirani in socialno šibki. Širjenje novih tehnologij naj bi namreč pozitivno vplivalo tudi na krepitev demokratičnih vrednot (Howard 2015, 1. pogl.). Tehnološka omrežja rastejo skupaj z družbenimi omrežji, kar pomeni, da imajo tudi naprave, ki jih uporabljamo, vpliv na politične, gospodarske in kulturne vidike naših življenj. To bi lahko imelo v prihodnosti nepredvidene, a pozitivne posledice na geopolitični položaj držav, saj bi tehnologija interneta stvari svet povezala do te mere, da bi se zmanjšala možnost konfliktov v mednarodnem političnem prostoru, ker bi bili vsi akterji gospodarsko in tehnološko povezani ter soodvisni eden od drugega. Internet stvari bo obenem ustvaril tudi tako zajetne količine podatkov o naših vrednotah in vedenju, da jim klasično družboslovje ne bo kos pri iskanju razlag in rešitev (Howard 2015, 2. pogl.). Da bi jih izkoristili v največji možni meri v dobro vseh ljudi, bo treba razviti nova orodja, pristope in metode preučevanja družbe.

5.3.2 *Internet stvari in zasebnost*

Doba interneta stvari naj bi bila tudi doba "radikalne odprtosti" (Miller 2015, 15. pogl.), kjer bo transparentnost zaznamovala vse transakcije, dejanja in udeležene osebe, kar bo nujno za doseganje zaupanja, ki bo potrebno za povezavo vseh naprav v skupno celoto. Koristi, ki naj bi jih s tem pridobili vsi uporabniki interneta stvari, bodo po napovedih njegovih entuziastov v marsičem odtehtale odpovedovanje zasebnosti. Takšna utilitaristična računica je logična izpeljava razmišljanja, da je zasebnost v sodobni informacijski družbi zastarel in celo škodljiv koncept, ki zavira ustvarjalnost in napredek ter bo v prihodnjih letih in desetletjih popolnoma izginil. Na drugem bregu je skupina zagovornikov zasebnosti, ki menijo, da se s premišljenim

pristopom lahko ohrani nekatere temeljne vrednote tudi ob prihajajočem internetu stvari, čeprav priznavajo, da bodo za to potrebne nekatere radikalne spremembe v razmišljanju in pojmovanju zasebnosti v kontekstu sodobne tehnologije.

Več deset milijard senzorjev, ki bodo noč in dan zajemali podatke in jih prek naprav, povezanih v omrežja ter internet, pošiljali drugim napravam in računalniškim centrom za obdelavo podatkov, bo predstavljalo izziv zasebnosti, s kakršnim se še nismo srečali v vsej človeški zgodovini. Kot je bilo rečeno že uvodoma, bo velika količina teh podatkov neosebne narave, saj bodo pridobljeni iz okolja in delovnih procesov, in takšni podatki ne bi smeli ogrožati zasebnosti posameznikov. A vzporedno s tem se bo izjemno povečal tudi nabor podatkov, zajetih posredno ali neposredno od človeških uporabnikov, in ti podatki bodo lahko razkrili tudi najbolj intimne podrobnosti iz življenj ljudi.

Ta trend je jasno viden že danes. Na pametne naprave današnjega interneta stvari običajno gledamo kot na televizorje, telefone in avtomobile z vgrajenimi senzorji in računalniki, vendar je prav tako na mestu opazka, da gre v resnici za miniaturne računalnike, ki znajo tudi predvajati televizijski program, telefonirati in upravljati z motorjem vozila. Ti računalniki se bodo v prihodnosti pojavljali v vse večjem številu predmetov, ki nas obdajajo. V naših domovih se bodo nahajali v pečicah, sijalkah, oblekah in igračah. Zunaj bodo vgrajeni v semaforje, cestišča, parke in druge javne površine. V obliki čipov bodo prisotni v naših domačih živalih in v nas samih.

Današnji pametni telefoni so sposobni o svojih uporabnikih zbirati najrazličnejše podatke, od zvoka in slike, do fizične lokacije in določenih biometričnih informacij. Ker so postali nepogrešljiv del vsakdana večine ljudi v sodobni družbi, predstavljajo primerno orodje za spremljanje in beleženje dejavnosti posameznikov od jutra do večera. Internet stvari bo še razširil možnosti sledenja uporabnikom in zbiranja podatkov iz njihovih življenj. Pametni domovi ne bodo spremljali zgolj porabe energije in okoljskih parametrov, temveč tudi vzorce bivanja njihovih lastnikov. Podobno velja za pametne avtomobile, ki lahko poleg motenj v delovanju vozila analizirajo tudi način vožnje svojih voznikov ter razkrijejo, kje se v katerem koli trenutku vozila nahajajo. Poleg tega že danes obstajajo namenske naprave in aplikacije, ki nenehoma beležijo osebne podatke uporabnikov z namenom zbiranja in shranjevanja kar največje možne količine informacij (Schneier 2015, 17). Googlova pametna očala so eden prvih primerov tovrstne nosljive tehnologije, ki bo v kratkem prodrla tudi na druga področja. Kmalu bodo lahko stalo povezana s spletom in neprestano zajemala avdio in video

informacije iz okolja (Tapscott 2012). Ni si težko predstavljati naprav, ki bodo spremljale tudi naše razpoloženje, vitalne znake ali možgansko delovanje in informacije o tem sporočale drugim napravam in v računalniške centre. Ob padanju cen sekvenciranja genetskega materiala bo verjetno napočil tudi trenutek, ko bo analize lastne DNK mogoče izvajati s pametnimi napravami, povezanimi z internetom stvari.

Takšne naprave bodo predstavljale naslednjo stopnjo v evoluciji potrošniške računalniške tehnologije, a nikakor ne zadnjo. Kar se je začelo z namiznimi napravami (ang. *desktop*), kot so osebni računalniki, in je pred nekaj leti prešlo v prenosne naprave (ang. *handheld*), kamor spadajo mobilni telefoni, to že zdaj zamenjujejo nosljive naprave (ang. *wearable*), kakršna so pametna očala ali zapestne ure nove generacije, v prihodnosti pa jih bodo dopolnile še naprave, ki bodo neposredno vgrajene v biološka tkiva živih bitij[41] (ang. *implantable*). Ta tehnologija bo z neznanskimi količinami podatkov, ki jih bo ustvarila, potencirala današnje probleme z zagotavljanjem zasebnosti njenih uporabnikov, obenem pa sprožila še kopico novih izzivov, na katere v tem trenutku zagotovo nismo pripravljeni. Jasno je, da zakonodaja ne dohaja razvoja tehnologije, zato je iluzorno pričakovati, da bodo ob polnem razcvetu interneta stvari, torej okoli leta 2020, na voljo zadovoljive zakonske rešitve, ki bodo učinkovito ščitile zasebnost posameznikov.

Težave z varovanjem zasebnosti so na vidiku že danes. Znani so primeri vdorov v pametne naprave za nadzorovanje dojenčkov, kjer so nepridipravi upravljali s kamero na napravi in vzpostavljali glasovno komunikacijo z otroki (Cvjetović 2015). Podobno se lahko zgodi z vsemi napravami z vgrajeno kamero, pri čemer ne gre zanemariti pomislekov o tajnem nadzoru, ki ga lahko na ta način vršijo države nad svojimi državljani, kjer zopet prednjačijo ZDA s svojim programom PRISM[42]. Nadalje je neka raziskava pokazala, da je mogoče s pomočjo senzorjev v igralnih konzolah z veliko natančnostjo na daleč ugotoviti, koliko oseb se nahaja v prostoru in kaj tam počnejo (Payton in Claypoole 2014, 11. pogl.). Problematične so lahko tudi otroške igrače, kar je pokazal primer vdora in razkritja podatkov o 6,4 milijona otrok, ki so uporabljali takšne igrače (Thielman 2016), oziroma odpoklic pametnih plišastih

[41] Prvi zametki "biološkega interneta" obstajajo že danes. V Avstraliji so denimo raziskovalci opremili več kot 300 morskih psov s senzorji, ki sporočajo njihovo lokacijo prek Twitterja in tako opozarjajo plavalce pred morebitnimi bližnjimi srečanji z morskimi psi (Goodman 20015, 12. pogl.).

[42] V program tajnega nadzora PRISM so bila domnevno vključena tudi nekatera velika tehnološka podjetja, kot so Apple, Microsoft, Google, Facebook, Yahoo! in Dropbox, ki so posredovala podatke o svojih uporabnikih ameriški vladi (Lardinois 2013).

igrač znanega proizvajalca, ker so bile odkrite resne varnostne luknje v njegovi programski opremi (Cvjetović 2016). Podobno je tudi s pametnimi domovi in pametnimi avtomobili, ki lahko oddaljenemu opazovalcu (legalnemu ali ne) razkrijejo, kje se v danem trenutku nahajajo oziroma ne nahajajo uporabniki (Thielman 2016).

Opisani primeri se nanašajo na nezakonite vdore v povezane naprave, ki jih pravni red sankcionira v vseh državah, medtem ko je vprašanje legalnega zbiranja informacij o uporabnikih s strani ponudnikov precej bolj nedorečeno in v marsičem odraža dileme, opisane v prejšnjih poglavjih, namreč glede lastništva nad podatki, težav z zagotavljanjem anonimnosti in nepredvidljivosti uporabe pridobljenih podatkov. Uporabniki pametnih gospodinjskih aparatov so morda mnenja, da informacije o delovanju teh naprav pripadajo njim samim, ker so z nakupom postali njihovi lastniki, a resnica je drugačna, saj so za podjetja, ki naprave izdelujejo in prodajajo, ti podatki izredno dragocen vir prihodkov in nadaljnjega razvoja (Rozenfeld 2014). Ena rešitev bi bila, da bi v skrajnih primerih uporabniki zavrnili pošiljanje informacij v oddaljene centre oziroma izbrali selektivno izmenjavo podatkov (prav tam), vendar to predpostavlja, da bi tehnologija interneta stvari sploh omogočala tolikšno stopnjo avtonomije uporabnikov, obenem pa bi takšno odklanjanje storitev pomenilo tudi, da se uporabniki s tem odpovedujejo vsem prednostim, ki jih prinaša internet stvari.

Tudi če bi uporabniki omejili izmenjavo osebnih podatkov, ki jih povezane naprave zberejo o njih, še vedno ostaja težava identifikacije posameznih naprav (preko IP naslova ali kako drugače), kar bo eden temeljnih kamnov interneta stvari in posledične avtomatizacije procesov ("IoT Privacy, Data Protection, Information Security" 2013, 3). Če bodo te naprave vezane na posameznike, bo z njihovo identifikacijo razkrita tudi identiteta posameznika, tudi če bodo zajeti podatki neosebne narave. S povezovanjem takšnih podatkov z drugimi, pridobljenimi s pomočjo drugih naprav, ki prav tako pripadajo isti osebi (spomnimo, da naj bi v prihodnjih letih uporabniki imeli v lasti tudi tisoč ali več povezanih naprav), bodo ponudniki storitev s pomočjo analize masovnih podatkov prišli do spoznanj uporabnikih, ki jih ena sama naprava ne bi mogla razkriti.

Da bi zasebnost v dobi interneta stvari sploh lahko preživela (kaj šele zaživela), bi morali vse bistvene komponente sistema že vnaprej zasnovati tako, da bi uporabnikom nudile nadzor nad lastnimi podatki, omogočale transparentnost in nasploh podpirale načela, ki jih predvideva napredna zakonodaja, kot je evropska *Splošna uredba o varstvu podatkov*, torej pravico do

izbrisa podatkov, pravico do pozabe, prenosljivost podatkov, zaščito osebnih podatkov in podobno. Realno stanje danes je, da ponudniki šele naknadno dodajo svojim napravam funkcionalnosti za varovanje zasebnosti, kar otežuje standardizacijo pristopov in pogosto stane več od rešitev, ki so že vdelane v sistem ("IoT Privacy, Data Protection, Information Security" 2013, 2). Nekaj takšnih predlogov rešitev za varovanje zasebnosti v dobi interneta stvari, računalništva v oblaku in masovnih podatkov je podrobneje predstavljenih v naslednjem poglavju. Uspešnost njihove implementacije bo odvisna tudi od ustrezne zakonske podlage, ki bo bržkone predstavljala šibko točko vseh prizadevanj za krepitev zasebnosti in zagotavljanja varnosti osebnih podatkov.

6 ISKANJE REŠITEV ZA VAROVANJE ZASEBNOSTI V LUČI NOVIH DRUŽBENO-TEHNOLOŠKIH FENOMENOV

6.1 Vgrajena zasebnost

Vgrajena zasebnost (ang. *privacy by design* oziroma PBD) je koncept varovanja zasebnosti, pri katerem ponudniki zasebnost upoštevajo že pri samem snovanju izdelka ali storitve oziroma v vseh fazah razvoja (Strandburg v Lane in drugi 2014, 1. del, 1. pogl.). Zasebnost je namreč v večini primerov precej nizko na prioritetni lestvici podjetij, ki ukrepe za zaščito zasebnosti upoštevajo šele, ko so v to prisiljena ali ko jim to izrecno narekuje zakonodaja. Zato so rešitve, s katerimi takšna podjetja odgovarjajo na zahteve glede varovanja zasebnosti, vpeljane v uporabo šele po razvoju izdelka in pogosto niso optimalne. *A posteriori* rešitve ne ščitijo uporabnikov v največji možni meri, ker so običajno zasnovane s premalo premisleka in pod časovnimi pritiski ali pa ne morejo biti v celoti implementirane v že obstoječe izdelke in storitve. Poleg tega so dražje tudi za ponudnika, kot če bi bila zasebnost "vgrajena" v izdelek že od samega začetka.

To je temelj koncepta vgrajene zasebnosti, ki želi ponudnike prepričati v razvoj izdelkov in storitev, ki imajo elemente zaščite zasebnosti vdelane že privzeto. Pri razvojnem procesu takšnih izdelkov in storitev je upoštevan sistem človeških vrednot, ki niso neposredno povezane s donosnostjo ali tržno vrednostjo. Prav zato številna podjetja pri lansiranju izdelkov na trg zanemarijo zasebnost uporabnikov. Da bi izdelki in storitve zadostili konceptu vgrajene zasebnosti, morajo upoštevati sedem načel (Cavoukian 2011, 2):

- proaktivno in preventivno delovanje: predvidevanje kršitev zasebnosti, še preden se zgodijo;
- privzete nastavitve zasebnosti: izdelek ali storitev že od začetka uporablja največjo možno zaščito zasebnosti, ki jo nato uporabniki lahko na lastno željo omilijo (pristop *opt in* namesto *opt out*);
- vdelava zasebnosti v razvoj: rešitve za varovanje zasebnosti ne smejo biti naknadno dodane izdelku ali storitvi, ampak morajo predstavljati sestavni del izdelka ali storitve;
- polna funkcionalnost: rešitve za varovanje zasebnosti ne smejo okrniti funkcionalnosti izdelka ali storitve (pristop pozitivne vsote namesto ničelne vsote);

- zaščita skozi celoten življenjski cikel: podatki, ki jih zajemajo izdelki ali storitve, morajo biti zaščiteni v vseh fazah, od zbiranja in shranjevanja, do obdelave in končnega uničenja;
- transparentnost: sestavni deli izdelka ali storitve morajo biti javno dostopni oziroma transparentni;
- osredotočenost na uporabnika: želje in vrednote uporabnikov morajo biti na prvem mestu pri razvoju izdelkov in storitev.

Primera vgrajene zasebnosti v izdelke in storitve sta denimo Googlovo družbeno omrežje Google+, ki daje relativno velik poudarek zasebnosti uporabnikov[43], in Applov telefon iPhone, ki uporabnika opozori vsakič, ko se podatki o njegovi lokaciji prenesejo v aplikacijo (Hill 2011).

Zaradi specifičnosti masovnih podatkov, sploh v količini, kakšno bo ustvarjal internet stvari, implementacija vgrajene zasebnosti na tem področju predstavlja dodaten izziv. Izdelki in storitve, ki se tako ali drugače nanašajo na masovne podatke, bi lahko upoštevali načela vgrajene zasebnosti, če bi dosledno beležili izvor podatkov in kakršne koli spremembe teh podatkov, izvajali obdelavo zgolj anonimiziranih podatkov, preprečili manipulacijo podatkov s strani nepooblaščenih oseb, uporabljali metode, ki so nagnjene k vračanju lažno negativnih rezultatov, odpravljali lažno pozitivne rezultate v realnem času ter spremljali vse sekundarne prenose podatkov (Cavoukian in Jonas 2012, 10–13). Takšen pristop je sicer korak v pravo smer, a še zdaleč ne odpravlja vseh težav z ogrožanjem zasebnosti, ki jih prinaša obdelava masovnih podatkov, v prvi vrsti z zagotavljanjem robustne anonimnosti.

Kritiki vgrajene zasebnosti konceptu očitajo, da je preveč splošen in da se v svojem bistvu ne razlikuje od koncepta prostovoljnega sodelovanja podjetij, kjer je odločitev za upoštevanje načel za varovanje zasebnosti prepuščena samim podjetjem in zato pogosto zanemarjena. Takšen premik od prisile do zavestne odločitve v prid zasebnosti mora akterjem zagotoviti zadostno motivacijo, da se zanj odločijo. S tem bi varovanje zasebnosti prešlo iz sfere zakonodaje v sfero prostega trga, vendar podporniki vgrajene zasebnosti ne ponudijo konkretnih argumentov, kako naj bi se to zgodilo, razen neprepričljive trditve, da bi se potrošniki raje odločali za ponudnike, ki spoštujejo njihovo zasebnost. Za uspešno

[43] Vsaj v primerjavi z družbenim omrežjem Facebook in Googlovo predhodno storitvijo Google Buzz, ki je neslavno pogorela prav zaradi posegov v zasebnost uporabnikov.

implementacijo vgrajene zasebnosti bi morala svojo vlogo odigrati tudi zakonodaja. Evropska komisija je pri snovanju *Splošne uredbe o varstvu podatkov* upoštevala tudi načela vgrajene zasebnosti, vendar ni jasno, kako naj bi jih uredba uveljavljala. V ZDA vgrajena zasebnost nima nikakršne zakonske podlage, a je koncept podprla Zvezna komisija za trgovino kot enega treh priporočenih pristopov[44] za varovanje zasebnosti na spletu ("Protecting Consumer Privacy in an Era of Rapid Change" 2012, 1).

6.2 Kontekstna integriteta

Osrednja zamisel koncepta kontekstne integritete[45] (ang. *contextual integrity*) je, da so vsa področja življenja pod vplivom norm pretoka informacij oziroma da se vsi dogodki, dejanja in transakcije izvršijo v določenem kontekstu, ki ni vezan samo na fizično lokacijo, ampak tudi na politiko, navade in kulturna pričakovanja (Nissenbaum 2004, 119). Ta pristop skuša relativizirati zasebnost v smislu, da ukrepi za zaščito zasebnosti ne smejo biti monolitni in enotni za vsa področja oziroma dejavnosti, kar je značilnost nekaterih krovnih zakonskih dokumentov, kakršna je evropska *Direktiva o varstvu podatkov* 95/46/EC, ker se tudi pričakovanja glede zasebnosti v različnih kontekstih lahko zelo razlikujejo.

Primer takšne kontekstne obravnave zasebnosti je odnos med zdravnikom in pacientom, kjer ustaljene norme narekujejo, da zdravnik nikakor ne sme razkriti pacientovih zdravstvenih podatkov tretjim osebam, ki niso udeležene v procesu zdravljenja, medtem ko je razkritje istih podatkov drugemu zdravniškemu osebju običajno sprejemljivo in samoumevno. V takšnem položaju kontekstna integriteta narekuje, da morajo ukrepi za zaščito zasebnosti upoštevati različne vrste interakcij med udeleženci in družbene norme, ki usmerjajo pretok informacij med njimi. Bistveno je, da te norme niso statične, ampak se spreminjajo, razvijajo ali celo spreobračajo, včasih postopoma, drugič hipoma, zaradi sprememb v kulturi, pravnem redu in družbi ali pa zaradi dejavnikov, ki niso pod neposrednim nadzorom ljudi in družbe (Barocas in Nissenbaum v Lane in drugi 2014, 1. del, 2. pogl.). Tehnologija prav gotovo spada med spremembe, ki so vplivale na preoblikovanje informacijskih norm in dojemanje zasebnosti.

[44] Preostala dva pristopa sta poenostavljena možnost izbire za podjetja in potrošnike ter večja transparentnost.

[45] Teorija kontekstne integritete ima tudi rigoroznejšo definicijo, razvito na podlagi formalnega logičnega modela (Barth in drugi 2006).

Ključni parametri teh družbenih informacijskih norm v teoriji kontekstne integritete so (Nissenbaum 2011, 33):

- akterji oziroma subjekti, pošiljatelji in prejemniki;
- atributi oziroma vrste informacij;
- načela prenosa oziroma omejitve pretoka informacij.

Upoštevajoč te parametre informacijskih norm skušajo zagovorniki kontekstne integritete ta koncept aplicirati tudi na masovne podatke z vsemi pripadajočimi posebnostmi. Z analizo pretoka informacij želijo identificirati procese, ki odstopajo od ustaljenih norm na področju zasebnosti, kar pogosto ni lahko, saj so v dobi masovnih podatkov meje med pošiljatelji in prejemniki informacij pogosto zabrisane, kar bo še bolj izrazito ob naraščajoči količini podatkov iz najrazličnejših virov, ki bo neizbežna posledica interneta stvari.

Teoretski temelji kontekstne integritete so očitni, zato ni jasno kako bi ta pristop k varovanju zasebnosti iz akademske sfere lahko uspešno prenesli v prakso in kdo bi v tem primeru skrbel za uveljavljanje informacijskih norm in ustrezno identifikacijo vseh udeleženih akterjev.

6.3 Diferencialna zasebnost

Kot je bilo razloženo v poglavju o masovnih podatkih, anonimizacija oziroma psevdonimizacija velike količine heterogenih podatkov ni zagotovilo za varovanje zasebnosti posameznikov, ki s svojimi informacijami sestavljajo takšne podatke, pri čemer informacije tipa PII niso potrebne za ponovno identifikacijo. Da bi odpravili ta problem, znanstveniki in informatiki razvijajo različne pristope, med katere spada tudi diferencialna zasebnost (ang. *differential privacy*).

Cilj diferencialne zasebnosti je zakriti prisotnost oziroma odsotnost posameznikov ali manjših skupin v bazah podatkov z uvajanjem naključnosti v sistem ter obenem ohraniti statistično uporabnost podatkov (Dwork in drugi 2011; Dwork v Lane in drugi 2014, 3. del, 14. pogl.). Formalna definicija diferencialne zasebnosti ni v domeni tega dela, zato naj zadostuje intuitivno pojasnilo, da princip deluje z vnašanjem umetno ustvarjenega šuma v baze podatkov s pomočjo računalniških algoritmov. Če je šum premišljeno ustvarjen in vnesen na pravih mestih, potem ostane statistična uporabnost nabora podatkov *kot celote* neokrnjena,

zato je takšne podatke še vedno mogoče obdelovati in analizirati. Pri tem morajo algoritmi posebno pozornost nameniti podatkom, ki najbolj odstopajo od povprečja na ravni celotnega nabora. Če na primer iz sodelovanja v bazi podatkov izstopi ena sama oseba in se pri tem povprečna vrednost določenega parametra v naboru anonimiziranih podatkov drastično spremeni, potem je mogoče zanesljivo sklepati, kakšna vrednost je pripadala tej osebi. Z vnosom dodatnega šuma v sistem na ustreznih mestih je vsaj v teoriji takšne napade na zasebnost mogoče preprečiti.

Diferencialna zasebnost ni popolna in ima svojo ceno, saj ne pride v poštev, ko morajo biti analize podatkov zelo natančne ali ko kompromis med anonimnostjo in uporabnostjo podatkov, ki ga pristop uvaja, preprosto ni sprejemljiv (Bryne 2014). Kljub temu je diferencialna zasebnost eden redkih pristopov, ki se ukvarja neposredno s problematiko ogrožanja zasebnosti v luči novih družbeno-tehnoloških fenomenov, kakršni so masovni podatki.

6.4 Storitve na podlagi osebnih podatkov

Storitve na podlagi osebnih podatkov (ang. *personal data services* oziroma PDS) so predlagani model uporabe osebnih podatkov, ki bi bil pravičnejši, transparentnejši in ne nazadnje donosnejši za različne akterje, ki so vključeni v sistem. Danes je način uporabe in obdelave osebnih podatkov zgrajen na piramidi, ki jo spodaj sestavljajo posamezniki s svojimi osebnimi podatki, na sredini ponudniki storitev oziroma obdelovalci podatkov in na vrhu uporabniki spoznanj, ki jih prinese analiza podatkov (ki so lahko obenem tudi obdelovalci, ni pa nujno). Največje koristi v tem procesu pripadajo akterjem na sredini in vrhu piramide, medtem ko je doprinos posameznikom, ki dejansko prispevajo podatke, pogosto vprašljiv ali nesorazmeren z njihovim prispevkom.

Na takšnem odnosu temelji dobršen del današnje digitalne ekonomije, saj je dobiček številnih podjetij postal v veliki meri odvisen od spoznanj, ki jih pridobivajo z analizo in rudarjenjem masovnih podatkov. V ZDA podjetja, ki se sama ne ukvarjajo z obdelavo podatkov, kupujejo storitve od podjetij, ki so specializirana za to, ta pa pogosto podatke pridobivajo neposredno iz javnega sektorja oziroma baz podatkov, ki jih vzdržujejo državne institucije (Tanner 2014, 6. pogl.), obenem pa slednje tudi same sodelujejo pri kupovanju storitev in podatkov od zasebnega sektorja (Solove 2006, 41). Posameznikom, ki predstavljajo vir podatkov, v večini

primerov kot korist ostanejo storitve ponudnikov, s katerimi jih ti premamijo v sodelovanje. Takšne storitve so mnogokrat brezplačne, posamezniki pa z njihovo uporabo podajo soglasje za obdelovanje svojih podatkov, nad katerimi na ta način izgubijo lastništvo.

Spoznanja, da bi morala digitalna ekonomija sloneti na pravičnejšem ekosistemu uporabnikov in ponudnikov storitev ter tretjih oseb, ki koristijo osebne podatke, je privedla do zamisli o spremembi vrednotenja osebnih podatkov. Da bi digitalna ekonomija zaživela v polnem razmahu, bi morali na osebne podatke gledati kot na gonilo gospodarske dejavnosti in valuto, s katero lahko trgujejo njihovi lastniki, to pa bi morali biti v prvi vrsti uporabniki storitev[46] in ne ponudniki, ki se dokopljejo do podatkov. Takšna ureditev bi posameznikom omogočila večji nadzor nad lastnimi podatki, več zasebnosti in ustreznejšo kompenzacijo za uporabo teh podatkov, medtem ko bi spodbudila podjetja in državne organizacije k pogostejši in preglednejši izmenjavi podatkov v korist vseh udeleženih ("Personal Data" 2011, 10). V nasprotnem primeru je ustvarjanje gospodarske vrednosti oteženo ali celo onemogočeno, ker lahko pride do a) nesorazmernega zbiranja in uporabe podatkov s strani podjetij, b) pretirane regulacije s strani države z namenom zaščite državljanov in negativnim vplivom na gospodarstvo ter c) samoorganizacije posameznikov in nekomercialnega kopičenja podatkov ("Personal Data" 2011, 18–19).

Uravnotežen pristop bi omogočil pojav novega poslovnega modela oziroma storitev na podlagi osebnih podatkov. Posamezniki bi bili za uporabo svojih osebnih podatkov primerno poplačani, bodisi s storitvami bodisi celo v denarju, podjetja in državne organizacije pa bi na ta način prišli do kakovostnejših informacij, kot so jim na voljo danes (Rubinstein 2012, 13). Vpeljava takšnih storitev se sicer sooča številnimi izzivi tehnične, pravne in poslovne narave, med katerimi je verjetno najpomembnejši izziv, kako podjetja prepričati, da opustijo trenutne poslovne modele, ki so zaradi rudarjenja podatkov in oglaševanja na podlagi pridobljenih informacij donosni in uveljavljeni (prav tam). Vprašanje je tudi, kako bi takšen pristop na načelih prostega trga deloval brez ustreznih zakonskih omejitev. In ne nazadnje bi uvedba storitev na podlagi osebnih podatkov pomenila, da je zasebnost dokončno izgubila status pravice, ki jo treba zaščititi z zakonom, in postala dobrina, s katero je smiselno in zaželeno trgovati.

[46] Z določenimi izjemami: težko bi namreč trdili, da so nekatere vrste osebnih podatkov, kot so podatki o kaznovanosti ali kreditni sposobnosti, last posameznikov.

6.5 Prenovljeno načelo obveščanja in soglasja

Načelo obveščanja in soglasja je danes poglavitni mehanizem urejanja odnosov med subjekti, ki prispevajo svoje podatke, in obdelovalci teh podatkov, čeprav je bilo prvotno mišljeno, da bo predstavljal le enega od načinov, v okviru katerih se izvajajo zakonite obdelave osebnih podatkov (Cate in Mayer-Schönberger 2012, 3). V kontekstu interneta se načelo obveščanja in soglasja najpogosteje pojavlja v obliki licenčnih pogodb s končnim uporabnikom (EULA), katerih pomanjkljivosti so znane vsakomur, ki je se že kdaj soočil z njimi na spletu in jih, tako kot velika večina uporabnikov, ni niti prebral. Neka raziskava je pokazala, da branje ene takšne pogodbe vzame do 12 minut uporabnikovega časa in da bi zato morali uporabniki vsako leto nameniti od 181 do 304 ur, če bi želeli temeljito prebrati vse dokumente o politikah zasebnosti podjetij na internetu (Tanner 2014, 9. pogl.).

Zato se že dalj časa pojavljajo pobude za reformo načela obveščanja in soglasja, ki se sooča z dodatnimi težavami tudi v povezavi z masovnimi podatki, kar je bilo podrobneje opisano v temu namenjenem poglavju. Težava je, da bi spodbujanje uporabnikov k bolj aktivnemu prebiranju politik zasebnosti verjetno pomenilo, da bi morali takšne dokumente ustrezno skrajšati in poenostaviti, obenem pa so grožnje zasebnosti, ki jih prinašajo novi družbeno-tehnološki fenomeni, kompleksne in večslojne, zato bi morale licenčne pogodbe postati še podrobnejše, da bi zadovoljivo seznanile uporabnike s problematiko.

Konkretnih rešitev še ni na vidiku, se pa večina strokovnjakov strinja, da bi se morale licenčne pogodbe iz načina "vzemi ali pusti", preoblikovati v večstopenjski mehanizem upravljanja z lastnimi osebnimi podatki (Cate in Mayer-Schönberger 2012, 3). Trenutna binarna izbira uporabnikom namreč nudi zgolj sprejetje ali zavrnitev pogoje uporabe njihovih podatkov, medtem ko bi bilo smotrneje in za vse udeležence koristneje, če bi uporabniki imeli več nadzora nad svojimi podatki in bi lahko pristali na njihovo obdelavo v določenih okoliščinah, v drugih pa raje ohranili svojo zasebnost. Zamisel je težko uresničljiva v praksi, a je skladna s konceptov storitev na podlagi osebnih podatkov, opisanim v prejšnji točki.

7 ZAKLJUČEK

7.1 Verifikacija hipotez

V tem delu so bili obravnavani trije družbeno-tehnološki fenomeni, ki se medsebojno dopolnjujejo in bodo v bodočih letih igrali vse večjo vlogo v informacijski družbi in digitalni ekonomiji, predstavljeni pa so bili v kontekstu ogrožanja zasebnosti. Ti fenomeni so masovni podatki, računalništvo v oblaku in internet stvari ter predstavljajo velik potencial za gospodarski in človeški napredek, a obenem tudi velike izzive za zagotavljanje zasebnosti, ki z razvojem tehnologije vse težje ohranja status neodtujljive pravice, ki jo je treba zaščiti.

Pri tej obravnavi družbeno-tehnoloških fenomenov je bil poudarek tudi na primerjavi dveh velikih akterjev v svetovni areni, ki sta ubrala različna pristopa k varovanju zasebnosti, pogojena z dolgoletno tradicijo in razlikujočimi se vrednotami. ZDA so skozi večino 20. stoletja uživale nesporen status najpomembnejše tehnološke velesile. Z gospodarstvom, ki temelji na načelih prostega trga, in pravnim redom, ki daje velik poudarek sodni praksi in interpretaciji ustave, se je v ZDA razvil odnos do zasebnosti, kjer je ta koncept razumljen kot dobrina, s katero je mogoče trgovati, zakonodaja pa ga ureja sektorsko, torej z mnogimi zakoni in pravili na različnih področjih. Na drugi strani ima Evropa za seboj krvavo zgodovino, v kateri je bila zasebnost pogosto zlorabljena tako s strani zavojevalcev kot lastnih državnih organizacij, zato na stari celini ta koncept še vedno velja za pravico, ki je kljub modernim trendom ne gre trivializirati. V večini evropskih držav je zato zasebnost ustavna kategorija in tudi Evropska unija jo skuša zaščititi z enotnim in obsežnim krovnim dokumentom, ki ga morajo vse države članice prenesti v svoj pravni red.

Relevantnost tega dela je, da skuša povezati nove družbeno-tehnološke fenomene, ki so običajno obravnavani ločeno, v odnosu do zasebnosti, saj ti fenomeni že sami po sebi prinašajo načine ogrožanja zasebnosti, ki poprej niso bili znani ali niso imeli takšnega pomena, njihov sinergijski učinek pa zastavljeno problematiko še stopnjuje, kar se bo brez dvoma odvijalo tudi v prihodnjih letih. Z mislijo na to je bila zastavljena prva hipoteza, ki se je glasila:

H1: Družbeno-tehnološki fenomeni, kot so uporaba masovnih podatkov, računalništva v oblaku ter interneta stvari, ne prinašajo zgolj povečanega obsega ogrožanja zasebnosti v

informacijski družbi, ampak tudi povsem nove izzive in težave, ki bodo zahtevali razvoj drugačnih rešitev oziroma pristopov, kot so v uporabi danes.

V delu je bilo sistematično predstavljeno na kakšen način novi družbeno-tehnološki fenomeni ogrožajo zasebnosti. Razloženo je bilo, da masovni podatki zaradi svojega izjemnega obsega in heterogenosti predstavljajo kvalitativno drugačen fenomen, kot je obdelovanje podatkov v manjših količinah. Analiza masovnih podatkov namreč lahko postreže z nepredvidljivimi korelacijami, ki so bile pred tem preprosto nedostopne. To pomeni, da subjekti, ki s svojimi podatki sodelujejo v takšnih analizah, ne morejo vnaprej vedeti, kakšni bodo rezultati uporabe njihovih podatkov, zato načelo obveščanja in soglasja, ki danes predstavlja poglavitni način urejanja varovanja zasebnosti in lastništva nad podatki, izgubi svoj smisel. Poleg tega anonimizacija podatkov, ki je dolgo veljala za temelj zaščite zasebnosti udeleženih subjektov, v prisotnosti heterogenih podatkov ni več zadostna rešitev, ker so raziskave dokazale, da je ponovna identifikacija realna nevarnost, ki jo treba upoštevati. Če na obdelavi masovnih podatkov temelji tudi avtomatsko odločanje in profiliranje posameznikov, potem obstaja tudi možnost napak, lažno pozitivnih rezultatov in diskriminacijskih odločitev, ki nadalje grobo posegajo v zasebnost in druge pravice subjektov.

Računalništvo v oblaku s tega vidika prav tako predstavlja grožnje zasebnosti, čeprav morda manj inovativne. Pri uporabi storitev računalništva v oblaku je ob neustrezni zaščiti lahko ogrožena tako identiteta posameznikov, ki so lastniki podatkov, kot tudi varnost in integriteta samih podatkov. Pri tem kršitelji lahko prihajajo od zunaj (vdori v sistem) ali pa je kršitelj zasebnosti kar ponudnik storitev, bodisi zaradi nesposobnosti, malomarnosti, pomanjkanja etičnih standardov, škodljivih namenov ali drugih dejavnikov. Položaj je lahko še dodatno zapleten zaradi dejstva, da so podatkovni in računalniški centri ponudnikov računalništva v oblaku razpršeni po mnogih lokacijah, ki niso nujno vse v isti državi. Zakoni o varovanju zasebnosti se v državah, kjer se takšni centri nahajajo, lahko med seboj zelo razlikujejo in uporabniki storitev so pri tem redko seznanjeni z dejansko lokacijo svojih podatkov.

Največjo uganko v tej računici predstavlja internet stvari, saj njegov čas šele prihaja. Če je danes z internetom povezanih okoli 15 milijard naprav, napovedi kažejo, da jih bo leta 2020 vsaj 50 milijard, kar pomeni, da se bo količina ustvarjenih in obdelanih podatkov skokovito povečala. Lahko bi poenostavili in rekli, da bo zato internet stvari samo še povečal količino že obstoječih težav na področju varovanja zasebnosti, ki jih prinašajo masovni podatki, a stvar je bolj zapletena. Če bo obveljala trditev, da bo leta 2020 vsak posameznik imel v lasti

povprečno tisoč povezanih naprav, ki bodo med seboj in z oddaljenimi centri izmenjavale informacije iz njegovega življenja, potem postanejo razsežnosti ogrožanja zasebnosti zares velikanske. Podjetja in državne institucije bodo prvič v zgodovini lahko prišli do izredno podrobnih in intimnih podatkov o veliki večini prebivalstva in ti podatki bodo govorili zgodbe iz vseh področji njihovih življenj – o delu, zdravju, zabavi, ljubezni, zanimanjih, političnih in verskih stališčih, družini in prijateljih, prostem času in mnogo več. Specializirane naprave, ki denimo zbirajo podatke o fizioloških parametrih in zdravstvenem stanju uporabnikov, obstajajo že danes in zakonodaja preprosto ne dohaja razvoja novih tehnologij, da bi lahko uspešno zaščitila zasebnost ljudi. Dejstvo je, da se je težko pripraviti na vse izzive, ki jih bo prinesel internet stvari, vendar bi stežka oporekali, da bo ti presegli težave z zaščito zasebnosti, s katerimi se soočamo danes.

Zaradi vsega naštetega se je prva hipoteza izkazala za pravilno in je zato **potrjena**.

Z mislijo na probleme, ki jih ima zakonodaja pri ohranjanju stika z razvojem tehnologije, je bila zasnovana druga hipoteza, ki se glasi:

H2: Z uveljavljanjem in razcvetom družbeno-tehnoloških fenomenov, kot so uporaba masovnih podatkov, računalništva v oblaku ter interneta stvari, formalno-pravni pristop k varovanju zasebnosti v informacijski družbi ni dovolj učinkovit, zato bosta vse večjo vlogo prevzemala obravnava koncepta zasebnosti na internetu po načelih delovanja prostega trga ter iskanje tehnoloških rešitev.

Čeprav drži, da so nekateri zakoni (predvsem v ZDA), ki urejajo področje varovanja zasebnosti, stari že več desetletij in zaradi tega niso kos sodobnim izzivom, in da se specifičnost novih družbeno-tehnoloških fenomenov ne odraža dovolj izrazito tudi v novejši zakonodaji, formalno-pravni pristop k urejanju zasebnosti gotovo še ni rekel zadnje besede. Na tem področju prednjači Evropska unija, ki ima najbolj sistematično, obsežno in strogo zakonodajo za zaščito zasebnosti na svetu, s svojim vplivom in zgledom pa deluje tudi na ostale države, predvsem tiste, ki želijo v informacijskem sektorju sodelovati z državami članicami. V ZDA se zakoni sprejemajo in spreminjajo izredno počasi[47], zato tam ni na vidiku

[47] Da v ZDA stanje ni povsem statično, dokazuje nedavna pobuda spodnjega doma Kongresa, ki je brez enega samega glasu proti izglasoval osnutek zakona, ki bi zahteval sodni nalog za vsak dostop do elektronske pošte, shranjene v oblaku, čeprav je pot do končnega zakona še dolga (Kravets 2016).

nobenega krovnega dokumenta za varovanje zasebnosti, kakršen je v Evropi *Direktiva o varstvu podatkov* 95/46/EC. Evropska komisija ima tudi namen okrepiti informacijsko zasebnost in s tem odgovoriti na izzive, ki jih prinašajo nove tehnologije, zato je pripravila *Splošno uredbo o varstvu podatkov,* krovni dokument, ki bo zamenjal obstoječo direktivo. Uredbo je v aprilu 2016 najprej sprejel Svet Evrope in nato še Evropski parlament. V polno veljavo bo predvidoma stopila po dvoletnem obdobju. Čeprav gre za pomemben razvoj zakonskih ukrepov za zaščito zasebnosti in doprinos k varovanju zasebnosti na svetovni ravni, nova uredba v obstoječi obliki kljub temu ne bo razrešila vseh dilem, ki se pojavljajo v luči novih družbeno-tehnoloških fenomenov. Krepitev zasebnosti z novo uredbo gre predvsem na račun uvajanja nekaterih novih pravic in širitve definicije osebnih podatkov, kar se zdi bolj začasna rešitev kot trajen ukrep, ki bi uspešno odgovoril na vse izzive novih tehnologij. Čas bo povedal, kako se bo uredba obnesla v dobi interneta stvari, naraščajoče količine masovnih podatkov in vse večje uporabe storitev v oblaku.

Vendar na drugi strani ne gre zanikati naraščajočega vpliva tržnih rešitev za varovanje zasebnosti. Koncept vgrajene zasebnosti je zajet tako v novi evropski uredbi kot v priporočilih ameriške Zvezne agencije za trgovino in temelji na prepričanju, da bi morali biti izdelki in storitve že v osnovi zasnovani z mislijo na zasebnost uporabnikov oziroma na način, da bi bile rešitve za zaščito zasebnosti vdelane že v sam izdelek ali storitev in ne dodane šele kasneje pod pritiskom zakonodaje. Takšen pristop predvideva, da se bodo posamezniki po načelih prostega trga odločali za izdelke in storitve, ki ne bodo ogrožali njihove zasebnosti, zato bodo tudi ponudniki motivirani zaščititi zasebnost svojih uporabnikov. S tem je povezan tudi koncept storitev na podlagi osebnih podatkov, v okviru katerega bi osebni podatki postali nekakšna valuta digitalne ekonomije, s katero bi subjekti trgovali z namenom povečevanja lastne koristi. V tem oziru tudi zasebnost ni več razumljena kot izrecna pravica, temveč postane dobrina kot vsaka druga v tržnem gospodarstvu. Če pustimo ob strani večno vprašanje, ali so tržne rešitve sploh prava izbira za zagotavljanje kakršne koli splošne dobrobiti, potem še vedno ostane dejstvo, da trenutno stanje, v katerem je zasebnost posameznikov prepuščena zastareli zakonodaji ter podatkov lačnim državnim institucijam in podjetjem, ustreza vsem akterjem na vrhu piramide, ki se okoriščajo z vse večjo količino podatkov in ne vidijo razloga, da bi jo prostovoljno omejevali. Urejanje zasebnosti v bodoče bo zato verjetno kombinacija tržnih in zakonskih rešitev, pri čemer ni nobenega zagotovila, da bo tržni pristop nudil optimalne koristi tudi posameznikom in ne le podjetjem ter državi.

Zaradi naštetega je druga hipoteza **potrjena**, vendar s pomisleki, opisanimi v prejšnjem odstavku.

Zadnja hipoteza se je nanašala na primerjavo ZDA in Evrope, ki imata, kot že rečeno, zelo različna pristopa k varovanju zasebnosti v informacijski dobi. Hipoteza se glasi:

H3: Zaradi ameriške prevlade v informacijskem sektorju, vpliva ameriških korporacij in pritiskov ameriške zunanje politike je evropski model varovanja zasebnosti v informacijski družbi ogrožen in se bo v prihodnosti, z razcvetom družbeno-tehnoloških fenomenov, kot so uporaba masovnih podatkov, računalništva v oblaku ter interneta stvari, približeval ameriškemu pristopu.

Hipoteza je predpostavljala, da je ameriška vloga v svetovni digitalni ekonomiji tako pomembna, da bo ta država v prihodnjih letih in desetletjih narekovala "pravila igre" in s tem tudi vplivala na varovanje zasebnosti v luči novih družbeno-tehnoloških fenomenov. Vendar preučevanje literature in spremljanje trendov v razvoju novih tehnologij nista razkrila nedvoumnih znakov, da je temu res tako. Še več – obstaja precejšen konsenz, da s pojavom novih tehnologij ZDA izgubljajo absoluten primat tehnološke velesile in da bo prihodnost, ko bo na milijarde naprav povezalo velik del človeštva, bolj enakopravna in demokratična za ves svet, kot je sedanjost. Utopične napovedi je vselej treba jemati s pregovornim ščepcem soli in družbeno-tehnološke fenomene, obravnavane v tem delu, spremljajo še posebno napihnjena pričakovanja, a je obenem mogoče ugotoviti tudi, da nove tehnologije podjetja in razvite države po svetu uporabljajo z enakim zagonom kot ZDA.

Obstajajo sicer primeri vplivanja ZDA na ostale države, da bi liberalizirale svojo zakonodajo na področju varovanja zasebnosti, toda Evropska unija je s sprejetjem nove uredbe jasno pokazala, da ne misli izgubiti statusa entitete, kjer je zasebnost najbolj cenjena in zaščitena, čeprav po mnenju najbolj gorečih zagovornikov še vedno premalo. Veliko vprašanje predstavlja tudi sporni bodoči trgovinski sporazum med ZDA in Evropsko unijo (TTIP), ki v imenu krepitve gospodarske rasti na obeh straneh Atlantika predvideva liberalizacijo in deregulacijo številnih področij, med katere spada tudi varstvo informacijske zasebnosti. Toda v trenutku nastajanja tega dela je še prezgodaj za ocenjevanje vpliva tega sporazuma na zaščito zasebnosti v državah Evropske unije, zato ni zajet v obravnavo hipoteze.

Zaradi pomanjkanja dejstev in dokazov v prid tretji hipotezi, je ta **zavrnjena**.

7.2 Sklepna beseda

Brez pretiravanja lahko sklenemo, da bo naša družba v prihodnosti temeljila na informacijah in izrabi podatkov vseh vrst. To ima izjemen potencial za napredek človeške družbe, olajšanje življenj vseh njenih posameznikov, reševanje naših najbolj perečih težav in ustvarjanje novih oblik bogastva. Toda ta optimistična vizija se lahko tudi sprevrže v situacijo, kjer je tehnologija zbrana v rokah peščice velikih, premožnih in močnih akterjev, ki jo izkoriščajo v svoj prid, medtem ko vsem preostalim puščajo zgolj digitalne drobtinice. Da bi povečali možnosti za usmeritev sveta na prvo pot in se izognili drugi, bo treba kolektivno poskrbeti za zaščito in vzdrževanje nekaterih temeljnih pravic, na katerih bo slonela pravičnejša in egalitarnejša informacijska družba prihodnosti.

Če je tudi zasebnost takšna pravica ali pa morda zgolj dobrina kot vsaka druga v tržnem gospodarstvu, je predmet številnih filozofskih, političnih in ekonomskih razprav med zagovorniki in nasprotniki tega koncepta. Morda je zasebnost res anomalija v človeški zgodovini, ki v informacijski družbi nima prihodnosti in jo bomo brez večjih pomislekov zamenjali za učinkovitost, varnost in udobje, vendar na drugi strani tudi drži, da je družba, ki je pod takšno ali drugačno obliko nadzora, v nevarnosti, da postane konformistična in pasivna, kar je bil vedno cilj tiranov in represivnih režimov. Vprašati se je treba, če vse koristi, ki nam jih bo nesporno prinesla izraba neznanskih količin podatkov, odtehtajo človeško ureditev, v kateri bodo posamezniki nemara nezavedno omejevali svoje misli in dejanja, saj bodo vedeli, da digitalne sledi, ki jih puščajo na vsakem koraku, predstavljajo celoto njihovih prepričanj, motivov in aspiracij.

Nikakršne potrebe ni, da se dejansko vzpostavi takšno stanje v družbi. Novi družbeno-tehnološko fenomeni, kot so masovni podatki, računalništvo v oblaku ter internet stvari, niso inherentno nastrojeni proti zasebnosti, temveč predstavljajo orodja, katerim pravila uporabe lahko ustvarimo sami. Ta pravila so lahko zapisana v zakonih, utelešena v vrednotah prostega trga, ali pa vgrajena v samo tehnologijo, vendar jih lahko tudi povsem zanemarimo, če ne bomo prepoznali njihove vrednosti za celotno družbo. Gotovo je le dejstvo, da bosta pomen in raba naših novih družbeno-tehnoloških fenomenov naraščala in da bodo družbo prihodnosti usmerjala spoznanja, pridobljena iz digitalnih informacij vseh vrst.

8 LITERATURA

Angwin, Julia. 2014. ***Dragnet Nation: A Quest for Privacy, Security, and Freedom in a World of Relentless Surveillance***. New York: Times Books. Dostopno prek: Kindle.

Armbrust, Michael, Armando Fox, Rean Griffith, Anthony D. Joseph, Randy H. Katz, Andrew Konwinski, Gunho Lee, David A. Patterson, Ariel Rabkin, Ion Stoica in Matei Zaharia. 2009. "Above the Clouds: A Berkeley View of Cloud Computing". Tehnično poročilo št. UCB/EECS-2009-28, 10. 2. 2009. Dostopno prek: http://www.eecs.berkeley. edu/Pubs/TechRpts/2009/ EECS-2009-28.pdf (19. april 2016).

Barth, Adam, Anupam Datta, John C. Mitchell in Helen Nissenbaum. 2006. "Privacy and Contextual Integrity: Framework and Applications". Predstavljeno v okviru IEEE simpozija o varnosti in zasebnosti. Dostopno prek: https://www.andrew.cmu.edu/user/danupam/bdmn-oakland06.pdf (22. februar 2016).

Baxter, Ryan J. 2014. "Bluemix and the Internet of Things". *IBM*, 16. 7. 2014. Dostopno prek: https://developer.ibm.com/bluemix/2014/07/16/bluemix-internet-things/ (27. april 2016).

boyd, danah. 2014. *It's Complicated: The Social Lives of Networked Teens*. New Haven: Yale University Press.

Bryne, Michael. 2014. "What Is Differential Privacy?". *Motherboard*, 28. 12. 2014. Dostopno prek: http://motherboard.vice.com/read/what-is-differential-privacy (30. april 2016).

Bunn, Julian. 2012. "How Big Is a Petabyte, Exabyte, Zettabyte, or a Yottabyte?" *High Scalability*, 11. 9. 2012. Dostopno prek: http://highscalability.com/blog/2012/9/11/how-big-is-a-petabyte-exabyte-zettabyte-or-a-yottabyte.html (9. april 2016).

Cate, Fred H. 2008 "Government Data Mining: The Need for a Legal Framework". *Harvard Civil Rights-Civil Liberties Law Review* 43: 435–489. Dostopno prek: http://www.law.harvard. edu/students/orgs/crcl/vol43_2/435-490_Cate.pdf (26. februar 2016).

Cate, Fred H. in Minow Newton. 2008. "Government Data Mining". *McGraw-Hill Handbook of Homeland Security*: 1–23. Dostopno prek: http://papers.ssrn.com/sol3/papers.cfm?abstract_ id= 1156989 (26. februar 2016).

Cate, Fred H. in Viktor Mayer-Schönberger. 2012. "Notice and Consent in a World of Big Data". Predstavljeno v okviru vrha Microsoft Global Privacy Summit and Regional Privacy Dialogues: 1–23. Dostopno prek: http://download.microsoft.com/download/9/8/F/98FE20D2-FAE7-43C7-B569-C363F45C8B24/Microsoft%20Global%20Privacy%20Summit%20Report.pdf (26. februar 2016).

Cavoukian, Ann. 2011. "Privacy By Design: The 7 Foundational Principles". *Information and Privacy Commissioner*. Dostopno prek: https://www.ipc.on.ca/images/Resources/7foundationalprinciples.pdf (22. februar 2016).

Cavoukian, Ann in Jeff Jonas. 2012. "Privacy By Design in the Age of Big Data". *Information and Privacy Commissioner*. Dostopno prek: https://www.ipc.on.ca/images/ Resources/pbd-big_data.pdf (22. februar 2016).

Columbus, Louis. 2015. "Analytics, Cloud Computing Dominate Internet of Things App Developers' Plans". *Forbes*, 26. 7. 2015. Dostopno prek: http://www.forbes.com/sites/louiscolumbus/2015/07/26/analytics-cloud-computing-dominate-internet-of-things-app-developers-plans/#316e957714fc (9. april 2016).

Craig, Terence, Mary E Ludloff. 2011. *Privacy and Big Data: The Players, Regulators, and Stakeholders*. Sebastopol: O'Reilly Media.

Cvjetović, Srdjan. 2015. "Brez ustreznih varnostnih prijemov se internet stvari lahko prelevi v internet škodljivcev". *Siol.net*, 20. 11. 2015. Dostopno prek: http://siol.net/digisvet/novice/brez-ustreznih-varnostnih-prijemov-se-internet-stvari-lahko-prelevi-v-internet-skodljivcev-396425 (28. april 2016.).

--- 2016. "Plišasti medvedek s povezavo v internet? Pazite, morda razkriva preveč podatkov o vašem otroku!". *Siol.net*, 20. 11. 2015. Dostopno prek: http://siol.net/ digisvet/novice/plisasti-medvedek-s-povezavo-v-internet-pazite-morda-razkriva-prevec-podatkov-o-vasem-otroku-404650 (28. april 2016.).

Davis, Kord, Doug Patterson. 2012. *Ethics of Big Data: Balancing Risk and Innovation*. Sebastopol: O'Reilly Media.

De Capitani di Vimercati, Sabrina, Sara Foresti in Pierangela Samarati. 2012. "Managing and Accessing Data in the Cloud: Privacy Risks and Approaches". Predstavljeno v okviru

konference CRiSIS 2012: 1–9. Dostopno prek: http://spdp.di.unimi.it/papers/crisis2012.pdf (25. februar 2016).

Deibert, Ronald J. 2013. ***Black Code: Surveillance, Privacy, and the Dark Side of the Internet***. Toronto: McClelland & Stewart. Dostopno prek: Kindle.

Direktiva 95/46/ES Evropskega parlamenta in sveta o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov. 1995. Dostopno prek: https://www.ip-rs.si/fileadmin/user_upload/Pdf/razno/Direktive_E_parlamenta_in_Sveta.pdf (26. april 2016).

Dwork, Cynthia, Frank McSherry, Kobbi Nissim in Adam Smith. 2011. "Differential privacy – a primer for the perplexed." Predstavljeno v okviru Skupne UNECE/Eurostat delovne skupine o zaupnosti statističnih podatkov. Dostopno prek: http://www.unece.org/fileadmin/ DAM/stats/documents/ece/ces/ge.46/2011/26_Dwork-Smith.pdf (25. februar 2016).

European Convention on Human Rights. 1948. Dostopno prek: http://www.echr.coe.int/ Documents/Convention_ENG.pdf (27. marec 2016).

Ferenstein, Greg. 2015. ***The Age of Optimists: A Quantitative Glimpse of How Silicon Valley Will Transform Political Power and Everyday Life***. Knjiga v nastajanju, posamezna poglavja dostopna prek: https://medium.com/the-ferenstein-wire/silicon-valley-s-political-endgame-summarized-1f395785f3c1#.ncivpy14n (26. januar 2016).

Gavison, Ruth. 1980. "Privacy and the Limits of Law". *The Yale Law Journal* 89 (3): 421–471. Dostopno prek: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2060957 (8. februar 2015).

Golden, Bernard. 2015. "Amazon Opens Up About AWS Revenues". *CIO*, 12. 5. 2015. Dostopno prek: http://www.cio.com/article/2921180/cloud-computing/amazon-opens-up-about-aws-revenues.html (17. april 2016).

Goodman, Marc. 2015. ***Future Crimes: Everything Is Connected, Everyone Is Vulnerable and What We Can Do About It***. New York: Doubleday. Dostopno prek: Kindle.

Hardy, Quentin. 2012. "Rethinking Privacy in an Era of Big Data". *The New York Times*, 4. 6. 2012. Dostopno prek: http://bits.blogs.nytimes.com/ 2012/06/04/rethinking-privacy-in-an-era-of-bigdata/ (26. februar 2016).

Hill, Kashmir. 2011. "Why 'Privacy By Design' Is the New Corporate Hotness". *Forbes*, 28. 7. 2011. Dostopno prek: http://www.forbes.com/sites/kashmirhill/ 2011/07/28/why-privacy-by-design-is-the-new-corporate-hotness (26. februar 2016).

Howard, Philip N. 2015. *Pax Technica: How the Internet of Things May Set Us Free or Lock Us Up*. New Haven: Yale University Press.

"IoT Privacy, Data Protection, Information Security". 2013. *Ec.Europa.eu*: 1–9. Dostopno prek: http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=1753 (29. april 2016).

Kirkpatrick, Marshall. 2010. "Facebook's Zuckerberg Says The Age of Privacy is Over". *ReadWrite*, 9. 1. 2010. Dostopno prek: http://readwrite.com/2010/01/09/facebooks_ zuckerberg_says_the_age_of_privacy_is_ov (26. januar 2016).

Kovačič, Matej. 2000. "Zasebnost v informacijski družbi". *Teorija in praksa* 37 (6): 1019–1034.

--- 2003. *Zasebnost na internetu*. Ljubljana: Mirovni inštitut.

--- 2006. *Nadzor in zasebnost v informacijski družbi: Filozofski, sociološki, pravni in tehnični vidiki nadzora in zasebnosti na internetu*. Ljubljana: Fakulteta za družbene vede.

Kravets, David. 2016. "US House Unanimously Passed Bill Requiring Warrants for E-mail". *Ars Technica*, 27. 4. 2016. Dostopno prek: http://arstechnica.com/tech-policy/2016/04/us-house-unanimously-passed-bill-requiring-warrants-for-e-mail/ (2. maj 2016).

Lane, Julia, Victoria Stodden, Stefan Bender in Helen Nissenbaum, ur. 2014. ***Privacy, Big Data, and the Public Good: Frameworks for Engagement***. New York: Cambridge University Press. Dostopno prek: Kindle.

Lardinois, Frederic. 2013. "Google, Facebook, Dropbox, Yahoo, Microsoft, Paltalk, AOL And Apple Deny Participation In NSA PRISM Surveillance Program". *TechCrunch*, 6. 6. 2013. Dostopno prek: http://techcrunch.com/2013/06/06/google-facebook-apple-deny-participation-in-nsa-prism-program/ (28. april 2016).

Lazer, David in Ryan Kennedy. 2015. "What Can We Learn from the Epic Failure of Google Flu Trends". *Wired*, 10. 1. 2015. Dostopno prek: http://www.wired.com/2015/10/can-learn-epic-failure-google-flu-trends (9. april 2016).

Lessig, Lawrence. 2006. *Code: Version 2.0*. New York: Basic Books.

Linthicum, David. 2015. "Thank the Cloud for Making Big Data and IoT Possible". *InfoWorld*, 16. 1. 2015. Dostopno prek: http://www.infoworld.com/article/2867978/cloud-computing/ thank-the-cloud-for-making-big-data-and-internet-of-things-possible.html (9. april 2016).

Lohr, Steve. 2015. ***Data-ism: The Revolution Transforming Decision Making, Consumer Behavior, and Almost Everything Else***. New York: HarperCollins. Dostopno prek: Kindle.

Mayer-Schönberger, Viktor in Kenneth Cukier. 2013. ***Big Data: A Revolution That Will Transform How We Live, Work, and Think***. Boston: Houghton Mifflin Harcourt. Dostopno prek: Kindle.

Millard, Christopher, ur. 2013. ***Cloud Computing Law***. Oxford: Oxford University Press. Dostopno prek: Kindle.

Miller, Michael. 2015. ***The Internet of Things: How Smart TVs, Smart Cars, Smart Homes, and Smart Cities Are Changing the World***. Indianapolis: Que Publishing. Dostopno prek: Kindle.

Morozov, Evgeny. 2013. "The Real Privacy Problem". *MIT Technology Review*, 22. 10. 2013. Dostopno prek: https://www.technologyreview.com/s/520426/the-real-privacy-problem/ (25. februar 2015).

Mosco, Vincent. 2014. *To the Cloud: Big Data in a Turbulent World*. Boulder: Paradigm Publishers.

Movius, Lauren B. in Nathalie Krup. 2009. "U.S. and EU Privacy Policy: Comparison of Regulatory Approaches". *International Journal of Communication* 3: 169–187. Dostopno prek: http://ijoc.org/index.php/ijoc/article/view/ 405/305 (26. februar 2016).

Narayanan, Arvind in Vitaly Shmatikov. 2008. "Robust De-anonymization of Large Sparse Datasets" Predstavljeno v okviru IEEE simpozija o varnosti in zasebnosti. Dostopno prek: http://www.cs.utexas.edu/~shmat/shmat_oak08netflix.pdf (22. februar 2016).

Nissenbaum, Hellen. 2004. "Privacy As Contextual Integrity". *Washington Law Review* 79: 101–139. Dostopno prek: https://crypto.stanford.edu/portia/papers/RevnissenbaumDTP31.pdf (22. februar 2016).

--- 2010. Privacy *in Context: Technology, Policy, and the Integrity of Social Life*. Stanford: Stanford University Press.

--- 2011. "A Contextual Approach to Privacy Online". *Dædalus* 140 (4): 32–48. Dostopno prek: http://www.amacad.org/publications/daedalus/11_fall_nissenbaum.pdf (22. februar 2016).

O'Brien, Danny. 2014. "Data Retention Directive Invalid, says EU's Highest Court". *Electronic Frontier Foundation*, 8. 4. 2014. Dostopno prek: https://www.eff.org/deeplinks/2014/04/data-retention-violates-human-rights-says-eus-highest-court (5. 4. 2016).

Ohm, Paul. 2009. "Broken Promises of Privacy: Responding to the Surprising Faliure of Anonymization". *UCLA Law Review* 57: 1701–1777. Dostopno prek: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1450006 (25. februar 2016).

--- 2015. "Sensitive Information". *Southern California Law Review* 88: 1–55. Dostopno prek: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2501002 (25. februar 2015).

Ozer, Nicole in Chris Conley. 2010. "Cloud Computing: Storm Warning for Privacy?". Publikacija ACLU of Northern California. Dostopno prek: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1611820 (25. februar 2016).

Payton, Theresa M. in Theodor Claypoole. 2014. ***Privacy in the Age of Big Data: Recognizing Threats, Defending Your Rights, and Protecting Your Family***. Lanham: Rowman & Littlefield. Dostopno prek: Kindle.

Pentland, Alex. 2014. ***Social Physics: How Good Ideas Spread – The Lessons from a New Science***. New York: Penguin Books. Dostopno prek: Kindle.

"Personal Data: The Emergence of a New Asset Class". 2011. Pobuda Svetovnega gospodarskega foruma. Dostopno prek: http://www3.weforum.org/docs/WEF_ITTC_ PersonalDataNewAsset_Report_2011.pdf (1. maj 2016).

Porter, Christine. 2008. "De-Identified Data and Third Party Data Mining: The Risk of Reidentification of Personal Information". *Shidler Journal of Law, Commerce & Technology* 3. Dostopno prek: http://digital.law.washington.edu/dspace-law/bitstream/handle/1773.1/417/ vol5_no1_art3.pdf (25. februar 2016).

Pretz, Kathy. 2014. "Smarter Sensors: Making the Internet of Things Soar". *Special Report: The Internet of Things*, 7. 3. 2014. Dostopno prek: http://theinstitute. ieee.org/technology-focus/technology-topic/the-value-of-privacy (28. april 2016).

Reding, Viviane. 2011. "Privacy in the Cloud: Data Protection and Security in Cloud Computing". *European Commission Press Release Database*, 7. 12. 2011. Dostopno prek: http://europa.eu/rapid/press-release_SPEECH-11-859_en.htm (26. april 2016).

Rifkin, Jeremy. 2014. ***The Zero Marginal Cost Society: The Internet of Things, the Collaborative Commons, and the Eclipse of Capitalism***. New York: Palgrave Macmillan. Dostopno prek: Kindle.

Rosen, Jeffrey in Benjamin Wittes, ed. 2011. *Constitution 3.0: Freedom and Technological Change*. Washington: Brookings Institution Press.

Rozenfeld, Monica. 2014. "The Value of Privacy: Safeguarding Your Information in the Age of the Internet of Everything". *Special Report: The Internet of Things*, 7. 3. 2014. Dostopno prek: http://theinstitute.ieee.org/technology-focus/technology-topic/the-value-of-privacy (28. april 2016).

Rubinstein, Ira. 2013. "Big Data: The End of Privacy or a New Beginning?". *International Data Privacy Law*, članek št. 12–56: 1–14. Dostopno prek: http://papers.ssrn.com/sol3/ papers.cfm? abstract_id=2157659 (25. februar 2016).

Samarati, Pierangela in Sabrina De Capitani di Vimercati. 2010. "Data Protection in Outsourcing Scenarios: Issues and Directions". Predstavljeno v okviru simpozija ACM AsiaCCS 2010: 1–14. Dostopno prek http://spdp.di.unimi.it/papers/sd-asiaccs10.pdf (25. februar 2016).

Schneier, Bruce. 2006. "The Eternal Value of Privacy". *Wired*, 18. 5. 2006. Dostopno prek: http://archive.wired.com/politics/security/commentary/securitymatters/2006/05/70886 (25. februar 2016).

--- 2009. "Homomorphic Encryption Breakthrough". *Schneier on Security*, 9. 7. 2009. Dostopno prek: https://www.schneier.com/blog/archives/2009/07/homomorphic_enc.html (25. april 2016).

--- 2015. ***Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World***. New York: W. W. Norton & Company. Dostopno prek: Kindle.

Simitis, Spiros. 1987. "Reviewing Privacy In an Information Society". *University of Pennsylvania Law Review* 135 (3): 707–746. Dostopno prek: http://scholarship.law.upenn. edu/penn_law_review/ vol135/iss3/3/ (13. marec 2016).

Solove, Daniel J. 2001. "Privacy and Power: Computer Databases and Metaphors for Information Privacy". *Stanford Law Review* 53: 1393–1462. Dostopno prek: http://papers.ssrn. com/sol3/papers.cfm?abstract_id=248300 (26. februar 2016).

--- 2004. *The Digital Person: Technology and Privacy in the Information Age*. New York: New York University Press.

--- 2007. *The Future of Reputation: Gossip, Rumor, and Privacy on the Internet*. New Haven: Yale University Press.

--- 2011. *Nothing to Hide: The False Tradeoff Between Privacy and Security*. New Haven: Yale University Press.

Springer, Polly. 1999. "Sun on Privacy: 'Get Over It'". *Wired*, 26. 1. 1999. Dostopno prek: http http://archive.wired.com/politics/law/news/1999 /01/17538 (25. marec 2016).

Tanner, Adam. 2014. *What Stays in Vegas: The World of Personal Data – Lifeblood of Big Business – and the End of Privacy as We Know It*. New York: PublicAffairs.

Tapscott, Don. 2012a. "Should we ditch the idea of privacy?". *Reuters*, 11. 5. 2012. Dostopno prek: http://blogs.reuters.com/great-debate/2012/05/11/should-we-ditch-the-idea-of-privacy/ (24. april 2016).

--- 2012b. "Can we retain privacy in the era of Big Data?". *Reuters*, 16. 5. 2012. Dostopno prek: http://blogs.reuters.com/great-debate/2012/05/16/can-we-retain-privacy-in-the-era-of-big-data/ (24. april 2016).

--- 2012c. "How to resist Big Brother 2.0". *Reuters*, 17. 5. 2012. Dostopno prek: http://blogs.reuters.com/great-debate/2012/05/17/how-to-resist-big-brother-2-0/ (24. april 2016).

The Constitution of the United States of America. 1787. Dostopno prek: https://www.congress.gov/constitution-annotated/ (26. marec 2016).

"The Knowledge Effect". 2012. *Thomson Reuters*, 9. 10. 2012. Dostopno prek: http://blog.thomsonreuters.com/index.php/big-data-graphic-of-the-day/ (8. maj 2016).

"The Logic of Privacy: A New Way to Think About Computing and Personal Information". *The Economist*, 4. 1. 2007. Dostopno prek: http://www.economist.com/node/8486072 (25. marec 2016).

Thielman, Sam. 2016. "The Internet of Things: How Your TV, Car and Toys Could Spy on You". *The Guardian*, 10. 2. 2016. Dostopno prek: http://www.theguardian.com/world/2016/feb/10/internet-of-things-surveillance-smart-tv-cars-toys?CMP=fb_gu (22. februar 2016).

Thomas, Rob in Patrick McSharry. 2015. ***Big Data Revolution: What Farmers, Doctors and Insurance Agents Teach Us About Discovering Big Data Patterns***. Chichester: John Wiley and Sons. Dostopno prek: Kindle.

Ustava Republike Slovenije. 1991. Uradni list RS, št. 47/2013. Dostopno prek: https://zakonodaja.com/ustava/urs (27. marec 2016).

Vesel, Aljaž in Ajda Bevc. 2015. "Oblaka ni – so le računalniki drugih". *Dnevnik*, 19. 12. 2015. Dostopno prek: https://www.dnevnik.si/1042727166 (20. april 2016).

Walsh, Bryan. 2014. "Google's Flu Project Shows the Failings of Big Data" *Time*, 13. 3. 2014. Dostopno prek: http://time.com/23782/google-flu-trends-big-data-problems/ (9. april 2016).

Witchalis, Clint. 2013. "The Internet of Things Business Index". *The Economist*, 29. 10. 2013. Dostopno prek: http://www.economistinsights.com/analysis/internet-things-business-index (27. april 2016).

Yakowitz Bambauer, Jane R. 2011. "Tragedy of the Data Commons". *Harvard Journal of Law and Technology* 25 (1): 1–67. Dostopno prek: http://jolt.law.harvard.edu/articles/pdf/v25/25HarvJLTech1.pdf (25. februar 2016).

Završnik, Aleš in Pia Levičnik. 2014. "Zasebnost po Snowdnu: novejša pojmovanja zasebnosti in odnos javnosti do le-te v Sloveniji". *Zbornik znanstvenih razprav* LXXIV: 117–152.

Zittrain, Jonathan. 2008. *The Future of the Internet: And How to Stop It*. New York: Penguin Books.