UNIVERZA V LJUBLJANI
EKONOMSKA FAKULTETA

DIPLOMSKO DELO

INTEGRACIJA INFORMACIJSKIH SISTEMOV IN PRAVICA DO ZASEBNOSTI

Ljubljana, marec 2016 DANIEL JURMAN

IZJAVA O AVTORSTVU

Spodaj podpisani Daniel Jurman, študent Ekonomske fakultete Univerze v Ljubljani, izjavljam, da sem avtor diplomskega dela z naslovom Integracija informacijskih sistemov in pravica do zasebnosti, pripravljenega v sodelovanju s svetovalcem prof. dr. Jurijem Jakličem.

Izrecno izjavljam, da v skladu z določili Zakona o avtorski in sorodnih pravicah (Ur. l. RS, št. 21/1995 s spremembami) dovolim objavo diplomskega dela na fakultetnih spletnih straneh.

S svojim podpisom zagotavljam, da

- je predloženo besedilo rezultat izključno mojega lastnega raziskovalnega dela;
- je predloženo besedilo jezikovno korektno in tehnično pripravljeno v skladu z Navodili za izdelavo zaključnih nalog Ekonomske fakultete Univerze v Ljubljani, kar pomeni, da sem
    - poskrbel, da so dela in mnenja drugih avtorjev oziroma avtoric, ki jih uporabljam v zaključnem diplomskem delu, citirana oziroma navedena v skladu z Navodili za izdelavo zaključnih nalog Ekonomske fakultete Univerze v Ljubljani, in
    - pridobil vsa dovoljenja za uporabo avtorskih del, ki so v celoti (v pisni ali grafični obliki) uporabljena v tekstu, in sem to v besedilu tudi jasno zapisal;
- se zavedam, da je plagiatorstvo – predstavljanje tujih del (v pisni ali grafični obliki) kot mojih lastnih – kaznivo po Kazenskem zakoniku (Ur. l. RS, št. 55/2008 s spremembami);
- se zavedam posledic, ki bi jih na osnovi predloženega zaključnega diplomskega dela dokazano plagiatorstvo lahko predstavljalo za moj status na Ekonomski fakulteti Univerze v Ljubljani v skladu z relevantnim pravilnikom.

V Ljubljani, dne 15. 4. 2016 Podpis avtorja: _____

KAZALO

KAZALO SLIK

UVOD

Tako kot ima po eni strani vse večja integracija informacijskih sistemov in podatkov za posledico večjo učinkovitost delovanja organizacije in njenih članov (in s tem vsaj načeloma večjo produktivnost celote) – če sklepamo na podlagi tega, da integracija olajša dostopnost do podatkov in informacij, poenostavi in pohitri nekatere postopke (vključno s sprejemanjem informiranih odločitev na podlagi lažje dostopnih informacij oz. kombinacij le-teh) ter poveča kakovost in ažurnost podatkov – pa je po drugi strani pri načrtovanju zadevnih sprememb potrebno upoštevati vse omejitve, ki jih narekujejo zakonodaja in splošna načela povezanih človekovih pravic na področju zasebnosti in osebnega dostojanstva. Integracija informacijskih sistemov je pomembna kot del neprestanega razvoja informacijske tehnologije in obdelav podatkov, za katere v prvi vrsti pričakujemo optimizacijo procesov in postopkov (tako znotraj organizacije kot med organizacijami) in sicer v delu, ki povezuje prej ločene sisteme in podatkovne zbirke (Bhatt, 2000). Vendar pa za sabo tovrstne spremembe potegnejo precej drugih sprememb in odprejo številna nova vprašanja – predvsem v luči tega, kako se bodo (osebni) podatki v povezanem (integriranem) sistemu obnašali, kdo bo do njih imel dostop (kako se bo to razlikovalo glede na prejšnje, neintegrirano stanje), kdo jih bo lahko spreminjal ipd.

Predpostavimo lahko, da se organizacija ali družba giblje znotraj okvira, ki ima na eni strani hipotetično stanje popolnega spoštovanja vse zakonodaje, vseh omejitev in vseh človekovih pravic ne glede na kvaliteto in ažurnost podatkov ter učinkovitost obvladovanja in obdelovanja le-teh ter dostopanja do njih, na drugi skrajni strani pa je hipotetično stanje, kjer je bistvo maksimalna oz. celo popolna učinkovitost, polna dostopnost do podatkov, vseprisotnost dostopnosti do podatkov, večno hranjenje podatkov, vse to pa na račun zanemarjanja tako zakonodaje kot človekovih pravic, med katere štejemo tudi pravico do zasebnosti oz. varstva osebnih podatkov. V realnosti se organizacije gibljejo znotraj meja določenega manjšega območja, ki je od obeh hipotetičnih skrajnosti lahko precej oddaljeno, gre pa za območje, kjer je dosežen glede na vsakokratne zahteve in potrebe ustrezen kompromis med večjo učinkovitostjo ter spoštovanjem zakonodaje in načel.

Namen mojega diplomskega dela je prispevati k razumevanju tega, kaj pomenita varovanje osebnih podatkov in pravica do zasebnosti za integracijo informacijskih sistemov ter kako integracije informacijskih sistemov vplivajo na varstvo osebnih podatkov in povezane pravice. Ugotoviti poskušam okvir, znotraj katerega se lahko organizacija ali širša družba še giblje, da po eni strani ne posega v človekove pravice in ne krši zakonodaje, po drugi strani pa seveda ne ovira nenehnega izboljševanja učinkovitosti, ki je posledica neprestanega poglabljanja integracije informacijskih sistemov in podatkovnih zbirk.

Cilji diplomskega dela so spoznati vidike različnih omejitev integracij informacijskih sistemov, kot jih določajo zakonodaja, priporočila in osnovna načela na področju zasebnosti; orisati upoštevanje tega pri načrtovanju nadaljnjih integracij informacijskih

sistemov oz. različnih podatkovnih zbirk; in preučiti nekatere dosedanje primere integracij iz prakse.

Za dosego ciljev v prvem delu pregledam osnovne pojme in zakonodajo obravnavanega področja tako s pravnega kot tehničnega vidika ter zadevne pravice posameznika, v drugem orišem možne nadaljnje trende na obravnavanem področju in obravnavam načrtovanje informacijskih sistemov in integracij ob danih omejitvah, v zadnjem pa preučim izbrane primere iz prakse, njihove dobre in slabe strani ter morebitne možnosti za izboljšave v prihodnje.

V začetku je predstavljena za tematiko relevantna aktualna zakonodaja in standardi ter priporočila (s področja varstva osebnih podatkov v Sloveniji, EU in svetu). Predstavljene so nekatere pravice posameznika na področju varstva osebnih podatkov. Nadaljujem s pregledom izzivov integracij informacijskih sistemov in podatkov ter njihovih prednosti in nevarnosti ter orišem morebitne trende nadaljnjih integracij informacijskih sistemov, nato se dotaknem nekaterih načel in smernic, ki naj bi jih organizacija upoštevala pri načrtovanju sprememb na tem področju, in predstavim nekatere primere iz prakse.

V zaključku poskušam odgovoriti na vprašanje, kako daleč je še možno nadaljevanje integracij različnih informacijskih sistemov in podatkovnih zbirk, ne da bi ob tem kršili zakonodajo, pravico do zasebnosti in ostale povezane pravice ter škodili večanju učinkovitosti in produktivnosti posamezne organizacije in napredku družbe kot celote.

1 TEORETIČNA IZHODIŠČA IN OPREDELITEV POJMOV

Pomembnost varovanja osebnih podatkov in nadzora nad njihovo uporabo še nikoli ni bila tako v ospredju kot zadnja leta, za katera je značilen pospešen razvoj in prodor različnih mobilnih tehnologij in vseprisotnost različnih oblik računalnikov in drugih mobilnih naprav, ki zajemajo, hranijo, obdelujejo in posredujejo najrazličnejše podatke. Še ne tako dolgo nazaj, ko uporaba interneta in globalizacija še nista bili tako razširjeni, je bilo vprašanje integracije informacijskih sistemov v povezavi z varstvom (osebnih) podatkov nepomembno ali pa se ga nihče niti ni loteval. Za rojstvo sodobnega računalništva lahko štejemo 1940-a in 1950-a leta, ko so se pojavili prvi računalniški sistemi (Moumina & Bergin, b. l.). Vsako podjetje ali organizacija je imelo sprva svoje podatkovne zbirke, ki so bile pretežno internega značaja, zanje je bilo znano (čeravno ne vedno formalizirano), katera oseba ali osebe znotraj organizacije imajo pravico dostopa do teh podatkov in katere pravico spreminjanja le-teh, iznašanje podatkov iz organizacije pa je bilo navadno omejeno predvsem na natisnjene kopije teh podatkov. Če je šlo za iznos podatkov s konkretnim namenom v drugo, sodelujočo organizacijo, je to ponavadi lahko pomenilo, da je na drugi strani nekdo moral take podatke v njihove zbirke vnesti ročno (oz. prepisati s prejetega papirja) ali pa jih ustrezno klasificirati in uvrstiti v relevanten fascikel. Pri tem se ni nihče pretirano ukvarjal z vprašanjem, kaj se s podatki na poti od prve do druge organizacije dogaja, kdo ima do njih dostop in navsezadnje tudi to, kako se obravnava napake, do

katerih pride pri (ročnem) prenašanju podatkov iz prve v drugo podatkovno zbirko. Za pospešen razvoj informacijske tehnologije je imela nedvomno zasluge tudi t. i. hladna vojna, saj so bile na obeh straneh železne zavese prav država, vojska in obveščevalne službe ene izmed glavnih gonilnih sil pri raziskovanju novih tehnologij in odkrivanju novih možnosti, ki so jih ponujale novosti – vse seveda z namenom biti boljši od »sovražnika« in biti tehnološko pred njim. IBM se lahko, denimo, za svojo začetno veliko rast in uspeh v pomembnem delu zahvali prav ameriškim oblastem, saj je bila takrat ameriška oblast eden njihovih največjih kupcev tudi zaradi naraščajočih potreb po podatkih in obdelavi – npr. sistem socialne varnosti (angl. *social security system*) in program »New Deal« (Solove, 2001).

S pojavom informacijskih tehnologij (in v tem oziru še zlasti medsebojnega povezovanja informacijskih sistemov preko organizacijskih omrežij in kasneje globalno tudi interneta) in vse večjim zavedanjem o vrednosti osebnih podatkov in varstvu le-teh je postalo vprašanje integracije informacijskih sistemov ob upoštevanju omejitev, ki izhajajo iz naravne pravice posameznika do zasebnosti in dostojanstva, vse bolj aktualno. Poleg povezovanja informacijskih sistemov med organizacijami je pomemben dejavnik, ki prispeva k vse večji pomembnosti področja in zavedanju o pravicah tudi naraščajoča informatizacija, digitalizacija in avtomatizacija vseh aspektov naših življenj, saj je takorekoč že skoraj vsak naš korak ali aktivnost nekje zabeležen (Richards, 2013).

Med nekatere od poglavitnih motivov za različne integracije informacijskih sistemov lahko štejemo večanje učinkovitosti procesov in postopkov v organizaciji ter različne oblike sodelovanja in povezovanja med organizacijami. Ob tem sta pomembna dejavnika tudi zmanjševanje količine podvojenih podatkov tako znotraj organizacije kot med (povezanimi) organizacijami ter optimizacija hrambe podatkov in manipuliranja z njimi (Roy, 2008). V postopku integracij se organizacija večkrat sooči z dilemo, katere podatke se sme združevati in na kakšen način urediti dostope do teh podatkov (zlasti ob upoštevanju dejstva, da so bili prej podatki v ločenih zbirkah, do katerih so imeli dostope različni deležniki, po integraciji pa je to združeno v eni zbirki ali manjšem številu teh).

Na širšem področju – t. j. družbe kot celote – se kot »stranski učinek« vse večjega integriranja informacijskih sistemov pojavlja tudi vse enostavnejša možnost nadzora in prisluškovanja posameznikom bodisi s strani državnih organov bodisi na mednarodni ravni ali na ravni gospodarskega vohunjenja (angl. *industrial espionage*), (Bugging the boardroom, 2006).

1.1 Nekateri relevantni pojmi

V nadaljevanju tega poglavja sledi osnovni pregled nekaterih pojmov, ki so relevantni za obravnavano problematiko.

Podatek postane informacija, ko je povezan z ostalimi podatki. Ko torej povežemo različne množice podatkov, da ti tvorijo razumljivo celoto, je rezultat tega **informacija**. Informacija postane **znanje**, ko je ustrezno interpretirana in povezana z ostalim oz. predhodnim znanjem (Eppler, 2003).

S pojmom **masovni podatki** (angl. *big data*) označujemo velike količine tako strukturiranih kot nestrukturiranih podatkov, ki lahko prihajajo iz različnih virov, se kreirajo ali spreminjajo izredno hitro in obstajajo v velikem obsegu in v najrazličnejših formatih. Zahtevajo kompleksnejše načine obdelave, prikaza in analize v primerjavi z obdelavo klasičnih naborov podatkov. Lahko se analizirajo z namenom sprejemanja boljših odločitev in strateškega usmerjanja organizacije (What Is Big Data?, 2015).

Osebni podatek predstavlja katerokoli informacijo, ki se nanaša na določeno osebo ali na osebo, ki se jo da s pomočjo takega podatka enoznačno določiti s sklicevanjem na identifikacijsko številko ali dejavnike, ki so značilni za fizično, fiziološko, duševno, socialno idr. identiteto take osebe (Direktiva 95/46/ES o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov, Ur. l. EU L 281).

Glede na Zakon o varstvu osebnih podatkov je **zbirka osebnih podatkov** »vsak strukturiran niz podatkov, ki vsebuje vsaj en osebni podatek, ki je dostopen na podlagi meril, ki omogočajo uporabo ali združevanje podatkov, ne glede na to, ali je niz centraliziran, decentraliziran ali razpršen na funkcionalni ali geografski podlagi; strukturiran niz podatkov je niz podatkov, ki je organiziran na takšen način, da določi ali omogoči določljivost posameznika« (Zakon o varstvu osebnih podatkov, Ur. l. št. 94/2007-UPB1).

Upravljavec podatkovne zbirke je fizična ali pravna oseba, ki sam ali skupaj z drugimi določa namene in sredstva obdelave osebnih podatkov (Direktiva 95/46/ES o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov, Ur. l. EU L 281). Ne smemo ga zamešati s pojmom **skrbnika podatkovne zbirke**, kjer pa gre za delavca, ki kreira sistem podatkovne zbirke in je odgovoren za njegovo delovanje (Damij, Grad, & Jaklič, 1995).

S pojmom **podatkovni subjekt** (angl. *data subject*) razumemo posameznika, ki je predmet obdelovanih osebnih podatkov oz. na katerega se ti podatki nanašajo (Key definitions of the Data Protection Act, 2015).

Obdelava osebnih podatkov pomeni postopek ali niz postopkov, ki se izvajajo v zvezi z osebnimi podatki (bodisi z avtomatskimi sredstvi bodisi brez njih). Sem spadajo npr. vnašanje, zbiranje, zapisovanje, urejanje, shranjevanje, prilagajanje, predelava, iskanje, širjenje, kombiniranje in drugo (Direktiva 95/46/ES o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov, Ur. l. EU L 281).

Osebne podatke se lahko hrani in obdeluje le toliko časa, kolikor je potrebno za dosego namena, za katerega so bili zbrani. Namen obdelave podatkov mora biti jasno določen in znan pred začetkom zbiranja in obdelave. Če nastopi potreba, da se podatke hrani in obdeluje tudi po izteku te časovne omejitve, je potrebno take podatke anonimizirati ali psevdonimizirati. Anonimizirani podatki so vsi tisti, ki ne vsebujejo več elementov, na podlagi katerih bi se lahko ugotovilo identiteto osebe, na katero se ti podatki nanašajo. Kot taki potem niso več osebni podatki. Pri psevdonimiziranih podatkih pa gre za to, da se določene identifikatorje (kot so npr. ime, datum rojstva, spol itn.) nadomesti s psevdonimom (Agencija Evropske unije za temeljne pravice & Svet Evrope, 2014).

Pri **posredovanju osebnih podatkov** gre za razmerje med enim upravljavcem in enim uporabnikom podatkov. Uporabnik izvede vpogled ali dostop do podatkov v zbirki, teh pa ne vključi v drugo zbirko. Upravljavec mora za vsako posredovanje zagotoviti kasnejšo možnost pregleda, kateri podatki so bili posredovani, komu, kdaj in na kakšni podlagi. Če prejemnik/uporabnik podatkov te vključi v svojo zbirko, postane tudi upravljavec teh podatkov (Informacijski pooblaščenec, 2009a).

Zbirki osebnih podatkov sta **povezani**, če se določeni podatki iz ene zbirke neposredno vključijo v drugo, pri čemer se druga spremeni – poveča, ažurira ipd. (Informacijski pooblaščenec, 2009a).

Integracija informacijskih sistemov predstavlja (fizično ali funkcijsko) integracijo elementov več različnih informacijskih sistemov (tako strojne kot programske opreme) v celoto, ki kot nov oz. izboljšan sistem prinaša odjemalcu večjo vrednost kot njegovi posamični elementi. Je proces in končni rezultat tega, da se skupaj poveže različne (lahko tudi sprva nekompatibilne) podsisteme tako, da podatki vseh prej ločenih sistemov postanejo del obširnejšega (Integration, b. l.).

Sistemski integrator je podjetje (ali posameznik), ki strankam ponuja rešitve izgradnje ali nadgradnje informacijskih sistemov s kombiniranjem strojne in programske opreme različnih proizvajalcev. Sistem načrtuje, izvede in vzdržuje, določene faze pa lahko tudi prepusti zunanjim izvajalcem, ki jih koordinira (Systems Integrator, b. l.).

1.2 Zasebnost in pravica do zasebnosti

Že Splošna deklaracija človekovih pravic (Generalna skupščina Združenih narodov, 1948) v svojem 12. členu navaja:

»Nikogar se ne sme nadlegovati s samovoljnim vmešavanjem v njegovo zasebno življenje, v njegovo družino, v njegovo stanovanje ali njegovo dopisovanje in tudi ne z napadi na njegovo čast in ugled. Vsakdo ima pravico do zakonskega varstva pred takšnim vmešavanjem ali takšnimi napadi.«

Sam pojem zasebnosti ni povsem pravni termin, ampak vsebuje tudi psihološke, sociološke in politične aspekte, zato je pravico do zasebnosti v tem oziru težko definirati, ker je lahko tudi odvisna od konteksta. Lahko bi rekli, da je pravica do zasebnosti pravica do tega, da okoli sebe definiramo območje (ki vsebuje različne elemente naše osebnosti ali našega »sveta« kot so telo, dom, misli, občutke, identiteto itn.) in sami odločamo o tem, kateri deli tega območja bodo dostopni drugim, in nadziramo obseg, način in čas uporabe tako deljenih elementov. Kot pri drugih pravicah tudi tu lahko nastopi konflikt interesov, zato je potrebno vzpostavljati ustrezno ravnovesje med to pravico in ostalimi interesi, kot so denimo svoboda govora, svoboda raziskovalnega dela, pravica vedeti, varnost idr. (Onn et al., 2005).

Prvi zapis na temo pravice do zasebnosti v sodobnem času je esej »The Right to Privacy« (Pravica do zasebnosti), ki sta ga leta 1890 v Harvard Law Review objavila Samuel Warren in Louis Brandeis (1890). V eseju obravnavata pravico do zasebnosti kot »pravico biti puščen pri miru« (angl. *the right to be let alone*). Primarna teza je, da naj bi se zakonodaja na tem področju prilagajala in razvijala kot odgovor na neprestane tehnološke spremembe, ki vse bolj olajšujejo oblastem, tisku in drugim podobnim institucijam dostop do zasebnosti posameznika, ki pred takimi tehnološkimi spremembami ni bil možen in posledično obravnavan. Omenjata tudi nekatere omejitve, ki se nanašajo na pravico do zasebnosti, in predlagata kazni za kršenje pravice, hkrati pa priznavata, da bo za ta namen potrebna posodobljena zakonodaja. Čas, ko je bil napisan esej, je bil tudi čas, ko sta v vsakdanje življenje vse bolj posegala fotografija in (rumeni) tisk, ki sta omogočala poseg v zasebnost posameznika na načine, ki pred tem niso bili možni oz. izvedljivi (t. j. ločenost osebe oz. dogodka v zvezi s to osebo od načina in kraja predstavitve teh podatkov oz. njihovo pomnoženost in razširjanje neodvisno od osebe oz. dogodka).

V primeru Olmstead proti Združenim državam (Olmstead v. United States, 1928) je bilo odločeno, da prisluškovanje ne posega v ustavne pravice, saj (telefonske) žice, ki povezujejo dve lokaciji, niso del hiše obtoženega, zato četrti amandma (ki zagotavlja nedotakljivost osebne lastnine pred neupravičenimi vstopi in pregledi) ameriške ustave s tem ni bil kršen. Brandeis je kot en izmed sodnikov izrazil do odločbe odklonilno stališče, v katerem je označil pravico biti puščen pri miru kot eno najbolj obširnih pravic, ki je tudi najbolj spoštovana s strani civiliziranih ljudi. Vsak neupravičen poseg oblasti v zasebnost posameznika – ne glede na uporabljene metode – naj bi predstavljal kršitev četrtega amandmaja ameriške ustave, uporaba tako pridobljenih dokazov pa naj bi pomenila kršitev petega amandmaja (ki zagotavlja pošten sodni postopek). V nestrinjanju je tudi predvideval, da z napredkom prisluškovanje ne bo zgolj ostalo na žicah, ampak s časom spremembe prinašajo novosti, ki jih pisci ustave in amandmajev niso mogli dobesedno vnesti v besedilo, zato teh ne smemo jemati zgolj dobesedno, ampak širše – kot načela, ki veljajo za naprej ne glede na okoliščine in metode, ki se z napredkom spreminjajo (in se vse bolj oddaljujejo od klasičnega dobesednega akta kršenja pravice do zasebnosti zgolj s fizičnim vlomom v hišo in pregledom predalov oz. predmetov v njej). Odločba je bila kasneje ovržena v primeru Katz proti Združenim državam (Katz v. United States, 1967), v

katerem sta pravica do zasebnosti in preiskovanje bolje opredeljena in razširjena na vsa področja, kjer obstaja razumno pričakovanje zasebnosti (angl. *reasonable expectation of privacy*), za kar je od takrat naprej potreben sodni nalog.

Primer Griswold proti Connecticutu (Griswold v. Connecticut, 1965) je bil precedenčni primer, kjer je bilo razsojeno, da ameriška ustava ščiti pravico do zasebnosti oz. je proti temu, da se država vmešava v zasebnost posameznikov. Sodnik William O. Douglas je bil mnenja, da kljub temu, da ta pravica ni eksplicitno zapisana, je možno trditi, da »izhaja iz pokrivanja« (angl. *penumbras and emanations*) s strani ostalih pravic, zapisanih v ustavi in amandmajih. V primeru Komisija javnih služb Washingtona proti Pollaku (Public Utilities Comm'n v. Pollak, 1952) pa je sodnik Douglas med drugim dejal, da je »pravica biti puščen pri miru začetek vse svobode«[1] ter da je »pravica do zasebnosti […] močno sredstvo odvračanja tistih, ki bi želeli nadzirati, kako ljudje mislijo«[2].

V ZDA sicer velja t. i. »doktrina tretje strani« (angl. *third-party doctrine*), ki je pravno načelo, ki zagovarja, da se posamezniki, ki podatke prostovoljno oddajo tretji strani (npr. posredujejo svoje osebne podatke bankam, ponudnikom različnih storitev itn.), tako odpovedujejo pravicam iz četrtega amandmaja ameriške ustave in v tem primeru nimajo razumnega pričakovanja zasebnosti. Doktrina služi predvsem kot podlaga za zbiranje dokazov v kazenskih preiskavah, o njeni primernosti v digitalni dobi pa se vse bolj razhajajo mnenja med različnimi pravnimi strokovnjaki tudi v ZDA (Kerr, 2009).

Kljub temu, da spada zasebnost pod naravne pravice človeka (s čimer mislimo na univerzalne, neodtujljive, »od narave dane« pravice, ki niso odvisne od zakonodaje oz. naj jih ta ne bi omejevala), je smiselno reči, da že esej Pravica do zasebnosti in Splošna deklaracija človekovih pravic postavljata tudi pravni temelj za varstvo zasebnosti in posledično dostojanstva posameznika. Pravica do zasebnosti je namreč ena temeljnih pravic posameznika tudi zato, ker je osnovna pravica, pri kateri ne gre za to, da bi nekdo rad nekaj prikril, ampak predstavlja veliko vrednost za demokracijo, svobodo in človečnost (Schneier, 2009).[3] Dejstvo je, da se človek, ki živi pod vtisom, da je nadziran in opazovan (in ni nujno, da to tudi v resnici je), obnaša drugače od svobodnega človeka, saj si hote ali nehote, zavedno ali nezavedno postavlja okvire in meje v svojem obnašanju, ki niso nujno koristni zanj ali za družbo kot celoto. Ob tem je treba poudariti tudi to, da je zmotno in škodljivo prepričanje tistih, ki razmišljajo z danes že »klasičnim« načelom »če nimam ničesar za skrivati, se nimam ničesar za bati«, saj na ta način pasivno prepuščajo pravico do zasebnosti in varstva podatkov v roke nevidne oblasti (ki jo s takim stališčem kreirajo). Kardinalu Richelieu-ju pripisujejo citat »Če mi pokažete šest vrstic, ki jih je napisala roka najbolj poštenega med ljudmi, bom v njih našel nekaj, na podlagi česar ga bom lahko

[1] »The right to be let alone is indeed the beginning of all freedom.« (Public Utilities Comm'n v. Pollak, 1952)
[2] »The right of privacy […] is a powerful deterrent to any one who would control men's minds.« (Public Utilities Comm'n v. Pollak, 1952)
[3] »Privacy isn't just about having something to hide; it's a basic right that has enormous value to democracy, liberty, and our humanity.« (Schneier, 2009)

obesil.«[4] (Richelieu, b. l.). To kaže na relativnost zapisov (in včasih tudi pomembnost posameznega zapisa v smislu celotnega konteksta, saj ima lahko zbran podatek izven prvotnega konteksta ali namena popolnoma drugačno razlago ali uporabo) oz. pomeni, da je lahko prav vsak pogled, izjava, stališče ali drug zapis uporabljen na kakršenkoli način – v skrajnem primeru seveda, da se nekoga za nekaj obtoži ali mu pripiše določene lastnosti, ki ga diskreditirajo ali uničijo oz. se to posredno prenese na celotno družbo. Zasebnost oz. pravica do zasebnosti nas ščiti pred subjekti na poziciji moči (ki je lahko formalna ali pa izvedena kot posledica tega, da ima nekdo dostop do ogromne količine uporabnih podatkov), ki imajo lahko tendenco zlorabljanja te pozicije (oblasti in režimi lahko spreminjajo koncept tega, kaj je v danem trenutku »prav« in kaj »narobe«, posledično pa lahko zlorabijo prav vse v preteklosti zbrane informacije, kot se jim zdi ustrezno, zato je v vsakem trenutku potreben nadzor nad zbiranjem, obdelovanjem in hranjenjem osebnih podatkov). Zasebnost je tudi, kot navaja Bruce Schneier (2006), »osnovna človeška potreba«. Tudi Edward Snowden je podobnega mnenja glede tega in pravi: »Zatrjevanje, da ti je vseeno glede pravice do zasebnosti, ker nimaš ničesar skriti, je enako, kot da bi dejal, da ti je vseeno za svobodo govora, ker nimaš ničesar povedati«[5].

Stevens (2009) trdi, da je »ničesar za skrivati, ničesar za bati« mit oz. trojanski konj, ki ga poganjajo tisti, ki ne morejo ustrezno argumentirati svojih shem nadzora, podatkovnih zbirk in napadov na zasebnost, in ki temelji na nekaterih napačnih predpostavkah, kot so:

- kontinuiteta: sistem bo večkrat preživel dlje od njegovih ustvarjalcev in snovalcev, ki v danem trenutku niso predvideli, da se bodo njegove sposobnosti lahko v prihodnosti (saj je vsaka oblast ali korporacija podvržena spremembam vodstva in politike, ki jih je nemogoče predvideti vnaprej) zlorabile za nepoštene namene;
- kontekst: zagovorniki trditve predpostavljajo, da je uporabljeno zgolj v kontekstu zbiranja informacij o posameznikih s strani državnih oblasti (denimo za namene izvajanja zakonodaje), s tem pa ignorirajo dejstvo, da je v informacijski dobi informacija stalno v gibanju in podvržena tudi deljenju med javnim in zasebnim sektorjem;
- nadzor: informacija bo prej ali slej deljena – skozi dogovor o deljenju podatkov, z združevanjem podatkovnih zbirk ali pa enostavno s tem, ko bo nekdo pozabil ali pustil pomnilniško napravo na javnem mestu ali drugje – in posledično ne bo več pod nadzorom;
- konsistentnost: konsistentna uporaba pravilnih informacij med vsemi avtoritetami in posamezniki – podatkovne zbirke delajo s 100 % točnimi informacijami, informacije so uporabljene v skladu z izvirnim namenom, o katerem je bilo strinjanje, vsi procesi delujejo korektno, izidi vseh subjektov v zbirki so predvidljivi – vse to je v realnosti v zadostni meri nemogoče.

[4] »If you give me six lines written by the hand of the most honest of men, I will find something in them which will hang him. « (Richelieu, b. l.)
[5] »Arguing that you don't care about the right to privacy because you have nothing to hide is no different than saying you don't care about free speech because you have nothing to say.« (Kleeman, 2015)

Solove (2011) omenja, da zagovorniki načela »ničesar nimam za skrivati« pogosto utemeljujejo svoj pogled s tem, da poudarjajo (slabe) stvari, ki jih ljudje hočejo skriti. Problem je tako predpostavka, da je bistvo zasebnosti v skrivanju slabih stvari (ali dejanj) in da se gleda na zasebnost (pravico) kot na obliko tajnosti (skrivanja nečesa slabega), s tem pa se zaradi domnevnega večanja varnosti zmanjšuje pravico do zasebnosti.

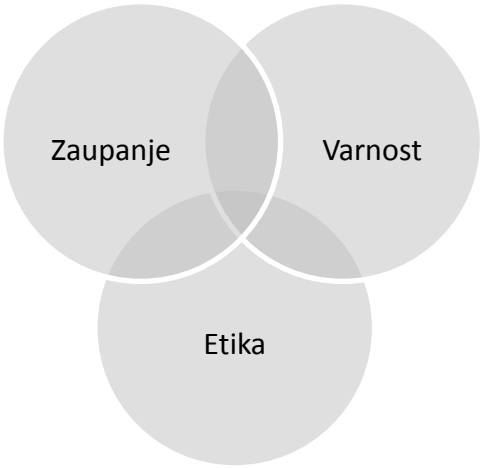
Tudi Falkvinge (2012) zavrača mit »ničesar za skrivati, ničesar za bati« in navaja štiri razloge:

- Pravila se lahko spreminjajo: Ob postavitvi sistema nadzora oz. spremljanja so bila v veljavi nesporna pravila, ki pa se kasneje zaradi različnih razlogov lahko spremenijo na slabše. Vsak tovrsten sistem naj bi bil tako že na začetku obravnavan ob predpostavki, kako ga je možno zlorabiti, če je pod nadzorom slabše oblasti.
- Posameznik ni tisti, ki določa, če se ima česa za bati: Bistveno je to, kako so podatki in zapisi o njem videni v sistemu (bodisi s strani zadolženega bodisi s sistemom avtomatskega sklepanja). Tudi predpostavka, da ima nadzor vedno dostop do popolnih in pravilnih podatkov, je v tem kontekstu pogosto napačna.
- Zakone je potrebno občasno kršiti, da družba napreduje: Z napredkom družbe kot celote se razmišljanje in določena načela, ki so v preteklosti veljala, lahko spremenijo (v luči tega pa lahko postanejo že zbrani podatki predmet zlorab, bodisi namenoma bodisi sistemsko).
- Zasebnost je osnovna človekova potreba, zato je tudi napačno vsakršno namigovanje na to, da imajo samo nepošteni potrebo po zasebnosti in skrivanju teh ali onih podatkov.

V zvezi s pravico do zasebnosti velja omeniti tudi Mednarodni pakt o državljanskih in političnih pravicah, ki ga je sprejela Generalna skupščina Združenih narodov 16. decembra 1966 (Generalna skupščina Združenih narodov, 1966), ki v svojem 17. členu med drugim prepoveduje samovoljno ali nezakonito vmešavanje v zasebnost in vsakomur zagotavlja pravico zakonskega varstva pred takim vmešavanjem ali napadi.

Uresničevanje zasebnosti, zlasti v virtualnem okolju, je možno le, če vse tri njene komponente – zaupanje, varnost in etika – nastopajo skupaj in skladno (Slika 1), (Marcella, Jr. & Stucki, 2003).

Slika 1: Infrastrukturne komponente zasebnosti



Vir: A. J. Marcella, Jr. & C. Stucki, Privacy Handbook: Guidelines, Exposures, Policy Implementation, and International Issue, 2003, str. 5.

1.3 Varstvo osebnih podatkov

Medtem ko s pojmom zasebnosti mislimo na vrednoto in pravico, ki se nanaša predvsem neposredno na posameznika oz. fizično osebo in njegovo najbližjo okolico, pa varstvo osebnih podatkov predstavlja vrsto aktivnosti, določil in ukrepov, ki se nanašajo na varovanje podatkov, ki so nekje zapisani o posamezniku (Pogosta vprašanja, 2015). Pri tem so lahko taki podatki neposredno vezani na eno lokacijo oz. imetnika (lastnika) in so na voljo samo na tej lokaciji, lahko pa so v nekem povezanem (medorganizacijskem) sistemu, pri katerem obstaja možnost dostopanja do podatkov s strani različnih oseb ali organizacij ter možnost razmnoževanja teh podatkov, zato naj bi bile med drugim določene pravice dostopa do podatkov in načini njihovega razširjanja. Tu pride tudi do ločitve med lastnikom oz. imetnikom (osebnega) podatka in osebo, na katero se podatek nanaša (podatkovni subjekt).

1.4 Informacijski pooblaščenec

V Evropski uniji (in nekaterih drugih državah po svetu) je bil vzpostavljen institut informacijskega pooblaščenca (angl. *information commissioner*). Slovenija je kot del Evropske unije morala med drugim v svoje okolje prenesti zahteve Direktive 95/46/ES, ki med drugim zahtevajo ustanovitev neodvisnega nadzornega organa na področju varstva osebnih podatkov in dostopa do informacij javnega značaja.

V Sloveniji je bil do uveljavitve Zakona o varstvu osebnih podatkov leta 2005 za področje varstva osebnih podatkov zadolžen Inšpektorat za varstvo osebnih podatkov, ki je bil organ v sestavi Ministrstva za pravosodje. Po uveljavitvi Zakona o informacijskem pooblaščencu v istem letu sta se s 1. 1. 2006 združila Inšpektorat za varstvo osebnih podatkov in Pooblaščenec za dostop do informacij javnega značaja v nov državni nadzorni organ z nazivom Informacijski pooblaščenec. Gre za samostojen in neodvisen državni organ, ki

ima različne pristojnosti na področjih varstva osebnih podatkov in dostopa do informacij javnega značaja (Zgodovina pooblaščenca, 2014).

V okviru tega izdaja informacijski pooblaščenec tudi različna mnenja, sklepe, priročnike in smernice ter periodična poročila s področja varstva osebnih podatkov in dostopa do informacij javnega značaja. Lahko bi rekli, da je vloga informacijskega pooblaščenca na področju varstva osebnih podatkov za ljudi podobna vlogi varuhov potrošniških pravic na področju trgovine: tako kot se je s povečevanjem raznolikosti in kompleksnosti produktov in trgov povečevala nepogrešljivost neodvisnega varstvenega organa za potrošnike, se je tudi z vse večjim razmahom informacijskih tehnologij in povezovanjem različnih informacijskih sistemov povečevala potreba po neodvisnem organu na področju varstva osebnih podatkov. Lahko tudi rečemo, da gre tu za »specialističnega« varuha človekovih pravic z osredotočanjem na področje varstva osebnih podatkov in dostopa do informacij javnega značaja.

1.5 Druge institucije v povezavi z varstvom osebnih podatkov

Na ravni EU obstaja **evropski nadzornik za varstvo podatkov** (angl. *European Data Protection Supervisor,* v nadaljevanju EDPS), ki je neodvisen nadzorni organ, ki zagotavlja, da evropske institucije in administracija spoštujejo pravila v zvezi z zbiranjem in obdelavo osebnih podatkov. Med pristojnosti spadajo poleg nadzorovanja obdelave osebnih podatkov in preprečevanja kršitve pravil glede zasebnosti med drugim tudi svetovanje institucijam in organom EU glede tega področja, obravnavanje pritožb in vodenje preiskav, sodelovanje z nacionalnimi organi držav EU in spremljanje novih tehnologij, ki lahko posežejo v varstvo podatkov (The EDPS Q&A, 2015).

Na podlagi resolucije, sprejete v marcu 2015, je julija 2015 Organizacija združenih narodov (oz. njen Svet za človekove pravice) prvič imenovala **Posebnega poročevalca za zasebnost** (angl. *Special Rapporteur on the Right to Privacy*). S tem dejanjem so tudi Združeni narodi dodatno priznali pravico do zasebnosti na nivoju, kot velja za preostale človekove pravice, in ji s tem dali še večjo mednarodno potrditev in zaščito (Rodriguez, 2015).

Kot prva država je Belgija jeseni 2014 imenovala **ministra (oz. državnega sekretarja) za zasebnost** (Van Eecke, 2014). Med pristojnosti njegovega resorja spada poleg zasebnosti tudi boj proti (družbenim) prevaram (angl. *social fraud*). S to potezo je nova vlada pokazala, da je zasebnost (in mdr. z njo povezane prevare) pomembna prioriteta in ne zgolj obrobna skrb.

Kot **evropski dan varstva osebnih podatkov** (angl. *Data Protection Day*) se od leta 2006 naprej obeležuje 28. januar v počastitev odprtja za podpis Konvencije 108 Sveta Evrope za varstvo posameznikov na področju avtomatskega procesiranja osebnih podatkov (dne 28. januarja 1981). Konvencija je bila podpisana s strani 43 držav članic Evropskega sveta in

je odprta za podpis s strani katerekoli druge države na svetu (Svet Evrope, 1981). Namen je bil, da se s tem dnevom posebej ozavešča ljudi o varstvu osebnih podatkov (in s tem povezanih pravicah) in dobrih praksah varstva osebnih podatkov (Data Protection Day, b. l.). Izven Evrope se dan imenuje Dan zasebnosti (angl. *Privacy Day*).

2 PREGLED RELEVANTNE ZAKONODAJE, STANDARDOV IN PRIPOROČIL V REPUBLIKI SLOVENIJI IN EVROPSKI UNIJI

Obstaja vrsta načel, standardov, zakonov, evropskih in drugih pravnih aktov, ki tako v Sloveniji kot širše opredeljujejo pravice in dolžnosti na področju varstva osebnih podatkov in zasebnosti ter kot taki omejujejo prekomerne posege v zasebnost, pretirano zbiranje in hranjenje podatkov in prekomerno združevanje podatkovnih zbirk ali sistemov. Nekateri so splošni in pokrivajo več različnih področij in panog, medtem ko so drugi specifični in veljajo predvsem za konkretne panoge ali področja. V nadaljevanju sledi oris pomembnejših dokumentov in njihovih delov, ki jih je potrebno upoštevati pri načrtovanju ali izvajanju integracij informacijskih sistemov oz. osebnih podatkov.

2.1 Ustava Republike Slovenije

Ustava Republike Slovenije (Ur. l. RS št. 33/91-I, 42/97, 66/2000, 24/03, 69/04, 68/06 in 47/13) je temeljni pravni akt na ozemlju Republike Slovenije. Ratificirana je bila 23. decembra 1991. Za varstvo osebnih podatkov neposredno najbolj relevantni so naslednji členi (razdelek II »Človekove pravice in temeljne svoboščine«):

- 15. člen, ki opredeljuje uresničevanje in omejevanje pravic;
- 16. člen, ki opredeljuje začasno razveljavitev in omejitev pravic;
- 34. člen, ki navaja, da ima vsak pravico do osebnega dostojanstva in varnosti;
- 35. člen, ki zagotavlja varstvo pravic zasebnosti in osebnostnih pravic;
- 36. člen, ki opredeljuje nedotakljivost stanovanja;
- 37. člen, ki zagotavlja varstvo tajnosti pisem in drugih občil;
- 38. člen, ki zagotavlja varstvo osebnih podatkov; prepoveduje uporabo teh podatkov v nasprotju z namenom njihovega zbiranja; definira, da zbiranje, obdelovanje, namen uporabe, nadzor in varstvo tajnosti osebnih podatkov določa zakon; in določa, da ima vsak pravico, da se seznani z zbranimi osebnimi podatki, ki se nanašajo nanj, oz. do sodnega varstva ob njihovi zlorabi.

2.2 Zakon o varstvu osebnih podatkov

Zakon o varstvu osebnih podatkov (Ur. l. št. 94/2007-UPB1) je krovni zakon s področja varstva osebnih podatkov v Republiki Sloveniji, s katerim »se določajo pravice, obveznosti, načela in ukrepi, s katerimi se preprečujejo neustavni, nezakoniti in

neupravičeni posegi v zasebnost in dostojanstvo posameznika pri obdelavi osebnih podatkov«. Zakon v začetku določa naslednja načela pri obdelavi osebnih podatkov:

- načelo zakonitosti in poštenosti obdelave osebnih podatkov;
- načelo sorazmernosti: obdelovani osebni podatki morajo biti ustrezni in po obsegu primerni glede na namene, za katere se zbirajo in obdelujejo;
- prepoved diskriminacije: zagotovitev varstva osebnih podatkov vsakemu posamezniku ne glede na njegove lastnosti.

V II. delu določa področje obdelave osebnih podatkov. Tu je zelo pomemben 20. člen z naslovom »Uporaba istega povezovalnega znaka«, ki se v prvi alineji glasi: »Pri pridobivanju osebnih podatkov iz zbirk osebnih podatkov s področja zdravstva, policije, obveščevalno-varnostne dejavnosti države, obrambe države, sodstva in državnega tožilstva ter kazenske evidence in prekrškovnih evidenc ni dovoljena uporaba istega povezovalnega znaka na način, da bi se za pridobitev osebnega podatka uporabil samo ta znak.«

V III. delu so opredeljene pravice posameznika:

- pravica do seznanitve: posameznik ima pravico do vpogleda v katalog zbirke osebnih podatkov, seznanitve s temi podatki ter informacij in pojasnil v zvezi s temi podatki in njihovim obdelovanjem;
- pravica do dopolnitve, popravka, blokiranja, izbrisa in ugovora: posameznik ima pravico od upravljavca zahtevati, da se njegove osebne podatke dopolni, popravi, blokira ali izbriše.

V tem delu so tudi opisani zadevni postopki, sodno varstvo pravic in omejitve pravic v izjemnih okoliščinah.

IV. del opisuje institucionalno varstvo osebnih podatkov (opredeljuje državni nadzorni organ za to področje, inšpekcijski nadzor in pristojnosti).

V. del opredeljuje iznos osebnih podatkov izven države. Za članice EU in države Evropskega gospodarskega prostora velja prost pretok osebnih podatkov, medtem ko je za iznos podatkov v t. i. tretje države (t. j. države, ki niso članice EU oz. Evropskega gospodarskega prostora) zahtevano, da državni nadzorni organ izvede postopek ugotavljanja ustreznosti ravni varstva osebnih podatkov v tretji državi. Ta postopek ni zahtevan, če je tretja država na posebnem seznamu držav, »za katere je ugotovljeno, da delno zagotavljajo ustrezno raven varstva osebnih podatkov, če se posredujejo tisti osebni podatki in za tiste namene, za katere je ugotovljena ustrezna raven varstva« (3. odstavek 63. člena).

VI. del opredeljuje področne ureditve in sicer: neposredno trženje, videonadzor, dostop v uradne službene oz. poslovne prostore, večstanovanjske stavbe, poslovne prostore, uporabo

biometrije, evidenco vstopov in izstopov v prostore, javne knjige in strokovni nadzor. V tem delu velja posebej izpostaviti 6. poglavje (členi 84 do 86), v katerem je opredeljeno povezovanje zbirk osebnih podatkov (iz uradnih evidenc in javnih knjig) za subjekte javnega sektorja. V 84. členu določa, da

- je zbirke osebnih podatkov iz uradnih evidenc in javnih knjig dovoljeno povezovati, če tako določa zakon;
- upravljavci osebnih podatkov, ki povezujejo dve ali več zbirk, morajo predhodno o tem obvestiti državni nadzorni organ;
- povezovanje ni dovoljeno brez predhodnega dovoljenja državnega nadzornega organa, če vsaj ena od zbirk vsebuje občutljive podatke oz. če bi tako povezovanje imelo za posledico razkritje občutljivih podatkov ali pa če je za izvedbo povezovanja potrebna uporaba istega povezovalnega znaka (razen če državni nadzorni organ ugotovi, da upravljavci osebnih podatkov zagotavljajo ustrezno varovanje osebnih podatkov).

V 85. členu prepoveduje povezovanje zbirk osebnih podatkov iz kazenske evidence in prekrškovnih evidenc z drugimi zbirkami (in povezovanje zbirk osebnih podatkov iz kazenske in prekrškovne evidence).

V VII. delu zakona so opredeljene kazenske določbe.

2.3 Zakon o Informacijskem pooblaščencu

Zakon o informacijskem pooblaščencu (Ur. l. RS št. 113/2005) je bil sprejet leta 2005. S sprejetjem tega zakona je bil ustanovljen informacijski pooblaščenec in določene so bile njegove pristojnosti in pooblastila. Zakon tudi opredeljuje imenovanje, sestavo in financiranje organa ter postopke za pridobitev informacij in dokumentov v zadevah dostopa do informacij javnega značaja. Glede na 2. člen tega zakona je informacijski pooblaščenec »samostojen in neodvisen državni organ« ter »prekrškovni organ, pristojen za nadzor nad tem zakonom in nad zakonom, ki ureja varstvo osebnih podatkov«.

2.4 Zakon o tajnih podatkih

Zakon o tajnih podatkih (Ur. l. RS št. 50/2006-UPB2) določa »skupne osnove enotnega sistema določanja, varovanja in dostopa do tajnih podatkov z delovnega področja državnih organov Republike Slovenije, ki se nanašajo na javno varnost, obrambo, zunanje zadeve ali obveščevalno in varnostno dejavnost države, ter prenehanja tajnosti takšnih podatkov« (1. člen).

Med drugim določa postopke za varnostno preverjanje posameznika, ki je v postopku pridobitve dovoljenja za dostop do tajnih podatkov, vrste osebnih podatkov, ki se pri tem zbirajo, in način njihove pridobitve, hrambo dokumentacije v zvezi z varnostnim preverjanjem in obdelovanje zadevnih osebnih podatkov.

V 12. členu določa, da »[p]ooblaščena oseba določi za tajen tudi podatek, ki je nastal z združevanjem ali povezovanjem podatkov, ki sami po sebi sicer niso tajni, če tako združeni ali povezani pomenijo podatek oziroma dokument, ki ga je treba zavarovati iz razlogov, določenih s tem zakonom«.

2.5 Zakon o elektronskih komunikacijah

Zakon o elektronskih komunikacijah (Ur. l. RS št. 109/2012, 110/13, 40/14 - ZIN-B, 54/14 - odločba Ustavnega sodišča RS št. U-I-65/13) je obširen zakon s področja elektronskih komunikacij, ki v pravni red Republike Slovenije prenaša nekatere direktive Evropskega parlamenta in Sveta s področja elektronskih komunikacij, omrežij, storitev in pravic uporabnikov pri uporabi le-teh. Za obravnavano tematiko je najbolj relevanten XII. del »Obdelava osebnih podatkov in varstvo zasebnosti elektronskih komunikacij«. Ta del »ureja obdelavo osebnih podatkov v zvezi z zagotavljanjem javnih komunikacijskih storitev v javnih komunikacijskih omrežjih, vključno z javnimi komunikacijskimi omrežji, ki podpirajo zbiranje podatkov in identifikacijske naprave« (2. odstavek 144. člena).

V 145. členu določa, da morajo izvajalci javnih komunikacijskih storitev sprejeti ustrezne organizacijske in tehnične ukrepe, ki naj zagotavljajo predvidenemu tveganju ustrezno raven varnosti in zavarovanja ter

- da ima dostop do osebnih podatkov le pooblaščeno osebje za namene, dovoljene z zakonom;
- da je zagotovljeno varovanje osebnih podatkov pred nenamernim ali nezakonitim uničenjem, spremembo in izgubo ter nepooblaščenim ali nezakonitim shranjevanjem, obdelavo, dostopom ali razkritjem;
- izvajanje varnostne politike pri obdelavi osebnih podatkov.

147. člen opredeljuje zaupnost komunikacij, ki se zagotavlja »z namenom varovanja pričakovane zasebnosti na področju uporabe elektronskih komunikacij, zagotavljanja svobode komuniciranja in svobode izražanja« in se nanaša na vsebino komunikacij, podatke o prometu in lokacijske podatke ter dejstva in okoliščine glede prekinitve povezave ali tega, da povezava ni bila vzpostavljena.

V 148. členu je določeno, katere podatke o svojih naročnikih lahko izvajalci storitev zbirajo in za kakšne namene jih lahko obdelujejo. V naslednjih členih so opredeljena tudi določila glede javnosti dostopnih imenikov uporabnikov in pravic uporabnikov glede svojih podatkov v zvezi s tem; obdelovanje in hramba podatkov o prometu; lokacijskih podatkov (tudi v primeru življenjske nevarnosti); prikaz identitete priključka; sledenja zlonamernih ali nadležnih klicev; preusmeritev klicev; uporabe piškotkov na spletnih straneh; ravnanja v primeru kršitve varstva osebnih podatkov in zakonitega prestrezanja komunikacij. Določen je tudi nadzor izvajanja določb tega poglavja s strani Agencije za komunikacijska omrežja in storitve oz. Informacijskega pooblaščenca.

Celoten XIII. del »Hramba podatkov«, ki je določal obvezno in neselektivno hrambo prometnih podatkov, pa je Ustavno sodišče RS dne 3. julija 2014 razveljavilo, saj je šlo za popolnoma nesorazmeren poseg v pravico do zasebnosti iz 38. člena Ustave RS (Odločitve Ustavnega sodišča US30439, Ur. l. RS št. 54/2014 in OdlUS XX).

2.6 Zakon o pacientovih pravicah

Zakon o pacientovih pravicah (Ur. l. RS št. 15/2008) določa pravice, ki jih ima pacient kot uporabnik zdravstvenih storitev pri vseh izvajalcih zdravstvenih storitev, postopke uveljavljanja pravic in z njimi povezane dolžnosti. V 3. členu tega zakona so navedena načela, ki se uporabljajo pri uresničevanju pravic pacientov, med katerimi je tudi načelo spoštovanja zasebnosti. V 5. členu je naveden seznam pacientovih pravic, med katerimi je tudi pravica do varstva zasebnosti in varstva osebnih podatkov, ki je podrobneje obdelana v členih od 43 do 46 (razdelek 13. »Pravica do varstva zasebnosti in varstva osebnih podatkov«) po naslednjih temah:

- zasebnost pri opravljanju zdravstvenih storitev;
- varstvo osebnih podatkov;
- varovanje poklicne skrivnosti;
- nedovoljena obdelava osebnih podatkov.

2.7 Kazenski zakonik

Kazenski zakonik (Ur. l. RS št. 50/2012-UPB2) v svojem 143. členu podrobno določa kazni za kršitve s področja zlorabe osebnih podatkov, kot so neupravičena javna objava osebnih podatkov, vdor ali nepooblaščen vstop v zbirko podatkov in kraja identitete.

2.8 Konvencija 108 Sveta Evrope o varstvu posameznika glede na avtomatsko obdelavo osebnih podatkov

Konvencija 108 Sveta Evrope je prvi mednarodni akt na temo varstva osebnih podatkov, ki so ga podpisale članice Sveta Evrope 28. januarja 1981 (Svet Evrope, 1981), v veljavo pa je stopila 1. oktobra 1985 (pogoj je bil, da je ratificirana s strani najmanj 5 podpisnikov). Slovenija je konvencijo podpisala 23. novembra 1993, ratificirala pa 27. maja 1994. Trenutno je podpisnikov 47, med katerimi sta tudi dve ne-članici Sveta Evrope in sicer Maroko in Urugvaj (Svet Evrope, 2015).

Konvencija definira varstvo osebnih podatkov kot temeljno pravico, njen namen je »zagotovitev na ozemlju vsake pogodbenice vsakemu posamezniku ne glede na državljanstvo in prebivališče spoštovanje njegovih pravic in temeljnih svoboščin in v tem okviru še posebej spoštovanje pravice do zasebnosti glede na avtomatsko obdelavo osebnih podatkov, ki se nanašajo nanj« (Svet Evrope, 1981). Med drugim vsebuje definicije in

določila o kakovosti osebnih podatkov, ki se avtomatsko obdelujejo, o posebnih vrstah podatkov, ki se ne smejo avtomatsko obdelovati (t. i. občutljivih osebnih podatkov, kot so npr. rasno poreklo, politična, verska ali druga prepričanja ipd.), o zavarovanju in zaščiti podatkov, o dodatnih ukrepih varstva posameznikov, izjemah in omejitvah ter sankcijah in pravnih sredstvih, postavlja pa tudi smernice o prenosu podatkov čez meje in sodelovanju med pogodbenicami.

2.9 Direktiva Evropskega parlamenta in Sveta 95/46/ES o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov

Direktiva EU pomeni pravni akt na ravni EU, s katerim so določeni cilji, ki jih morajo uresničevati države, članice EU, in rok, do katerega morajo biti nacionalne zakonodaje usklajene z njimi. Načini, na katerega bodo ti cilji uresničevani, so prepuščeni posameznim državam članicam, ki morajo na ustrezen način prenesti vsebino direktive v lokalno pravo in uskladiti nacionalno zakonodajo s cilji direktive (Evropska komisija, 2012b).

Direktiva 95/46/ES (Ur. l. EU L 281, sprememba Uredba (ES) 1882/2003, Ur. l. EU L 284) je referenčni pravni akt na ravni EU za področje varstva osebnih podatkov, ki vzpostavlja okvir ravnovesja med ravnjo varstva zasebnosti posameznika in prostim pretokom osebnih podatkov znotraj EU in Evropskega gospodarskega prostora. Z namenom zaščite pravic in svoboščin fizičnih oseb in njihovo pravico do zasebnosti pri obdelavi osebnih podatkov postavlja stroge meje glede zbiranja in uporabe osebnih podatkov ter zahteva vzpostavitev neodvisnega organa (pri nas je to informacijski pooblaščenec) za varstvo teh podatkov v državah članicah. Direktiva se uporablja za obdelavo osebnih podatkov z avtomatskimi sredstvi in podatkov, ki so vsebovani v zbirkah, ki niso avtomatske.

Vodilna načela, ki določajo zakonitost obdelave osebnih podatkov (Povzetki zakonodaje EU, 2011), zadevajo:

- kakovost podatkov: podatki morajo biti točni in ažurni, zbrani in obdelani zakonito in pošteno ter za točno določene, izrecne in zakonite namene;
- zakonitost obdelave podatkov: zahtevana je nedvoumna privolitev posameznika glede obdelovanja njegovih osebnih podatkov;
- posebne vrste obdelave: prepoveduje se obdelave, ki imajo potencial zlorab, npr. rasni ali etnični izvor, politično in drugo prepričanje, zdravje itn.;
- informacije o posameznikih, na katere se nanaša obdelava: upravljavec mora posamezniku zagotoviti določene informacije o upravljavcu, namenu obdelave, prejemnikih itn.;
- pravica do dostopa do podatkov posameznika, na katerega se nanašajo podatki;
- pravica do ugovora posameznika na obdelavo podatkov, ki se nanašajo nanj;

- zaupnost in varnost obdelave podatkov: opredelitev odgovornosti in dolžnosti upravljavca;
- uradno obveščanje nadzornega organa o obdelavi podatkov s strani upravljavca;
- izjeme in omejitve teh pravic zaradi potrebe državne in javne varnosti, obrambe, pregona kaznivih dejanj ipd.

V 7. členu te direktive so opredeljena merila za zakonitost obdelave podatkov, kot so:

- privolitev posameznika v obdelavo njegovih podatkov;
- potrebnost obdelave osebnih podatkov za izvajanje pogodbe ali ukrepov, ki zadevajo posameznika;
- potrebnost obdelave za skladnost z zakonsko obveznostjo za upravljavca;
- potrebnost obdelave za varstvo življenjskih interesov posameznikov, na katere se nanašajo podatki;
- potrebnost obdelave za izvajanje nalog v javnem interesu ali pri izvrševanju javne oblasti;
- potrebnost obdelave zaradi zakonitih interesov.

V Oddelku V so v 12. členu opredeljene pravice posameznika do dostopa do podatkov, ki nalagajo državam članicam, da morajo vsakemu posamezniku, na katerega se nanašajo osebni podatki, jamčiti pravico, da od upravljavca pridobi:

- potrditev tega, ali se podatki v zvezi z njim obdelujejo, in informacije o namenih obdelave, vrste podatkov in njihovih prejemnikov;
- odgovor o osebnih podatkih v obdelavi in vseh informacijah njihovega vira;
- informacije o logiki, ki je zajeta v vse avtomatske obdelave podatkov, vsaj pri avtomatiziranih odločitvah (kot so definirane v 15. členu);
- zahteva popravke, izbris ali blokiranje podatkov;
- uradno obvestilo tretjim strankam o vseh popravkih, izbrisih ali blokiranjih.

14. člen opredeljuje pravice posameznika, na katerega se nanašajo osebni podatki, do ugovora. Poglavje IV (25. in 26. člen) opredeljuje prenos osebnih podatkov v tretje države. To področje je z vse večjo globalizacijo poslovanja (in rastjo online storitev, ki vse bolj brišejo meje med državami) v zadnjih letih postalo še zlasti aktualno.

V 28. členu zahteva vzpostavitev neodvisnega nadzornega organa in delovne skupine za področje varstva posameznikov pri obdelavi osebnih podatkov v skladu s to direktivo. Točka 3 tega člena opredeljuje, da se nadzornemu organu podeli predvsem naslednje naloge:

- »preiskovalna pooblastila, kakršna so pooblastila za dostop do podatkov, ki sestavljajo vsebino postopkov obdelave, in pooblastila za zbiranje vseh informacij, ki so potrebne za izvajanje njegovih nadzornih nalog,
- učinkovita pooblastila za posredovanje, kakršna so npr. dajanje mnenj pred izvajanjem postopkov obdelave v skladu s členom 20 in zagotavljanje ustrezne objave takih mnenj, odrejanje blokiranja, izbrisa ali uničenja podatkov, naložitev začasne ali dokončne prepovedi obdelave, opozarjanje ali opominjanje upravljavca ali napotitev zadeve v nacionalne parlamente ali druge politične institucije,
- pooblastila za sodelovanje v sodnih postopkih, kadar so kršene nacionalne določbe, sprejete v skladu s to direktivo, ali za seznanitev sodnih organov s temi kršitvami.«

2.10 Ostali zadevni pravni akti in reforma zakonodaje varstva podatkov v EU

Listina Evropske unije o temeljnih pravicah (Ur. l. EU C 83 (2010/C 83/02)) je bila slovesno razglašena 7. decembra 2000 v Nici, pravno zavezujoča pa je postala 1. decembra 2009 z uveljavitvijo Lizbonske pogodbe (Evropska komisija, 2013b). V svojem 8. členu opredeljuje varstvo osebnih podatkov, ki postavlja tri načela:

- vsak ima pravico do varstva osebnih podatkov;
- obdelava mora biti poštena, za določen namen, na podlagi privolitve ali drugi legitimni podlagi;
- vsak ima pravico do dostopa in popravka;
- nadzor s strani neodvisnega organa.

Direktiva 2002/58/ES evropskega parlamenta in Sveta z dne 12. julija 2002 (Ur. l. EU L 201) o obdelavi osebnih podatkov in varstvu zasebnosti na področju elektronskih komunikacij (imenovana tudi Direktiva o zasebnosti in elektronskih komunikacijah) je bila sprejeta leta 2002 hkrati z novim zakonodajnim okvirom za področje elektronskih komunikacij. Pokriva področja shranjevanja prometnih podatkov, pošiljanja neželenih sporočil, uporabe indikatorjev povezanosti (t. i. piškotkov) in vključevanja podatkov v imenike (Povzetki zakonodaje EU, 2011).

Glede prenosa podatkov v tretje države sta relevantni **Odločba Komisije 2004/915/ES** z dne 27. decembra 2004 o spremembi Odločbe 2001/497/ES glede uvedbe alternativnega sklopa standardnih pogodbenih klavzul za prenos osebnih podatkov v tretje države (Ur. l. EU L 385) ter **Odločba Komisije 2001/497/ES** z dne 15. junija 2001 o standardnih pogodbenih klavzulah za prenos osebnih podatkov v tretje države v skladu z Direktivo 95/46/ES (Ur. l. EU L 181). Med drugim določata tipske pogodbene pogoje, ki jih lahko podjetja uporabljajo kot ustrezna zagotovila pri prenosu osebnih podatkov v tretje države.

Področje varstva osebnih podatkov, ki jih obdelujejo institucije in organi EU, in vzpostavitve neodvisnega nadzornega organa, ki je pristojen za nadzor uporabe teh določil

(t. j. evropskega nadzornika za varstvo podatkov), pokriva **Uredba (ES) št. 45/2001** evropskega parlamenta in Sveta z dne 18. decembra 2000 o varstvu posameznikov pri obdelavi osebnih podatkov v institucijah in organih Skupnosti in o prostem pretoku takih podatkov (Ur. l. EU L 8).

25. januarja 2012 je Evropska komisija izdala predlog za obsežno **reformo področja varovanja podatkov** (angl. *General Data Protection Regulation,* v nadaljevanju GDPR), ki je trenutno precej razdrobljeno in posledično povzroča dodatne administrativne stroške. Z reformo naj bi prihranili podjetjem 2,3 milijarde evrov na letni ravni, saj bi en pravni akt pokril sedanje razdrobljene. Nov pravni okvir za področje varstva osebnih podatkov v EU naj bi tudi okrepil zaupanje v online storitve, pravice posameznikov in njihovo informiranost o teh. Ključne spremembe v predlagani reformi so (Evropska komisija, 2012a):

- enotni skupek pravil za varovanje podatkov v celotni EU in umik nepotrebnih administrativnih zahtev;
- povečanje odgovornosti za upravljavce zbirk osebnih podatkov namesto določenih administrativnih zahtev;
- podjetja in druge organizacije morajo obvestiti nacionalni nadzorni organ o resnih kršitvah varovanja osebnih podatkov ali vdora v sistem;
- organizacije bodo imele opravka samo z enim nadzornim organom varstva podatkov v državi;
- posamezniki imajo pravico dostopa do svojih podatkov in prenosa le-teh od enega ponudnika storitev k drugemu (pravica do prenosljivosti podatkov);
- posamezniki imajo pravico izbrisa svojih podatkov, če ne obstaja več noben legitimen razlog, da se ti obdržijo (pravica biti pozabljen);
- vzpostavitev zahteve, da veljajo pravila EU tudi, če se podatki obdelujejo v tretjih državah s strani podjetij, ki operirajo na trgu EU;
- neodvisni nacionalni organi za varstvo podatkov bodo pridobili nova pooblastila za lažje uveljavljanje teh EU pravil v posameznih državah (vključno s tem, da lahko oglobijo podjetja, ki kršijo zakonodajo EU s področja varovanja podatkov);
- nova direktiva bo zahtevala uporabo splošnih načel varstva podatkov v postopkih kazenskega pregona za policijsko in sodno sodelovanje, tako pri pretoku podatkov znotraj države kot med državami.

Trenutno je ta regulacija še v postopkih pogajanj in razprav, njen sprejem pa je predviden za leto 2017. Ker gre za regulacijo in ne direktivo, to pomeni, da ima njeno sprejetje takojšen vpliv na zakonodajo vseh članic in je takoj kot zakon veljavna hkrati v vseh državah, članicah EU (Evropska unija, 2015).

2.11 Načela varnega pristana

Glede na direktivo 95/46/ES podjetja v EU ne smejo posredovati osebnih podatkov v tretje države (t. j. države izven območja EU in Evropskega gospodarskega prostora), razen če te zagotavljajo zadosten nivo zaščite (bodisi na ravni organizacije, ki se nahaja v taki državi, bodisi na ravni celotne tretje države). Glede na Zakon o varstvu osebnih podatkov je dovoljen prenos podatkov v tretje države, če so te na seznamu držav, ki zagotavljajo ustrezno raven varovanja teh podatkov (Iznos osebnih podatkov v tretje države, 2015).

Načela varnega pristana (angl. *safe harbor privacy principles*), ki so bila razvita v letih 1998–2000 (Documents and Public Comments Provided through the Duration of the Safe Harbor Negotiations, 2009), omogočajo, da nekatera podjetja oz. organizacije (t. j. tiste, ki so se zavezale tem načelom) iz ZDA poslujejo skladno z evropsko zakonodajo s področja zasebnosti. Uveljavila jih je Odločba Evropske komisije 2000/520/ES (Ur. l. EU L 215). Ta načela so:

- obvestilo: posameznik mora biti seznanjen z nameni zbiranja in uporabe podatkov;
- možnost izbire: organizacija mora posamezniku nuditi možnost izbire oz. zavrnitve razkritja podatkov;
- prenos tretji strani: tudi morebitna tretja stran mora nuditi ustrezno raven zaščite podatkov;
- varnost: organizacije morajo izvajati ustrezne ukrepe za zaščito podatkov;
- integriteta podatkov: podatki morajo biti zanesljivi in točni ter ustrezati namenu, za katerega bodo uporabljeni;
- dostop: posameznik mora imeti dostop do svojih podatkov in možnost popravka, spremembe ali izbrisa;
- izvajanje: vzpostavljeni morajo biti ustrezni mehanizmi izvajanja pravil.

Sodišče Evropske unije je v oktobru 2015 v primeru »Max Schrems proti irskemu informacijskemu pooblaščencu« (Maximillian Schrems v. Data Protection Commissioner, 2015) razglasilo, da je odločba 2000/520/ES (in s tem načela varnega pristana) neveljavna. Podjetja so imela po tem tri mesece časa, da se prilagodijo novim razmeram, v pripravi pa je bila že nova verzija načel (t. i. *Safe Harbor 2.0*). V nasprotnem primeru (t. j. če se zainteresirane strani v predvidenem roku ne bi uspele dogovoriti o novi podlagi za izmenjavo (osebnih) podatkov med Evropo in ZDA) bi bile take organizacije v prekršku. V začetku februarja 2016, torej v okviru predvidenega roka, je bil tako dosežen sporazum, imenovan »ščit zasebnosti« (angl. *privacy shield*), ki pa v tem trenutku potrebuje še obširnejšo pravno analizo (Evropska komisija, 2016).

Evropska komisija se je že pred tem zavedala, da načela varnega pristana niso več zadovoljiva in bi jih bilo potrebno revidirati (Evropska komisija, 2013a). Med drugim so v dokumentu navedli, da državni organi za varstvo podatkov nekaterih članic EU kritizirajo

preveliko splošnost teh načel in preveliko zanašanje na samocertificiranje in samoregulacijo (prostovoljno) zavezanih organizacij ter da jih bo potrebno revidirati v novem kontekstu glede na porast količine pretoka podatkov v zadnjih letih, kritično pomembnost tega pretoka za gospodarsko sodelovanje in gospodarsko rast, strmo rast števila podjetij v ZDA, ki so zavezana tem načelom, in glede na nova razkrita dejstva o izvajanju množičnega nadzora in prisluhov s strani ZDA oz. njihovih pristojnih agencij ali partnerjev.

V skrajnem primeru bi se lahko pojavila tudi zahteva, da morajo biti (osebni) podatki o evropskih subjektih hranjeni izključno na strežnikih, ki se nahajajo znotraj ozemlja EU oz. Evropskega gospodarskega prostora. Podobno potezo je z novim zakonom (t. i. zakon o lokalizaciji podatkov), ki je stopil v veljavo 1. septembra 2015, uveljavila Ruska federacija (Priebe & Tomaszewski, 2015). Nova zakonodaja zahteva, da se osebni podatki o ruskih državljanih hranijo in obdelujejo na strežnikih na ozemlju Ruske federacije. Avgusta je vlada izdala podrobnejša pojasnila (Blagov, 2015), kjer med drugim navajajo, da je lokalna hramba podatkov obvezna le za tiste osebne podatke, ki se spremenijo ali dodajo po 1. septembru 2015 (in so namerno zbrani kot del aktivnosti zbiranja osebnih podatkov), ne pa tudi za obstoječe oz. predhodno zbrane, prav tako v to zahtevo niso zajeti osebni podatki, ki se izmenjujejo za namene izvajanja (mednarodnih) poslovnih odnosov (npr. podatki na pogodbah poslovnih partnerjev, raznih naročilih, turističnih aranžmajih ipd.). Poudariti pa velja, da je v praksi lahko (vsaj pri nekaterih večjih ponudnikih) geografsko (politično) ločevanje hrambe podatkov težje izvedljivo brez večjih posegov v arhitekturo omrežja ponudnika, saj imajo ti lahko omrežje globalno optimizirano tako, da se podatki zrcalijo med različnimi lokacijami po svetu z namenom zagotavljanja hitrejšega dostopa do storitev in podatkov različnim uporabnikom na različnih lokacijah po svetu, ali pa celo za ta namen uporabljajo storitve tretjih strani (kot so npr. omrežja za dostavo vsebin, angl. *content delivery networks*) oz. uporabljajo oddaljene lokacije (na različnih kontinentih) zgolj z namenom izdelave varnostnih kopij (angl. *backups*) na oddaljenih lokacijah.

2.12 Načela kakovosti osebnih podatkov

Načela kakovosti osebnih podatkov v zvezi z varstvom osebnih podatkov mora upravljavec zagotavljati skozi vse postopke obdelave. Med ta načela spadajo (Agencija Evropske unije za temeljne pravice & Svet Evrope, 2014):

- načelo sorazmernosti: podatki morajo biti ustrezni in ne pretirani glede na namene, za katere so bili zbrani in se obdelujejo. V zvezi s tem je včasih v obdelavah smiselno uporabljati psevdonimizirane podatke;
- načelo točnosti: upravljavec lahko uporablja podatke samo, če z razumno gotovostjo poskrbi, da so ti podatki točni in ažurni;
- načelo omejene hrambe: v obliki, ki dopušča identifikacijo posameznikov, na katere se podatki nanašajo, se lahko podatki hranijo le toliko časa, kolikor je potrebno za dosego namenov, za katere so bili zbrani in se obdelujejo. Po izteku roka je podatke možno

hraniti samo, če so bili podvrženi anonimizaciji ali psevdonimizaciji (npr. za namene zgodovinskih, statističnih ali znanstvenih raziskav).

3 PRAVICE POSAMEZNIKA NA PODROČJU VARSTVA OSEBNIH PODATKOV

V nadaljevanju je predstavljenih nekaj temeljnih pravic, ki zadevajo področje varstva osebnih podatkov oz. varovanja zasebnosti, ki so kot take omenjene v različnih pravnih aktih ali pa so kot načela na dobri poti, da se jih v prihodnosti tudi vpelje v ustrezno zakonodajo.

Pravica biti puščen pri miru oz. pravica do zasebnosti kot temeljna pravica na tem mestu ni posebej omenjena, saj je zaradi svoje kompleksnejše narave in pomembnosti podrobneje obravnavana z različnih aspektov kot pravica in kot koncept v poglavju 1.2.

3.1 Pravica do varstva osebnih podatkov

Pravica je kot krovna pravica tega področja omenjena v različnih pravnih aktih na različnih ravneh, med drugim:

- 12. člen Splošne deklaracije človekovih pravic Združenih narodov (Generalna skupščina Združenih narodov, 1948);
- 38. člen Ustave Republike Slovenije (Ur. l. RS št. 33/91-I, 42/97, 66/2000, 24/03, 69/04, 68/06 in 47/13);
- Zakon o varstvu osebnih podatkov (Ur. l. št. 94/2007-UPB1);
- Direktiva Evropskega parlamenta in Sveta 95/46/ES (Ur. l. EU L 281, sprememba Uredba (ES) 1882/2003, Ur. l. EU L 284);
- 8. člen Listine Evropske unije o temeljnih pravicah (Ur. l. EU C 83 (2010/C 83/02));
- Konvencija 108 Sveta Evrope (Svet Evrope, 2015).

S tem naj bi bilo zagotovljeno (pravno) varstvo osebnih podatkov vsakega posameznika, kar vključuje tudi to, da mora biti obdelava podatkov določena z zakonom, upravljavec zbirke podatkov potrebuje pisno privolitev posameznika, posameznik pa mora biti predhodno seznanjen z namenom obdelave podatkov in njihove uporabe ter s časom shranjevanja le-teh.

3.2 Pravica do seznanitve z lastnimi osebnimi podatki

Ta pravica je na ozemlju Republike Slovenije zagotovljena že v 3 odstavku 38. člena Ustave Republike Slovenije, podrobneje pa opredeljena v 30. členu Zakona o varstvu osebnih podatkov, kjer je določeno, da mora upravljavec posamezniku na njegovo zahtevo:

- omogočiti vpogled v katalog zbirk osebnih podatkov;
- potrditi, ali se podatki obdelujejo, ter omogočiti vpogled in njihovo prepisovanje oz. kopiranje;
- posredovati seznam uporabnikov, ki so jim bili podatki posredovani, vključno s časom in namenom posredovanja;
- dati informacijo o virih in metodi obdelave;
- dati informacijo o namenu obdelave in vrsti osebnih podatkov, vključno s potrebnimi pojasnili;
- pojasniti tehnične oz. logično-tehnične postopke odločanja, če se izvaja avtomatizirano odločanje z obdelavo teh podatkov.

3.3 Pravica do dopolnitve, popravka, blokiranja, izbrisa in ugovora

Ta pravica in postopek njenega uveljavljanja sta opredeljena v 32. in 33. členu Zakona o varstvu osebnih podatkov. Bistvo te pravice je, da mora upravljavec osebnih podatkov na zahtevo posameznika, na katerega se ti podatki nanašajo, le-te dopolniti, popraviti, blokirati ali izbrisati, če posameznik dokaže, da so nepopolni, netočni, neažurni ali so bili zbrani oz. obdelani v nasprotju z veljavno zakonodajo. Prav tako mora upravljavec obvestiti vse uporabnike teh podatkov in pogodbene obdelovalce, ki jim je posredoval te podatke, o njihovi dopolnitvi, popravku, blokiranju ali izbrisu.

3.4 Pravica biti pozabljen

Pravico biti pozabljen (angl. *the right to be forgotten*) na ozemlju Republike Slovenije delno pokriva Zakon o varstvu osebnih podatkov v svojem 32. členu (»Pravica do dopolnitve, popravka, blokiranja, izbrisa in ugovora«), ki nalaga upravljavcem osebnih podatkov, da morajo na zahtevo posameznika podatke o njem izbrisati, če je prenehal namen njihovega zbiranja oz. če se izkaže, da so bili ti zbrani nezakonito.

Vendar pa je to pravico zaradi mednarodne oz. globalne narave interneta večkrat težje univerzalno zagotavljati, prav tako je lahko v koliziji z interesi organov pregona ali obveščevalnih služb zaradi možnosti uničevanja dokazov preko njenega uveljavljanja. Posledično se je nekatera zakonodaja, ki se dotika te pravice, v zadnjih letih večkrat spremenila oz. dopolnila. Prvi odmeven aspekt v EU je bil obvezna hramba prometnih podatkov, ki jo je nalagala direktiva 2006/24/EC (Ur. l. EU L 105), za katero je 8. aprila 2014 Sodišče Evropske unije (Digital Rights Ireland Ltd v. multiple parties, 2014) razsodilo, da je neveljavna. Kmalu (3. julija 2014) je tudi Ustavno sodišče Republike Slovenije razveljavilo celoten XIII. del Zakona o elektronskih komunikacijah, ki je nalagal obvezno hrambo prometnih podatkov (Odločitve Ustavnega sodišča US30439, Ur. l. RS št. 54/2014 in OdlUS XX, 27). Odmevna je bila tudi razsodba Sodišča Evropske unije, ki je 13. maja 2014 razsodilo (Google Spain SL and Google Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, 2014), da morajo tudi spletni

iskalniki kot upravljavci osebnih podatkov na zahtevo posameznikov odstraniti podatke (povezave do njihovih podatkov), saj so odgovorni za njihovo obdelavo (ki se pojavljajo na drugih spletnih straneh, na katere kažejo iskalni rezultati) in mora biti obdelava skladna z Direktivo 95/46.

Pravica ima korenine v francoski zakonodaji, ki priznava pravico do pozabe (franc. *le droit à l'oubli*), ki omogoča, da obsojeni po tem, ko je odslužil kazen in bil rehabilitiran, ne dovoli več objave zadevnih podatkov o njegovi obsodbi in zaprtju (oz. služenju kazni), kar je ravno nasprotno kot velja v ZDA, kjer objavo takih podatkov ščiti prvi amandma z zaščito svobode govora (Rosen, 2012).

V okviru reforme zakonodaje s področja varstva podatkov v EU bo ta pravica razširjena in podrobneje določena, saj med drugim nalaga upravljavcu, da mora ob prejemu zahteve po izbrisu to posredovati tudi naprej morebitnim tretjim strankam, ki so preko tega upravljavca prišle do teh podatkov, jih hranile in obdelovale. To pomeni, da bo ena zahteva veljala tudi za povezave do teh podatkov, njihove kopije ali replikacije (Dumortier, 2012).

3.5 Pravica do prenosljivosti podatkov

Pri pravici do prenosljivosti podatkov (angl. *the right to data portability*) gre za relativno nov koncept, ki prihaja v veljavo z reformo evropske zakonodaje na področju varstva osebnih podatkov. Ta pravica bo omogočala, da ima posameznik, na katerega se podatki nanašajo, možnost pridobitve kopije teh podatkov in možnost, da te podatke prenese iz enega sistema v drugega, npr. od enega ponudnika družabnega omrežja do drugega (Dumortier, 2012). Glede na osnutek reforme je pravica omejena na osebne podatke, ki so obdelovani v strukturiranem in splošno uporabljanem formatu. Podrobne definicije tega še ni, ob trenutni pa bi se lahko ponudniki izgovarjali na to, da za hrambo in obdelavo podatkov ne uporabljajo strukturiranega oz. splošno uporabljanega formata.

Na to pravico se lahko gleda tudi kot na potrošnikovo pravico, skozi katero bi svoboda izbire in prosta prenosljivost podatkov med ponudniki imela za posledico tudi večjo konkurenčnost med ponudniki storitev (Bapat, 2013) – podobno kot je to na primer pri prenosljivosti telefonskih številk ali prenosljivosti elektronskega naslova na lastni internetni domeni – saj naj bi se zmanjšala nevarnost priklenjenosti (angl. *lock-in*) uporabnika na enega ponudnika in s tem olajšalo njegovo prehajanje med različnimi ponudniki. Po drugi strani pa nasprotniki trdijo, da bi ravno uveljavljanje te pravice zmanjšalo konkurenčnost in posledično koristi za končnega uporabnika, saj naj bi veljala enako za vse nastopajoče na trgu ne glede na njihovo velikost in tržni delež – za razliko od obstoječe protimonopolne in konkurenčnostne zakonodaje, ki navadno regulira samo ponudnike s prevladujočo tržno močjo oz. deležem (Swire & Lagos, 2013).

Prvi ponudnik, ki je v svoje storitve vnesel tudi možnost prenosljivosti podatkov, je bil Google s storitvijo Google Takeout (The Data Liberation Front Delivers Google Takeout,

2011). Storitev je bila lansirana že sredi leta 2011, začetnemu naboru podatkov za izvoz so kasneje dodajali tudi druge, še vedno pa ni omogočen izvoz prav vseh podatkov, ki jih ima uporabnik pri njih. Medtem ko je strukturiran izvoz podatkov sicer omogočen, pa trenutno večje uporabnosti (razen lokalnega arhiviranja na strani uporabnika) tega še ni, saj ne obstajata interoperabilnost in standardizacija strukture podatkov med različnimi ponudniki. Ta pravica je v teoriji sicer smiselno zastavljena, vendar pa prav pomanjkanje standardov, medsebojnih dogovorov in interoperabilnosti zaenkrat postavlja njeno izvedljivost še pod vprašaj.

Ker je evropska reforma še v postopkih pogajanj, je trenutno stanje te pravice (oz. njen končni izgled) vprašljivo, saj je 18. člen predlagane regulacije, ki to podrobneje opredeljuje, Evropski parlament jeseni 2013 umaknil oz. izbrisal (Steenkamp, 2013).

4 INTEGRACIJE IN POVEZOVANJA INFORMACIJSKIH SISTEMOV, PODATKOVNIH ZBIRK IN PODATKOV

Obstajajo različne vrste integracij in povezav različnih informacijskih sistemov, podatkovnih zbirk in podatkov. Pojem integracije podatkov definira Lenzerini (2002) kot proces združevanja podatkov iz različnih virov in zagotavljanje enotnega pogleda na te podatke končnemu uporabniku. Gre za kombiniranje tehničnih in poslovnih procesov z namenom združevanja podatkov iz povsem različnih virov v smiselno in koristno informacijo (Data Integration, b. l.). Tehnologija podatkovnih zbirk je bila vpeljana v podjetjih v poznih 1960-ih letih za podporo (vsaj v začetku) razmeroma enostavnim poslovnim aplikacijam. Zaradi naraščanja uporabe aplikacij in podatkovnih repozitorijev se je pojavila tudi potreba po integraciji podatkov (Ziegler & Dittrich, 2004).

Pojem integracije sistemov je širši – Goodside (2011) ga zelo poenostavi z definicijo, da sistemska integracija predstavlja »omogočanje, da moje stvari delujejo s tvojimi«. V splošnem se lahko nanaša na integracije različnih vrst sistemov, vendar se v tem delu omejujemo na integracije informacijskih sistemov, podatkovnih zbirk in podatkov. Integracija več informacijskih sistemov ima za cilj kombiniranje izbranih sistemov, da ustvarijo novo celoto, ki se končnemu uporabniku kaže kot enoten sistem. Razloga sta dva: omogočanje integriranega dostopa do informacij skozi eno dostopno točko in kombiniranje podatkov z namenom pridobitve popolnejših informacij kot posledica združenega sistema (Ziegler & Dittrich, 2004). Glavni namen integracije je omogočiti konsistentno podporo informacijam skozi celotno organizacijo kot odgovor na dinamične izzive trgov (Bhatt, 2000).

4.1 Vidiki integracij in pristopi k integracijam

Prva namenska orodja za integracijo podatkov so se pojavila v začetku 1990-ih let. Temeljila so na tehnologiji ekstrakcije, preoblikovanja in nalaganja podatkov (angl.

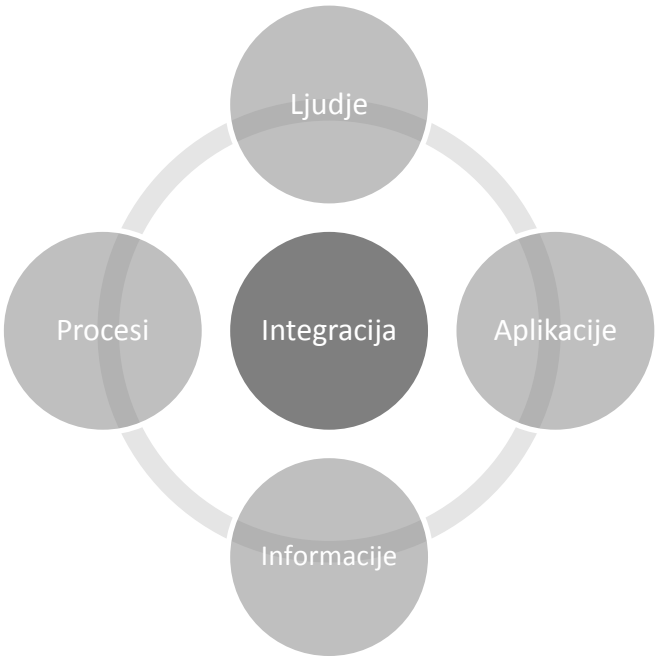
extract, transform, load, v nadaljevanju ETL), kjer gre za nabiranje podatkov iz heterogenih virov, njihovo preoblikovanje v ustrezno strukturo in format ter nalaganje teh v skupni pregled, kjer lahko podatki iz takih različnih virov postanejo kompatibilni znotraj homogenega okolja. Ob tem so se pojavila tudi orodja za čiščenje in primerjanje podatkov (Howard, 2006). Med procesom ETL potekajo naslednje glavne aktivnosti, pri katerih pa ne gre vedno za striktno zaporedje teh korakov, ampak se lahko izvajajo vzporedno (Managing the Data Warehouse Environment, 2016):

- ekstrakcija: Pri tej aktivnosti gre za izbiranje podatkov, ki se jih potrebuje za nadaljnjo uporabo v drugem okolju, iz izvornega sistema oz. izvornih virov podatkov (podatkovne zbirke, datoteke, aplikacije, spletni servisi, sporočilne vrste, nestrukturirani podatki itn.). Na tej stopnji se identificira podatke, ki jih potrebujemo v končnem sistemu in jih je potrebno pridobiti (ekstrahirati) iz različnih virov. Pogosto ni možno identificirati ožjega področja oz. nabora podatkov, zato je v takem primeru potrebno pridobiti več podatkov, identifikacija relevantnih pa je izvedena kasneje. Glede na zmožnosti izvornega sistema in obliko prenosa se lahko na tej stopnji izvaja tudi že določeno preoblikovanje podatkov. Po ekstrakciji je treba podatke tudi fizično prenesti v ciljni sistem (ali vmesnega za nadaljnjo obdelavo);
- preoblikovanje: Gre za preoblikovanje podatkov iz formata oz. strukture izvornega sistema v format ali strukturo, primerno za poizvedbe in analize v končnem sistemu. Preoblikovanje podatkov je pogosto najkompleksnejši in z vidika časa, potrebnega za procesiranje, tudi najdražji del procesa, njegov razpon pa sega od enostavnih pretvorb podatkov do kompleksnejšega čiščenja podatkov (angl. *data scrubbing*), kot npr. izločanje podvojenih in nepotrebnih podatkov, standardizacija identifikatorjev in nabora vrednosti, poenotenje šifrantov, standardizacija oblik nekaterih podatkov (kot so npr. telefonske številke, naslovi, poštne številke ipd.);
- nalaganje: Podatke, za katere so bili zaključeni koraki ekstrakcije in preoblikovanja (in morebitnega čiščenja), se v zadnji fazi naloži v ciljni sistem (npr. podatkovno skladišče).

V začetku so te tehnologije omogočale predvsem integracijo strukturiranih podatkov, kasneje pa je bilo omogočeno tudi integriranje delno strukturiranih in nestrukturiranih podatkov (Ziegler & Dittrich, 2004).

Po Jhingran, Mattos in Piranesh (2002) se integracija v splošnem vrti okoli štirih komponent: ljudi, procesov, aplikacij in informacij (Slika 2). Pri vseh fazah integracije je namreč potrebno upoštevati vse te štiri komponente, saj vplivajo na integracijo in integracija vpliva nanje – poslovne procese, ki se odvijajo v organizaciji (in jih bo potrebno prilagoditi), aplikacije, ki so v uporabi v organizaciji, informacije, ki se obdelujejo v zadevnih sistemih, in navsezadnje ljudi, ki delajo s temi komponentami ali so uporabniki podatkov.

Slika 2: Vidik integracije glede na štiri osnovne komponente



Vir: A. D. Jhingran, N. Mattos, & H. Piranesh, Information integration: A research agenda, 2002, str. 556.

Jhingran et al. (2002) navajajo štiri različne oblike integracij:

- integracija skozi portal: najosnovnejša oblika, ki skupaj povezuje različne aplikacije oz. sisteme skozi enotno točno vnosa ali vpogleda (npr. preko spletnega brskalnika);
- integracija poslovnih procesov: ta oblika povezuje procese preko meja aplikacij in podjetij (npr. partnerji, vključeni v preskrbovalno verigo). Tu postanejo pomembni spletni servisi in njihove izvedenke;
- aplikacijska integracija: aplikacije, ki se dopolnjujejo ali obdelujejo sorodne postopke, komunicirajo druga z drugo, fokus pa je ponavadi na preoblikovanju podatkov in sporočilnih vrstah. Za namen prenašanja podatkov med aplikacijami je najbolj razširjen format XML (t. i. razširljivi označevalni jezik oz. angl. extensible markup language);
- informacijska integracija: gre za združevanje medsebojno dopolnjujočih se podatkov na fizičnem ali logičnem nivoju, aplikacijam pa omogoča, da dostopajo in uporabljajo vse relevantne podatke v podjetju, tudi če ti niso pod njihovim neposrednim nadzorom.

Pristopi k integraciji glede na različne arhitekturne nivoje so (Ziegler & Dittrich, 2004):

- ročna integracija: Uporabniki neposredno komunicirajo s sistemom in ročno integrirajo izbrane podatke. Pri tem imajo opravka z različnimi uporabniškimi vmesniki in poizvedbenimi jeziki;

- skupen uporabniški vmesnik: Uporabniki imajo enoten uporabniški vmesnik, ki še vedno prikazuje podatke iz različnih sistemov ločeno, integracijo pa tudi v tem primeru izvajajo uporabniki sami;
- integracija s pomočjo aplikacij: Ta pristop uporablja integracijske aplikacije, ki dostopajo do različnih virov podatkov in uporabniku prikažejo integrirane rezultate. Aplikacije je potrebno stalno nadgrajevati in dopolnjevati, da lahko dostopajo do različnih novih sistemov in formatov;
- integracija z vmesnim slojem (angl. *middleware integration*): Vmesni sloj omogoča, da lahko preko njega komunicirajo različni sistemi, ki se brez tega ne bi razumeli, vendar pa je končno integracijo podatkov še vedno potrebno izvesti ročno;
- enoten podatkovni dostop: Tu je logična integracija podatkov izvedena na nivoju dostopa do podatkov. Enoten je vpogled do podatkov, ki pa so lahko še vedno v različnih sistemih. Ker se integracija izvaja sproti, je lahko tak dostop počasen;
- skupna shramba podatkov: Tu je izvedena dejanska fizična integracija ob prenosu podatkov v novo shrambo. Prejšnji viri podatkov se lahko ukinejo ali se ohranijo. Ob ukinitvi je potrebno na nov sistem migrirati tudi obstoječe aplikacije, ob ohranitvi pa omogočiti posodabljanje podatkov med staro in novo shrambo.

Ob integraciji podatkov je treba paziti tudi na kakovost podatkov. Procesa integracije in čiščenja podatkov naj bi tako potekala kot skupni proces, programske rešitve za podporo integraciji pa naj bi vsebovale tudi funkcije, ki omogočajo kontrolo kakovosti podatkov (Ozimek, 2008).

4.1.1 Ključni izzivi, ki jih prinašajo integracije

Integracije informacijskih sistemov prinašajo s seboj raznovrstne nove izzive, s katerimi se pred tem organizacija ni nujno ukvarjala. Gre za različne dejavnike tako znotraj organizacije kot v njenem okolju, ki jih ob načrtovanju integracij in kasnejšem nadzoru ali izboljšavah ne moremo zaobiti.

Izzivi integracij informacijskih sistemov, kot jih navaja Goodside (2011), so:

- različni formati podatkov oz. morebitna konverzija podatkov. Tu sta v grobem na voljo dve možnosti:
  - pretvorba podatkov enega sistema v format drugega ali
  - strinjanje glede skupnega standarda formata podatkov (tu mora najmanj ena stran modificirati svoj sistem, da bo deloval z drugim). Ta prilagoditev ne dodaja funkcionalnosti, ampak zgolj omogoča interoperabilnost med sistemi, terja pa čas in stroške ter je povezana s tveganji;
  - omeniti pa kaže še možnost, da se med oba sistema postavi ustrezen »pretvornik« (vmesni sloj), preko katerega podatki potujejo in se pretvarjajo v vsaki strani ustrezen format. Tu je lahko problem upočasnitev delovanja procesiranja zaradi dodatnega, vmesnega člena;

- omrežje: Sistemi, ki se povezujejo, morajo med seboj komunicirati v vsem razumljivih protokolih;
- varnost: Velja princip najšibkejšega člena, zato mora najmanj ena stran prilagoditi obnašanje drugi. Varnost celotne integracije je tolikšna, kolikor je varen njen najšibkejši člen;
- učinkovitost oz. zmogljivost: Povezan sistem bo deloval tako hitro, kolikor je hiter najpočasnejši element v vseh povezanih delih (tudi tu velja princip najšibkejšega člena);
- skladnost z zakonodajo in standardi;
- (grafični) uporabniški vmesnik: Končni uporabnik naj ne bi zaznal, da je sistem sestavljen iz različnih delov, ampak mora ta delovati kot nedeljiva celota. Če ni tako, je integracija neuspešna;
- različnost podatkovnih zbirk in operacijskih sistemov: Tu lahko pride do potrebe po podobnih kompromisih kot pri različnosti formata podatkov in uporabljenih protokolov;
- število in kompleksnost točk integracije: Po načelu učinkovitega načrta naj bi bilo boljše čim manjše število točk integracije;
- vključenost deležnikov: Glede na kompleksnost integracije je smiselno v dele procesov vključiti vse relevantne deležnike, ki se jih bo sprememba dotaknila.

4.1.2 Prednosti, ki jih prinašajo integracije

Integracije informacijskih sistemov prinašajo številne prednosti, ki lahko že v sorazmerno kratkem času povrnejo stroške investicij, ki so bile potrebne za izvedbo sprememb. Pozitivni učinki integracij za posamezna podjetja, kot jih navaja Schmidt (2008), so:

- nižji stroški kot posledica zmanjšanja podvojenosti v sistemih, podatkih in poslovnih procesih;
- krajši čas uvajanja novih produktov na trg kot posledica standardizacije nivoja poslovnih storitev;
- povečevanje prihodka od prodaje ob omogočanju inovacij v posameznih poslovno-funkcijskih enotah in ohranitvi nekaterih skupnih funkcij;
- večje zadovoljstvo potrošnikov kot posledica celovitejšega pregleda nad stranko in upravljanja odnosov s strankami;
- izboljšanje kakovosti življenja in dela zaposlenih z omogočanjem dostopa do informacij, ki jih potrebujejo, ko jih potrebujejo in kjer jih potrebujejo pri svojem delu.

Ziegler in Dittrich (2004) navajata naslednje primere prednosti kot posledico integriranih informacij v podjetju:

- področje poslovnega obveščanja (angl. business intelligence, v nadaljevanju BI): integriran sistem olajša poizvedbe in izdelavo poročil o poslovnih aktivnostih,

statistične analize, sprotno analitično obdelavo podatkov (angl. online analytical processing, v nadaljevanju OLAP) in podatkovno rudarjenje (angl. data mining) z nameni predvidevanj, sprejemanj odločitev in planiranja na ravni podjetja, kar lahko znatno prispeva k povečanju konkurenčnih prednosti podjetja;

- področje upravljanja odnosov s strankami (angl. customer relationship management, v nadaljevanju CRM): Povezane informacije o strankah, trendih poslovnega okolja in trenutni prodaji so lahko med drugim koristno uporabljene za izboljšavo storitev, ki jih podjetje nudi strankam, ali celo povečanje prodaje;
- področje elektronskega trgovanja in poslovanja (angl. e-commerce, e-business): Integriran sistem omogoča lažje izvajanje različnih transakcij in storitev;
- portali za dostop do informacij (angl. *enterprise information portals*, v nadaljevanju EIP): Ti predstavljajo enotno točko dostopa do informacij v podjetju tako za zaposlene kot za stranke, poslovne partnerje in javnost.

4.1.3 Nevarnosti, ki jih prinašajo integracije

Integracije pa ne prinašajo samo koristi in prednosti za organizacijo, ampak se z njimi odpirajo tudi nekatere potencialne nevarnosti, ki so lahko posledica zlorab, neustrezne organizacije in pravic dostopa ali pa zgolj rezultat nevednosti ali nepoznavanja predpisov in zakonodaje. Nekatere izmed nevarnosti, ki jih prinašajo integracije in koncentracije podatkovnih zbirk in podatkov, kot jih navajajo Onn et al. (2005), so lahko prisotne na naslednjih področjih:

- uhajanje informacij (angl. *information leaks*): Do podatkov, ki obstajajo v digitalni obliki oz. so dostopni preko interneta, je lažje dostopati z različnih strani, zato je ob neustreznem varovanju in nadzoru dostopnosti večja verjetnost, da ti postanejo dostopni nepooblaščenim osebam;
- nekateri rezultati, ki so možni z uporabo metod podatkovnega rudarjenja (angl. data mining): Olajšano je iskanje in zbiranje določenih informacij iz različnih podatkovnih zbirk, kar je sicer prednost, vendar pa v primeru nepooblaščenega dostopa to lahko postane velik problem in zato s seboj prinaša dodatna tveganja;
- lastništvo podatkov: Lahko prihaja do razhoda v definiciji tega, kdo je lastnik podatkov: subjekt, na katerega se ti podatki nanašajo, ali tisti, ki te podatke zbira, hrani in obdeluje;
- kraja identitete: Digitalno okolje in internet olajšata potvarjanje identitete oz. izdajanje za nekoga drugega, kar lahko izvira iz nepooblaščene pridobitve podatkov ali pa ima za posledico nepooblaščeno pridobivanje informacij, nepooblaščene aktivnosti na podatkih, spremembe podatkov itn.;
- popačenje informacij (angl. distortion of information): Do popačenja pride v primeru, ko tisti, ki ima dostop do informacij, te uporablja brez pooblastila ali izven konteksta. Smiselno je trditi, da je sprememba konteksta (podatkov) tudi kršitev zasebnosti;

- kreiranje profila aktivnosti: Zbiranje različnih informacij o posamezniku skozi čas njegove aktivnosti omogoči njegovo profiliranje, kar ima lahko za posledico možnost manipuliranja s tem posameznikom;
- stalnost digitalnih informacij (angl. permanence of digital information): Predvsem v primeru, ko je shranjena nepravilna, popačena ali nelegalna informacija brez odobritve, je tako »permanentno« hranjenje informacij lahko škodljivo;
- koncentracija informacij: S kreiranjem ogromnih podatkovnih zbirk, ki hranijo podatke o ogromnem številu ljudi, se lahko moč in kontrola koncentrirata pri imetnikih teh podatkov oz. zbirk;
- izguba nadzora nad informacijami: Ta izziv je povezan z vsemi predhodno omenjenimi, izvira pa iz ločitve med subjektom, na katerega se podatki nanašajo, in lastnikom podatkovnih zbirk, ki te podatke vsebujejo (zlasti ob prenosu informacije od subjekta do zbirke in tretjih strani).

V skrajnem primeru lahko pride do sklopa aktivnosti, ki ga Clarke (1988) imenuje »dataveillance« (iz angl. *data* + *surveillance*; slovensko bi temu lahko rekli »podatkovno nadziranje«), t. j. nadzora, ki se ne izvaja s pomočjo klasičnih sistemov nadzora (kot so denimo kamere in mikrofoni), ampak na podlagi sistematične uporabe in obdelave množično zbranih osebnih podatkov. Ta je problematičen z velikega števila vidikov, od katerih sta morda najpomembnejša prav možnost (pre)nizke kvalitete zbranih podatkov v sistemu, s pomočjo katerega se »dataveillance« izvaja, in uporaba zbranih podatkov izven konteksta (in namena zbiranja).

Solove (2001) omenja dve metafori, ki zadevata možne negativne posledice koncentracije podatkov v integriranih sistemih in prevelikega zanašanja na odločanje na podlagi teh. Pri prvi je za razliko od Orwellovega »velikega brata« (t. j. avtokratske države s popolnim nadzorom nad svojimi državljani – po romanu »1984« avtorja Georgea Orwella) možen pojav velikega števila t. i. »malih bratov« (t. j. subjektov zasebnega sektorja oz. korporacij, ki imajo dostop do velike količine informacij o posameznikih, kar jim lahko ob nezadostnem nadzoru in neustrezni regulaciji omogoča nadzor nad vsemi zbranimi informacijami, možnost njihove uporabe v nelegitimne namene, iz tega izvedeno izkoriščanje tako pridobljene ekonomske moči ter manipulacije s trgom in odjemalci). Druga metafora omenja »kafkovsko« percepcijo (po romanu »Proces« avtorja Franca Kafke) problema zasebnosti: vsak zakonodajni sistem, ki izvaja odnose z ljudmi izključno skozi podatkovne zbirke oz. avtomatizirane sisteme, postane dehumaniziran in ljudi preneha tretirati kot človeška bitja. V tem kontekstu bi pomenilo, da pri odločanju nastopa popolno birokratsko zanašanje na avtomatizacijo in procese, izvedene na podlagi shranjenih podatkov, brez uporabe »zdravega razuma« človeka kot nujnega vmesnega člena, rezultati takega avtomatiziranega odločanja pa so lahko slabi oz. celo škodljivi. V splošnem je mnenja, da je problem dvoplasten, in sicer, da gre za problem (pridobljene) moči in problem (tako nastale) birokracije.

4.2 Posredovanje osebnih podatkov in povezovanje zbirk osebnih podatkov

Razlika med posredovanjem podatkov in povezovanjem zbirk podatkov je v tem, da mora uporabnik podatkov pri posredovanju vstopiti v vsako zbirko posebej, medtem ko pri povezovanju zbirk vstopi le v eno, sistem pa v ozadju poskrbi za pridobitev ali ažuriranje določenih podatkov iz drugih povezanih zbirk (Informacijski pooblaščenec, 2009a).

Po 22. členu Zakona o varstvu osebnih podatkov mora pri posredovanju osebnih podatkov upravljavec osebnih podatkov za vsako posredovanje zagotoviti, »da je mogoče pozneje ugotoviti, kateri osebni podatki so bili posredovani, komu, kdaj in na kakšni podlagi, in sicer za obdobje, ko je mogoče zakonsko varstvo pravice posameznika zaradi nedopustnega posredovanja osebnih podatkov«.

Pri povezovanju zbirk osebnih podatkov ločimo dve definiciji povezovanja (Informacijski pooblaščenec, 2009a):

- ožja definicija: sprememba določenega podatka v eni zbirki se odrazi v vseh povezanih zbirkah (samodejno oz. takoj ali na zahtevo povezane zbirke). Tovrstna integracija podatkov ima namen zagotavljati ažurnost, točnost, popolnost in zanesljivost podatkov po principu hrambe in ažuriranja na enem mestu in uporabe na več mestih;
- širša definicija: tu se podatki ne ažurirajo hkrati v vseh povezanih zbirkah, ampak samo v zbirki, v katero neposredno dostopa uporabnik podatkov (in ki lahko pridobiva podatke tudi iz drugih povezanih zbirk), in samo v času poizvedbe.

4.3 Nadaljnji trendi integracij in povezovanj

Vzporedno z nadaljevanjem razvoja informacijsko-komunikacijskih tehnologij (in s tem povezanima stalno minimizacijo uporabljenih elementov in dolgoročnim padanjem stroškov razvoja, produkcije in vzdrževanja tehnologij) potekajo tudi trendi integracij in povezovanj informacijskih sistemov, podatkovnih zbirk in podatkov, ki posegajo vse bolj tudi na področja, ki do nedavnega v tem oziru niti niso bila v ospredju.

Sem spadata med drugim internet stvari (angl. *internet of things*, v nadaljevanju IoT) in nosljivo računalništvo (angl. *wearable computing*). Pri IoT gre za to, da se različne stvari (predmete, naprave) v okolju, ki do zdaj niso bile povezane ali pa so delovale znotraj svojega ožjega sistema, poveže preko skupnega protokola (oz. priključi na internet) in se jih tako lahko spremlja, nadzira, prebira njihove podatke in senzorje ter nastavlja preko poljubne druge naprave, povezane v internet. Lahko torej rečemo, da gre tudi tu za neke vrste integracijo in sicer tako, ki posega v združevanje tudi v t. i. »fizičnem svetu«. Podobno je pri nosljivem računalništvu, le da se to nanaša na stvari, ki se jih nosi na oz. ob telesu (vključuje pa lahko tudi senzorje za različne telesne funkcije ali okolico). Pri IoT gre tako za zbiranje podatkov z različnih naprav, zato se pojavi potreba po prenosu zbranih

podatkov iz take naprave v aplikacijo ali podatkovno zbirko, ki naj bi potekala z veliko hitrostjo oz. najbolje v realnem času (Linthicum, 2015).

V povezavi z nosljivim računalništvom je (vsaj trenutno) v ospredju področje zdravstva (pa tudi telesne aktivnosti oz. rekreacije), kjer se podatki o vitalnih funkcijah osebe, ki jih nosljive naprave zberejo in producirajo, prenesejo v podatkovne zbirke, kjer se ti lahko analizirajo (in z novimi pristopi izvede tudi prediktivna analiza), kar lahko v nekaterih primerih celo rešuje življenja (Linthicum, 2015).

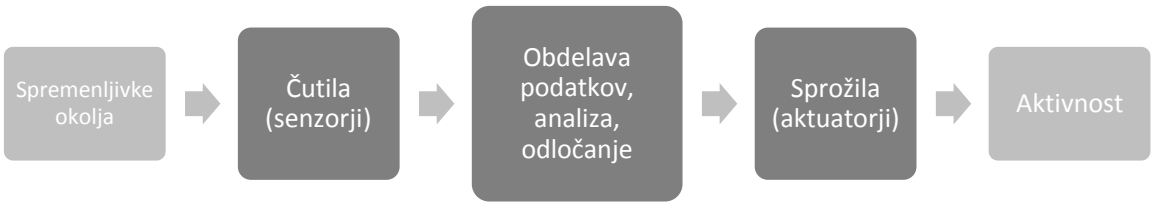
Internet stvari se znotraj hiše povezuje v t. i. »pametno hišo« in te naprej v »pametno mesto« oz. »pametno mrežo«. Vendar pa tovrstna povezljivost poleg nekaterih prednosti prinaša tudi številne nove izzive in možnosti zlorab, ki do zdaj še niso bili v zadostni meri obravnavani: Ponudnikom storitev ali trgovcem denimo predstavlja veliko vrednost možnost popolnega spremljanja (potencialnega ali obstoječega) kupca za namene neposrednega trženja – spremljanje in analiza različnih spremenljivk v okolju, povezanem s kupcem: kaj ga je vodilo k nakupni odločitvi, kaj se je predvajalo na različnih napravah, preden je bil nakup sprožen, kaj je pregledal pred nakupno odločitvijo itn. Njihov cilj je enoznačno povezati množico različnih naprav s konkretno osebo, kupcem, stranko. Zato se pojavlja problem identifikacije uporabnikov s pomočjo navzkrižnega sledenja med napravami (angl. *cross-device tracking*), (Schneier, 2016a). Na tem področju bo tako potrebno še veliko kvalitetne javne razprave, varnostne utrditve modelov povezovanja in nenazadnje tudi ustrezne regulacije. Drugi večji izziv predstavlja zadostna varnostna utrditev priključenih naprav, saj večje število na internet priključenih naprav v hiši (ali podjetju) pomeni tudi večje število potencialnih varnostnih lukenj in posledično novih možnosti napadov oz. zlorab. Naprave imajo lahko dostop do lokalnega omrežja in datotek, privzete nastavitve niso nujno varne, v uporabi so lahko gesla, ki so bodisi šibka bodisi se jih ne da spremeniti, naprava ima skrite dodatne uporabniške račune, do katerih se lahko dokopljejo nepooblaščene osebe, kamero ali mikrofon lahko aktivira ali do nje dostopa nepooblaščena oseba, mikrofon lahko stalno »posluša« konverzacijo, če je aktiviran način prepoznave govornih ukazov; navsezadnje pa se povprečen uporabnik ne bo »spomnil«, da mora občasno posodobiti programsko opremo termostata, klime, hladilnika, televizorja, kamere za varovanje dojenčka ipd., saj še pri klasičnih računalnikih in pametnih telefonih to večini predstavlja predvsem »nujno zlo«. Tu je zato v veliki meri odvisno od proizvajalcev, da pravočasno zaznajo ranljivosti in izdajo ustrezne popravke ter da vzdrževalnega procesa naprave ne zapustijo prehitro, saj imajo te navadno življenjsko dobo precej daljšo od življenjske dobe tipične programske opreme (Krebs, 2016). Clapper (2016) ocenjuje, da bodo obveščevalne službe lahko izkoriščale IoT za namene identifikacije, nadzora, spremljanja, sledenja lokacije, ciljnega rekrutiranja ali pridobitve dostopa do omrežij oz. prijavnih podatkov. Omeniti pa velja, da so tisti, ki trenutno sedijo na največjem potencialu dostopa do (tudi osebnih in občutljivih) podatkov ter njihovega zbiranja in preprodajanja, v bistvu ponudniki dostopa do interneta (ISP-ji) in ne ponudniki vsebin ali spletnih storitev kot so npr. Facebook, Google, Microsoft ipd. (čeprav se o teh največ govori in so največkrat predmet razprav o omejitvah in regulaciji zaradi velike

količine podatkov, ki jo posedujejo in obdelujejo), saj imajo prav ISP-ji možnost celotnega presečnega pogleda navad posameznih uporabnikov – za razliko od vseh prej omenjenih ponudnikov, ki pa imajo vpogled samo v del uporabnika, t. j. tisti segment, ki se nanaša na njihove storitve oz. njihovo ožjo okolico (Fung, 2016). Z združevanjem ponudnikov dostopa in njihovih storitev (kot je npr. ponujanje različnih vrst dostopa – domači internet, mobilni internet, TV in video na zahtevo, telefonija – pod isto streho) pa se njihova tozadevna moč še povečuje.

Schneier (2016b) trdi, da z internetom stvari gradimo »največjega robota na svetu«, ki ima dva bistvena dela (Slika 3):

- čutila (senzorji): zbirajo podatke o okolju z vsega sveta; sem spadajo npr. termometri in drugi merilniki spremenljivk okolja, GPS lokatorji, spremljanje gibanja, senzorji prometa, kamere, mikrofoni ipd.;
- sprožila (aktuatorji): vplivajo na okolje z izvedbo določene aktivnosti, kot npr. nastavljanje temperature prostora, posredovanje informacije o lokaciji in pridobitev najustreznejše poti glede na stanje prometa, izvajanje dostave s pomočjo brezpilotnih letalnikov, vklapljanje in izklapljanje razsvetljave, izvedba obveščanja v primeru prometne nesreče itn.

Slika 3: Internet stvari kot »največji robot na svetu«



Vir: B. Schneier, The Internet of Things Will Be the World's Biggest Robot, 2016b.

Med obema deloma je pomemben del obdelava podatkov (ki se lahko izvaja bodisi v velikih podatkovnih centrih bodisi v okviru naprave ali skupine naprav, kot npr. znotraj pametne hiše), kjer se podatki, zbrani preko senzorjev, interpretirajo, obdelajo v povezavi z obstoječimi shranjenimi in analizirajo, nato pa je preko ustreznih algoritmov izbrana določena aktivnost, ki jo nato izvedejo sprožila.

Internet stvari bo bistveno povečal skupno število različnih naprav, priključenih v omrežje, in spremenil navade uporabnikov glede uporabe le-teh. Zaradi velike vrednosti zbranih podatkov je možno, da bo prihajalo do »vojn« glede pravic dostopa do podatkov in njihove uporabe, internet stvari pa bo omogočil tudi nove možnosti vizualizacije podatkov in analiz v realnem času, prav tako bo narasla uporaba orodij za poslovno obveščanje, ki bodo

izkoriščala tako zbrane podatke (Klostermann, 2015). Vendar pa se tudi pri internetu stvari glede na trenutne trende kaže nevarnost, da bi posamezni ponudniki izvajali priklenjenost (angl. *lock-in*) nase in na svoje storitve ter namesto omogočanja interoperabilnosti zahtevali uporabo ožjega (»odobrenega« ali lastnega) nabora predmetov in storitev znotraj svojega ekosistema (Schneier, 2015). Zaradi tega bosta potrebni pravočasna in ustrezna regulacija in standardizacija, saj bi v nasprotnem primeru lahko pristali v situaciji, ki je podobna današnjemu stanju na področju storitev takojšnjega sporočanja in internetne (avdio in video) telefonije, kjer za razliko od klasične telefonije in elektronske pošte med seboj večina ponudnikov ni združljivih in uporabniki različnih ponudnikov medsebojno ne morejo neposredno komunicirati.

Tehnologija RFID (radiofrekvenčno prepoznavanje, angl. *radio-frequency identification*, poljudno imenovano tudi »brezkontaktni čip«), ki se zadnja leta vse bolj uporablja tudi v občutljivejših elementih kot so potni listi, osebni dokumenti in instrumenti plačevanja, prinaša dodatne izzive pri zaščiti dostopanja do podatkov, shranjenih na RFID čipu. Juels, Molnar in Wagner (2005) posebej izpostavljajo naslednje:

- skrivno branje: RFID čipi so podvrženi potencialnemu nepooblaščenemu skrivnemu branju na kratkih razdaljah (kar ima lahko za posledico potencialno dostopanje do osebnih podatkov, shranjenih na takem mediju);
- skrivno zasledovanje: edinstvenost vsakega dokumenta z RFID do neke mere omogoča tudi zasledovanje ali spremljanje gibanja nosilca tega elementa;
- snemanje, kopiranje, kloniranje: ta problem ni omejen samo na to tehnologijo, je pa z možnostjo branja na daljavo še toliko večji;
- prisluškovanje: gre za prisluškovanje prometu med RFID in bralnikom. Ker gre za razliko od branja za pasivno opravilo, ga je še toliko težje zaznati;
- puščanje biometričnih podatkov: zlasti pri potnih listih je problematično hranjenje biometričnih podatkov (kot so slika imetnika, prstni odtisi itn.) na RFID čipu, saj gre za izjemno občutljive podatke;
- potencialno šibka kriptografija: Tudi če obstajajo ustrezni sistemi šifriranja in zaščite podatkov, so ti lahko vedno izpostavljeni potencialnim vdorom ali poskusom vdora ali razbitja zaščite.

Eden od možnih načinov zaščite pred nepooblaščenimi dostopi do RFID je uporaba Faradayeve kletke. Gre za to, da ovitek, etui ali drug predmet, v katerem hranimo dokument z RFID, vsebuje ustrezne materiale in konfiguracijo, ki preprečujejo aktiviranje in branje, ko je ta zaprt. Kljub temu pa ta oblika zaščite ne ščiti pred potencialnim prisluškovanjem (saj je takrat dokument odprt oz. izven ovitka in ga bralnik bere).

Taylor (1986) trdi, da se bodo največji problemi informacijskih sistemov v prihodnosti (z vidika časa nastanka omenjene knjige smo zdaj že nekaj let v tej prihodnosti) vrteli okrog procesov zmanjšanja obsega in povečevanja kvalitete informacij, ki pride do končnega uporabnika. Schneier (2012) imenuje sedanje stanje odnosa med glavnimi ponudniki

internetnih storitev in njihovimi odjemalci sodobni fevdalizem. Tako kot je v srednjem veku fevdalni gospodar v zameno za določene dajatve svojim podložnikom nudil vsaj do neke mere varnost in relativno mirno življenje, je podobno pri današnjih velikih ponudnikih kot so Google, Apple, Facebook ipd. Težko se je izogniti temu, da ne »prisežeš« vsaj enemu »gospodarju« (ali pa tudi večim), noben od njih ni brez napak, občasno spremenijo pravila ali ponudbo, prav tako lahko postanejo (in s tem vsi naši podatki) predmet prevzema s strani drugega. Pri tem je lahko velik problem tudi neizbris podatkov (zlasti pri brezplačnih storitvah), saj zaradi relativno nizke cene nosilcev podatkov (ki z razvojem še naprej pada) ponudniki lahko težijo k temu, da podatkov ne izbrišejo, ampak jih hranijo »za vedno«. Ker ponavadi ne obstajajo neodvisne (zunanje) revizije postopkov brisanja podatkov, zaenkrat temelji ta del predvsem na zaupanju med ponudnikom in odjemalcem storitve.

Prihaja tudi do monetizacije zasebnosti, kar pomeni, da uporabnik v zameno za brezplačne storitve in personalizacijo preda ponudniku nekatere svoje osebne podatke oz. dovoli, da se ga na tak ali drugačen način spremlja in analizira. S tem v zvezi obstaja rek, ki pravi, da »če ne plačuješ za produkt oz. storitev, si potem ta produkt oz. storitev ti« (angl. *if you don't pay for the product, you are the product*). Pri personalizaciji (angl. *personalization*) gre za možnost prilagoditve karakteristik storitve ali produkta glede na preference in značilnosti uporabnika in njegovega vedenja v zvezi s storitvijo oz. uporabo le-te (pojma personalizacija ne smemo zamešati s podobnim pojmom prilagoditev (angl. *customization*), kjer pa je pobudnik sprememb uporabnik sam (preko nastavitev) in ne ponudnik storitev oz. avtomatski algoritem). Podlaga zanjo so lahko prav nekateri osebni podatki, po drugi strani pa lahko personalizacija omeji prenosljivost k drugemu ponudniku (primer: ponudnik videa na zahtevo zbira podatke o uporabnikovih navadah gledanja in glede na to prilagodi prikaz vmesnika, predlagane filme in serije; tako personalizirana storitev pa ni prenosljiva drugam, saj gre za lastno (angl. *proprietary*) specifiko ponudnika). Problem, ki tu nastopi, je zbiranje in preprodaja podatkov, saj so lahko podatki prodani ali posredovani tretjim stranem oz. je ponudnik predmet prevzema s strani druge organizacije (in s tem so prevzeti tudi vsi osebni podatki). Z osebnimi podatki se lahko med podjetji, ponudniki storitev, trguje kot z vsakim drugim blagom oz. surovino (Jentzsch, Preibusch, & Harasser, 2012).

Joh (2013) navaja, da se s povečevanjem nadzora s strani države pojavljajo posamezniki, ki protestirajo za zasebnost (t. i. *privacy protests*): blokirajo ali onemogočajo nadzor s strani policije zaradi namenov, ki s kriminalno dejavnostjo nimajo ničesar skupnega. Gre le za ugovarjanje vse bolj prisotnemu policijskemu ali državnemu nadzoru na vsakem koraku. V ta namen na primer prekrijejo registrske tablice na avtomobilih s plastjo, ki preprečuje fotografiranje ali meritve hitrosti, na obrazu uporabljajo poseben »make-up«, ki onemogoča prepoznavo obrazov v množici, uporabljajo navadne ali kako drugače neizsledljive telefone, uporabljajo naprave, ki najdejo in opozorijo na nadzorne kamere, plačujejo z gotovino in ne s karticami, blokirajo določene domene, strežnike ali IP naslove ipd. Razlogi za tako početje so lahko različni: politični, filozofski, osebni, paranoični …

Kot posledica razkritij o množičnem nadzoru v ZDA je bil jeseni 2015 s strani Edwarda Snowdena in sodelujočih predlagan Mednarodni sporazum o pravici do zasebnosti, zaščiti pred neprimernim nadzorom in zaščiti žvižgačev (angl. *International Treaty on the Right to Privacy, Protection Against Improper Surveillance and Protection of Whistleblowers*). Ta sporazum bi omejil ali prepovedal množično zbiranje podatkov in implementiral javni nadzor nad varnostnimi programi držav, pa tudi zahteval, da države nudijo azil žvižgačem. Zahteva uvedbo neodvisnega nacionalnega nadzornika področja z namenom zagotovitve transparentnosti in odgovornosti držav v svojih aktivnostih, povezanih z nadzorovanjem. Države podpisnice bodo morale varstvo podatkov in pravico do zasebnosti upoštevati v vseh prihodnjih programih in politikah ter okrepiti nadzor nad državnim nadzorom državljanov. Cilj je ohranitev zasebnosti kot temeljna odgovornost oblasti tudi za prihodnje generacije (Edward Snowden, Glenn Greenwald & David Miranda Call for Global Privacy Treaty, 2015).

5 NEKATERI DRUGI VIDIKI, KI JIH JE POTREBNO UPOŠTEVATI OB NAČRTOVANJU INFORMACIJSKIH SISTEMOV OZ. INTEGRACIJ

Pri načrtovanju integracij in povezovanj informacijskih sistemov, podatkovnih zbirk oz. podatkov je dobro, da se poleg zakonodaje, ki določa pravila glede varovanja osebnih podatkov in zasebnosti posameznika, upošteva še nekatere relevantne dobre prakse, načela in standarde za to področje. Pravočasno upoštevanje teh načel in vidikov lahko prihrani marsikatere nevšečnosti (ali celo to, da pridemo v navzkriž z zakonom) v prihodnosti, načrtovanje sistema, »odpornega« na prihodnje spremembe (angl. *future-proof*), torej takega, ki bo v prihodnosti potreboval ob spremembah čim manj novih naporov, pa naj bi bilo osnovno vodilo.

5.1 Načini ugotavljanja ali preverjanja identitete

Pri ugotavljanju ali preverjanju identitete gre za to, da sistem ugotovi, če je oseba, ki poskuša dostopati do podatkov, do tega upravičena, in kakšen je njen obseg pravic v zvezi s temi podatki. Glede na politiko zaščite podatkov oz. dostopa do njih delimo sisteme na naslednje skupine (Damij, Grad, & Jaklič, 1995):

- pravica do dostopa »po potrebi«: Uporabnik dobi pravico dostopanja do podatkov, ko jih potrebuje, pravica pa je omejena na natanko tiste podatke, ki jih potrebuje;
- podatki so dostopni v največji možni meri: Posameznemu uporabniku so nedostopni le tisti podatki, ki morajo biti res nedostopni, vsi ostali pa so dostopni;
- odprti pristop zaščite: Uporabniki imajo pravico dostopanja do vseh podatkov, razen do tistih, ki so eksplicitno zaščiteni;
- zaprti pristop zaščite: Uporabniki nimajo pravice dostopanja do nobenega podatka, razen do tistih, za katere imajo eksplicitno pravico.

Poznamo tri skupine metod ugotavljanja ali preverjanja identitete in sicer temeljijo na (Informacijski pooblaščenec, 2008):

- tistem, kar oseba ve oz. pozna (npr. geslo ali PIN);
- tistem, kar oseba ima (npr. magnetna, čip ali RFID kartica);
- tistem, kar oseba je (biometrija).

Pri biometriji gre za telesno ali vedenjsko značilnost, ki je lastna točno določeni osebi in na podlagi katere se lahko tako osebo ustrezno identificira. Med telesne značilnosti spadajo npr. prstni odtis, obraz, šarenica, očesna mrežnica, vonj, DNK itn., med vedenjske pa lastnoročno podpisovanje, govor oz. glas, način gibanja itn.

V povezavi s preverjanjem identitete moramo razlikovati med dvema pojmoma (Andress, 2014):

- identifikacija: ta išče odgovor na vprašanje »kdo je ta oseba« (tu sistem izvaja primerjavo 1:N, kjer N predstavlja vse shranjene podatke, s katerimi primerja prejetega);
- avtentikacija (ponekod tudi »verifikacija«): ta išče odgovor na vprašanje »ali je oseba res tista, za katero se predstavlja«, torej če trditev pri identifikaciji drži (tu sistem izvaja primerjavo 1:1, kjer primerja od določene osebe prejeti podatek ali podatke s shranjenimi).

V zvezi s tem velja omeniti, da pri avtorizaciji sistemu ni treba vedno »vedeti«, kdo je oseba, ki zahteva določen dostop ali izvedbo aktivnosti (oz. preverjati, kdo je ta oseba), ampak včasih zadošča, da zgolj preveri, ali je oseba upravičena do izvedbe določene aktivnosti oz. dostopa do določenih podatkov (v tem primeru sistem npr. iz drugega sistema pridobi samo podatek za potrditev ali zavrnitev odobritve izvedbe določene aktivnosti oz. dostopa do podatkov). To je skladno z načelom minimizacije podatkov, predstavlja dodatno varovalko pri varovanju zasebnosti in je primerno za uporabo na področjih, kjer se ne zahteva striktno evidentiranje tega, katera oseba je izvajala določeno aktivnost ali brala določene podatke, oz. podatki o tem, kdo zahteva dostop ali odobritev aktivnosti, niso nujni za izvedbo postopka (saj je končni rezultat zgolj odobritev ali zavrnitev, 1 ali 0). Taki primeri so lahko npr. pri uporabi javnega prometa (odobritev vstopa v območje podzemne železnice, preverjanje veljavnosti terminske vozovnice na avtobusu) in odpiranju vrat stanovanjskega bloka (s pomočjo RFID ali druge čip kartice) ipd., lahko pa bi se razširili tudi na druga področja (kot bi bila denimo preverjanje veljavnosti vozniškega dovoljenja ali preverjanje polnoletnosti, kjer pravzaprav identifikacija ne bi bila potrebna vse do točke, ko bi tisti, ki preverja, ugotovil, da nekaj ni v redu, in bi bili posledično v nadaljevanju zahtevani taki dodatni postopki, kjer brez identifikacije ne bi šlo; ali pa upravičenost do nakupa določenega tipa vozovnice (npr. šolske, za brezposelne, za upokojence), kjer bi v enem sistemu (nakup vozovnice)

potrebovali samo odobritev ali zavrnitev iz drugega sistema (urad za zaposlovanje, izobraževalna institucija ipd.) in bi tako lahko precej zmanjšali administrativne postopke).

5.2 Koncept vgrajene zasebnosti

Koncept vgrajene zasebnosti (angl. *privacy by design*) je pristop, ki skozi celoten proces načrtovanja sistemov upošteva zasebnost. Soroden je konceptu tehnologij za boljše varovanje zasebnosti (angl. *privacy-enhancing technologies,* v nadaljevanju PET), ki je bil prvič omenjen v poročilu »Privacy-enhancing technologies: the path to anonymity«, izdanem leta 1995 (Hustinx, 2010). Publikacija je orisovala nov pristop k varstvu zasebnosti in obdelala študije primerov, skozi katere je pokazala, kako lahko sistemi dosežejo enake funkcionalnosti tudi ob uporabi zmanjšane količine osebnih podatkov (ali celo brez teh) – čemur rečemo tudi načelo minimizacije podatkov (angl. *data minimization*). Vgrajena zasebnost je nastala tudi kot odziv na zahteve po »vgrajenem nadzorovanju« (angl. *surveillance by design*) in temelji na 7 načelih (Informacijski pooblaščenec, 2010b):

- proaktivnost namesto reaktivnosti: potencialne težave z vidika varstva zasebnosti in osebnih podatkov naj bi predvideli vnaprej in sistem temu ustrezno prilagodili (saj naj bi bilo morebitno kasnejše prilagajanje tudi dražje od ustreznega načrta vnaprej);
- zasebnost kot privzeta izbira: privzete (izhodiščne) nastavitve v sistemu oz. podatkovni zbirki naj bodo zasebnosti prijazne;
- zasebnost, ki je sestavni del zasnove rešitve: zasebnost mora biti obravnavana v fazi postavljanja funkcionalnih zahtev sistema in predvideni morajo biti načini zagotavljanja zasebnosti v celotnem življenjskem ciklu sistema;
- polna funkcionalnost – igra s pozitivno vsoto: pri upoštevanju oz. vgradnji zasebnosti ne smemo žrtvovati učinkovitosti delovanja sistema oz. njegovih ciljev, ampak moramo najti ustrezno ravnovesje, ki ne bo žrtvovalo enega za drugo;
- zavarovanje podatkov v celotnem ciklu obdelave podatkov: to mora biti obravnavano kot proces in ne le kot posamezne naloge, ki so končane, ko so opravljene; ta proces pa mora temeljiti na načrtovanju, izvajanju, preverjanju in reagiranju na odkrite nepravilnosti oz. pomanjkljivosti;
- transparentnost: omogočen mora biti neodvisen zunanji pregled in potrditev dejanskega varovanja osebnih podatkov, saj zaprte rešitve, ki temeljijo zgolj na zaupanju, niso v skladu s tem konceptom;
- spoštovanje posameznika: upoštevati je potrebno vidik posameznika, ki mu je treba omogočati ustrezno informiranost glede obdelave podatkov, privzete nastavitve zasebnosti ipd.

V povezavi s tem Informacijski pooblaščenec (2010b) svetuje, da se pri načrtovanju držimo naslednjih smernic:

- minimizacija: Ob določanju želenih funkcionalnosti določimo minimalni zadostni nabor osebnih podatkov, ki je potreben za doseganje namena obdelave. Če določeni podatki niso potrebni, jih ne zbiramo. Včasih zadoščajo tudi anonimizirani ali statistični podatki. Različni nameni lahko zahtevajo različen obseg zbiranja podatkov (obsega tako ne posplošujemo);
- sorazmernost: Uporabi naj se manj občutljive podatke. Ne zbira naj se več enoličnih identifikatorjev, če to ni nujno. Raje naj se uporabljajo psevdonimizirani kot »surovi« osebni podatki. Podatki naj se ne zbirajo »na zalogo«. Na sorazmernost bodimo pozorni v vseh fazah, npr. pri oblikovanju iskalnikov po podatkih in pri uporabniških pravicah dostopa (nivojski dostop);
- dostopne pravice: Te morajo biti jasne in skladne z nalogami, ki jih izvajajo uporabniki podatkov, ter upravljane ažurno (dodeljevanje, ukinjanje in spreminjanje mora biti ažurno), hierarhične in dokumentirane. Prepovedana morata biti tako uporaba skupnih pravic dostopa (npr. določenih skupinskih pravic ali skupnega uporabniškega imena) kot posojanje sredstev za avtentikacijo in avtorizacijo (razen v res izjemnih in nujnih primerih);
- sledljivost (beleženje dostopov do podatkov): Potrebno je zagotoviti popolno revizijsko sled in s tem beleženje vsakega dostopa do podatkov, odstopanje od tega načela pa naj bi bilo možno le na podlagi ustrezne analize in obravnave tveganj. Razvidno mora biti, kdo, kdaj in do katerih podatkov je dostopal. Ker mora biti identifikacija uporabnika enolična (t. j. nanašati se mora na konkretno osebo), so ustrezno urejene dostopne pravice predpogoj. Ker mora biti revizijska sled avtentična in celovita, je treba poskrbeti za tehnične in organizacijske ukrepe, da je uveden nadzor tudi nad administratorji oz. uporabniki s pravicami najvišjega nivoja (ne sme biti omogočena (začasna) izključitev beleženja dostopov ali možnost popravljanja, spreminjanja ali brisanja revizijske sledi). Možni ukrepi so npr. ločeno shranjevanje revizijske sledi (na lokacije izven dosega oseb, od katerih aktivnosti so beležene), sistem »štirih oči«, shranjevanje na neizbrisljiv način ali shranjevanje podatkov o dostopanju do revizijske sledi. Ustrezno sledljivi morajo biti tudi morebitni izvozi podatkov. Poleg notranje je zahtevana tudi zunanja sledljivost (v primeru posredovanja podatkov tretjim osebam);
- rok hrambe in pravica do pozabe: Rok hrambe podatkov mora slediti namenu obdelave in je omejen na čas, ki je potreben, da je dosežen namen, zaradi katerega so se podatki zbrali ali obdelovali. Po tem se morajo podatki izbrisati, uničiti, blokirati ali anonimizirati.

Nekatere od tehnologij, ki ogrožajo zasebnost (angl. *privacy-sensitive technologies*), ki jih omenja ameriški Urad za domovinsko varnost (Privacy Office, U.S. Department of Homeland Security, 2007), so:

- biometrija: vključuje neposredno uporabo fizičnih karakteristik posameznika in stremi k vzpostavitvi čim bolj zanesljive povezave med posameznikom in informacijo;

- geoprostorski podatki: vključujejo uporabo geografskih informacij. Kot taki so lahko univerzalna vez med vsemi ostalimi informacijami, saj se vsak objekt in posameznik nahaja na neki lokaciji. Zmožnost povezovanja lokacije in posameznika skozi čas (vključno z vsemi objekti in dogodki) odpira vprašanja glede možnosti sledenja in profiliranja posameznikov;
- RFID (oz. radiofrekvenčno prepoznavanje): predstavlja problem zaradi morebitnega nadzora in neprostovoljne identifikacije, saj podatki potujejo po zraku in so izpostavljeni vsem že omenjenim tveganjem;
- podatkovno rudarjenje: predstavlja potencial, da se povezuje zelo diverzificirane informacije izven konteksta prvotnega zbiranja le-teh.

Pri uporabi tovrstnih tehnologij je še toliko pomembneje, da se uporabljajo načela zasebnosti pri načrtovanju in izgradnji informacijskih sistemov.

5.3 Načela varovanja osebnih podatkov

Zavarovanje osebnih podatkov pomeni poleg tehničnih tudi organizacijske ukrepe, kot so npr. izobraževanje uporabnikov, notranji in zunanji nadzor, sprejem in izvajanje varnostnih politik ipd.. Ukrepi morajo biti ustrezni glede na značilnosti in tveganja v posamezni organizaciji. Zelo pomembna faza je analiza stanja, s katero dobimo pregled nad tem, katere podatke imamo, kateri so naši informacijski viri in sredstva itn. (Informacijski pooblaščenec, 2010b). Informacijski pooblaščenec navaja naslednjih pet osnovnih načel zavarovanja osebnih podatkov (Mišič & Tomšič, 2007):

- ugotavljanje, kateri osebni podatki so hranjeni v informacijskem sistemu;
- zmanjševanje količine hranjenih osebnih podatkov na tiste, ki so potrebni glede na namen njihovega zbiranja;
- zaščita osebnih podatkov, ki zajema:
  - fizično varovanje,
  - elektronsko varovanje,
  - izobraževanje zaposlenih,
  - striktno izvrševanje pogodbene obdelave;
- uničenje osebnih podatkov, za katere ni več pravne podlage za njihovo hrambo in obdelavo;
- planiranje nepredvidljivih dogodkov, ki bi lahko vplivali na varovanje in hrambo podatkov.

Pri zbiranju in obdelavi podatkov pa naj bi se upoštevalo naslednja temeljna načela varstva osebnih podatkov (Informacijski pooblaščenec, 2009b):

- poštenost: zahteva in pričakuje se nezavajajoče ravnanje tistih, ki obdelujejo osebne podatke;

- zakonitost: obstajati mora pravna podlaga za zbiranje in obdelavo osebnih podatkov (in osebna privolitev posameznika, če je to zahtevano);
- namenskost: namen zbiranja in obdelave mora biti določen in zakonit;
- sorazmernost: obdelujejo se lahko le tisti osebni podatki, ki so ustrezni in po obsegu primerni glede na namen obdelave.

5.4 Izjava o varstvu osebnih podatkov oz. politika zasebnosti

Pri nekaterih (npr. spletnih) storitvah se zahteva, da ima ponudnik na vidnem oz. dostopnem mestu objavljeno izjavo o varstvu osebnih podatkov oz. politiko zasebnosti (angl. *privacy policy*). Primerna izjava o varstvu osebnih podatkov naj bi zagotavljala transparentnost obdelave podatkov in vsebovala informacije o tem (Informacijski pooblaščenec, 2009c):

- kateri osebni podatki se obdelujejo;
- kakšen je namen njihovega obdelovanja;
- kdo jih obdeluje (podatki o upravljavcu ali zastopniku);
- pod kakšnimi pogoji in komu se podatki posredujejo naprej, če je to potrebno za doseganje namena;
- in druge podatke, če so ti potrebni za zagotavljanje zakonite in poštene obdelave (npr. kakšne so posledice zbiranja in obdelave podatkov);

napisana naj bi bila v ciljni publiki jasni obliki in ne v »pravniškem žargonu«, njen obseg in oblika pa naj uporabnika ne bi odvračala od branja. Žal pa večina ponudnikov vsaj zaenkrat objavlja zelo dolge tovrstne politike, ki sicer morda vsebujejo vse omenjene informacije, ampak so povprečnemu uporabniku »neberljive« ali pa zahtevajo veliko časa za branje in analizo.

Informacijski pooblaščenec (2009b) kot glavno vodilo podjetjem, ki zbirajo osebne podatke, svetuje, da se postavijo v položaj posameznika, o katerem zbirajo in obdelujejo podatke, in skušajo odgovoriti na naslednja vprašanja:

- bi kot posameznik vedel, kdo zbira moje osebne podatke;
- bi razumel, za katere namene se podatki zbirajo;
- bi razumel, kakšne so posledice obdelave teh podatkov;
- obstaja verjetnost, da bi se želel pritožiti ali nasprotovati obdelavi podatkov.

5.5 Presoja vplivov na zasebnost

Presoja vplivov na zasebnost (angl. *privacy impact assessment*) je »orodje za identifikacijo, analizo in zmanjševanje tveganj glede nezakonitih ravnanj z osebnimi podatki, do katerih lahko pride pri določenem projektu, sistemu ali uporabi tehnologije«

(Informacijski pooblaščenec, 2010a). Lahko se izvaja tako v javnem kot zasebnem sektorju, temelji pa na sistematičnem in pravočasnem identificiranju tveganj za nezakonita ravnanja z osebnimi podatki. Njen glavni namen je »predhodna analiza tveganj in optimizacija postopkov za doseganja zakonske skladnosti« (Informacijski pooblaščenec, 2010a).

Obstajata interna in zunanja presoja vplivov na zasebnost. Prvo izvaja sam upravljavec osebnih podatkov, pri drugi pa gre za najem zunanjega svetovalca ali pa posvet pri pristojnem organu za varstvo osebnih podatkov (npr. informacijskem pooblaščencu). V pomoč presoji je navadno kontrolni seznam, ki na enostaven in pregleden način omogoča pogled na najbolj pomembne elemente zakonodaje in drugih aspektov, kjer se lahko s pravočasno prepoznavo tveganj izognemo težavam, ki bi se lahko kasneje pojavile. Temeljna načela presoje vplivov na zasebnost, na podlagi katerih se lahko strukturira kontrolni seznam, so zasnovana na temeljnih načelih varstva osebnih podatkov in so (Informacijski pooblaščenec, 2010a):

- zakonitost: splošna pravila obdelave osebnih podatkov morajo biti v skladu z zakonodajo;
- poštenost in transparentnost: obdelava osebnih podatkov mora potekati na pošten in transparenten način do uporabnika;
- sorazmernost: obdeluje naj se najmanjši obseg podatkov, ki je potreben za doseganje namena obdelave;
- točnost in ažurnost: to načelo zahteva, da podatki niso napačni ali nepopolni (točnost) in da se uporablja zadnji podatek (ažurnost);
- rok hrambe: povezan je z načelom sorazmernosti in omejuje rok shranjevanja podatkov na toliko časa, kolikor je potrebno za doseganje namena obdelave;
- zavarovanje osebnih podatkov: nanaša se na organizacijske in tehnične ukrepe, s katerimi se zagotavlja varovanje podatkov in preprečuje nepooblaščena sprememba, izguba, uničenje ali nepooblaščena obdelava podatkov;
- upoštevanje pravic posameznika: upoštevanje pravic, ki jih ima posameznik glede svojih podatkov.

Presoje so bolj uveljavljene tam, kjer je poudarek na varstvu zasebnosti in ne toliko na varstvu osebnih podatkov (Informacijski pooblaščenec, 2010b), jih pa kaže vsaj skozi kontrolni seznam do neke mere smiselno uporabiti tudi pri načrtovanju integracije ali nadgradnje informacijskega sistema, ki obdeluje osebne podatke.

5.6 Upoštevanje ISO/IEC 27001, COBIT in ITIL

ISO 27001 je standard informacijske varnosti, ki ga izdajata Mednarodna organizacija za standardizacijo (angl. *International Organization for Standardization*, v nadaljevanju ISO) in Mednarodna elektrotehniška komisija (angl. *International Electrotechnical Commission*,

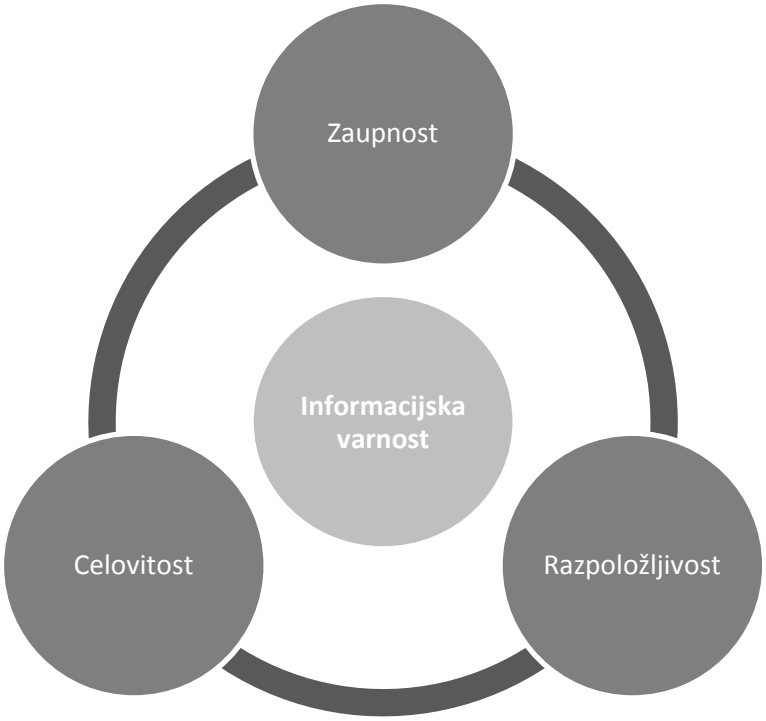
v nadaljevanju IEC). Predstavlja specifikacijo sistema obvladovanja informacijske varnosti (angl. *information security management system*) v različnih vrstah organizacij. Prvič je bil objavljen v letu 2005 in nadomešča predhodni britanski standard BS 7799 (oz. kasneje ISO 17799). Predstavlja osnovo za revizije informacijskih sistemov in je usklajen z drugimi sorodnimi standardi kot sta npr. ISO 9001 in ISO 14001. Organizacije, ki izpolnjujejo zahteve standarda, lahko po uspešni izvedbi uradnega revizijskega postopka s strani neodvisnega akreditiranega organa pridobijo certifikat o skladnosti. Organizacija, skladna s tem standardom, zagotavlja sistematičen pristop k identifikaciji in odpravljanju potencialnih tveganj, povezanih z informacijskimi resursi organizacije, deležnikom pa daje jasen signal, da ima varen sistem upravljanja z informacijami. Standard je del širše mednarodne serije standardov ISO 27000 za področje obvladovanja informacijske varnosti (Calder & Watkins, 2008).

Varovanje informacij oz. (osebnih) podatkov ni enkratna aktivnost, ampak proces, ki vključuje analizo tveganj, obravnavo tveganj, sprejem ukrepov za upravljanje tveganj, nadzor učinkovitosti sprejetih ukrepov in prilagajanje ukrepov. Kritične karakteristike oz. temeljni gradniki informacijske varnosti in varnosti podatkov predstavljajo (Informacijski pooblaščenec, 2015):

- zaupnost (angl. *confidentiality*): podatki ne smejo biti na voljo nepooblaščenim osebam;
- celovitost (angl. *integrity*): podatkov se ne sme izgubiti, javno objaviti ali nepooblaščeno spreminjati;
- razpoložljivost (angl. *availability*): podatki morajo biti na voljo takrat, ko so potrebni.

Tem gradnikom se s skupnim pojmom reče tudi »triada CIA« (angl. *CIA triad*), (Slika 4).

Slika 4: Ponazoritev gradnikov CIA triade



Vir:Y. Bhaiji, Chapter 1: Overview of Network Security, 2008.

Kljub temu, da skladnost z omenjenim standardom ni zahteva pri zakonodaji s področja zasebnosti in varovanja podatkov (je pa zahteva v obratni smeri – t. j. da standard med drugim zahteva, da je zagotovljeno varstvo podatkov in zasebnosti glede na zahteve relevantne zakonodaje, pravil in pogodb), je vseeno zlasti pri kompleksnejših projektih ali sistemih smiselno upoštevati vsaj nekatere smernice, ki jih določa ta standard, saj sta tako med drugim olajšana nadzor nad varovanjem podatkov in analiza tveganj, prav tako pa je to koristno tudi v primeru morebitne kasnejše želje po certifikaciji organizacije na podlagi omenjenega standarda.

Omeniti velja tudi COBIT, ki predstavlja ogrodje za upravljanje informacijske tehnologije (angl. *IT governance*) oz. skupek orodij in najboljših praks za razvoj, implementacijo, nadzor in izboljšavo upravljanja IT, ki omogočajo upravljavcem, revizorjem in uporabnikom informacijskih tehnologij lažje usklajevanje poslovnih ciljev s cilji informacijske tehnologije in IT procesov v organizaciji ter prispevajo k zmanjševanju odmikov med zahtevami nadzora, tehničnimi izzivi in poslovnimi tveganji (COBIT 4.1: Framework for IT Governance and Control, 2015). Okvir COBIT ustvarja in vzdržuje ISACA (angl. *Information Systems Audit and Control Association*, t. j. združenje za revizijo in nadzor informacijskih sistemov), ki je mednarodna organizacija, ki se ukvarja s področjem upravljanja informacijske tehnologije (angl. *IT governance*), revizijskih kontrol IT, informacijske varnosti in z drugimi povezanimi področji (About ISACA, 2015). Ob načrtovanju informacijskih sistemov pa je v veliko pomoč kot temelj za kakovostno upravljanje IT lahko tudi ITIL (angl. *IT Infrastructure Library*), ki zajema vrsto dokumentov za pomoč pri implementaciji okvira ravnanja z IT storitvami (angl. *IT service*

management), ki med drugim zajema tudi upravljanje (informacijske) varnosti (ITIL and IT Service Management, 2015).

5.7 Pristop AAA

Ta pristop je tehnološko nevtralen in neodvisen od vrste informacijskega sistema oz. uporabljenih tehnologij, zato je zelo uporaben za opredeljevanje postopkov in ukrepov za zavarovanje (osebnih) podatkov. Temelji na treh elementih varnosti in sicer (Informacijski pooblaščenec, 2009a):

- avtentikacija (angl. *authentication*): gre za ugotavljanje identitete posameznika, ki je uporabnik podatkov oz. pooblaščen za njihovo uporabo;
- avtorizacija (angl. *authorization*): gre za definicijo dostopnih pravic uporabnikov podatkov, t. j. kaj lahko s temi podatki počnejo;
- sledljivost (angl. *accountability*): gre za možnost naknadnega ugotavljanja, kdaj in s strani koga so bili podatki uporabljeni ali obdelani.

5.8 Pristop PriS

Pristop PriS (angl. *privacy safeguard* oz. »varovalka zasebnosti«) je metodologija vključevanja zahtev zasebnosti v proces načrtovanja informacijskega sistema, ki so jo konceptualno razvili Kavakli, Kalloniatis, Loucopoulos in Gritzalis (2006). V splošnem jo sestavljajo naslednje faze:

- identifikacija ciljev, povezanih z zasebnostjo: Ti cilji omejujejo pretvorbo organizacijskih ciljev neposredno v procese. Cilji organizacije so njeni temeljni cilji, ki jih je potrebno dosegati, cilji zasebnosti pa so generirani s področja zasebnosti glede na štiri osnovne zahteve:
  - anonimnost (angl. *anonymity*),
  - psevdonimnost (angl. *pseudonymity*),
  - nepovezljivost (angl. *unlinkability*) in
  - nezaznavnost (angl. *unobservability*);
- analiza vpliva identificiranih ciljev zasebnosti na procese v sistemu;
- identifikacija tehnik, ki najbolje podpirajo ali implementirajo procese ob doseganju obeh vrst ciljev.

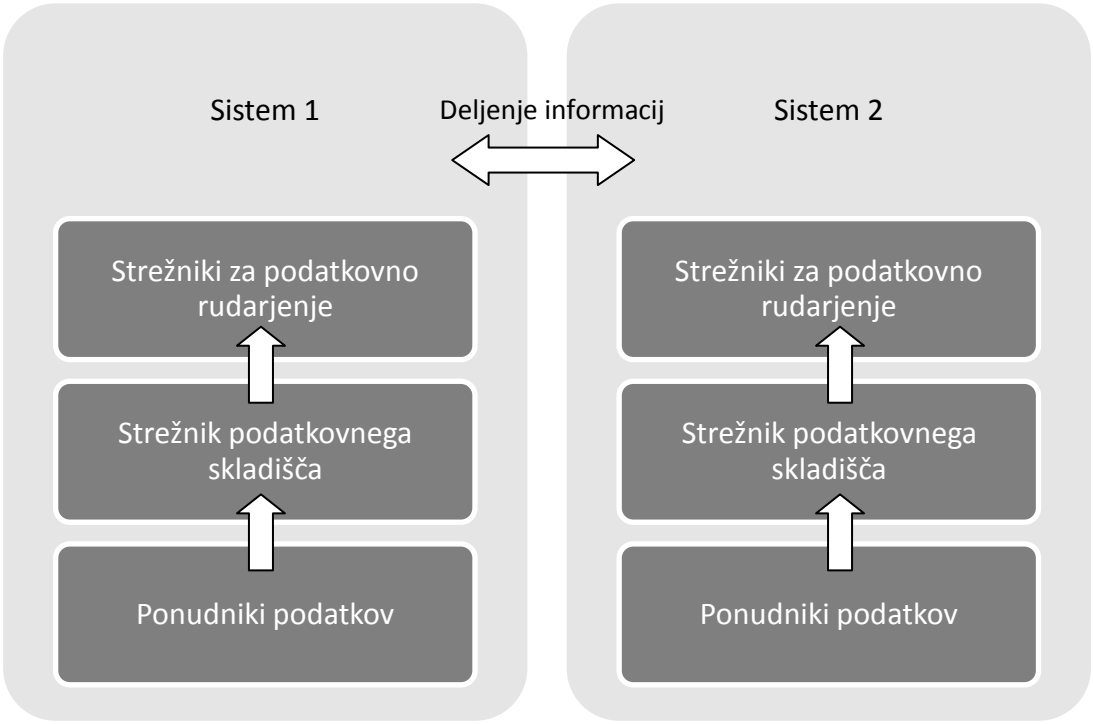
5.9 Sistemi za podatkovno rudarjenje, ki ohranjajo zasebnost

Sistemi za podatkovno rudarjenje (angl. *data mining*) pogosto predstavljajo velik izziv za varovanje zasebnosti. Vendar pa obstajajo različni načini izvedbe arhitekture sistema, ki ohranja zasebnost (angl. *privacy-preserving data mining systems*) in pri tem (vsaj do neke mere) ne ovira izvajanja podatkovnega rudarjenja (Zhang & Zhao, 2007).

Upoštevati je potrebno načelo minimalnega nabora podatkov, kar pomeni, da naj sistem za podatkovno rudarjenje od druge entitete pridobi najmanjšo količino osebnih podatkov, potrebnih za izvedbo postopka.

Predpostavlja tri stopnje (Slika 5): ponudniki podatkov (ki so tudi lastniki podatkov), strežnik podatkovnega skladišča (ki podpira sprotno analitično procesiranje), strežniki podatkovnega rudarjenja (ki izvajajo opravila podatkovnega rudarjenja in medsebojno deljenje informacij). Osnovni izziv je nadzor osebnih podatkov, ki se prenašajo med entitetami, ne da bi ob tem ovirali podatkovno rudarjenje.

Slika 5: Osnovna arhitektura sistema, ki ohranja zasebnost



Vir: N. Zhang, & W. Zhao, Privacy-Preserving Data Mining Systems, 2007, str. 53.

Osnova strategije pri tej arhitekturi so trije protokoli, ki urejajo razkritje osebnih podatkov med entitetami, ki jim je skupen cilj minimizirati za rudarjenje potrebne podatke, ki se prenašajo od ene entitete na drugo:

- zbiranje podatkov: ščiti zasebnost med prenosom podatkov od ponudnikov do podatkovnega skladišča;
- nadzor sklepanja: ščiti zasebnost med podatkovnim skladiščem in strežniki podatkovnega rudarjenja;
- deljenje informacij: nadzira informacije, ki se delijo med strežniki podatkovnega rudarjenja v različnih sistemih.

Načelo minimizacije osebnih podatkov omenjajo tudi Skinner, Han in Chang (2006). Kot načelo načrtovanja in implementacije sistemov z namenom zagotavljanja ščitenju

zasebnosti boljših sistemskih konfiguracij izpostavljajo princip minimizacije osebnih podatkov in maksimizacije anonimnih/anonimiziranih podatkov (angl. *personal data minimization & anonymous data maximization,* v nadaljevanju PDM-ADM). Poleg tega načela omenjajo tudi ločitev dolžnosti in podatkov (angl. *separation of duty and data,* v nadaljevanju SDD). Ločitev dolžnosti in podatkov zahteva, da za niz transakcij noben posamezen uporabnik nima pravic izvajanja vseh transakcij, ki obstajajo v nizu. V povezavi z osebnimi podatki to pomeni, da za določen niz osebnih podatkov in transakcij, ki te podatke obdelujejo, nima en posamezen uporabnik dostopa do vseh osebnih podatkov ali transakcij v nizu.

5.10 Povezovanje zbirk osebnih podatkov v javni upravi

V javni upravi se vse bolj povečuje potreba po večjem povezovanju (in tudi dejanska povezljivost) podatkovnih zbirk – tako z namenom povečanja učinkovitosti izvajanja postopkov kot v okviru različnih projektov e-uprave, ki omogočajo državljanom enostavnejše izvajanje upravnih postopkov ali povezanih aktivnosti. Na prvi pogled najenostavnejša rešitev – t. j. združitev vseh podatkovnih zbirk javne uprave v eno samo – pa pomeni prekomeren poseg v zasebnost posameznika in zato ni sprejemljiva. Tako obsežna zbirka bi predstavljala nevarno približevanje totalitarnim sistemom, saj nikoli ne moremo predvideti, kaj bi s podatki pričele prihodnje oblasti, poleg tega pa vsi podatki na enem kupu predstavljajo zelo visoko tveganje vdorov in zlorab ne glede na morebitne visoke stopnje nadzora in varnosti, ki bi bile vzpostavljene. Potrebno pa je tudi učinkovito nadziranje in presojanje posameznih korakov združevanj in povezovanj, ko gre za povezovanje obstoječih zbirk, da potem ne bi po takih posameznih manjših korakih v perspektivi prišli ravno do neželenega rezultata možnosti prekomernega nadzora (Informacijski pooblaščenec, 2009a).

Glede na 20. člen Zakona o varstvu osebnih podatkov ni dovoljena uporaba istega povezovalnega znaka na način, da bi se za pridobitev osebnega podatka uporabil zgolj ta znak, če gre za pridobivanje osebnih podatkov iz zbirk s področja zdravstva, policije, obveščevalno-varnostne dejavnosti države, obrambe države, sodstva, državnega tožilstva, kazenske evidence in prekrškovnih evidenc.

6 PRIMERI IZ PRAKSE

V nadaljevanju so obravnavani trije primeri integracij iz prakse, analiziran je njihov pristop k spremembam vpletenih informacijskih sistemov in prikazani so izzivi, s katerimi so se ob integracijah srečali.

Prvi primer obravnava sistem za sprejem vlog in izdajo vizumov Vizis. Za namene pridobitve informacij, ki niso na voljo na internetu ali v knjižnicah, sem izvedel intervju z g. Antonom Pirihom, vodjo vizumskega oddelka na Ministrstvu za zunanje zadeve. Intervju je potekal dne 22. marca 2016 in je trajal 1 uro in 20 minut. Vodil sem ga po

vnaprej pripravljenih vprašanjih, ki pokrivajo različna področja obravnavane teme (od osnovnih podatkov o informacijskem sistemu in integraciji, preko informacij o notranjih uporabnikih, njihovih pravicah dostopa, izobraževanjih v zvezi z varovanjem podatkov in revizij pravic, pa do tega, kateri podatki in kako se obdelujejo, kako je zagotovljeno varstvo pravic podatkovnih subjektov in če so bili kakšni posebni izzivi v zvezi s tem). Vprašanja sem pripravil na podlagi teorije, obdelane v tem diplomskem delu, in tako skušal pridobiti relevantne informacije, ki bi pokazale, kako se ta teorija izkazuje v praksi: poudarek je bil na pravicah posameznika na področju varstva osebnih podatkov, na obdelani (oz. za ožje področje relevantni) zakonodaji, izzivih, s katerimi so se ob integraciji srečali, morebitnih interakcijah z nadzornimi organi glede varovanja osebnih podatkov in zasebnosti ter na tem, kaj se z osebnimi podatki dogaja, ko potujejo skozi različne procese v organizaciji, kako se beleži njihovo pregledovanje, spreminjanje in brisanje ter kako je s tem seznanjen podatkovni subjekt. K ustreznemu oblikovanju in grupiranju vprašanj so pripomogla tudi znanja in izkušnje, ki sem jih pridobil ob različnih intervjujih pri reviziji informacijskih sistemov. Zapis intervjuja se v celoti nahaja v Prilogi 1. Dodatno sem nekatere relevantne informacije pridobil tudi iz javno dostopnih publikacij na spletnih straneh slovenskih in evropskih javnih institucij.

Drugi primer obravnava geodetski prostorski portal Prostor. Tudi tu sem nekatere relevantne informacije pridobil s pomočjo javno dostopnih publikacij in člankov na različnih spletnih straneh, glavnina informacij pa je bila pridobljena s pomočjo intervjuja z g. Urošem Mladenovičem, vodjo oddelka za informatiko, in go. Kristino Perko, vodjo oddelka za izdajanje podatkov, na Geodetski upravi Republike Slovenije. Intervju je potekal dne 7. marca 2016 in je trajal 1 uro in 30 minut. Struktura intervjuja (in vprašanja sama) je bila podobna tisti v prvem primeru, zato sem tudi tu za njihovo oblikovanje upošteval podobne kriterije in prej omenjeno obravnavano teorijo, saj je bil namen enak – preučiti, kako se obdelana teorija kaže v praksi. Zapis tega intervjuja se v celoti nahaja v Prilogi 2. Dodatno sem pridobil še poenostavljen diagram procesa spremembe lastništva (ki se nahaja v Prilogi 3), s katerega je med drugim tudi razvidna pot podatkov ob spremembi lastništva nepremičnine in kateri informacijski sistemi oz. podatkovne zbirke so v tem procesu vključeni.

V tretjem primeru sem analiziral družbeno omrežje Facebook kot poseben primer integracije, čigar dejavnosti so posredno v letu 2015 tudi vplivale na spremembo nekatere zakonodaje (t. j. pravil varnega pristana med ZDA in EU) in ki še vedno postavlja nekatere precedense na področju varovanja zasebnosti in osebnih podatkov. Tu sem nekatere informacije pridobil s pomočjo opisov na sami spletni strani Facebook, s pomočjo različnih člankov, povezanih z aktivnostmi in dejanji omrežja, na podlagi zapisov na strani »Europe v. Facebook« (vključujoč nekatere relevantne izjave ali odločbe s strani javnih institucij) ter tudi z lastnim opazovanjem in beleženjem opažanj v vseh letih uporabe njihovih storitev.

6.1 Vizis

Republika Slovenija je postala del schengenskega območja 21. decembra 2007. Schengensko območje obsega evropske države, ki so podpisale schengenski sporazum, in pomeni območje odpravljenih notranjih mejnih kontrol držav članic ter okrepitev kontrol na zunanjih mejah območja. Sem spadata tudi uvedba t. i. schengenskega vizuma (kot posledica skupne vizumske politike) ter standardizacija mejnih nadzornih sistemov in podatkovnih zbirk (Urad Vlade Republike Slovenije za komuniciranje, b. l.).

V okviru priprav in izpolnjevanja pogojev za vstop Slovenije v schengensko območje je moralo Ministrstvo za zunanje zadeve (v nadaljevanju MZZ) omogočiti, da bo nacionalni sistem za izdajo vizumov Vizis integrirano deloval v skupnem evropskem sistemu preverjanja prosilcev za vizume in izdajanja vizumov. Že pred tem so bili zadevni postopki učinkovito informatizirani in diplomatsko-konzularna predstavništva Republike Slovenije (v nadaljevanju DKP) so se povezovala s centralnimi podatkovnimi zbirkami na MZZ in Policiji.

6.1.1 Okvir integracije

Osnovna zbirka na nacionalni ravni v sistemu Vizis vsebuje vloge za vizume (ki vključujejo zahtevane podatke o prosilcih za vizume) in se povezuje z naslednjimi nacionalnimi zbirkami (Priloga 1):

- fonetični indeks oseb (FIO): gre za indeks, s pomočjo katerega se po principu fonetike išče osebe po vseh policijskih podatkovnih zbirkah (npr. če je za določeno osebo vneseno kaznivo dejanje ipd.);
- črna lista: vsebuje seznam oseb, ki jim je bil izrečen ukrep prepovedi vstopa v Republiko Slovenijo;
- tuje ukradene potne listine: ta vsebuje, kot že samo ime pove, seznam ukradenih tujih potnih listin.

Integracija teh zbirk na nacionalni ravni se pred vstopom v schengen ni spreminjala, so se pa zaradi zahtev skupne vizumske politike vzpostavile dodatne povezave z zbirkami schengenskega sistema kot sta SIS in VIS. Na skupni evropski ravni sta torej pomembna dva informacijska sistema (Agencija Evropske unije za temeljne pravice & Svet Evrope, 2014):

- schengenski informacijski sistem (v nadaljevanju SIS): uporabljajo ga nacionalni organi kazenskega pregona, organi za nadzor meja ter carinski, vizumski in pravosodni organi (za koordinacijo in izmenjavo informacij kot so npr. iskane ali pogrešane osebe, ukradena vozila in dokumenti ipd.), dostop pa imajo do tistih podatkov, ki jih potrebujejo za izvajanje svojih nalog;

- vizumski informacijski sistem (v nadaljevanju VIS), ki je v uporabi za izmenjavo podatkov med državami članicami za namene zbiranja vlog za vizume in izdaje vizumov.

Oba sistema sta v grobem sestavljena iz treh delov:

- centralni sistem schengenskega območja (C-SIS oz. C-VIS);
- nacionalni sistemi schengenskih držav (N-SIS oz. N-VIS);
- komunikacijska infrastruktura med centralnim in nacionalnimi sistemi.

Podatki za SIS se vnašajo na nacionalni ravni, ki vsebuje popolno kopijo centralnega sistema, ki se posledično ažurira iz vseh nacionalnih zbirk. V VIS se podatki polnijo iz nacionalnih sistemov, vendar pa nacionalne kopije centralnega sistema ne obstajajo, saj vsaka država na tej ravni upravlja zgolj s svojimi vlogami za vizume v okviru nacionalnega sistema (in iz centralnega sistema pridobi podatke zgolj ob vnašanju konkretne vloge za vizum, če v njem že obstaja zapis o prosilcu).

Ker je bila ena od zahtev pravnega reda EU tudi ta, da je potrebno pred izdajo vizumov izvajati preverjanje prosilcev v skupnem sistemu SIS, je bilo pred vstopom Slovenije v schengen tako potrebno izvesti tudi vzpostavitev in prilagoditev nacionalnega sistema za uporabo s SIS, ki ga je Slovenija pričela uporabljati dne 1. septembra 2007. Zaradi težav pri vzpostavitvi novega sistema SIS II (ki bi odpravil nekatere omejitve kot so bile npr. nizko število hkratnih povezav in majhna prepustnost omrežja) je bila uporabljena nadgrajena verzija obstoječega pod imenom »SIS I za vse« (Urad Vlade Republike Slovenije za komuniciranje, b. l.). Uporaba SIS (torej pred tem vzpostavitev povezljivosti nacionalnega sistema s SIS) je tudi eden od predpogojev za državo, ki želi postati del schengenskega območja (Schengen Area, 2016).

Druga generacija SIS (SIS II) je prešla v uporabo aprila 2013 in je nadgradila funkcije kot so dodajanje biometričnih podatkov (prstni odtisi in fotografije), nove vrste opozoril (ukradena letala, ladje, kontejnerji, oblike plačil) ali možnost povezave različnih opozoril (npr. na osebi in vozilu) in dodajanje evropskega naloga za prijetje in predajo. Zagotavlja visoko stopnjo varovanja podatkov: dostop je omejen na nacionalne mejne kontrole, policijo, carino in organe s področja sodstva, izdaje vizumov in registracije vozil. Vsak posameznik ima pravico dostopa do podatkov, ki se nanašajo nanj in so v SIS II, prav tako lahko tudi zahteva pri pristojnem nacionalnem organu, da popravi ali izbriše te osebne podatke. Vsakdo lahko zahteva sodno varstvo glede dostopa, popravka, izbrisa ali pridobitve informacij ali kompenzacijo v povezavi z izdanim opozorilom iz sistema. Dostop do sistema imata poleg držav schengenskega območja tudi Europol in Eurojust (z omejitvijo izvajanja poizvedb). Nacionalni nadzorni organi in evropski nadzornik za varstvo podatkov sodelujejo in izvajajo koordiniran nadzor (Schengen Area, 2016). Evropski nadzornik bdi nad centralnim sistemom (C-SIS), nacionalni nadzorni organ pa nadzoruje nacionalni sistem (N-SIS), ki je kopija centralnega sistema (C-SIS), ter preverja

kakovost podatkov, ki jih država vnaša, in zagotavlja, da se vsaj na štiri leta izvede revizija postopkov obdelave osebnih podatkov v N-SIS (Agencija Evropske unije za temeljne pravice & Svet Evrope, 2014).

Integracija z VIS je bila vzpostavljena kasneje in sicer leta 2010, saj tudi sistem kot tak pred tem še ni bil zaključen. V tem vmesnem času so države schengenskega območja uporabljale konzultacijski sistem Vision (ki ni bil podatkovna zbirka), v katerem je lahko posamezna država definirala, katere tretje države so zanjo rizične države in želi biti dodatno obveščena, ko se vizumski postopek izvaja za osebo iz take rizične države. V takem primeru je bilo pred izdajo vizuma potrebno počakati na odgovore teh držav (Priloga 1).

Namesto Visiona je sedaj v uporabi VisMail2, ki služi istemu namenu in je vsebinsko podoben. V okviru tega sistema se pošiljajo podatki (vendar ne osebni podatki) navzven – če določena schengenska država zahteva, da se jo za določeno tretjo državo dodatno obvesti o iz nje izhajajočih prosilcih za vizum, sledi vpisu vloge prosilca iz take države avtomatska elektronska pošta taki schengenski državi, v kateri je omenjeno, da v VIS-u sedaj obstaja vloga z določeno ID številko, ter opombo, da imajo 7 dni časa, da sporočijo, če se strinjajo z izdajo vizuma ali ne (Priloga 1).

VIS povezuje konzulate v državah, ki niso članice EU, in zunanje mejne prehode držav schengenskega območja. V njem se obdelujejo podatki o vlogah za vizume za kratkoročno bivanje zaradi obiska ali tranzita skozi schengensko območje. Sistem omogoča biometrijsko preverjanje (prvenstveno prstnih odtisov) za namene identifikacije in verifikacije. Verifikacija tu pomeni, da sistem preveri, če se prstni odtisi, zajeti na mejni kontrolni točki, ujemajo s tistimi v biometričnem zapisu, vezanem na aktualni vizum. Pri identifikaciji pa preverja prstne odtise na mejnem prehodu z vsebino celotne podatkovne zbirke (kar traja dlje). Dostop do VIS je omejen tako, da lahko vnos, spremembo ali izbris podatkov izvajajo zgolj vizumski organi držav članic, vpogled v podatke pa poleg tega tudi organi, pristojni za preverjanje na zunanjih mejnih prehodih, kontrolo nad priseljevanjem in azil. Pod določenimi pogoji lahko zaprosijo za dostop do podatkov tudi nacionalni policijski organi in Europol (Agencija Evropske unije za temeljne pravice & Svet Evrope, 2014).

V zvezi s povezavami med DKP in MZZ je v uporabi sistem replikacij. Na vsakih 14 minut se replicirajo podatki z DKP na centralno zbirko na MZZ (uporabniki na DKP nimajo možnosti neposrednega dostopa do centralnih evidenc, ampak samo do delne kopije Vizisa na njihovem DKP-ju – delna kopija tu pomeni, da se tja replicirajo zgolj vloge, ki zadevajo ta DKP). Z naslednjo replikacijo v smeri od MZZ proti DKP pa so potem na DKP na voljo in prikazani morebitni zadetki (Priloga 1).

Na relaciji med centralnim sistemom VIS in nacionalnim sistemom (Vizis) se vsi podatki, ki so v Vizisu in se nanašajo na schengenske vizume, prenesejo v VIS (v katerem so

shranjeni vsi podatki vseh schengenskih držav). Na strani nacionalnega sistema gre za vpis podatkov, po prenosu v VIS pa se tam preverja, če že obstajajo zapisi v zvezi s prosilcem, nato pa se samo tisti podatki prikažejo konzulu na DKP (Priloga 1).

Pri SIS-u pa ima vsaka država celotno kopijo centralne zbirke C-SIS (ki se v Sloveniji hrani pri Policiji). Na enak način, kot je izvedeno dostopanje do VIS-a, se podatke v SIS-u tako preverja pri Policiji (t. j. če obstajajo kakšna opozorila v zvezi s prepovedjo vstopa v schengenski prostor, sistem avtomatsko preveri v N-SIS in v takem primeru vrne zadetke).

6.1.2 Osebni podatki, ki se obdelujejo

V okviru obravnavane integracije se za namene izdaje vizumov od prosilcev za vizume (in morebitnih garantov) zbirajo vsi osebni podatki, kot jih določa Zakon o tujcih v svojem 112. členu. To so med drugim: ime, priimek, priimek ob rojstvu, EMŠO (če je določen), spol, rojstni datum, rojstni kraj in država, državljanstvo, državljanstvo ob rojstvu, zakonski stan, poklic, ime in priimek staršev ali zakonitih zastopnikov, ime in priimek zakonca, priimek zakonca ob rojstvu, ime in priimek in datum rojstva otrok itn. Zbirajo pa se lahko tudi osebni podatki o garantu (ki je fizična ali pravna oseba iz Republike Slovenije).

Podatki o prosilcu za vizum se vedno zbirajo neposredno od prosilca, del podatkov pa je možno pridobiti ali uporabiti tudi iz evidence garantnih pisem, ki se vodi na upravnih enotah. Vsako garantno pismo, vključno s podpisom garanta, mora biti overjeno. Vsebina in oblika garantnega pisma sta določeni z zakonom, hranijo pa se podatki o tem, kdo je koga povabil. Iz te evidence je tako možno na podlagi številke na garantnem pismu pridobiti podatke o garantu. Obstajajo tudi spletne vizumske vloge, kjer pa gre samo za drugo obliko zbiranja podatkov s strani prosilcev – za razliko od fizičnega obiska prosilca na DKP in izpolnjevanja obrazca na licu mesta (Priloga 1). Osnova vnesenih podatkov je potni list prosilca za vizum, za zapise imen in drugih podatkov iz drugih (ne-latiničnih) abeced pa se uporablja standarde ICAO (Mednarodna organizacija za civilno letalstvo), kot je zapisano tudi v strojno berljivem delu potnega lista.

Obstaja več kontrol pravilnosti podatkov in sicer (Priloga 1):

- preverjanje pravilnosti podatkov ob vnosu (kar izvaja tisti zaposleni, ki vpisuje podatke);
- preverjanje s strani konzula, ki odloča o vlogi;
- kontrola pri tiskanju vizumske nalepke (tu se preverja, če se podatki na potnem listu in vizumski nalepki ujemajo);
- prosilec za vizum (vsaka stranka mora ob prejemu vizuma preveriti pravilnost podatkov).

V primeru napak je lahko potreben preklic vizuma (razveljavitev vizumske nalepke), popravek napačnih podatkov in izdaja nove vizumske nalepke.

Pri VIS-u je osnovna entiteta (vizumska) vloga. Vloge se povezujejo v dosjeje, kjer velja, da mora biti za eno osebo načeloma en dosje (čeprav se lahko v praksi kdaj tudi zgodi, da ima ena oseba več dosjejev, kar ni pravilno). Vloge se povezujejo, ko je opravljen zajem prstnih odtisov in so vpisani alfanumerični podatki ter se vsi ti podatki prenesejo v VIS. Na osnovi vnesenih podatkov država članica izvaja t. i. iskanja v VIS-u (t. j. ali za to osebo že obstajajo zapisi v sistemu), za kar se lahko uporabi različne kriterije, ki jih določi posamezna država zase. Za Slovenijo velja, da se najprej išče po prstnih odtisih. Ti so shranjeni v VIS-u, zahtevan pa je zajem vseh deset prstov. Če prstnih odtisov ni, so lahko razlogi naslednjih štirih kategorij:

- otrok, ki še ni dopolnil 12 let;
- stranka je izjavila, da je prstne odtise zajela že pri predhodnem vizumskem postopku, ki se je zgodil v zadnjih 59 mesecih (v VIS-u se ti hranijo 60 mesecev);
- začasna ali trajna poškodba (npr. oseba je brez enega ali več prstov ali roke ali je kako drugače poškodovana, da zajem prstnih odtisov ni možen);
- poglavarji držav, ministri in drugi funkcionarji, ko prihajajo z namenom v okviru uradnega obiska – tu zajem prstnih odtisov ni zahtevan (za njihov zasebni obisk to ne velja).

V teh primerih se potem iščejo zadetki v VIS-u s pomočjo alfanumeričnih podatkov. Slovenija je razvila niz različnih iskalnih kriterijev, ki gredo od ožjega proti širšemu (dokler sistem ne najde zadetka): Najprej »ime, priimek, datum rojstva«; nato »predhodno izdana vizumska nalepka«; nato »priimek, letnica rojstva, državljanstvo« itn. Vseh iskalnih kriterijev je sedem. Če po nobenem iskalnem kriteriju sistem ne najde zadetka, se postopek nadaljuje in se predpostavlja, da gre za nov vpis.

6.1.3 Varovanje pravic

Za izdajo schengenskih vizumov določa okvire (in s tem tudi pravice podatkovnih subjektov) pravni red EU in sicer (Priloga 1):

- Uredba VIS: Ta določa vsebino – opredeljuje vizumski postopek in to, katere podatke se zbira, na kakšen način in kdo jih sme uporabljati (DKP-ji za obravnavanje vizumskih vlog, mejni prehodi ob kontroli, določeni policijski organi ob izvajanju dela mejne kontrole v notranjosti države). Tu je tudi določeno obdobje 60 mesecev za hrambo podatkov posameznih vlog;
- Odločba VIS: Ta določa pristop do podatkov in njihovo uporabo s strani drugih varnostnih organov, kot so obveščevalne službe, kriminalistična policija ipd. Vsaka država sama sporoči komisiji, kateri so ti drugi organi, ki bodo potrebovali dostop.

Vsak posameznik ima pravico do seznanitve z lastnimi osebnimi podatki. Na spletni strani MZZ je za ta namen objavljen opis postopka in obrazec. Posameznik, ki želi pridobiti vpogled v to, kateri njegovi osebni podatki se obdelujejo, tako izpolni ta obrazec in ga

dostavi na MZZ, ki potem preveri stanje v VIS in izpiše morebitne podatke o takem posamezniku.

V zvezi s pravico do popravka podatkov velja načelo, da mora vsak prosilec najkasneje ob prejemu vizumske nalepke preveriti, če so podatki na njej dejanski in ustrezni, saj se morajo ujemati s tistimi v potnem listu.

Čas hranjenja podatkov (ki se nanaša na nacionalno zbirko) je definiran v Zakonu o tujcih, za hrambo v VIS in SIS pa veljajo uredbe EU. Za oboje je določeno, da se podatki lahko hranijo 5 let po prenehanju veljavnosti vizuma oz. 5 let po izdaji odločbe, da je bila vloga zavrnjena. Hranijo se vloge oz. podatki na njih; ko je izbrisana zadnja vloga v dosjeju osebe, tudi ne obstaja več dosje osebe kot tak. Brisanje se izvaja avtomatsko v ozadju. Sicer pa do posameznih podatkov v sistemu uporabnik oz. zaposleni ne more dostopati ali po njih brskati, če ne gre za vnašanje konkretne vloge, v katero se pridobi morebitne obstoječe podatke iz VIS.

Kot upravljavec zadevnih podatkovnih zbirk je na MZZ določena konzularna služba.

Pravice in vloge notranjih uporabnikov so razmejene in sicer imajo zaposleni na DKP-jih tri nivoje dostopa (Priloga 1):

- lokalni uslužbenci: ti smejo vpisovati vloge, ne morejo pa videti zadetkov, odločati o vlogah in upravljati z vizumskimi nalepkami (lahko pa jih natisnejo, ko je o vlogi odločeno);
- podpisovalci: to so konzuli, ki imajo vse pravice kot prej omenjeni, dodatno pa imajo še pravico odločati o vlogah in preverjati zadetke (nimajo pa pravice upravljanja z vizumskimi nalepkami);
- vodja: ta ima vse prej omenjene pravice, poleg tega pa tudi upravlja z vizumskimi nalepkami (in je edina oseba, ki ima to pravico na posameznem DKP).

Sledljivost dostopanja do podatkov je zagotovljena: beleži se vsako odpiranje zbirke, vsako iskanje, kaj je kdo gledal, kaj je videl, kaj je spreminjal itn. V okviru tega je zabeležen tudi morebitni dostop do podatkov s strani zunanjega vzdrževalca. Administrator ima vpogled v te podatke, nima pa možnosti njihovega brisanja ali spreminjanja.

Preglede upravičenosti in načina dostopa izvaja interna kontrola MZZ skupaj z diplomatskim inšpektorjem (včasih pa tudi konzularna služba sama). Ob menjavah osebja in s tem povezanih morebitnih spremembah glede pravic dostopa je za ažurnost odgovorna kadrovska služba. Obstajajo tudi neodvisne zunanje revizije s strani urada informacijskega pooblaščenca, ki širše preverja celoten sistem varovanja osebnih podatkov na DKP in na konzularnem oddelku, vključno z uporabo podatkov iz VIS-a (npr. koliko časa se hranijo, kaj in zakaj se zbirajo, kako se hranijo, kdo dostopa, kako dostopa itn.). Ti pregledi nimajo vnaprej znanega razporeda (lahko jih v kakšnem letu tudi ni).

Izvajajo se tudi izobraževanja zaposlenih v zvezi z varstvom podatkov v okviru rednih priprav na nastop dela v tujini (okvirno dvakrat do trikrat letno).

6.1.4 Trenutno stanje in odprti izzivi

Bistvenih posebnosti, večjih sprememb ali izzivov se trenutno ne pričakuje. Poleg že omenjenih pregledov s strani informacijskega pooblaščenca se izvajajo tudi schengenske evalvacije na nivoju EU. Komisija izvede periodični nadzor za posamezno državo običajno na dveh DKP-jih. To se izvaja približno vsakih 5 let (v smislu izvajanja določb vizumskega zakonika in uredbe, vključno s tem, kdo uporablja podatke in na kakšen način). Fokus teh pregledov pa je kvaliteta vizumskih postopkov in ne varovanje osebnih podatkov.

6.2 Prostorski portal Prostor

Sredi leta 2010 je Geodetska uprava Republike Slovenije (v nadaljevanju GURS) zaključila integracijo prikaza več registrov v okviru spletnega portala Prostor. Šlo je za brezplačni javni spletni portal za namene vpogledovanja v podatke o nepremičninah, njihovih lastnikih in vrednosti, z namenom na enem mestu omogočiti uporabnikom dostop do vseh evidenc skupaj.

Zakon o evidentiranju nepremičnin je določal javnost vpogleda v evidence (t. j. v zemljiški kataster, kataster stavb, register nepremičnin, evidenco državne meje in register prostorskih enot), geodetski upravi pa je nalagal tudi vzpostavitev računalniškega distribucijskega okolja za prikaz podatkov iz omenjenih evidenc.

6.2.1 Okvir integracije

V obravnavano integracijo je vključenih pet podatkovnih zbirk oz. evidenc in sicer (Priloga 2):

- zemljiški kataster;
- kataster stavb;
- register nepremičnin;
- register prostorskih enot;
- zbirni kataster gospodarske javne infrastrukture.

Od omenjenih vsebujejo osebne podatke prve tri zbirke. Omeniti velja še zemljiško knjigo, ki tudi vsebuje osebne podatke, z njo pa upravlja Vrhovno sodišče. V zemljiški knjigi se vodijo podatki o stanju nepremičnin (lastništvo, obremenitve, pravice in obveznosti lastnikov ipd.), medtem ko se podatki v evidencah GURS nanašajo predvsem na fizične lastnosti in identifikatorje nepremičnin.

Zemljiški kataster in kataster stavb sta kot registra oz. zbirki obstajali že prej, register nepremičnin pa je bil vzpostavljen leta 2006 v skladu z Zakonom o evidentiranju nepremičnin (ki tudi predpisuje, kateri osebni podatki se zbirajo in za kakšen namen, torej v tem oziru pokriva področje, za katere Zakon o varstvu osebnih podatkov zahteva specifične področne zakone) kot večnamenska zbirka podatkov o nepremičninah, ki prikazuje dejansko stanje nepremičnin v naravi (za razliko od zemljiškega katastra, katastra stavb in zemljiške knjige, ki prikazujejo pravno stanje nepremičnin). Med viri za vzpostavitev registra so bili poleg podatkov, nastalih oz. pridobljenih na podlagi popisa nepremičnin, tudi podatki iz zemljiške knjige, zemljiškega katastra, katastra stavb, evidence trga nepremičnin, vrednotenja nepremičnin, centralnega registra prebivalstva, poslovnega registra Slovenije, podatki občin, podatki ministrstva za kmetijstvo in drugi (Rotar, 2008). Osebni podatki, zbrani v okviru popisa nepremičnin, so se hranili samo v registru nepremičnin. Iz te zbirke se podatki ne prenašajo v katastra, ki imata višji status in je del upravnih postopkov (Priloga 2).

Zakon je tudi določal, da so zemljiški kataster, kataster stavb, register nepremičnin, evidenca državne meje in register prostorskih enot javne evidence ter da ima vsakdo pravico vpogleda v podatke, vključno z osebnimi podatki lastnika (ime in priimek, naslov stalnega prebivališča in letnica rojstva).

Prikaz podatkov v javnem vpogledu v okviru spletnega portala Prostor je bil izveden v okviru rednih delovnih nalog na GURS. Predhodno je bil izdelan namenski pregledovalnik za namene popisa nepremičnin, kasneje je sledila prenova javnega vpogleda in odprtje tega za uporabo javnosti.

Pri integraciji je šlo predvsem za ponujanje enotnega pogleda na podatke skozi portal in za dostop do podatkov na enem mestu, zato se zbirke in sistemi v ozadju niso spreminjali in je bila integracija vidna samo navzven kot enotni spletni prostorski portal Prostor.

6.2.2 Osebni podatki, ki se obdelujejo

V okviru obravnavane integracije GURS obdeluje osebne podatke v treh zbirkah – zemljiškem katastru, katastru stavb in registru nepremičnin. Osebni podatki, ki se zbirajo, so: ime, priimek, naslov, EMŠO (če ta obstaja), datum smrti (če ta obstaja), datum rojstva (ta se izvede iz EMŠO; kjer pa EMŠO ne obstaja, se ga vnese neposredno). Povezovalni znak je EMŠO (za fizične osebe) in matična številka pravne osebe (za pravne osebe). Pravilnost teh podatkov se preverja s pomočjo centralnega registra prebivalstva (za fizične osebe) in poslovnega registra Slovenije (za pravne osebe). Dostop do centralnega registra prebivalstva s strani GURS je omogočen samo za zapise o tistih prebivalcih, ki so hkrati tudi lastniki nepremičnine.

Sistem je povezan z zemljiško knjigo, ki jo vodi Vrhovno sodišče. Elektronska izmenjava je bila vzpostavljena pred dvema letoma po prenovi sistema zemljiške knjige. Ko se

spremeni lastnik nepremičnine v zemljiški knjigi, prejme GURS obvestilo in relevantne podatke. Spremembe mora pregledati in potrditi referent, preden so te vnesene v vse zbirke GURS (če npr. lastnik v zemljiški knjigi nima identifikacijske številke, t. j. EMŠO ali matične številke pravne osebe, ali če je na eni nepremičnini zaveden z EMŠO, na drugi pa brez, mora to referent naknadno dopolniti, saj je v evidencah GURS matična številka povezovalni znak), kontrola pravilnosti zapisa osebnih podatkov oz. osvežitev podatkov zaradi sprememb naslovov in nazivov pa se izvaja avtomatsko na dnevni ravni preko elektronske povezave do centralnega registra prebivalstva in poslovnega registra (Prilogi 2 in 3).

Podatki v registru nepremičnin se ne hranijo dlje kot je potrebno za doseganje namena zbiranja, v katastrih pa se hranijo trajno tudi kot zbirek listin.

Dostop do podatkov imajo za lastne nepremičnine lastniki (fizične in pravne osebe) na podlagi zakonskih določil, pa tudi drugi državni organi, notarji in geodetska podjetja. Posebej ščiten podatek je EMŠO, do katerega lahko dostopa samo drug državni organ, ki ima to izrecno opredeljeno v zakonu. Za namene dostopa do podatkov, ki vključujejo tudi osebne podatke, sta na voljo dva vpogleda:

- osebni vpogled: lastnik lahko pregleduje podatke o lastnih nepremičninah;
- pregledovalnik za geodetske podatke (za registrirane uporabnike): ta omogoča, da drugi državni organi, geodetska podjetja in notarji lahko vpogledujejo (tudi osebne podatke) v skladu z zakonskimi pravicami, njihovi nivoji dostopa pa so različni.

Podatki o vpogledih v osebne podatke se beležijo, ti zapisi pa se skladno z zakonodajo zaradi varstva pravic posameznika (ki med drugim lahko zahteva seznam tega, kdo in kdaj je dostopal do katerih njegovih podatkov) hranijo še 6 let po njihovem nastanku. Dostop do tega znotraj organizacije ima samo ena točno določena oseba.

Nivoji vlog notranjih uporabnikov so določeni in razmejeni. Do podatkov imajo dostop:

- administratorji (tehnični) – njihovo dostopanje se ne beleži;
- referenti – tisti, ki lahko ažurirajo podatke; beleži se, kdo je podatke spreminjal. Spremembe podatkov so zabeležene za stalno (v okviru vodenja zgodovine sprememb na zapisu).

Med zunanje oz. pogodbene obdelovalce podatkov spadajo:

- Ministrstvo za javno upravo (kjer je podatkovni center s strežniki);
- zunanji izvajalci, ki skrbijo za razvoj informacijskega sistema (in so v pogodbi opredeljeni kot pogodbeni obdelovalci osebnih podatkov). Ti imajo po potrebi lahko omogočen tudi dostop do produkcijskega okolja, vendar se to omejuje in je odprto samo takrat, ko je res potrebno za izvedbo naloge.

Osebni podatki se prenašajo tudi do različnih državnih organov, ki imajo za to ustrezno zakonsko podlago, vsak zahtevek pa preuči pravna služba. Tako se npr. podatki registra nepremičnin predajajo Statističnemu uradu glede na potrebe državne statistike in v skladu z zakonodajo, ki ureja to področje, za njihovo anonimizacijo pa skrbi Statistični urad.

Vsi uporabniki sistema se vodijo v enotni varnostni shemi. Pravice uporabnikov glede nivoja dostopa do podatkov pri notranjih uporabnikih opredeljujejo poleg sistemizacije delovnih mest podrobneje vodje organizacijskih enot, ki imajo dolžnost, da preko predpisanih zahtevkov skrbijo za spremembe pravic, če se spremenijo uporabniki ali njihove delovne naloge.

Za zunanje uporabnike velja, da so ti (npr. kontaktne osebe organov) dolžni pravočasno sami javljati spremembe glede pravic dostopanja z njihove strani, saj GURS ne more nadzirati tega, kdo je pri njih upravičen do dostopa. Enkrat letno se izvrši preverjanje zadnjih datumov prijave zunanjih uporabnikov; za uporabnike, pri katerih je minilo od tega več kot eno leto, pa se blokira dostop.

Občasno se za notranje uporabnike izvajajo tudi izobraževanja glede standardov in določil varstva osebnih podatkov, vendar zanje ni določen reden periodičen termin.

6.2.3 Varovanje pravic

Podatki so zbrani na podlagi zakonodaje in na podlagi upravnih postopkov; podatkovni subjekti spreminjajo lastnosti svojih nepremičnin na GURS, lastništvo pa na zemljiški knjigi.

V povezavi s pravicami uporabnikov oz. podatkovnih subjektov je naveden katalog podatkov v skladu z Zakonom o dostopu do informacij javnega značaja na spletni strani GURS. Postopki o dostopu do podatkov in postopki v zvezi z nepremičninami so objavljeni na straneh na eUprave, ostali napotki glede osebnih podatkov pa so na strani Informacijskega pooblaščenca.

Posebnih notranjih revizij glede varovanja osebnih podatkov se ne izvaja (razen v primeru, če je npr. kakšna zahtevana s strani Informacijskega pooblaščenca). Za vsako evidenco je s sklepom imenovan odgovorni skrbnik za osebne podatke.

V obzir pri načrtovanju in uveljavljanju sprememb oz. obravnavane integracije je bilo potrebno vzeti predvsem naslednje pravne akte:

- Zakon o evidentiranju nepremičnin;
- Pravilnik o pogojih in načinu računalniškega dostopa do podatkov iz evidenc in zbirk geodetskih podatkov;
- Zakon o varstvu osebnih podatkov;

- Zakon o dostopu do informacij javnega značaja.

V letu 2006, ko se je pričel popis nepremičnin in vzpostavljanje registra nepremičnin, je informacijska pooblaščenka zahtevala presojo ustavnosti tistih členov Zakona o evidentiranju nepremičnin, ki urejajo namen zbiranja podatkov o nepremičninah, njihovo javno dostopnost in združevanje evidenc, saj bi po njenem mnenju javnost registra nepremičnin lahko pomenila, da se zbrani osebni podatki lahko uporabljajo za kakršenkoli namen (torej to, da se osebni podatki v tem primeru zbirajo »na zalogo«), kar bi bilo v neskladju z ustavo. Pooblaščenka je bila mnenja, da država v želji po večanju učinkovitosti poslovanja ne bi smela prekomerno posegati v posameznikovo zasebnost.

Ustavno sodišče je tako julija 2007 odločilo, da so podatki, ki se evidentirajo v registru nepremičnin, osebni podatki, ker (z imenom, priimkom, EMŠO, naslovom itn.) kažejo na določeno oz. določljivo osebo. Tako je delno razveljavilo določbe Zakona o evidentiranju nepremičnin (1. in 2. odstavek 114. člena), ki so nalagale javnost teh (osebnih) podatkov za primer, če gre za fizično osebo, saj je bilo to v neskladju z ustavo. Iz registra nepremičnin se po tem ni več smelo javno prikazovati osebnih podatkov (Odločba Ustavnega sodišča US27747, Ur. l. RS št. 65/2007 in OdlUS XVI, 67).

Integracija, ki je privedla do spletnega portala Prostor, ki je vseboval javni vpogled v stanje nepremičnin, pa je prikazovala osebne podatke o lastnikih iz zemljiškega katastra in katastra stavb – kar pomeni, da na tisti točki to ni bilo v neskladju z zakonodajo. Kljub temu, da je šlo zgolj za integracijo v okviru portala (torej da v ozadju ni bilo spremembe arhitekture sistema ali dejanske integracije več podatkovnih zbirk v eno oz. novo zbirko), pa je bil skladu z definicijo v Zakonu o varstvu osebnih podatkov ta portal lahko obravnavan kot nova zbirka osebnih podatkov, za katero zakonska podlaga ni obstajala (Informacijski pooblaščenec, 2012).

Informacijska pooblaščenka je tako dne 3. januarja 2012 izdala začasno odločbo, s katero je pozvala GURS, da mora v roku 3 dni od vročitve na portalu onemogočiti javni dostop do imen, priimkov, naslovov in podatkov o letu rojstva vseh fizičnih oseb, do katerih se je lahko s pomočjo iskalnika »javni vpogled« dostopalo v okviru novo ustvarjene zbirke katastra stavb, zemljiškega katastra, registra nepremičnin (s podatki o vrednosti nepremičnin), registra prostorskih enot in evidence državne meje. Začasna odločba je predstavljala »izvršbo v zavarovanje določene pravice, v konkretnem primeru pravice do varstva osebnih podatkov« (Informacijski pooblaščenec, 2012).

Podatki v zvezi s pravnimi razmerji glede nepremičnin so že javni v okviru zemljiške knjige, ki je javna evidenca, kjer se do njih dostopa z identifikacijsko številko parcele, stavbe ali dela stavbe, zato naj bi to povsem zadoščalo zahtevam zakonodaje o javnosti nepremičninskih podatkov. Vzporedno z začasno odločbo je informacijska pooblaščenka tudi vložila na Ustavno sodišče zahtevo za oceno ustavnosti tistega dela Zakona o evidentiranju nepremičnin, ki določa javnost nekaterih osebnih podatkov (pred tem je

njeno spomladi 2011 vloženo zahtevo za oceno ustavnosti Ustavno sodišče zavrnilo zaradi nepopolnosti).

GURS je v zahtevanem roku umaknil možnost prikaza spornih osebnih podatkov v okviru javnega vpogleda na spletnem portalu Prostor ter na spletni strani objavil obvestilo o spremembi dostopa oz. onemogočanju dostopa do podatkov o lastnikih, ki so fizične osebe (Onemogočen dostop, 2016).

Jeseni 2012 je Ustavno sodišče razveljavilo sporne člene tudi za zemljiški kataster in kataster stavb. Podatke o lastnikih nepremičnin, ki so fizične osebe, odtlej lahko pridobijo:

- vsak lastnik nepremičnine (za lastne nepremičnine);
- državni organi in notarji (za namene izvajanja uradnih nalog);
- geodetska podjetja (za namene izvajanja geodetskih storitev);
- druge osebe (če tako določa zakon).

V primeru, ko je nepremičnina v solastnini, pa lahko podatke o lastnikih te nepremičnine dobi katerikoli od njenih solastnikov.

Sprememba je veljala za elektronske storitve vpogleda in prenosa podatkov ter za izdajanje podatkov in dokumentov, zato je bila na GURS izvedena tudi uskladitev in prilagoditev elektronskih storitev za vpogled in posredovanje podatkov, programske opreme za izdajanje potrdil, programske opreme za izdajanje podatkov in postopkov poslovanja z arhivskimi gradivi in elaborati (Onemogočen dostop, 2016).

6.2.4 Trenutno stanje in odprti izzivi

Načrtuje se celovita prenova informacijskega sistema v okviru projekta e-prostor, ki bi odpravila določene pomanjkljivosti podedovanih (angl. *legacy*) informacijskih sistemov in povečala optimalnost sistema kot celote. V okviru tega naj bi bil sistem predvidoma iz treh evidenc poenoten v eno celoto, v celoti pa naj bi se avtomatiziralo tudi prenašanje podatkov iz zemljiške knjige (prevzem podatkov, kot so zapisani v zemljiški knjigi, oz. neposreden vpogled v nje). S tem in z drugimi izboljšavami bi se pospešilo postopke, izboljšalo delo s strankami, optimiziralo poslovanje in zagotovilo višje standarde varovanja in zaščite podatkov.

Trenutno pa so s tem povezane aktivnosti še v fazi pogovorov in razprav, saj je osnovni predpogoj za kakršnokoli spremembo na tem področju ustrezna sprememba zakonodaje (Priloga 2).

6.3 Facebook

Facebook je že nekaj časa največje družbeno omrežje (angl. *social network*) na svetu – njegova trenutna »populacija« obsega približno 1,6 milijarde aktivnih uporabnikov (Statista, 2016). V letu 2015 je to število prvič preseglo število prebivalcev Kitajske (kot države z največjim številom prebivalcev) in tako je Facebook postal skupnost z največ »prebivalci« na svetu (Stenovec, 2015).

Facebook si kot trenutno največje družbeno omrežje na svetu zasluži posebno omembo tudi zaradi dejstva, da je stalno »v gradnji«, saj zaradi posledic ekonomije obsega in njegove relativno dolge življenjske dobe v primerjavi s predhodno popularnimi družbenimi omrežji – ustanovljen je bil leta 2004, za uporabnike odprt pa 2006 (Facebook Expansion Enables More People to Connect with Friends in a Trusted Environment, 2006) – lahko počne in ponuja stvari, ki jih predhodniki v svojem kratkem času obstoja niso; s svojim delovanjem postavlja nove precedense, z nenehnimi spremembami storitev, pogojev in nastavitev pa se odpirajo vedno nova vprašanja in kreirajo nove situacije, ki kličejo k ustreznim razjasnitvam, izboljšavam z vidika pravic uporabnikov in nenazadnje tudi k boljši regulaciji področja.

6.3.1 Okvir integracije

Tukaj ne gre za integracijo informacijskih sistemov v klasičnem smislu, saj ni šlo za načrtno posodabljanje »starejših sistemov« in njihovo združevanje v enoten sistem ali pogled, ampak za pretežno »evolucijski« proces, kjer so se iz velikega števila različnih osebnih spletnih strani, blogov, storitev takojšnjega sporočanja, forumov in zgodnjih zametkov družbenih omrežij uporabniki postopoma v večjem številu pričeli zgrinjati pod eno streho hitro rastočega in v perspektivi največjega družbenega omrežja.

Nekatere od storitev, ki jih je Facebook uspel integrirati znotraj svojega ekosistema (in lahko delno ali v celoti nadomeščajo »zunanjo« konkurenco), so (What are the Facebook Services?, 2016):

- osebne spletne strani (angl. *personal homepage*s): V drugi polovici 1990-ih let in še prva leta 21. stoletja so bile med uporabniki interneta popularne osebne spletne strani, s katerimi so se predstavili svetu. Te strani so bile med seboj lahko precej različne, gostovane pa so bile pri velikem številu različnih ponudnikov. Kasneje so to pričeli izpodrivati zgodnji poskusi družbenih omrežij kot npr. Friendster in MySpace, sedaj pa večini zadošča že profil na Facebooku;
- različni sporočilniki (angl. *messenger*): Proti koncu 1990-ih let so prihajali v splošno uporabo sistemi takojšnjega sporočanja (angl. *instant messaging*) za namene (tekstovnega) klepetanja preko interneta, ki so se kasneje s porastom razširjenosti širokopasovnega dostopa do interneta nadgradili še z možnostjo glasovnih in video

klicev ter klicanja telefonskih številk. Danes vse to omogoča tudi Facebook v okviru storitve »Facebook Messenger«;

- spletne strani podjetij, organizacij, skupin: Večina podjetij sicer ima svoje spletne strani, v okviru svojih storitev pa Facebook nudi storitev »Facebook Pages« (oz. strani), s pomočjo katere lahko uporabnik kreira stran, ki ni osebni profil fizične osebe, torej gre za organizacijo, podjetje, storitev, skupino, stvar ipd. Podjetja lahko to uporabijo poleg svoje spletne strani kot dodaten kanal za promocijo sebe in svojih storitev, lahko pa tudi kot izključno spletno stran;
- forumi, skupinsko sodelovanje ipd.: Za namene debat ali skupinskega sodelovanja ponuja storitev »Facebook Groups« (skupine), kjer se lahko kreira skupine, ki so bodisi javne bodisi zaklenjene ali skrite;
- različne igre (lokalno in omrežno) in aplikacije: Med najbolj obiskanimi storitvami je platforma za aplikacije in igre. Facebook omogoča, da se na njegovi platformi kreirajo različne aplikacije za različne namene in igre, ki se lahko igrajo lokalno ali z drugimi uporabniki;
- elektronska pošta: V okviru svojega sistema sporočil (angl. *Messages*) je Facebook načrtoval, da bi ta storitev postopoma prerasla na nivo elektronske pošte (in prehitela konkurenco), vendar se to ni obneslo, tako da sedaj v tem okviru omogoča storitve takojšnjega sporočanja, avdio in video klice. Še vedno pa je možno tudi pošiljanje elektronskega sporočila na naslov uporabnika v domeni @facebook.com, ki je dostavljeno med ostala sporočila znotraj Facebooka;
- imenik: Seznam prijateljev oz. kontaktov na Facebooku se lahko do neke meje uporablja tudi kot imenik (angl. *addressbook*) – predvsem v kombinaciji s komunikacijskimi orodji in zlasti v primeru, če je večina kontaktov tudi aktivnih uporabnikov Facebooka. Nekatere mobilne aplikacije za Facebook tudi omogočajo integracijo med lokalnim imenikom in spiskom kontaktov na Facebooku;
- blogi ali druge interaktivne osebne/spletne strani: V okviru osebnega profila ali Facebook strani je na voljo več različnih možnosti objavljanja krajših ali daljših objav, tekstov, fotografij, vprašanj, video posnetkov idr., na katere publika komentira ali kako drugače reagira;
- fotoalbumi: Številnim ponudnikom shranjevanja in deljenja fotografij ali fotoalbumov na internetu precej dobro konkurira Facebookova storitev v zvezi s fotografijami, ki nenazadnje tudi podpira (tako kot vse ostale objave znotraj Facebooka) precej dobro razdelano možnost definiranja tega, kdo ima dostop do katere fotografije ali albuma;
- naročila na vsebine v okviru virov RSS (angl. *really simple syndication*) in okrožnic (angl. *newsletters*) ali druge periodike: V okviru različnih storitev Facebooka je možno izvajati obveščanje večjega števila ljudi oz. jim omogočiti, da se naročijo na taka obveščanja oz. periodične dostave. To je možno tako pri osebnih profilih kot straneh in skupinah. Do leta 2015 je Facebook za storitev »Pages« tudi omogočal vir RSS (kar je pomenilo, da je nekdo lahko redno spremljal objave na poljubni Facebook strani v kateremkoli RSS bralniku, četudi sam ni bil uporabnik Facebooka), vendar pa je tega ukinil. To zdaj pomeni, da nekdo, ki želi neko stran redno spremljati, nima več druge

možnosti naročila na objave kot to, da strani sledi znotraj Facebooka – s to potezo pa je Facebook še bolj zaprl ta segment znotraj svojega ekosistema in izničil interoperabilnost, ki je prej obstajala;
- planiranje dogodkov in koledar: V okviru storitve »Events« oz. dogodki je omogočeno kreiranje zasebnih ali javnih dogodkov in s tem povezano planiranje z vsemi elementi, ki se na tem področju pričakujejo;
- prijava na druge strani oz. v druge storitve: Že nekaj časa je na voljo možnost uporabe Facebook računa za namene prijave na strani ali v storitve drugih ponudnikov različnih storitev in vsebin na internetu (t. i. »social login«). Prav tako je možno, da se na različnih spletnih straneh vgradi vtičnike (angl. *plugins*), s pomočjo katerih se na strani, novici, članku ipd. lahko neposredno komunicira skozi Facebook (bodisi deli tako stran, nanjo reagira (»like«) ali pa naroči na ponudnikovo Facebook stran neposredno z njegove spletne strani).

To seveda ne pomeni, da prej omenjene storitve ne obstajajo več kot samostojne, ampak zgolj to, da jih je veliko število uporabnikov interneta v zadnjih letih pričelo uporabljati znotraj Facebooka; obstajajo pa celo taki (predvsem mlajši) uporabniki, ki enačijo pojma »internet« in »Facebook« oz. zanje internet predstavlja Facebook (Hatmaker, 2015). To pa je lahko že problematično z vidika narave odprtosti in interoperabilnosti interneta, saj ima lahko posamezen ponudnik (v tem primeru Facebook) tendenco k preferiranju svojih standardov in pravil ter zanemarjanju ostalih (odprtih oz. interoperabilnih) – nedavna žrtev, kot je že bilo omenjeno, je bil recimo RSS vir na Facebook straneh. Slaba stran z vidika zasebnosti in varovanja identitete (želje po anonimnosti) pa je lahko, da je (vsaj načelno) zahtevana uporaba dejanskega imena osebe, kar pri »neodvisnih« ponudnikih nekaterih storitev, kot so npr. forumi in sporočilniki, ni vedno predpogoj za uporabo.

Ob vsem tem Facebook razpolaga z enim največjih potencialov za najrazličnejše analize in izdelavo takih ali drugačnih povezav med podatki in podatkovnimi subjekti. Zato je tudi za oglaševalce privlačna platforma za namene ciljnega oglaševanja.

Do integracije storitev v okviru Facebooka je prišlo kot posledica ekonomij obsega (z rastjo števila uporabnikov) predvsem zaradi:

- večje enostavnosti za končne uporabnike (ni potrebno znanje HTML ali spletnega oblikovanja za oblikovanje prisotnosti na internetu, ni potrebno kreirati novih ali več računov za različne storitve ipd.);
- dostopnosti na različnih sistemih (računalniki, tablice, pametni telefoni) brez večjega napora in ponujanje enotnega pogleda z različnih naprav;
- do neke mere tudi zaupanja uporabnikov v storitve in medsebojno povezanost (uporaba, vsaj načelno, pravih imen in fotografij, povezanost med skupinami ljudi, princip »ker so že vsi drugi gor«);
- posledično pa je platforma postala privlačnejša tudi za podjetja kot pomemben kanal za promocijo svojega delovanja ali ciljno oglaševanje.

Ob tem pa kljub integrativni naravi Facebooka prihaja do svojevrstnega paradoksa, saj je po eni strani pod eno streho združeno veliko število podatkov, po drugi strani pa se zaradi velikega števila različnih aplikacij (za različne namene uporabe in od raznih ponudnikov oz. avtorjev) lahko pojavlja visoka razpršenost teh podatkov po podatkovnih zbirkah drugih ponudnikov in njihovih storitev (denimo ob uporabi načina prijave »social login« ali uporabi aplikacij ali iger, ki imajo lahko večji apetit po podatkih s profila kot pa ga dejansko za svoje delovanje potrebujejo).

Navzlic stalnim kritikam Facebooka glede uporabe osebnih podatkov pa je vseeno treba omeniti, da je ta ravno zaradi svoje dolge življenjske dobe skozi evolucijo do sedaj uspel že razmeroma varno (glede na konkurente ali predhodnike) utrditi in omogočiti uporabnikom, da odločajo o tem, kaj bo komu dostopno. Osebne spletne strani so bile dostopne bolj ali manj vsakomur, stara družabna omrežja so bila tudi predmet kraje podatkov ali fotografij, pri Facebooku pa do tega dandanes pride lahko samo še kot rezultat slabih nastavitev ali neumnosti na strani končnega uporabnika. Seveda pa še vedno ni popolne garancije glede tega, kaj se s temi podatki počne »v ozadju«, saj so ti lahko vedno predmet analiz in uporabe za namene oglaševanja in profiliranja (na strani Facebooka) ter, kot že omenjeno, preprodaje oz. posredovanja tretjim stranem (njegovim pogodbenim partnerjem ali organom pregona).

6.3.2 Osebni podatki, ki se obdelujejo

Nekateri od osebnih podatkov, ki jih Facebook obdeluje, so (Facebook's Data Pool, 2016): ime, priimek, druga imena in vzdevki, spremembe imen, datum rojstva, kraj rojstva, kraj bivanja, pretekla bivališča, fizični naslov, spol, stopnja izobrazbe, telefonske številke, naslovi elektronske pošte, politična orientiranost, religiozni in filozofski pogledi, obiskovane izobraževalne institucije, delodajalci, stanje osebnega razmerja, različni življenjski dogodki, znanje jezikov, interesi in hobiji, družinski člani in povezave med njimi, lokacije gibanja, IP naslovi in enolične oznake seje ali naprave idr.

Večino podatkov (tistih, ki se ne spremljajo samodejno) vnese uporabnik prostovoljno oz. vnos vseh za nemoteno uporabo ni zahtevan (z izjemo imena in priimka, datuma rojstva in elektronske pošte – v nekaterih primerih pa ob kreiranju računa zahteva tudi mobilno telefonsko številko za aktivacijo). Ima pa sistem najrazličnejše načine in spodbude pridobivanja dodatnih podatkov od uporabnikov. To izvaja med drugim z občasnim prikazom pojavnih oken (npr. predlaga, da vnesete telefonsko številko zaradi večje varnosti oz. za implementacijo dvofaktorske avtentikacije); naključno vpraša, od kod poznate to ali ono osebo (in hkrati ponudi kraje ali institucije, ki bi nakazovale na povezavo); spodbuja k izpolnitvi »manjkajočih« podatkov v profilu (in na podlagi določenega algoritma pripravi npr. spisek krajev, ki so po njegovem »mnenju« potencialni kraji bivališča uporabnika, ali seznam izobraževalnih institucij, za katere domneva, da jih je uporabnik obiskoval); spodbuja k označevanju oseb na fotografijah; spodbuja k vnosu telefonske številke in sinhronizacije imenika pri uporabi Messengerja na mobilni napravi;

spodbuja k vklopu sinhronizacije fotografij z mobilne naprave (z namenom zagotavljanja varnostne kopije); »sesa« podatke z drugih virov – s pomočjo povezav z drugimi aplikacijami, preko uporabe Facebook računa za prijavo v druge storitve ali aplikacije, s pomočjo vtičnikov na drugih spletnih straneh in s pomočjo slabše zaščitenih pametnih telefonov.

Glede zadnjega je problematična denimo večina verzij operacijskega sistema Android do zadnje verzije »Marshmallow«, saj povprečnemu uporabniku ne omogočajo podrobnih nastavitev posameznih pravic aplikacij, zato ima tam tudi Facebook aplikacija (ali z njo povezane, kot npr. Messenger) več pravic dostopa kot bi jih sicer potrebovala za običajno delovanje: med drugim ima ali zahteva poln dostop do kontaktov oz. imenika na napravi, dostop do drugih uporabniških računov, ki so shranjeni na napravi, prebiranje uporabnikove lastne vizitke, poln dostop do koledarja, dostop do trenutne lokacije, do shranjenih sporočil SMS, seznama klicev, fotografij, kamere, mikrofona, seznama wifi omrežij, identitete in statusa telefona (Facebook, 2016).

Veliko podatkov o osebi oz. uporabniku pa lahko sistem pridobi tudi posredno – preko prijateljev in širšega omrežja (»friends of friends«) uporabnika. Sistem relativno enostavno poveže podatke, ki jih imajo različni uporabniki shranjene v imeniku o različnih osebah. Ne glede na to, kako je en uporabnik skrben glede varnosti, izdajanja osebnih podatkov in dostopa do imenika, so nekateri njegovi podatki shranjeni tudi v imenikih ali elektronskih predalih drugih oseb, ki morebiti niso tako varnostno osveščene. Tu velja princip najšibkejšega člena, kar predstavlja veliko varnostno pomanjkljivost, saj oseba praktično nima nadzora nad tem, kaj se dogaja z njenimi podatki, ki se nahajajo v (vsaj načeloma zasebnih) imenikih drugih oseb, do katerih imajo lahko dostop tudi aplikacije oz. storitve kot je Facebook.

V preteklosti je Facebook (kot del njegove politike uporabljanja pravih oz. dejanskih imen oseb) poskušal posredno (t. j. preko prijateljev) pridobiti potrditev identitete osebe, če je ta uporabljala (domnevni) psevdonim (Vatteble, 2012). To je izvajal z namenom zagotavljanja načela, da en uporabniški račun predstavlja natanko eno resnično osebo, za namene poročanja o zlorabah, identifikacijo neavtoriziranih ali nepravilnih uporab storitev ter kraje identitete in ugrabljanja računov. Te aktivnosti potrjevanja naj bi bile sicer dokaj redke. V novejšem času so pogostejše aktivnosti, kjer sistem spodbuja uporabnika, da označi osebo na fotografiji (angl. *tag*). Sistem ima že vgrajen prefinjen način za prepoznavo obrazov in zaznavo oseb na fotografijah – tako lahko na poljubni fotografiji zazna, da se na njej pojavljajo ljudje, in tudi prepozna, kdo te osebe so (seveda če v sistemu že obstaja povezava med imenom in biometrijo obraza konkretne osebe). Končno potrditev (»tag«) mora še vedno izvesti uporabnik (bodisi zase bodisi za prijatelja), rezultat pa je še bolj popolna zbirka in izpolnjen algoritem za prepoznavo obrazov. To v kombinaciji z internetom stvari (Facebook je prisoten na najrazličnejših napravah, ki med drugim vsebujejo ali so na tak ali drugačen način povezane npr. s kamero) pa je že nevaren precedens, ki ima velik potencial iskanja obrazov v množici »na ulici«. Facebook trenutno

namreč razpolaga z največjo zbirko fotografij (ki so tudi vezane na posamezne osebe) na svetu izven okvira oblasti oz. držav ali organov pregona (Wellington, 2011).

Ob upoštevanju dejstva, da sta v lasti in tako pod nadzorom družbe Facebook Inc. tudi zelo razširjeni omrežji Instagram (za deljenje fotografij) in WhatsApp (komunikacije), pa sta doseg ter možnost zajemanja in povezovanja podatkov še toliko večja (če varnostno osveščen uporabnik na primer na svoji napravi Facebooku ne dovoli dostopa do imenika, pa je zelo verjetno, da bo to dovolil WhatsApp, saj ta za svoje delovanje potrebuje uporabnikovo telefonsko številko, za lažje delovanje in dostop do stanj ostalih uporabnikov pa tudi dostop do imenika).

Poleg »golega« zbiranja podatkov pa sistem skrbi tudi za vzdrževanje zanesljivih povezav in odnosov med tako zbranimi podatki. Ob stalnem spremljanju interakcij med uporabniki v okviru različnih storitev (npr. s kom se kdo več pogovarja ali komentira in reagira na objave) pridobiva stanje odnosov oz. povezav med uporabniki (kot ključnimi entitetami v sistemu, na katere se potem vežejo vsi ostali podatki in dogodki) tudi s pomočjo ustvarjenih skupin oz. prikazov novic (t. j. kako uporabniki oblikujejo te skupine in sezname oz. koga vključijo v katero skupino, kot npr. bližnji prijatelji, družina, sodelavci, znanci itn.) in vnosa nekaterih kategorij kot so npr. zapuščinski stik (ki upravlja z računom v primeru smrti uporabnika), zaupniki oz. zaupljivi stiki (s pomočjo katerih se lahko vzpostavi ponovni dostop do računa v primeru, ko se ta zaklene ali je geslo izgubljeno), uporabljen jezik vmesnika, uporabljena enota za temperaturo (Celzij ali Fahrenheit) ipd.

Facebook je precej rigiden glede oblike in sestave profilov (in njihovega prikaza), ki jo ponuja svojim uporabnikom. Lahko bi rekli, da je do neke mere v tem kontekstu celo tako »tog« kot povprečna aplikacija za vnos podatkov na tem ali onem državnem uradu, saj so določena polja zaklenjena oz. omejena na predviden nabor vrednosti. Tako denimo polja za vnos lokacij ne dopuščajo vnosa poljubnega ali izmišljenega imena lokacije oz. kraja, ampak zgolj vnos (v njihovi zbirki) obstoječih krajevnih imen (za razliko od Google Plus, kjer je to polje prostega vnosa in ki tudi pri drugih poljih ni tako strikten). Po drugi strani pa so pred kratkim sprostili vnos vrednosti za polje »spol« (Wong, 2015). S tem principom – t. j. da so določena polja omejena na zgolj predvidene (realne oz. dejansko obstoječe) vrednosti (in v kombinaciji z zahtevo po uporabi dejanskih osebnih imen in načela »en uporabnik, en profil«) – si je Facebook zastavil skrb za večjo kvaliteto vnesenih podatkov in s tem večjo vrednost za oglaševalce ali druge uporabnike teh podatkov.

6.3.3 Varovanje pravic

Družba Facebook Inc. ima sedež v Kaliforniji v ZDA in je tako podložna tamkajšnji zakonodaji (in posledično tudi njihovim pravilom glede nadzora). Za njene uporabnike v ZDA in Kanadi veljajo ta pravila, medtem ko je za uporabnike izven teh dveh držav zadolžena Facebookova podružnica na Irskem. Tako je za nadzor nad njihovimi evropskimi operacijami zadolžen irski informacijski pooblaščenec.

Vsak uporabnik lahko kadarkoli sam popravi svoje podatke, ki naj bi odražali dejansko stanje. Določene omejitve so v izogib zlorabam pri spremembah ključnih podatkov kot so ime, priimek in datum rojstva. V splošnem pa lahko rečemo, da so pravice do popravka, dopolnitve in brisanja na tem nivoju zagotovljene.

Bolj zapleteno je pri pravici do prenosljivosti, saj je to težje zagotavljati, ker imajo različni ponudniki različne standarde in različno oblikovane podatkovne zbirke. Facebook sicer ponuja možnost prenosa podatkov s profila na lokalni sistem (na računalnik), vendar gre zgolj za shranjevanje aktualnih podatkov z oddaljenega profila v lokalni sistem, saj ti podatki niso v obliki, ki bi omogočala tudi uvoz drugam (večinoma gre za HTML datoteke za besedilni del in JPG datoteke za fotografije). Možnost shranjevanja tako predvsem zagotavlja pravico do seznanitve z lastnimi podatki, saj shranjen komplet vsebuje tudi nekatere druge elemente, ki sicer niso vidni v profilu kot takem, kot so npr. prijavne seje, spremembe statusa računa, aktivnosti v zvezi s sejami in z računom (vključno z IP naslovi, oznako brskalnika, točnim časom aktivnosti, oznako piškotka …), reakcije na oglase ipd. Kljub temu pa so podatki v nestrukturirani obliki in shranjen je le del podatkov s profila (od najbolj očitnih manjkajo komentarji in reakcije s strani drugih uporabnikov na objave na tem profilu, enako velja tudi v obratni smeri). Za primerjavo: Google Plus ponuja možnost pridobitve lastnih podatkov v okviru storitve »Google Takeout«, ki pa določene segmente profila ponuja v takih vrstah datotek, ki jih je vsaj teoretično možno uvoziti drugam. Tako so kontaktni podatki v datotekah vCard (.vcf), ostali (tekstovni) deli profila pa v datotekah .json, ki so strukturirane in tako primernejše za morebitno nadaljnjo obdelavo.

V zvezi s pravico do seznanitve z lastnimi podatki bi veljalo omeniti tudi dnevnik dejavnosti (angl. *Activity Log*), v okviru katerega lahko uporabnik pregleduje svojo aktivnost na Facebooku po različnih kategorijah (in tudi izbriše ali skrije določene dogodke). Ker ta funkcionalnost ni bila na voljo od samega začetka, pa nekaterih starejših aktivnosti tu ni na voljo (bodisi niso prikazane bodisi jih je nemogoče sortirati oz. je do njih težko priti, saj je navigacija v primeru velikega števila dejavnosti lahko precej otežena). Nekatere starejše aktivnosti so prikazane, čeprav na profilu ne obstajajo več oz. so bile v preteklosti že pobrisane (kar kaže na to, da izbris verjetno ni bil popoln). Ob kliku na tak zapis se aktivnost (npr. objava) ne bo prikazala, ampak bo javljena napaka, da vsebine ni na voljo. Domnevamo lahko, da je problem tehnične narave, t. j. da se določene zadeve z vidika arhitekture sistema ali podatkovnih zbirk niso od vedno spremljale na način, ki bi omogočal spremljanje posameznih elementov ali njihov vpogled na način skozi dnevnik dejavnosti. Verjetno pa je, da se bo z nadaljnjo evolucijo te storitve postopoma odpravilo nekonsistentnost in hrošče ter transformiralo vse preostale podatke na način, da bo sistem deloval enotno. Pri novejših podatkih pa je opaziti, da ne beleži reakcij (npr. »like«) na komentarje pod objavami ali pa komentarjev na komentarje, torej podnivojev (tudi po prijavi napake tega niso odpravili oz. so zahtevek brez obrazložitve zaprli).

Najkompleksnejša je pravica biti pozabljen. Facebook zelo dolgo ni ponujal možnosti izbrisa računa, ampak zgolj možnost njegove deaktivacije. Sedaj je možno račun tako (začasno) deaktivirati kot (dokončno) izbrisati: Deaktivacija pomeni, da se račun deaktivira, uporabnikov profil in vsa aktivnost uporabnika (vključno s komentarji in reakcijami na drugih profilih) pa izgine iz vseh pogledov. Vse se ponovno pojavi, če se uporabnik odloči za reaktivacijo računa. Izbris računa pa pomeni, da se račun dokončno izbriše (vsaj v teoriji).

6.3.4 Europe v. Facebook in Max Schrems

V zvezi s pravico do seznanitve z lastnimi podatki in pravico biti pozabljen je treba omeniti še Maxa Schremsa in njegov projekt »Europe v. Facebook«, saj zadevne aktivnosti bistveno vplivajo tako na delovanje in obnašanje Facebooka ter odnose med Evropo in ZDA na področju prenosa podatkov o evropskih državljanih v ZDA.

Preden so uvedli možnost prenosa podatkov s profila na lokalni sistem preko spletnega brskalnika, je Facebook za zagotavljanje pravice do seznanitve z lastnimi podatki imel na svoji spletni strani poseben obrazec za zahtevek za izpis podatkov, ki jih ima o uporabniku. Po vnosu tega zahtevka je uporabnik v določenem času prejel CD, ki naj bi vseboval vse o njem shranjene podatke.

Avstrijski pravnik in zasebnostni aktivist Max Schrems je že v času študija zaznal, da vlada v ZDA precejšnje nerazumevanje ali pomanjkanje razumevanja evropske zakonodaje o varstvu osebnih podatkov. V okviru omenjenega zahtevka je Schrems prejel datoteko, ki je vsebovala preko 1200 strani izpisov (za približno 3 leta njegove uporabe Facebooka). Seznam je vseboval na stotine strani podatkov o uporabniku (tudi že izbrisane zadeve); med drugim tudi vse reakcije na dogodke, IP naslove, zgodovino sporočil, zgodovino sej, aktivnosti v zvezi z dodajanjem in odstranjevanjem prijateljev; naslove elektronske pošte, ki jih ni on sam vnesel, ampak so bili na profil verjetno povezani preko imenikov prijateljev; vmes je bil tudi seznam vseh, ki so bili na Facebook prijavljeni preko istega računalnika ali IP naslova kot on. Kljub ogromnemu številu podatkov je ugotovil, da izpis ni bil popoln in da je manjkalo še veliko stvari (med pomembnejšimi podatki, ki jih Facebook izrecno ni hotel posredovati, češ da gre za poslovno skrivnost, je bil biometrični zapis obraza). Kmalu zatem je Schrems osnoval skupino »Europe v. Facebook« in objavil izsledke (Hill, 2012). Omeniti velja, da je Facebook zaradi velikega števila zahtevkov po izpisu podatkov, ki so sledili objavi, umaknil to možnost in uvedel storitev prenosa podatkov preko brskalnika na računalnik. V tem okviru pa je shranjenih in razkritih še precej manj podatkov kot jih je bilo na voljo v fizični obliki.

V mesecih, ki so sledili, je Schrems posredoval kopico zahtevkov in pritožb irskemu informacijskemu pooblaščencu v zvezi z ravnanjem Facebooka z osebnimi podatki. V letu 2014 je s sodelavci pričel s postopki v zvezi z domnevno kršitvijo evropske zakonodaje s strani Facebooka – pričelo se je pri irskem informacijskem pooblaščencu, nadaljevalo na

irskem vrhovnem sodišču in v končni fazi na sodišču Evropske unije (Maximillian Schrems v. Data Protection Commissioner, 2015). Jeseni 2015 je razsodba evropskega sodišča rezultirala v preklicu veljavnosti načel varnega pristana med ZDA in EU (t. j. da je odločba 2000/520/ES (in s tem načela varnega pristana) neveljavna).

Po tem je Schrems vložil še vrsto drugih pritožb, v teku pa je tudi ena največjih skupinskih tožb proti Facebooku. Facebook med drugim obtožujejo naslednjega (Objectives of "europe-v-facebook.org", 2016):

- zapletena in uporabnikom neprijazna politika zasebnosti, ki ni v skladu z evropsko zakonodajo;
- domnevno sodelovanje v projektu PRISM ameriške varnostne agencije NSA;
- sledenje uporabnikom (in tudi ne-uporabnikom) na različnih spletnih straneh preko vdelanih gumbov »Like«;
- procesiranje podatkov dlje, kot je potrebno za dosego namena (brez zagotovila o dejanskem brisanju podatkov);
- odsotnost dejanskega strinjanja osebe glede velikega števila vrst podatkov, ki se zbirajo;
- neskladnost z zahtevki po dostopu do podatkov;
- dovoljenje za uporabo podatkov tretjim stranem (aplikacijam);
- nadzor aktivnosti uporabnikov s pomočjo analitike masovnih podatkov;
- in zahtevajo, da preneha z množičnim nadzorom, uveljavi primerno politiko zasebnosti, ki je ljudem razumljiva, uvede zasebnosti prijazne privzete nastavitve ob kreiranju računa in preneha zbirati podatke ljudi, ki niso njegovi uporabniki.

Poleg omenjenega so bile izdane tudi druge razsodbe v zvezi z obdelavo podatkov s strani Facebooka. Belgijska komisija za zasebnost v sodelovanju z Univerzo v Leuvnu je že februarja 2015 izdala podrobno poročilo o skladnosti operacij Facebooka (oz. njegovih takrat revidiranih pravilih in pogojih poslovanja) z evropsko zasebnostno zakonodajo. V splošnem je bilo ugotovljeno, da Facebook krši evropsko zakonodajo s področja zasebnosti oz. varstva osebnih podatkov ne glede na to, da je posodobil svojo politiko zasebnosti (KU Leuven, 2015). V februarju 2016 pa je tudi francoski nadzorni organ dal Facebooku tri mesece časa, da preneha s sledenjem oseb, ki niso njegovi uporabniki, in da preneha s prenosom nekaterih podatkov v ZDA (Fioretti, 2016), kar je prva pomembnejša oz. večja zahteva po tem, ko so bila načela varnega pristana razveljavljena. Pred tem je januarja 2016 nemško zvezno vrhovno sodišče razsodilo, da je Facebookova storitev »Friend Finder« nelegalna, saj s pomočjo naslovov, ki jih pridobi iz imenikov uporabnikov, novači ne-uporabnike h kreiranju računa (Wolde, 2016).

6.3.5 Trenutno stanje in odprti izzivi

Pred časom je bilo ugotovljeno, da Facebook shranjuje vsebino polj na svojih strežnikih tudi, če ne shranimo obrazca ali objavimo zapisa oz. kasneje prekličemo namero objave (hÚigínn, 2015). To je sicer lahko stranska posledica varnosti (avtomatsko shranjevanje zapisa, preden je dejansko shranjen oz. objavljen, da se zavaruje izguba vsebine, če vmes pride do sesutja brskalnika oz. sistema ali pride do izpada napajanja računalnika), problematično pa je, ker tako obstaja potencial, da se lahko hranijo prejšnje verzije zapisa ali stvari, ki jih v teku kreiranja zapisa, misli ali teksta uporabnik zaradi kakršnegakoli razloga v končni fazi ni imel namena objaviti ali razkriti.

Enega večjih problemov z vidika zasebnosti predstavljajo t. i. senčni profili (angl. *shadow profiles*), ki jih sistem kreira v ozadju (Morris, 2013). Gre za domnevo, da sistem v ozadju gradi profile, ki so popolnejša slika tistih, ki so vidni uporabnikom, s pomočjo vseh razpoložljivih virov in povezovanj med podatki. Tudi o tem teče ena od Schremsovih pritožb. Ti profili naj bi obstajali tako za uporabnike kot za ne-uporabnike, vsebovali pa naj bi tudi vse dejavnosti uporabnikov in vse podatke, ki so bili z vidnih profilov izbrisani. Obstaja celo domneva, da izbris objave, komentarja ali drugega elementa s profila dejansko izbriše samo prikaz v vidnem delu sistema, medtem ko v ozadju velja stalno shranjevanje vseh podatkov. Med vidnejšimi znaki, ki bi lahko nakazovali na obstoj senčnih profilov, bi bili lahko: prej omenjen prikaz določenih alinej (ki naj bi bile že pred leti izbrisane) v dnevniku dejavnosti; razlike med na profilu prikazanim skupnim številom fotografij ali video posnetkov v albumu in dejanskim stanjem teh elementov; prikazane so bile aplikacije, ki so bile že dolgo nazaj izbrisane; sistem je predlagal in vprašal za potrditev veljavnosti telefonske številke, ki je bila izbrisana pred nekaj leti. Možno pa je seveda tudi, da so vse to zgolj manifestacije hroščev kot posledica neprestanih nadgradenj in spreminjanj celotnega sistema. Poleg omenjenega pa je v kompletu podatkov, ki se jih lahko prenese na lokalni računalnik, tudi vrsta zapisov za celotno obdobje uporabe računa, kot so: prejšnja imena, odstranjeni kontakti (prijatelji), spremembe statusa računa (deaktivacije in reaktivacije), seznam aktivnih sej, spremembe statusa (prijave, odjave), seznam IP naslovov, podatki o piškotkih, spremembe nekaterih bistvenih podatkov v profilu (spol, profilna fotografija, imena, rojstni dan, geslo, varnostne nastavitve …).

V vsakem primeru pa menim, da – v luči tu omenjenih znakov nekonsistentnosti in Schremsovih ugotovitev – brez neodvisne revizije ni mogoče zagotoviti dejanske potrditve brisanja, saj ima lahko ponudnik ob stalnem padanju cen nosilcev podatkov in povezanih tehnologij naravno tendenco k stalnemu in večnemu shranjevanju vseh podatkov. Ker pri brisanju tako ni nikakršne garancije oz. ni vzpostavljenega sistema nadzora, neodvisne notranje in zunanje revizije ter potrditve, da je do izbrisa dejansko prišlo, lahko domnevamo, da pri izbrisu gre zgolj za »umik zapisa iz rednega oz. vidnega profila«. Če hočemo torej resnično zagotoviti ustrezno raven zaupanja v dejanski izbris podatkov, bi bila tu potrebna vsaj neodvisna zunanja revizija (ki periodično rotira, t. j. da izvajalec ni vedno isti), ob tem pa tudi ne smemo pozabiti, da na podatke, ki so se v času dostopnosti

kopirali drugam, izvorni upravljavec (v tem primeru Facebook) nima vpliva – razen v primeru, če gre za dogovorno (prikrito ali odkrito) kopiranje podatkov v podatkovni center obveščevalne ali varnostne službe oz. organov pregona, za kar je bil potreben konsenz tega upravljavca.

V zadnjem času je veliko prahu dvignila tudi pobuda Facebooka (v sodelovanju z nekaterimi drugimi družbami) Internet.org oz. »Free Basics« (Our Mission, 2016), ki namerava omogočati dosegljiv dostop do interneta na območjih, ki so manj razvita (npr. države tretjega sveta), saj zagovarjajo tezo, da je povezljivost oz. dostop do interneta človekova pravica. Pobuda je kritizirana predvsem z vidika tega, da naj bi kršila načela omrežne nevtralnosti (angl. *net neutrality*), saj naj bi preko tega bila na voljo le omejena povezljivost in brezplačen dostop samo do določenih vsebin ali ponudnikov. Zaradi tega je Indija storitev v februarju 2016 pri njih prepovedala (TRAI ruling on Net Neutrality, 2016). Dejstvo je, da ima s to ponudbo Facebook potencial, da svoji »populaciji« doda še ogromno število novih »prebivalcev« na območjih, ki do sedaj pretežno niso bila pokrita, in posledično tudi spremlja njihove aktivnosti, delovanje, navade, način razmišljanja in nenazadnje lahko tudi vpliva na odločanje.

V zadnjih letih so se pojavila tudi razmišljanja, da bi bilo potrebno družbene medije, kamor spada Facebook, kategorizirati kot javno službo (angl. *public utility*), da bi bili posledično (na podoben način kot to velja za službe na področju dobave vode, elektrike, kanalizacije ipd.) ustrezno regulirani (Boyd, 2010). Zagovorniki te teze trdijo, da je ponudnik dosegel nivo naravnega monopola (kar pomeni, da je bila največja stopnja učinkovitosti na trgu že dosežena pod eno streho), ima znatne koristi od ekonomij obsega (in se mu povečujejo vrednosti s povečevanjem števila uporabnikov), zelo težko je nadomestiti tržnega vodjo, težko se je izogniti, da bi ga ne uporabljali (ne glede na naše nasprotovanje), kreiranje in vzdrževanje profila je »naporno« in je malo verjetno, da bo uporabnik kreiral in aktivno vzdrževal profil in objave na več različnih omrežjih (tako kot tudi niso kabli ali ceste vzporedno položeni s strani več ponudnikov), prehod k alternativam, ki jih ni veliko, je vsaj neposredno takorekoč nemogoč, služi lahko kot (napol javni) imenik, preko katerega se pride do drugih uporabnikov ipd. Nasprotniki pa trdijo, da bi regulacija ovirala inovativnost, saj se tovrstne storitve in platforme pogosto spreminjajo, prihajajo novi ponudniki in izginejo stari (kar pa na primer ne velja za klasične javne službe), nenazadnje pa te storitve tudi niso nujne za preživetje.

Facebook je v zadnjem času bistveno prilagodil jasnost politike zasebnosti (stran, ki jo predstavlja, ni več enoličen težko berljiv pravniški tekst, ampak je predstavljena z različnimi barvami, oznakami in jasno berljivim zapisom in kategorizacijo po področjih, ki odgovarjajo na vprašanja, kot bi jih zastavil povprečen uporabnik) in vidnost nastavitev s področja zasebnosti, pa tudi uvedel dodatna opozorila glede nastavljanja ciljne publike pri vsaki objavi (Data Policy, b. l.). Kaže, da se torej zavedajo odgovornosti, ki jim jo prinaša visoka rast števila uporabnikov, in precedensov, ki jih s svojim delovanjem postavljajo na parket. Kljub temu pa ne gre pozabiti, da je njihova glavna »misija« še vedno zbiranje čim

večjega števila različnih podatkov, izdelava analiz in povezovanje različnih podatkov z namenom pridobitve čim natančnejše slike populacije, posameznikov in nenazadnje tudi predvidevanja prihodnjih akcij – in je tovrstna prijazno predstavljena politika lahko zgolj navzven prijazen obraz, da se posledično zmanjša zaskrbljenost uporabnikov glede tega.

6.4 Ugotovitve

Obravnavani trije primeri kažejo, da integracije informacijskih sistemov ali podatkovnih zbirk še zdaleč niso samo stvar tehničnega pristopa, ampak je za ustrezno vpeljavo sprememb v produkciji pomembno tudi natančno poznavanje omejitev pravnega okolja oz. družbe kot take.

Dobro je, da pri pripravi zadevne zakonodaje že od začetka sodelujejo nacionalni in evropski nadzorni organi za področje varstva osebnih podatkov (kot je bilo prikazano v primerih Vizis in Prostor). Kljub temu pa lahko kasneje še vedno pride do nekaterih kombinacij sistema, ki imajo za posledico (sicer nenamerno) kršitev zakonodaje in zahtevajo najprej naknadno ukrepanje s strani nadzornega organa (in po potrebi zakonodajalca) in potem še s strani upravljavca osebnih podatkov. V splošnem oba domača primera (tako Vizis kot Prostor) kažeta na ustrezno upoštevanje zahtevanega nivoja pravic podatkovnih subjektov, v praksi pa so uporabljena tudi druga načela in dobre prakse, kot so minimizacija podatkov (in dostopanje samo do tistih podatkov, ki so relevantni za posamezen postopek), brisanje podatkov po tem, ko je bil namen uporabe zaključen, ustrezna segregacija pravic dostopa s strani uporabnikov (in kontrola preverjanja njihove upravičenosti), skrb za kvaliteto obdelovanih podatkov (z različnimi kontrolami pravilnosti vnesenih podatkov) in seznanjenost uporabnikov s področjem varovanja (osebnih) podatkov, nenazadnje pa tudi omogočanje podatkovnim subjektom, da so preko spletne strani seznanjeni s pravicami.

Ker ima Evropa oz. EU razmeroma dobro urejeno področje varovanja osebnih podatkov in zasebnosti, tu načeloma ne prihaja do večjih neskladij; možnosti tega pa se povečajo pri odnosih s t. i. tretjimi državami oz. informacijskimi sistemi, ki se nahajajo v teh državah. Zlasti na relaciji med EU in ZDA tako lahko pogosto pride do nasprotij interesov ali zakonodaje, kot kažejo izsledki primera Facebook oz. »Europe v. Facebook«, kjer je bila v preteklih mesecih odmevna razveljavitev načel varnega pristana in priprava novega okvira za izmenjavo podatkov med EU in ZDA – to pa lahko posledično posega tudi širše v (poslovne) odnose gospodarskih družb, ki poslujejo med tema dvema prostoroma, in zahteva njihovo učinkovito prilagoditev spremenjenim razmeram.

SKLEP

Pravica do zasebnosti kot taka ni nov koncept. V povezavi z informacijsko-komunikacijskimi sistemi in njihovimi integracijami pa se njena pomembnost in izpostavljenost še povečujeta, saj z novimi tehnologijami in najrazličnejšimi

kombinacijami in integracijami le-teh prihaja do vedno novih situacij, ki prej niso obstajale in ki s sabo prinašajo nove izzive na področju varovanja zasebnosti, osebnih podatkov in nenazadnje tudi človekovega dostojanstva.

Trenutno veljavna zakonodaja ima vgrajene določene varovalke na podlagi preteklih izkušenj družbe (npr. prepoved zbiranja določenih osebnih podatkov, samodejnega povezovanja določenih podatkov ali iz njih izvedenega avtomatskega odločanja in prepoved ene vseobsegajoče državne podatkovne zbirke, če omenim najbolj očitne primere), ki bistveno omejujejo možnost, da bi se za ceno popolne učinkovitosti in dostopnosti integriranje podatkov in podatkovnih zbirk v končni fazi izpridilo do tiste stopnje, kjer bi že imelo potenciale velikih možnosti zlorab in posledično totalitarizma. Evropska sodna praksa in načela varstva zasebnosti in osebnih podatkov se zaenkrat uspešno zoperstavljajo željam korporacij, pa tudi državnih institucij, po prevelikem integriranju podatkov in podatkovnih zbirk.

Bistvena za uspešno evolucijo na tem področju je tudi kultura ljudi, t. j. njihovo razumevanje pomembnosti zasebnosti in varovanja podatkov ter zavračanje zmotnega mišljenja »če nimam ničesar skrivati, se nimam ničesar bati«. To je lahko težavno, saj gre tu večkrat za kompromis med udobjem in zasebnostjo, kjer pa je naravna tendenca človeka lahko predvsem v smeri udobja. Poleg tega gre tudi za kompromis med varnostjo družbe in zasebnostjo posameznika.

Menim, da problematika zaradi svoje kompleksnosti in ažurnosti oz. hitrega spreminjanja tako področja tehnologije kot varstva podatkov trenutno več vprašanj odpira kot pa nanje daje odgovore. Predvsem je ravno zaradi tega velik poudarek na sprotni sodni praksi – v Sloveniji (in EU) različnim odločbam Informacijskega pooblaščenca, v ZDA sodnim primerom, ki gradijo sodno prakso.

Med drugim bo v bližnji prihodnosti za obravnavano področje pomembno, v katero smer se bo razvijal projekt Maxa Schremsa »Europe v. Facebook« (ki zdaj že bistveno vpliva tudi na pravne elemente, ki niso več omejeni samo na Facebook); kaj se bo dogajalo s pravico »biti pozabljen« (ali se bo ukoreninila kot splošno sprejeta ali pa bo v konfliktu z delovanjem organov pregona; pa tudi to, kako se bo izražala in izvajala v praksi); kako bo obravnavana zasebnost v povezavi s t. i. protiteroristično zakonodajo; ali bo prevladal evropski model varstva zasebnosti in osebnih podatkov tudi širše; in nenazadnje tudi, kaj se bo dogajalo z internetom stvari in nosljivim računalništvom.

Ključno vprašanje v tem trenutku je, ali se bodo zakonodajne oblasti uspešno in z zadovoljivo hitrostjo prilagajale novim in nadgrajenim tehnologijam ter kombinacijam le-teh, da bo s pravnega vidika doseženo ustrezno ravnovesje med svobodo in zasebnostjo posameznika, varstvom konkurence in splošno varnostjo v družbi. Na tej točki je potrebno učinkovito obvladovanje vpliva interesnih skupin in lobijev ter pomembno pravočasno

zaznavanje novih izzivov in tega, kako tehnološke spremembe ovirajo ali v prihodnosti lahko vplivajo na zadevne pravice.

Področje je tudi zaradi svoje multidisciplinarne narave zanimivo za nadaljnja (tudi interdisciplinarna) raziskovanja z velikega števila aspektov: s pravnega, tehničnega, z ekonomskega, s sociološkega, nenazadnje pa tudi s psihološkega in političnega vidika.

Popolna integracija pa danes navsezadnje še ni možna tudi zaradi tega, ker človeštvo kot celota evolucijsko še ni na taki ravni, da bi bilo to izvedljivo brez potencialov zlorab ali totalitarizma.

LITERATURA IN VIRI

1. *About ISACA*. Najdeno 10. decembra 2015 na spletnem naslovu http://www.isaca.org/about-isaca/Pages/default.aspx
2. Agencija Evropske unije za temeljne pravice & Svet Evrope. (2014). *Priročnik o evropskem pravu varstva osebnih podatkov*. Luksemburg: Urad za publikacije Evropske unije.
3. Andress, J. (2014). *The Basics of Information Security (Understanding the Fundamentals of InfoSec in Theory and Practice).* Oxford: Elsevier Inc.
4. Bapat, A. (2013). The new right to data portability. *Privacy & Data Protection (PDP Journals), 13*(3), 3-4.
5. Bhaiji, Y. (2008, 25. julij). Chapter 1: Overview of Network Security. *Network World*. Najdeno 10. decembra 2015 na spletnem naslovu http://www.networkworld.com/article/2274081/lan-wan/chapter-1--overview-of-network-security.html
6. Bhatt, G. D. (2000). An empirical examination of the effects of information systems integration on business process improvement. *International Journal of Operations & Production Management, 20*(11), 1331-1359.
7. Blagov, S. (2015, 10. avgust). Russia Clarifies Looming Data Localization Law. *Bloomberg BNA*. Najdeno 6. decembra 2015 na spletnem naslovu http://www.bna.com/russia-clarifies-looming-n17179934521/
8. Boyd, D. (2010, 15. maj). Facebook is a utility; utilities get regulated. *Apophenia*. Najdeno 29. februarja 2016 na spletnem naslovu http://www.zephoria.org/thoughts/archives/2010/05/15/facebook-is-a-utility-utilities-get-regulated.html
9. Bugging the boardroom. (2006, 5. september). *BBC News*. Najdeno 12. decembra 2015 na spletnem naslovu http://news.bbc.co.uk/2/hi/technology/5313772.stm
10. Calder, A., & Watkins, S. (2008). *IT Governance: A Manager's Guide to Data Security and ISO27001/ISO27002* (4th Edition). London & Philadelphia: Kogan Page Limited.
11. Clapper, J. R. (2016). *Statement for the Record - Worldwide Threat Assessment of the US Intelligence Community*. Washington: United States Commitee on Armed Services.
12. Clarke, R. (1988). Information Technology and Dataveillance. *Communications of the ACM, 31*(5), 498-512.
13. COBIT 4.1: Framework for IT Governance and Control. (2015). *ISACA*. Najdeno 10. decembra 2015 na spletnem naslovu http://www.isaca.org/Knowledge-Center/COBIT/Pages/Overview.aspx
14. Damij, T., Grad, J., & Jaklič, J. (1995). *Izbrane teme iz informacijske tehnologije*. Ljubljana: Ekonomska fakulteta.
15. Data Integration. (b. l.). *IBM Analytics*. Najdeno 12. decembra 2015 na spletnem naslovu http://www.ibm.com/analytics/us/en/technology/data-integration/

16. *Data Policy*. (b. l.). Najdeno 1. marca 2016 na spletnem naslovu https://www.facebook.com/about/privacy/
17. *Data Protection Day*. (b. l.). Najdeno 15. maja 2015 na spletnem naslovu http://www.coe.int/t/dghl/standardsetting/dataprotection/Data_protection_day_en.asp
18. *Digital Rights Ireland Ltd v. multiple parties*. (2014, 8. april). C-293/12 & C-594/12. Najdeno 15. februarja 2016 na spletnem naslovu http://curia.europa.eu/juris/document/document.jsf?docid=150642&doclang=EN
19. Direktiva 2002/58/ES Evropskega parlamenta in Sveta o obdelavi osebnih podatkov in varstvu zasebnosti na področju elektronskih komunikacij (Direktiva o zasebnosti in elektronskih komunikacijah). *Uradni list EU* L 201.
20. Direktiva 2006/24/ES Evropskega parlamenta in Sveta o hrambi podatkov, pridobljenih ali obdelanih v zvezi z zagotavljanjem javno dostopnih elektronskih komunikacijskih storitev ali javnih komunikacijskih omrežij, in spremembi Direktive 2002/58/ES. *Uradni list EU* L 105.
21. Direktiva 95/46/ES o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov. *Uradni list EU* L 281, sprememba *Uredba (ES)* 1882/2003, UL L 284.
22. *Documents and Public Comments Provided through the Duration of the Safe Harbor Negotiations*. (2009, 5. februar). Najdeno 15. januarja 2016 na spletnem naslovu http://web.archive.org/web/20150914162301/http://export.gov/safeharbor/eu/eg_main_018496.asp
23. Dumortier, J. (2012, 7. februar). New draft European data protection regulation analysed. *Advocatenkantoor voor de informatiemaatschappij*. Najdeno 3. decembra 2015 na spletnem naslovu http://www.timelex.eu/nl/blog/detail/new-draft-european-data-protection-regulation-analysed
24. Edward Snowden, Glenn Greenwald & David Miranda Call for Global Privacy Treaty. (2015, 1. oktober). *Democracy Now*. Najdeno 11. decembra 2015 na spletnem naslovu http://www.democracynow.org/blog/2015/10/1/video_edward_snowden_glenn_greenwald_david
25. Eppler, M. J. (2003). *Managing Information Quality*. Berlin/Heidelberg: Springer-Verlag.
26. Evropska komisija. (2012a, 25. januar). Commission proposes a comprehensive reform of the data protection rules. Najdeno 15. maja 2015 na spletnem naslovu http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm
27. Evropska komisija. (2012b, 25. junij). Uporaba prava Evropske unije. Najdeno 28. julija 2014 na spletnem naslovu http://ec.europa.eu/eu_law/introduction/what_directive_sl.htm
28. Evropska komisija. (2013a, 27. november). Communication from the Commission to the European Parliament and the Council on the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU.

Najdeno 6. decembra 2015 na spletnem naslovu http://ec.europa.eu/justice/data-protection/files/com_2013_847_en.pdf

29. Evropska komisija. (2013b, 25. julij). EU Charter of Fundamental Rights. Najdeno 9. septembra 2014 na spletnem naslovu http://ec.europa.eu/justice/fundamental-rights/charter/index_en.htm
30. Evropska komisija. (2016, 3. februar). Statement of the Article 29 Working Party on the Consequences of the Schrems Judgment. Najdeno 5. februarja 2016 na spletnem naslovu http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2016/20160203_statement_consequences_schrems_judgement_en.pdf
31. Evropska unija. (2015, 30. avgust). European Union regulations. Najdeno 6. decembra 2015 na spletnem naslovu http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=URISERV:l14522
32. Facebook. (2016). V *Android Apps on Google Play*. Najdeno 1. marca 2016 na spletnem naslovu https://play.google.com/store/apps/details?id=com.facebook.katana&hl=en
33. Facebook Expansion Enables More People to Connect with Friends in a Trusted Environment. (2006, 26. september). *Facebook Newsroom*. Najdeno 20. marca 2016 na spletnem naslovu https://newsroom.fb.com/news/2006/09/facebook-expansion-enables-more-people-to-connect-with-friends-in-a-trusted-environment/
34. *Facebook's Data Pool*. (2016). Najdeno 2. marca 2016 na spletnem naslovu http://europe-v-facebook.org/EN/Data_Pool/data_pool.html
35. Falkvinge, R. (2012, 19. julij). Debunking The Dangerous "If You Have Nothing To Hide, You Have Nothing To Fear". *Falkvinge on Infopolicy*. Najdeno 8. septembra 2014 na spletnem naslovu http://falkvinge.net/2012/07/19/debunking-the-dangerous-nothing-to-hide-nothing-to-fear/
36. Fioretti, J. (2016, 8. februar). French data privacy regulator cracks down on Facebook. *Reuters*. Najdeno 1. marca 2016 na spletnem naslovu http://www.reuters.com/article/us-facebook-france-privacy-idUSKCN0VH1U1
37. Fung, B. (2016, 20. januar). Internet providers want to know more about you than Google does, privacy groups say. *The Washington Post*. Najdeno 16. februarja 2016 na spletnem naslovu https://www.washingtonpost.com/news/the-switch/wp/2016/01/20/your-internet-provider-is-turning-into-a-data-hungry-tech-company-consumer-groups-warn/
38. Generalna skupščina Združenih narodov. (1948, 10. december). *Splošna deklaracija človekovih pravic* (Resolucija št. 217 A (III)).
39. Generalna skupščina Združenih narodov. (1966, 16. december). *Mednarodni pakt o državljanskih in političnih pravicah* (Resolucija št. 2200 A (XXI)).
40. Goodside, M. (2011, 23. september). Modern-Day Systems Integration Through a Historical Lens. *PropertyCasualty360*. Najdeno 10. decembra 2015 na spletnem naslovu http://www.propertycasualty360.com/2011/09/23/modern-day-systems-integration-through-a-historica?page_all=1

41. *Google Spain SL and Google Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*. (2014, 13. maj). C-131/12. Najdeno 13. februarja 2016 na spletnem naslovu http://curia.europa.eu/juris/document/document.jsf?text=&docid=152065&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=603299
42. *Griswold v. Connecticut*. (1965, 7. junij). 381 U.S. 479. Najdeno 11. septembra 2015 na spletnem naslovu https://supreme.justia.com/cases/federal/us/381/479/case.html
43. Hatmaker, T. (2015, 9. februar). Facebook is becoming synonymous with 'Internet' to global users. *The Daily Dot*. Najdeno 29. februarja 2016 na spletnem naslovu http://www.dailydot.com/technology/facebook-internet-perception-global/
44. Hill, K. (2012, 7. februar). Max Schrems: The Austrian Thorn In Facebook's Side. *Forbes.* Najdeno 1. marca 2016 na spletnem naslovu http://www.forbes.com/sites/kashmirhill/2012/02/07/the-austrian-thorn-in-facebooks-side/#1bc3e5d56b30
45. Howard, P. (2006, 19. maj). The evolution of integration platforms. *The Register*. Najdeno 10. decembra 2015 na spletnem naslovu http://www.theregister.co.uk/2006/05/19/integration_platforms
46. hÚigínn, P. Ó. (2015, 7. april). Facebook sending 'nonposts' to its servers. *Enginn Solutions*. Najdeno 1. marca 2016 na spletnem naslovu http://blog.higg.im/2015/04/07/facebook-sending-nonposts-to-its-servers-and-stores-unpublished-thoughts/
47. Hustinx, P. (2010). Privacy by design: delivering the promises. *Identity in the Information Society, 3*(2), 253-255.
48. Informacijski pooblaščenec. (2008). *Smernice glede uvedbe biometrijskih ukrepov.* Ljubljana: Informacijski pooblaščenec.
49. Informacijski pooblaščenec. (2009a). *Varstvo osebnih podatkov pri povezovanju zbirk osebnih podatkov v javni upravi.* Ljubljana: Informacijski pooblaščenec.
50. Informacijski pooblaščenec. (2009b). *Kodeks obnašanja pri zbiranju osebnih podatkov (Smernice za zasebni sektor).* Ljubljana: Informacijski pooblaščenec.
51. Informacijski pooblaščenec. (2009c). *Smernice Informacijskega pooblaščenca za oblikovanje izjave o varstvu osebnih podatkov na spletnih straneh.* Ljubljana: Informacijski pooblaščenec.
52. Informacijski pooblaščenec. (2010a). *Presoje vplivov na zasebnost pri projektih eUprave (Smernice Informacijskega pooblaščenca).* Ljubljana: Informacijski pooblaščenec.
53. Informacijski pooblaščenec. (2010b). *Smernice za razvoj informacijskih rešitev.* Ljubljana: Informacijski pooblaščenec.
54. Informacijski pooblaščenec. (2012, 3. januar). Začasna odločba. Najdeno 28. februarja 2016 na spletnem naslovu http://www.gu.gov.si/fileadmin/gu.gov.si/pageuploads/novice/Teksti_novic/Zacasna_odlocba.pdf

55. Informacijski pooblaščenec. (2015). *Zavarovanje osebnih podatkov (Smernice Informacijskega pooblaščenca).* Ljubljana: Informacijski pooblaščenec.
56. Integration. (b. l.). V *The Tech Dictionary and IT Encyclopedia*. Najdeno 6. decembra 2015 na spletnem naslovu http://searchcrm.techtarget.com/definition/integration
57. *ITIL and IT Service Management*. Najdeno 10. decembra 2015 na spletnem naslovu http://www.itil.org.uk/
58. *Iznos osebnih podatkov v tretje države*. Najdeno 4. decembra 2015 na spletnem naslovu https://www.ip-rs.si/varstvo-osebnih-podatkov/obveznosti-upravljavcev/iznos-osebnih-podatkov-v-tretje-drzave/safe-harbor/
59. Jentzsch, N., Preibusch, S., & Harasser, A. (2012). *Study on monetising privacy - An economic model for pricing personal information.* Heraklion: European Union Agency for Network and Information Security (ENISA).
60. Jhingran, A., Mattos, N., & Pirahesh, H. (2002). Information integration: A research agenda. *IBM Systems Journal, 41*(4), 555-562.
61. Joh, E. E. (2013). Privacy Protests: Surveillance Evasion and Fourth Amendment Suspicion. *Arizona Law Review, 55*(4), 997-1029.
62. Juels, A., Molnar, D., & Wagner, D. (2005). Security and Privacy Issues in E-passports. *SecureComm 2005* (str. 74-88). Athens: IEEE.
63. *Katz v. United States*. (1967, 18. december). 389 U.S. 347. Najdeno 20. junija 2015 na spletnem naslovu http://supreme.justia.com/cases/federal/us/389/347/case.html
64. Kavakli, E., Kalloniatis, C., Loucopoulos, P., & Gritzalis, S. (2006). Incorporating privacy requirements into the system design process. *Internet Research, 16*(2), 140-158.
65. Kazenski zakonik. *Uradni list RS* št. 50/2012-UPB2.
66. Kerr, O. S. (2009). The Case for the Third-Party Doctrine. *Michigan Law Review, 107*(4), 561-602.
67. *Key definitions of the Data Protection Act*. Najdeno 6. decembra 2015 na spletnem naslovu https://ico.org.uk/for-organisations/guide-to-data-protection/key-definitions/
68. Kleeman, S. (2015, 29. maj). In One Quote, Snowden Just Destroyed the Biggest Myth About Privacy. *Mic*. Najdeno 6. decembra 2015 na spletnem naslovu http://mic.com/articles/119602/in-one-quote-edward-snowden-summed-up-why-our-privacy-is-worth-fighting-for
69. Klostermann, J. (2015, 15. december). The Evolution of Business Intelligence. *CloudTweaks.* Najdeno 31. januarja 2016 na spletnem naslovu http://cloudtweaks.com/2015/12/evolution-business-intelligence/
70. Krebs, B. (2016). IoT Reality: Smart Devices, Dumb Defaults. *Krebs on Security*. Najdeno 10. februarja 2016 na spletnem naslovu https://krebsonsecurity.com/2016/02/iot-reality-smart-devices-dumb-defaults/
71. KU Leuven. (2015, 25. avgust). KU Leuven Centre for IT & IP Law and iMinds-SMIT advise Belgian Privacy Commission in Facebook investigation. Najdeno 1. marca 2016 na spletnem naslovu

http://www.law.kuleuven.be/citip/en/news/item/icri-cir-advises-belgian-privacy-commission-in-facebook-investigation

72. Lenzerini, M. (2002). Data integration: a theoretical perspective. *ACM SIGMOD-SIGACT-SIGART symposium on Principles of database systems* (str. 233-246). New York: ACM.
73. Linthicum, D. (2015, 22. julij). 5 Things That Will Drive Data Integration Over the Next 10 Years. *The Informatica Blog – Perspectives for the Data Ready Enterprise*. Najdeno 2. februarja 2016 na spletnem naslovu http://blogs.informatica.com/2015/07/22/5-things-that-will-drive-data-integration-over-the-next-10-years/
74. Listina Evropske unije o temeljnih pravicah. *Uradni List EU* C 83 (2010/C 83/02).
75. *Managing the Data Warehouse Environment*. Najdeno 24. januarja 2016 na spletnem naslovu https://docs.oracle.com/cd/B19306_01/server.102/b14223/part4.htm
76. Marcella, Jr., A. J., & Stucki, C. (2003). *Privacy Handbook: Guidelines, Exposures, Policy Implementation, and International Issues.* Hoboken: John Wiley & Sons, Inc.
77. *Maximillian Schrems v. Data Protection Commissioner*. (2015, 6. oktober). C-362/14. Najdeno 1. marca 2015 na spletnem naslovu http://curia.europa.eu/juris/document/document.jsf?text=&docid=169195&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=604406
78. Mišič, K., & Tomšič, A. (2007). *Zavarujmo osebne podatke (Priročnik za upravljavce osebnih podatkov).* Ljubljana: Informacijski pooblaščenec.
79. Morris, K. (2013, 26. junij). Facebook Shadow Profiles: What You Need to Know. *Mashable.* Najdeno 1. marca 2016 na spletnem naslovu http://mashable.com/2013/06/26/facebook-shadow-profiles/#gGhQMLQBpqqG
80. Moumina, A., & Bergin, T. (b. l.). History of Operating Systems & History of Computing. *Online Computer Science Exam Preparation.* Najdeno 1. decembra 2015 na spletnem naslovu http://www.psexam.com/Notes-for-Computer-Science/operating-systems-history-of-operating-system-article/All-Pages.html
81. *Objectives of "europe-v-facebook.org"*. Najdeno 2. marca 2016 na spletnem naslovu http://europe-v-facebook.org/EN/Objectives/objectives.html
82. Odločba Evropske komisije 2000/520/ES. *Uradni list EU* L 215.
83. Odločba Komisije 2001/497/ES o standardnih pogodbenih klavzulah za prenos osebnih podatkov v tretje države v skladu z Direktivo 95/46/ES. *Uradni list EU* L 181.
84. Odločba Komisije 2004/915/ES o spremembi Odločbe 2001/497/ES glede uvedbe alternativnega sklopa standardnih pogodbenih klavzul za prenos osebnih podatkov v tretje države. *Uradni list EU* L 385.
85. Odločba Ustavnega sodišča US27747. *Uradni list RS* št. 65/2007 in *OdlUS* XVI, 67
86. Odločitve Ustavnega sodišča US30439. *Uradni list RS* št. 54/2014 in *OdlUS* XX, 27.

87. *Olmstead v. United States*. (1928, 4. junij). 277 U.S. 438. Najdeno 20. junija 2015 na spletnem naslovu http://supreme.justia.com/cases/federal/us/277/438/case.html
88. *Onemogočen dostop*. Najdeno 7. marca 2016 na spletnem naslovu http://www.gu.gov.si/si/javne_objave/aktualno_cele_novice/onemogocen_dostop/
89. Onn, Y., Druckman, Y., Timor, R., Maroun, A., Nachmani, Y., Sicklai, S., Fishman, M., Pery, L., Geva, M., Zyssman, A., Lev, I., Maron, T., Simsolo, Y., Fuches, A., Packer, S. (2005). *Privacy in the Digital Environment.* Haifa: Haifa Center of Law & Technology, Faculty of Law, University of Haifa.
90. *Our Mission*. Najdeno 20. marca 2016 na spletnem naslovu iz https://info.internet.org/en/mission/
91. Ozimek, G. (2008). *Integracija podatkov* (diplomsko delo). Ljubljana: Ekonomska fakulteta.
92. *Pogosta vprašanja*. Najdeno 13. aprila 2015 na spletnem naslovu https://www.ip-rs.si/pogosta-vprasanja/varstvo-osebnih-podatkov/
93. Povzetki zakonodaje EU. (2011, 1. februar). Najdeno 12. junija 2014 na spletnem naslovu http://europa.eu/legislation_summaries/information_society/data_protection/l14012_sl.htm
94. Priebe, J., & Tomaszewski, J. (2015, 4. maj). Fortress Russia – The Russian Data Localization Law. *The Global Privacy Watch.* Najdeno 6. decembra 2015 na spletnem naslovu http://www.globalprivacywatch.com/2015/05/fortress-russia-the-russian-data-localization-law/
95. Privacy Office, U.S. Department of Homeland Security. (2007). *Privacy Technology Implementation Guide.* Washington, DC: U.S. Department of Homeland Security.
96. *Public Utilities Comm'n v. Pollak*. (1952, 26. maj). 343 U.S. 451. Najdeno 11. septembra 2015 na spletnem naslovu https://supreme.justia.com/cases/federal/us/343/451/case.html
97. Richards, N. M. (2013, 25. marec). The Dangers of Surveillance. *Harvard Law Review, 126*, 1934-1965.
98. Richelieu, K. (b. l.). V *QuotationsBook*. Najdeno 5. junija 2014 na spletnem naslovu http://quotationsbook.com/quote/19331/
99. Rodriguez, K. (2015, 8. julij). EFF Welcomes The United Nations' New Privacy Watchdog. *Electronic Frontier Foundation.* Najdeno 6. decembra 2015 na spletnem naslovu https://www.eff.org/deeplinks/2015/07/eff-welcomes-united-nations-new-privacy-watchdog
100. Rosen, J. (2012, 13. februar). The Right to Be Forgotten. *Stanford Law Review.* Najdeno 4. decembra 2015 na spletnem naslovu http://www.stanfordlawreview.org/online/privacy-paradox/right-to-be-forgotten
101. Rotar, M. (2008). Vzpostavitev registra nepremičnin (REN). *Geodetski vestnik, 52*(2), 372-373.

102. Roy, A. (2008, 20. julij). History and Trends in Data Integration. *Toolbox.com*. Najdeno 28. februarja 2016 na spletnem naslovu http://it.toolbox.com/blogs/data-integration/history-and-trends-in-data-integration-26094
103. *Schengen Area*. Najdeno 15. februarja 2016 na spletnem naslovu http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/borders-and-visas/schengen/index_en.htm
104. Schmidt, J. (2008, 23. junij). Integration as Strategy. *Informatica.* Najdeno 10. decembra 2015 na spletnem naslovu http://web.archive.org/web/20090319063004/http://blogs.informatica.com/enterprise_data_management/index.php/2008/06/integration-as-strategy/
105. Schneier, B. (2006, 18. maj). The Eternal Value of Privacy. *Schneier on Security*. Najdeno 31. aprila 2014 na spletnem naslovu https://www.schneier.com/essay-114.html
106. Schneier, B. (2009, 26. februar). The Tech Lab: Bruce Schneier. *BBC News.* Najdeno 5. junija 2014 na spletnem naslovu http://news.bbc.co.uk/1/hi/technology/7897892.stm
107. Schneier, B. (2012, 26. november). When It Comes to Security, We're Back to Feudalism. *Wired.* Najdeno 13. decembra 2015 na spletnem naslovu http://www.wired.com/opinion/2012/11/feudal-security/
108. Schneier, B. (2015, 24. december). How the Internet of Things Limits Consumer Choice. *The Atlantic.* Najdeno 5. februarja 2016 na spletnem naslovu http://www.theatlantic.com/technology/archive/2015/12/internet-of-things-philips-hue-lightbulbs/421884/
109. Schneier, B. (2016a, 8. januar). The Internet of Things That Talk About You Behind Your Back. *Motherboard.* Najdeno 3. februarja 2016 na spletnem naslovu https://motherboard.vice.com/en_ca/read/the-internet-of-things-that-talk-about-you-behind-your-back
110. Schneier, B. (2016b, 4. februar). The Internet of Things Will Be the World's Biggest Robot. *Schneier on Security.* Najdeno 5. februarja 2016 na spletnem naslovu https://www.schneier.com/blog/archives/2016/02/the_internet_of_1.html
111. Skinner, G., Han, S., & Chang, E. (2006). A conceptual framework for Information Security and Privacy. *5th WSEAS International Conference on Applied Computer Science* (str. 410-415). Hangzhou: WSEAS.
112. Solove, D. J. (2001). Privacy and Power: Computer Databases and Metaphors for Information Privacy. *Stanford Law Review*(53), 1393-1462.
113. Solove, D. J. (2011, 15. maj). Why Privacy Matters Even if You Have 'Nothing to Hide'. *The Chronicle of Higher Education.* Najdeno 8. septembra 2014 na spletnem naslovu http://chronicle.com/article/Why-Privacy-Matters-Even-if-You-Have-Nothing-to-Hide/127461/
114. Statista. (2016). Leading social networks worldwide as of January 2016, ranked by number of active users (in millions). Najdeno 29. februarja 2016 na spletnem naslovu http://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/

115. Steenkamp, R. (2013). My annotated GDPR | Chapter III | Section 3 | Article 18. *Rina Steenkamp – Privacy and technology*. Najdeno 7. decembra 2015 na spletnem naslovu http://www.steenkamp-ict.com/gdpr/art18.html
116. Stenovec, T. (2015, 28. januar). Facebook Is Now Bigger Than The Largest Country On Earth. *The Huffington Post.* Najdeno 29. februarja 2016 na spletnem naslovu http://www.huffingtonpost.com/2015/01/28/facebook-biggest-country_n_6565428.html
117. Stevens, T. (2009, 25. februar). Debunking a myth: If you have nothing to hide, you have nothing to fear. *Identity, Privacy and Trust (The Data Trust Blog).* Najdeno 20. junija 2014 na spletnem naslovu http://www.computerweekly.com/blogs/the-data-trust-blog/2009/02/debunking-a-myth-if-you-have-n.html
118. Svet Evrope. (1981, 28. januar). Konvencija o varstvu posameznika glede na avtomatsko obdelavo osebnih podatkov. Najdeno 15. septembra 2015 na spletnem naslovu http://www.svetevrope.si/sl/dokumenti_in_publikacije/konvencije/108/
119. Svet Evrope. (2015, 3. december). Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, CETS No.: 108. Najdeno 3. decembra 2015 na spletnem naslovu http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures
120. Swire, P., & Lagos, Y. (2013, 31. maj). Why the Right to Data Portability Likely Reduces Consumer Welfare: Antitrust and Privacy Critique. *Maryland Law Review*, *72*(2), 335-380.
121. Systems Integrator. (b. l.). V *The Tech Dictionary and IT Encyclopedia*. Najdeno 6. decembra 2015 na spletnem naslovu http://searchitchannel.techtarget.com/definition/systems-integrator
122. Taylor, R. S. (1986). *Value-Added Processes In Information Systems.* Norwood: Ablex Publishing Corporation.
123. The Data Liberation Front Delivers Google Takeout. (2011, 28. junij). *Google Data Liberation Blog.* Najdeno 21. marca 2016 na spletnem naslovu http://dataliberation.blogspot.si/2011/06/data-liberation-front-delivers-google.html
124. *The EDPS Q&A*. Najdeno 4. decembra 2015 na spletnem naslovu https://secure.edps.europa.eu/EDPSWEB/edps/EDPS/Dataprotection/QA
125. TRAI ruling on Net Neutrality. (2016, 11. februar). *The Indian Express.* Najdeno 20. marca 2016 na spletnem naslovu http://indianexpress.com/article/technology/tech-news-technology/trai-facebook-free-basics-bans-international-media/
126. Urad Vlade Republike Slovenije za komuniciranje. (b. l.). Vstop v Schengen. Najdeno 15. februarja 2016 na spletnem naslovu http://www.arhiv.evropa.ukom.gov.si/si/vstop-v-schengen/
127. Uredba (ES) št. 45/2001 evropskega parlamenta in Sveta o varstvu posameznikov pri obdelavi osebnih podatkov v institucijah in organih Skupnosti in o prostem pretoku takih podatkov. *Uradni list EU* L 8.
128. Ustava Republike Slovenije. *Uradni list RS* št. 33/91-I, 42/97, 66/2000, 24/03, 69/04, 68/06 in 47/13.

129. Van Eecke, P. (2014, 10. oktober). Belgium's New Government Sets Privacy High on the Agenda, Appointing Minister of Privacy. *The International Association of Privacy Professionals (IAPP).* Najdeno 7. decembra 2015 na spletnem naslovu https://iapp.org/news/a/belgiums-new-government-sets-privacy-high-on-the-agenda-appointing-minister-of-privacy/
130. Vatteble, M. (2012, 24. julij). Facebook Has Added You As An Informant. *Owni*. Najdeno 25. julija 2012 na spletnem naslovu http://owni.eu/2012/07/24/facebook-added-informant/
131. Warren, S. D., & Brandeis, L. D. (1890, 15. december). The Right to Privacy. *Harvard Law Review, IV*(5).
132. Wellington, B. (2011, 14. junij). What Facebook fails to recognise. *The Guardian.* Najdeno 1. marca 2016 na spletnem naslovu http://www.theguardian.com/commentisfree/cifamerica/2011/jun/14/facebook-facial-recognition-software
133. *What are the Facebook Services?* Najdeno 29. februarja 2016 na spletnem naslovu https://www.facebook.com/help/1561485474074139
134. *What Is Big Data?* Najdeno 11. decembra 2015 na spletnem naslovu http://www.sas.com/en_us/insights/big-data/what-is-big-data.html
135. Wolde, H. T. (2016, 14. januar). German high court rules Facebook "Friend Finder" is unlawful. *Reuters.* Najdeno 1. marca 2016 na spletnem naslovu http://www.reuters.com/article/us-facebook-germany-idUSKCN0US27W20160114
136. Wong, C. M. (2015, 26. februar). Facebook Introduces Gender Free-Form Field For Users. *The Huffington Post.* Najdeno 29. februarja 2016 na spletnem naslovu http://www.huffingtonpost.com/2015/02/26/facebook-gender-free-form-field-_n_6762458.html
137. Zakon o elektronskih komunikacijah. *Uradni list RS* št. 109/2012, 110/13, 40/14 - ZIN-B, 54/14 - *odločba Ustavnega sodišča RS* št. U-I-65/13.
138. Zakon o Informacijskem pooblaščencu. *Uradni list RS* št. 113/2005.
139. Zakon o pacientovih pravicah. *Uradni list RS* št. 15/2008.
140. Zakon o tajnih podatkih. *Uradni list RS* št. 50/2006-UPB2.
141. Zakon o varstvu osebnih podatkov. *Uradni list RS* št. 94/2007-UPB1.
142. *Zgodovina pooblaščenca*. Najdeno 12. septembra 2014 na spletnem naslovu https://www.ip-rs.si/o-pooblascencu/zgodovina/zgodovina-pooblascenca/
143. Zhang, N., & Zhao, W. (2007). Privacy-Preserving Data Mining Systems. *Computer, 40*(4), 52-58.
144. Ziegler, P., & Dittrich, K. R. (2004). Three Decades of Data Integration - All Problems Solved? *Building the Information Society. 156*, str. 3-12. Zürich: IFIP International Federation for Information Processing.

PRILOGE

KAZALO PRILOG

Priloga 1: Zapis intervjuja z Antonom Pirihom (Ministrstvo za zunanje zadeve Republike Slovenije)

Čas in kraj: 22. 3. 2016 od 9:00 do 10:20 v pisarni g. Piriha
Sodelujoči: Anton Pirih, vodja vizumskega oddelka

Osnovna vprašanja

Katere zbirke, ki vključujejo osebne podatke in so bile del integracije, obstajajo? Katere informacijske sisteme, podatkovne zbirke in podatke se je integriralo?

Vizis – vsebuje vloge za vizume in je osnovna zbirka, ki se povezuje z naslednjimi nacionalnimi zbirkami:

- Fonetični indeks oseb (FIO): tu gre za indeks, s pomočjo katerega se išče osebe po vseh policijskih podatkovnih zbirkah po principu fonetike (če je za določeno osebo vneseno kaznivo dejanje ipd.);
- Črna lista: vsebuje seznam oseb, ki jim je bil izrečen ukrep prepovedi vstopa v Republiko Slovenijo;
- Tuje ukradene potne listine.

Ta del še vedno obstaja in je integriran tako, kot je bil, dodatno zaradi zahtev schengna pa so se vzpostavile povezave z zbirkami schengenskega sistema kot sta SIS in VIS.

Kakšen je bil osnovni namen integracije? Od kje je prišla pobuda za integracijo oz. kaj je bil osnovni razlog zanjo?

Namen je bil izvajanje skupne enotne vizumske politike EU, kot je to določeno s pravnim redom EU, ki med drugim predvideva, da je potrebno pred izdajo vizumov izvajati preverjanje v SIS.

Koliko časa je projekt trajal (od prejšnjega stanja do takrat, ko je bila načrtovana integracija v uporabi)?

Cel projekt je trajal okoli 3 leta, preklop na skupni sistem pa je bil izveden preko noči.

Katere metode za združevanje podatkov in orodja za integracijo so bile uporabljene? Kako je bilo ob integraciji poskrbljeno za zagotavljanje kakovosti podatkov?

Ob vključitvi v schengen smo se povezali dodatno samo s SIS-om, medtem ko je VIS šel v uporabo kasneje, leta 2010. Do takrat je zraven služil še konzultacijski sistem Vision (ki ni bil podatkovna baza), v katerem so posamezne države schengenskega območja definirale, katere tretje države so zanje rizične države in želijo biti dodatno obveščene, ko se vizumski

postopek izvaja za osebo iz take rizične države. V takem primeru je bilo potrebno počakati na odgovore teh držav, preden se je vizum izdalo.

Pri VIS-u je osnovna entiteta (vizumska) vloga. Lahko se zgodi, da je na kakšni vlogi kakšen del podatka zapisan drugače – po različnih kontrolah v postopku se potem napake popravi. Vloge se povezujejo v dosjeje – za eno osebo mora biti načeloma en dosje. V praksi se lahko zgodi, da ima ena oseba več dosjejev, kar pa je narobe. Vloge se povezujejo, ko se vpišejo alfanumerični podatki in opravi zajem prstnih odtisov in se ti podatki prenesejo v VIS. Na osnovi teh podatkov država članica opravi sama t. i. iskanja v VIS-u. Tu se lahko uporabi različne kriterije – od države je odvisno, katere kriterije bo uporabila pri iskanju. Pri nas so kriteriji naslednji: Zadeve (t. j. ali za to osebo že obstajajo zapisi v sistemu) se najprej poiščejo po prstnih odtisih. Ti so shranjeni v VIS-u, zahteva pa se zajem vseh deset prstov. Če prstnih odtisov ni, so lahko razlogi naslednjih štirih kategorij:

- otrok, ki še ni dopolnil 12 let;
- stranka je izjavila, da je prstne odtise zajela že pri predhodnem vizumskem postopku, ki se je zgodil v zadnjih 59 mesecih (60 mesecev se hranijo v VIS-u);
- začasna ali trajna poškodba (npr. oseba je brez enega ali več prstov ali roke ali je kako drugače poškodovana, da zajem prstnih odtisov ni možen);
- poglavarji držav, ministri in drugi funkcionarji, ko prihajajo z namenom v okviru uradnega obiska – tu zajem prstnih odtisov ni zahtevan (za privatni obisk to ne velja).

V teh primerih se iščejo zadetki v VIS-u s pomočjo alfanumeričnih podatkov. Slovenija je razvila set različnih kriterijev, ki gredo od ožjega na širše (dokler ne najde zadetka): Najprej »ime, priimek, datum rojstva«; nato »predhodno izdana vizumska nalepka«; nato »priimek, letnica rojstva, državljanstvo« itn. Vseh iskalnih kriterijev je sedem. Če po nobenem iskalnem kriteriju sistem ne najde zadetka, potem se postopek nadaljuje.

Osnova vnesenih podatkov je potni list prosilca za vizum, za zapise imen in drugih podatkov iz drugih (ne-latiničnih) abeced pa se uporablja standarde ICAO (Mednarodna organizacija za civilno letalstvo, op. avt.), kot je zapisano tudi v strojno berljivem delu potnega lista.

Katere slovenske in evropske pravne akte in morebitne druge standarde ali priporočila (predvsem s področja varstva osebnih podatkov in zasebnosti) je bilo potrebno upoštevati pri načrtovanju in uveljavljanju sprememb?

Za izdajo schengenskih vizumov določa okvire pravni red EU in sicer:

- Uredba VIS: Ta določa vsebino – opredeljuje vizumski postopek in to, katere podatke se zbira, na kakšen način in kdo jih sme uporabljati (DKP-ji za obravnavanje vizumskih vlog, mejni prehodi ob kontroli, določeni policijski organi ob izvajanju dela

mejne kontrole v notranjosti države). Tu je tudi določeno 60 mesecev za hrambo podatkov posameznih vlog.

- Odločba VIS: Ta določa pristop do podatkov in njihovo uporabo s strani drugih varnostnih organov, kot so obveščevalne službe, kriminalistična policija ipd. Vsaka država sama sporoči komisiji, kateri so ti organi, ki bodo potrebovali dostop.

So bile kakšne »težave« s pristojnimi organi za varstvo osebnih podatkov v Sloveniji (npr. z Informacijskim pooblaščencem) ali na evropski ravni? Je bilo zaradi tega potrebno spremeniti projekt ali načrt integracij? Kateri so bili največji izzivi v povezavi z osebnimi podatki in varovanjem le-teh (tehnični, pravni, organizacijski)?

Na evropski ravni obstaja posebna delovna skupina, ki obravnava akte, ki zadevajo zbiranje in obdelavo osebnih podatkov. Tako so tudi sodelovali pri pripravi Uredbe in Odločbe VIS. Ko pa je pravni akt sprejet, skrbijo, da se ta izvaja. V zadnjih letih sicer ni bilo nobenih reakcij s strani informacijskega pooblaščenca.

Je bila po zaključku narejena kakšna analiza glede integracije, ki je vključevala tudi vidik varstva osebnih podatkov oz. zasebnosti?

Izvajajo se občasne analize in evalvacije. S strani informacijskega pooblaščenca se izvajajo občasni pregledi, vendar termini ali periode niso določeni oz. natančno definirani.

Uporabniki in pravice dostopa

Koliko uporabnikov je dostopalo do podatkov pred integracijo, koliko sedaj?

Če se omejimo na dostop podatkov na vizumskih vlogah – tisti uporabniki, ki so že prej imeli pooblastilo, imajo enak dostop tudi zdaj. Njihov dostop je do Vizisa. Ta sistem potem komunicira z različnimi drugimi podatkovnimi bazami v Sloveniji in na ravni EU. Za konkretno vlogo, ki jo uporabnik vpiše, se lahko pridobi konkretne podatke, brskanje po podatkih pa ni možno. Na MZZ, DKP-jih in mejnih prehodih je trenutno vsega skupaj 237 uporabnikov.

So pravice in vloge jasno razmejene? Kako je zagotovljena notranja sledljivost transakcij in vpogledov v podatke? Se dostopi do podatkov in poskusi dostopov beležijo? Kako je zaščitena ta revizijska sled?

Pravice in vloge so razmejene. DKP-ji imajo 3 nivoje dostopa:

- lokalni uslužbenci: ti smejo vpisovati vloge, ne morejo pa videti zadetkov, ne odločati o vlogah in ne imeti managementa vizumskih nalepk. Lahko pa jih natisnejo, ko je o vlogi odločeno;

- podpisovalci: to so konzuli, ki imajo vse pravice kot prej omenjeni, dodatno pa še pravico odločati o vlogah in preverjati zadetke. Nimajo pa pravice managiranja vizumskih nalepk;
- vodja: ta ima vse prej omenjene pravice, poleg tega pa tudi management vizumskih nalepk (in je edina oseba, ki ima to pravico na posameznem DKP).

Sledljivost je zagotovljena. Sledenje je integrirano v Vizisu – beleži se vsako odprtje baze, vsako iskanje, kaj je kdo gledal, kaj je videl, kaj je spreminjal. Administrator ima vpogled v te podatke, nima pa možnosti brisanja ali spreminjanja podatkov.

Se opravljajo redne ali periodične revizije oz. pregledi upravičenosti dostopa uporabnikov do posameznih podatkov?

Se opravljajo. Pregled upravičenosti in načina dostopa izvaja interna kontrola MZZ skupaj z diplomatskim inšpektorjem (včasih tudi sama konzularna služba). Obstajajo tudi neodvisne zunanje revizije s strani urada informacijskega pooblaščenca – oni preverjajo širše celoten sistem varovanja osebnih podatkov na DKP, vključno z uporabo podatkov iz VIS-a (npr. koliko časa se hranijo, kaj in zakaj se zbira, kako se hrani, kdo dostopa, kako dostopa itn.). Ti pregledi nimajo vnaprej znanega razporeda, lahko jih v kakšnem letu tudi ni.

MZZ redno pregleda od 4 do 6 DKP-jev na leto. Kar zadeva menjave osebja in s tem povezanih pravic, pa se – če je to potrebno – ureja preko kadrovske službe.

Se izvajajo izobraževanja uporabnikov podatkov glede standardov in določil varstva osebnih podatkov?

V okviru rednih priprav na nastop dela v tujini se to izvaja (okvirno dvakrat do trikrat letno). Poudarek je na tem, kaj se zbira, kateri podatki, na kakšen način in kako. Če bi prišlo do kršitve, se posledice sanira in odpravi ter preprečuje, da bi se to ponovilo v prihodnje. V okviru oddelka se izvaja izobraževanje, če se nekdo zaposli na novo. Zadevne kontrole pa se lahko izvajajo tudi s strani informacijskega pooblaščenca na konzularnem oddelku.

Podatki in obdelava

Kateri osebni podatki se zbirajo?

Zbirajo se vsi osebni podatki, kot jih določa Zakon o tujcih v svojem 112. členu. To so med drugim: ime, priimek, priimek ob rojstvu, EMŠO (če je določen), spol, rojstni datum, rojstni kraj in država, državljanstvo, državljanstvo ob rojstvu, zakonski stan, poklic, ime in priimek staršev ali zakonitih zastopnikov, ime in priimek zakonca, priimek zakonca ob

rojstvu, ime in priimek in datum rojstva otrok itn. Zbirajo pa se lahko tudi osebni podatki o garantu (ki je lahko fizična ali pravna oseba iz Republike Slovenije).

Koliko časa se hranijo?

Tudi to je opredeljeno v Zakonu o tujcih (nanaša se na hranjenje podatkov v Vizisu). Za hrambo v VIS in SIS veljajo uredbe oz. pravni red EU. Za oboje je določeno, da se hranijo podatki 5 let.

Dosje, ki je bil omenjen, ni entiteta. Hranijo se vloge oz. podatki na njih; ko je izbrisana zadnja vloga v dosjeju osebe, potem tudi ne obstaja več dosje kot tak.

Kako so zavarovani (tehnološko, fizično, logično …)?

Strežniki z ustrezno zaščito se nahajajo na MZZ in DKP-jih. Centralna baza je na MZZ, del podatkovne baze Vizisa (t. j. za vsak DKP njim relevanten del) pa se vsakih 14 minut replicira z DKP. Obstaja še varnostna kopija tega strežnika in pomoč pri izvajanju operacij. Vsako noč se izvaja prenos varnostnih kopij na trak, ki se potem hrani v sefu.

Kako se jih zbira (neposredno ali tudi iz tretjih baz)?

Podatki o prosilcu za vizum se vedno zbirajo neposredno od prosilca, del podatkov pa je možno pridobiti ali pa se uporabi tudi iz evidence garantnih pisem, ki se vodi na upravnih enotah. Vsako garantno pismo mora biti overjeno in overjen mora biti podpis garanta (vsebina in oblika sta določeni z zakonom). Hranijo se podatki o tem, kdo je koga povabil. Iz te evidence je možno na podlagi številke na garantnem pismu pridobiti podatke o garantu. Obstajajo tudi spletne vizumske vloge, kjer pa gre samo za drugo obliko zbiranja podatkov (za razliko od obiska prosilca na DKP).

Kakšne povezovalne znake se uporablja?

Kot je že bilo omenjeno, so tu glavni prstni odtisi. Če teh ni, pa s procesom, specificiranim v uredbi VIS, konzul preveri, če je oseba že v sistemu (zabeleži se ID vloge v VIS-u kot povezava k obstoječi), da se poveže v dosje.

Kako je poskrbljeno za ažurnost in točnost podatkov?

Obstaja več kontrol in sicer: Najprej se pravilnost preverja ob vnosu (to izvaja tisti, ki vpisuje podatke), nato preverja še enkrat konzul, ki odloča o vlogi (če se recimo zgodi, da nekdo vpiše napačen datum rojstva in vloga ni bila povezana v dosje, pa konzul kasneje vidi v potnem listu, da že obstaja predhodni vizum, ki ni bil povezan, je potreben ponovni vnos). Tretja kontrola je pri tiskanju vizumske nalepke – tu se preveri, če se podatki na potnem listu in vizumski nalepki ujemajo. Četrta kontrola pa je prosilec sam, saj je vsaki

stranki rečeno, naj ob prejemu vizuma preveri pravilnost podatkov. V primeru napak je potreben preklic vizuma (razveljavitev nalepke), popravek podatkov in izdaja nove vizumske nalepke.

Kako je urejena sinhronizacija med (pod)sistemi (čas, urnik, smeri …)?

V uporabi je sistem replikacij. Na vsakih 14 minut se replicirajo podatki z DKP na centralno bazo na MZZ (uporabniki na DKP nimajo možnosti neposrednega dostopa do centralnih evidenc, ampak samo do delne kopije Vizisa na njihovem DKP-ju). Z naslednjo replikacijo v smeri od MZZ proti DKP pa so potem na voljo in prikazani morebitni zadetki na DKP.

Na relaciji med centralnim sistemom VIS in nacionalnim sistemom (Vizis) se vsi podatki, ki so v Vizisu in se nanašajo na schengenske vizume, prenesejo v VIS (v katerem so vsi podatki vseh schengenskih držav). Na naši strani podatke samo vpišemo, po prenosu v VIS pa se preverja, če tam že obstajajo zapisi, nato pa se samo tisti prikažejo konzulu.

Pri SIS-u pa je tako, da ima vsaka država celotno kopijo baze (torej centralna evidenca in nacionalne kopije te). V Sloveniji se N-SIS hrani pri Policiji. Na enak način kot dostopamo do VIS-a se podatke preverja pri Policiji (t. j. če obstajajo kakšna opozorila v zvezi s prepovedjo vstopa v schengenski prostor, sistem avtomatsko preveri in v takem primeru vrne zadetke).

Kako je sedaj poskrbljeno za kvaliteto podatkov? Kako se ureja podvojene zapise ali združuje duplikate?

Lahko se recimo zgodi, da je v sistem ista vloga vpisana dvakrat. Če je konec dneva preveliko število vlog, se ugotovi, kje je prišlo do napake, MZZ označi tako vlogo kot zaprto in se jo umakne iz procedure; neskladje se lahko opazi tudi pri knjižbah (dvakrat knjižena taksa, kar ne ustreza dejanskemu stanju blagajne).

V samem vizumskem postopku pa se preverja, če je bil v Vizisu že kdaj prej narejen kakšen vizumski postopek za prosilca.

Kako je urejeno posredovanje podatkov v tretje države ali prejem podatkov iz takih držav? Je sprememba pravil »varnega pristana« z ZDA kakorkoli vplivala na redne operacije?

Najprej je bilo to urejeno preko sistema Vision (vendar ni šlo za posredovanje podatkov v tretje države). Namesto Visiona je sedaj v uporabi VisMail2. V okviru tega sistema se pošiljajo podatki (vendar ne osebni): npr. če določena schengenska država zahteva, da se jo za določeno tretjo državo dodatno obvesti o prosilcih za vizum, sledi vpisu vloge prosilca iz take države avtomatski mail taki schengenski državi, ki omeni, da v VIS-u obstaja vloga

z naslednjo ID številko in da imajo 7 dni časa, da sporočijo, če se strinjajo z izdajo vizuma ali ne.

Pravice subjektov

Kako uveljavlja posameznik pravice glede varstva osebnih podatkov (izbris, ugovor, popravek, vpogled …)? Kje dobi posameznik informacije o pravicah v zvezi s svojimi podatki?

Najbolj bistvena je splošna pravica – da ima vsak posameznik pravico do vpogleda do svojih osebnih podatkov. Na spletni strani je v ta namen objavljen obrazec in opis postopka. Posameznik torej izpolni ta obrazec in ga pošlje na MZZ, ki potem preveri stanje v VIS in izpiše eventuelne podatke o takem posamezniku.

Kakšen je postopek izbrisa? Obstaja neodvisna revizija ali nadzor izvajanja oz. potrditve brisanja?

Brisanje se izvaja v ozadju avtomatsko. Sicer pa do podatkov v sistemu uporabnik ne more dostopati, če ne gre za vnašanje konkretne vloge.

V Uredbi VIS je definirano brisanje podatkov za VIS (odgovornost EU) in sicer po 5 letih. Na nacionalnem nivoju se podatki hranijo 5 let (kar definira Zakon o tujcih) – in sicer 5 let po prenehanju veljavnosti vizuma ali 5 let po izdaji odločbe, da je bila vloga zavrnjena.

Ostala vprašanja

Obstajajo zunanji oz. pogodbeni obdelovalci podatkov? Kako je tu zagotovljena sledljivost?

Razvoj in vzdrževanje izvaja zunanja firma. Sistem, kot rečeno, avtomatsko beleži, kdo odpira in kaj odpira – in to velja tudi v tem primeru.

Se izvajajo zunanje revizije skladnosti z varovanjem osebnih podatkov?

Poleg že omenjenih pregledov s strani informacijskega pooblaščenca se izvajajo tudi schengenske evalvacije na nivoju EU. Komisija izvede periodični nadzor za posamezno državo – običajno na dveh DKP-jih. To se izvaja približno na 5 let (v smislu izvajanja določb vizumskega zakonika in uredbe, vključno s tem, kdo uporablja podatke in na kakšen način). Fokus tega pa je kvaliteta vizumskih postopkov in ne varovanje osebnih podatkov.

Je določena odgovorna oseba za varstvo podatkov in pravice podatkovnih subjektov?

Kot upravljavec je na MZZ to konzularna služba oz. konkretno g. Pirih.

Kakšno je trenutno stanje in kateri so odprti izzivi (zlasti na področju varstva osebnih podatkov in zasebnosti)? Obstajajo še kakšna odprta tveganja glede varstva podatkov oz. zasebnosti?

Trenutni se ne pričakuje bistvenih sprememb ali dodatnih izzivov, razen rednega vzdrževanja sistema.

Priloga 2: Zapis intervjuja z Urošem Mladenovičem in Kristino Perko (Geodetska uprava republike Slovenije)

Čas in kraj: 7. 3. 2016 od 13:00 do 14:30 v pisarni g. Mladenoviča
Sodelujoči: Uroš Mladenovič, vodja oddelka za informatiko; Kristina Perko, vodja oddelka za izdajanje podatkov

Osnovna vprašanja

Katere zbirke, ki vključujejo osebne podatke in so bile del integracije, obstajajo? Katere informacijske sisteme, podatkovne zbirke in podatke se je integriralo?

V integracijo je bilo vključenih 5 zbirk in sicer: zemljiški kataster, kataster stavb, register nepremičnin, register prostorskih enot in zbirni kataster gospodarske javne infrastrukture. V prvih treh so vsebovani tudi osebni podatki.

Gre za zakonsko ločene zbirke – predvsem katastri morajo biti ločen od registra nepremičnin. Za zemljiški kataster in kataster stavb se podatki o lastništvu prevzemajo iz zemljiške knjige (ki jo vodi Vrhovno sodišče), kjer se vodijo podatki o stanju nepremičnin, lastnikih, obremenitvah ipd. GURS skrbi za podatke o »fizičnih lastnostih« in skrbi za identifikatorje nepremičnin, zemljiška knjiga pa na objekte, ki jih GURS opredeli, vpiše lastnika, njegove pravice in obveznosti.

Zemljiški kataster in kataster stavb sta obstajala že prej, register nepremičnin pa je nastal kot rezultat popisa nepremičnin oz. projekta vzpostavitve registra nepremičnin. Sedanji prikaz podatkov v javnem vpogledu, torej na spletnem portalu, je bil izveden kot del rednih nalog na GURS in ne kot del posebnega projekta. Osebni podatki, zbrani v okviru popisa nepremičnin, se hranijo samo v registru nepremičnin. Iz te evidence se podatki nikoli ne prenašajo v kataster, ki ima višji status oz. je del upravnih postopkov. Prvi javni vpogled v podatke zemljiškega katastra je bil objavljen januarja 2002 in se je sčasoma dopolnjeval. Vmes je bil narejen tudi namenski vpogledovalnik za potrebe popisa. V tej obliki, kot je sedaj, je bil javni vpogled načrtovan v letu 2007, potem so sledile le manjše dopolnitve in prilagoditve.

Kakšen je bil osnovni namen integracije?

Da uporabniku na enem mestu prikažemo informacije iz vseh relevantnih evidenc, tako da lahko tudi uporabnik vidi določene razlike med evidencami – torej biti prijazen do uporabnika ter prikazati in omogočiti prikaz vseh evidenc skupaj na enem mestu.

Od kje je prišla pobuda za integracijo oz. kaj je bil osnovni razlog zanjo?

Šlo je za zakonske zahteve Zakona o evidentiranju nepremičnin. Ta zakon tudi predpisuje, kateri osebni podatki se zbirajo, in njihov namen zbiranja (pokriva določene dele, za katere Zakon o varstvu osebnih podatkov zahteva specifične področne zakone). Ker je zakon nalagal javnost podatkov, je bil javni vpogled v okviru portala v začetku odprt vsem.

Koliko časa je projekt trajal (od prejšnjega stanja do takrat, ko je bila načrtovana integracija v uporabi)?

Razvoj javnega vpogleda je trajal približno eno leto.

Katere metode za združevanje podatkov in orodja za integracijo so bile uporabljene? Kako je bilo ob integraciji poskrbljeno za zagotavljanje kakovosti podatkov? Osnovni diagram omrežja oz. sistema pred spremembami, diagram po spremembah/integraciji (glej tudi Prilogo 3).

Ker je šlo za ponujanje enotnega pogleda na podatke oz. spletnega portala, se zbirke in sistemi v ozadju niso spreminjali oz. je integracija vidna samo navzven – kot enotni prostorski portal Prostor.

Vsaka evidenca je določena z zakonom, med njimi pa se pretakajo podatki. Ti so lahko še vedno zapisani v dveh evidencah. Zakon dovoljuje, da je lahko v drugi evidenci drugačen podatek, če se ti podvajajo. Ko se ne podvajajo ali se ne smejo, se tehnično gledano lahko črpajo iz ene v drugo, čeprav jih zakon zahteva v posamezni evidenci (ampak tu ne gre za osebne podatke).

Katere slovenske in evropske pravne akte in morebitne druge standarde ali priporočila (predvsem s področja varstva osebnih podatkov in zasebnosti) je bilo potrebno upoštevati pri načrtovanju in uveljavljanju sprememb?

V obzir je bilo potrebno vzeti predvsem naslednje zakone:

- Zakon o evidentiranju nepremičnin;
- Pravilnik o pogojih in načinu računalniškega dostopa do podatkov iz evidenc in zbirk geodetskih podatkov;
- Zakon o varstvu osebnih podatkov;
- Zakon o dostopu do informacij javnega značaja.

So bile kakšne »težave« s pristojnimi organi za varstvo osebnih podatkov v Sloveniji (npr. z Informacijskim pooblaščencem) ali na evropski ravni? Je bilo zaradi tega potrebno spremeniti projekt ali načrt integracij?

Tovrstnih težav ni bilo. Informacijski pooblaščenec je namreč sodeloval že pri pripravi Zakona o evidentiranju nepremičnin in je lahko podal pripombe nanj pred sprejetjem zakona.

Je pa prišlo do sprememb kasneje: V letu 2007 je Ustavno sodišče prepovedalo javnost osebnih podatkov, tako se potem iz registra nepremičnin ni več smelo javno prikazovati osebnih podatkov.

Januarja 2012 pa je Informacijski pooblaščenec izdal začasno odločbo, s katero je naložil GURS, da v roku treh dni odpravi javni dostop do osebnih podatkov preko javnega vpogleda na spletnem portalu.

Je bila po zaključku narejena kakšna analiza glede integracije, ki je vključevala tudi vidik varstva osebnih podatkov oz. zasebnosti?

Kakšnih posebnih analiz ni bilo. Po sprejetju začasne odločbe Informacijskega pooblaščenca so bili v zahtevanem roku umaknjeni osebni podatki (za pravne osebe ta omejitev ni veljala) iz javnega vpogleda, vložili smo tudi pritožbo, nato je jeseni Ustavno sodišče sprejelo odločbo in spremenilo Zakon o evidentiranju nepremičnin v tem delu, saj obstaja zemljiška knjiga, ki je javna evidenca in že omogoča dostop do teh podatkov, ZEN pa po mnenju ustavnih sodnikov ni dovolj jasno in konkretno opredelil namena javne objave osebnih podatkov.

Opazili pa smo, da se je po umiku prikaza osebnih podatkov tudi nekoliko zmanjšala obiskanost spletnega portala.

Uporabniki in pravice dostopa

Koliko uporabnikov je dostopalo do podatkov pred integracijo, koliko sedaj?

Tovrstnih analiz nimamo. Elektronski dostop (PREG, servisi) uporablja letno povprečno okoli 4500 registriranih uporabnikov in lani okoli 25 drugih informacijskih sistemov, števila uporabnikov na javnem vpogledu pa ne beležimo. Dostop imajo na podlagi zakonskih določil tudi drugi državni organi, notarji in geodetska podjetja, do tehničnih podatkov (brez osebnih podatkov) pa omogočamo dostop tudi drugim pravnim subjektom. Posebej je ščiten podatek EMŠO, do katerega lahko dostopa samo drug državni organ, ki ima to v zakonu opredeljeno.

Poleg tega obstajajo še:

- osebni vpogled: lastnik lahko sam zase pogleda, kje je vpisan;

- pregledovalnik za geodetske podatke (za registrirane uporabnike): kjer drugi državni organi, geodetska podjetja in notarji lahko vpogledujejo (tudi osebne podatke) v skladu z zakonskimi pravicami, njihovi nivoji dostopa pa so različni.

Podatki o vpogledih se beležijo. V skladu z zakonom se ti zapisi hranijo 6 let.

Glede zagotavljanja sledljivosti obdelave osebnih podatkov Zakon o varstvu osebnih podatkov - ZVOP-1 (Uradni list RS, št. 94/2007 – u.p.b.) v prvem odstavku 25. člena določa, da so dolžni upravljavci osebnih podatkov in pogodbeni obdelovalci zagotoviti zavarovanje osebnih podatkov na način iz 24. člena ZVOP-1. Zavarovanje osebnih podatkov mora med drugim obsegati tudi organizacijske, tehnične in logično-tehnične postopke in ukrepe, s katerimi se omogoča poznejše ugotavljanje, kdaj so bili posamezni osebni podatki vneseni v zbirko osebnih podatkov, uporabljeni ali drugače obdelani in kdo je to storil, in sicer za obdobje, ko je mogoče zakonsko varstvo pravice posameznika zaradi nedopustnega posredovanja ali obdelave osebnih podatkov (5. točka prvega odstavka 24. člena ZVOP-1). Po tretjem odstavku 22. člena ZVOP-1 mora upravljavec osebnih podatkov za enako časovno obdobje za vsako posredovanje osebnih podatkov zagotoviti, da je mogoče pozneje ugotoviti, kateri osebni podatki so bili posredovani, komu, kdaj in na kakšni podlagi.

Skrajni rok za civilno uveljavljanje pravic ob kršitvah pri obdelavi osebnih podatkov je praviloma 5 let od nastanka škode, kar je splošni zastaralni rok, ki ga določa Obligacijski zakonik – OZ (Uradni list RS, št. 97/2007 – u.p.b.) v 346. členu, vendar pa po prvem odstavku 353. člena OZ v primeru, če je bila škoda povzročena s kaznivim dejanjem, za kazenski pregon pa je predpisan daljši zastaralni rok, zastara odškodninski zahtevek proti odgovorni osebi, ko izteče čas, ki je določen za zastaranje kazenskega pregona. Pri tem je potrebno upoštevati zastaralni rok, ki je s 5. točko prvega odstavka 90. člena Kazenskega zakonika – KZ-1 (Uradni list RS, št. 50/2012 – u.p.b. in nasl.) določen za zastaranje kaznivega dejanja zlorabe osebnih podatkov iz prvega odstavka 143. člena KZ-1. *Tako velja, da je revizijsko sled zaradi varstva pravic posameznika potrebno hraniti 6 let od njenega nastanka* (pridobljeno naknadno po elektronski pošti s strani g. Mladenoviča).

So pravice in vloge notranjih uporabnikov jasno razmejene? Kako je zagotovljena notranja sledljivost transakcij in vpogledov v podatke? Se dostopi do podatkov in poskusi dostopov beležijo? Kako je zaščitena ta revizijska sled?

Nivoji vlog notranjih uporabnikov so določeni in razmejeni. Do podatkov imajo dostop:

- administratorji (tehnični) – njihovo dostopanje se ne beleži.
- referenti – tisti, ki lahko ažurirajo podatke; beleži se, kdo je podatke spreminjal. Spremembe podatkov so zabeležene za stalno (v okviru vodenja zgodovine sprememb na zapisu).

Do podatkov in storitev lahko uporabniki dostopajo samo preko distribucijskega sistema. Tja dnevno prepisujemo spremembe iz produkcije. Dnevniške zapise osebnih podatkov (vpogledov v osebne podatke) pa tekoče prepisujemo v posebno shemo na produkciji (na distribuciji se po prenosu brišejo). Zapisane številke EMŠO v dnevniških zapisih v nekaterih storitvah šifriramo, povsod pa ne. Dostop do dnevniških zapisov o vpogledih ima samo ena določena oseba.

Se opravljajo redne ali periodične revizije oz. pregledi upravičenosti dostopa uporabnikov do posameznih podatkov?

Samo na zahtevo. Za notranje uporabnike je naloga vodij organizacijskih enot, da skrbijo za spremembe pravic, če se spremenijo uporabniki (obrazci, skrbniki evidenc). Fluktuacije pa je malo.

Za zunanje uporabnike velja, da so ti dolžni javljati spremembe na zahtevanem obrazcu. Ne moremo pa ugotavljati, kdo je pri zunanjih uporabnikih upravičen do funkcije. Enkrat letno se preverjajo zadnji datumi prijave – in če je minilo več kot 1 leto, se takega uporabnika blokira.

Se izvajajo izobraževanja uporabnikov podatkov glede standardov in določil varstva osebnih podatkov?

Se izvajajo. Ena oseba je zadolžena za ta segment in izvaja ta izobraževanja, vendar zanje ni določen reden periodičen termin.

Podatki in obdelava

Kateri osebni podatki se zbirajo?

Ime, priimek, naslov, EMŠO (če obstaja), datum smrti (če obstaja), datum rojstva (se pobere iz EMŠO; pri tistih, ki nimajo EMŠO, pa se ga vnese samostojno, če je znan).

Koliko časa se hranijo?

V produkciji (register nepremičnin) se podatki prepišejo z novimi in se po dosegu namena ne hranijo več (če govorimo o lastnikih nepremičnin v registru nepremičnin, ko se menjajo). V katastrih pa se zgodovina trajno hrani.

Kako so zavarovani (tehnološko, fizično, logično …)?

Podatkovni center se nahaja na Ministrstvu za javno upravo. Za dostop do tja veljajo njihovi postopki.

Kako se jih zbira (neposredno ali tudi iz tretjih baz)? Katera je pravna podlaga za slednje?

Osnovna pravna podlaga je Zakon o evidentiranju nepremičnin. Za register nepremičnin je možno, da se na podlagi veljavnih listin (pogodbe, ki ni bila nikoli v zemljiški knjigi) vpiše lastništvo. Podatki iz katastra se lahko prenašajo v register nepremičnin, ni pa nujno, da so 100 % enaki.

Kakšne povezovalne znake se uporablja?

Za fizične osebe je uporabljen EMŠO, za pravne pa matična številka pravne osebe.

Kako je poskrbljeno za ažurnost in točnost podatkov?

Ažurnost pri katastru je odvisna od tega, v kolikšnem času po spremembi v zemljiški knjigi se ta sprememba tu evidentira in ali so vsi zapisi opremljeni z identifikatorjem. Vsak prenos mora odobriti referent, ki pregleda ustreznost podatkov, zato lahko včasih traja tudi dlje, da so podatki ažurirani.

Povezava z zemljiško knjigo je bila vzpostavljena pred dvema letoma; GURS sporoča zemljiški knjigi spremembe identifikatorja nepremičnin, oni pa na GURS glede spremembe lastništva. Od prenove zemljiške knjige je tam zapisan lastnik direktno na nepremičnino – so pa podatki včasih še nepopolni, vendar se izboljšujejo. Lahko je na eni parceli zaveden z EMŠO, na drugi pa brez; pri GURS pa je to povezovalni znak, zapisi se združujejo tako, da je npr. glavni posestni list in z njega povezani kazalci po posameznih nepremičninah. Zaradi tega lahko traja ažuriranje dlje in je potrebno posredovanje referentov.

Pri podatkovnem toku lastništva se preverja in ažurira podatke (naslovi, nazivi, imena in priimki) s pomočjo Poslovnega registra Slovenije in Centralnega registra prebivalstva.

V naslednji fazi je predvidena vsaj delna avtomatizacija prepisa lastništva iz zemljiške knjige (kjer so matične številke vseh lastnikov ene nepremičnine že vpisani v zemljiški knjigi) – trenutno pa je to še v fazi pogovorov. Lahko bo to izvedeno v okviru prenove celotnega sistema.

Kako je urejena sinhronizacija med (pod)sistemi?

Ko se na zemljiški knjigi spremenijo podatki, prejme GURS obvestilo, da so to izvedli. Ni čisto avtomatsko zaradi kakovosti podatkov; ker nimajo vsi lastniki v zemljiški knjigi identifikacijske številke – EMŠO ali matične številke pravne osebe – mora referent preveriti in to popraviti, če je potrebno. Davčne številke se v teh registrih ne uporablja. Rojstni datum pa ne more biti ključ, ker ne obstaja vedno v zemljiški knjigi ali pa lahko

osebi z istim rojstnim dnevom prebivata na istem naslovu. Zemljiška knjiga nato dnevno oddaja na sistem GURS datoteko sprememb, ki jo sistem tu obdela. GURS pa na zemljiško knjigo posreduje spremembe identifikatorjev preko spletnih servisov.

Kako je sedaj poskrbljeno za kvaliteto podatkov? Kako se ureja podvojene zapise ali združuje duplikate?

Za podatke se vodi sistem kakovosti podatkov (po lastni metodologiji) v oddelku, kjer skrbijo za kakovost podatkov. Enkrat dnevno se podatki osvežujejo iz registrov. Pri dostopu do poslovnega registra ni omejitev, pri centralnem registru prebivalstva pa je naša pravica dostopa omejena na dostop samo do tistih zapisov, kjer so državljani hkrati tudi lastniki, zato se mora na CRP poslati oznaka, da je nekdo lastnik, in do njegovih podatkov je tako potem odobren dostop.

Kako je urejeno posredovanje podatkov v tretje države ali prejem podatkov iz takih držav?

Za to skrbi in preverja pravna služba. Gre pa predvsem za zbiranje podatkov v primeru, če je kdo lastnik iz tuje države. Pri nakupu nepremičnine zemljiška knjiga poroča na AJPES ali CRP. Takrat se tej osebi, tudi tuji, določi matična številka. Še en primer je lahko, če je npr. postopek dediščine v tujini, pa od tam pozivajo oz. sprašujejo, če je imel lastnino v Sloveniji (ali če gre za uveljavljanje socialnih pravic iz tujine).

Pravice subjektov

Kako uveljavlja posameznik pravice glede varstva osebnih podatkov (izbris, ugovor, popravek, vpogled …)?

Podatki so zbrani na podlagi zakona in na podlagi upravnega postopka in so kot taki vpisani. Če želi nekdo spremeniti lastnost nepremičnine, ureja tu, spremembo glede lastništva pa na zemljiški knjigi. Lahko pa posameznik vedno zahteva informacijo o tem, kdo je vpogledoval v njegove osebne podatke.

Kje dobi posameznik informacije o pravicah v zvezi s svojimi podatki?

Na spletni strani je seznam zbirk osebnih podatkov in katalog v skladu z Zakonom o dostopu do informacij javnega značaja. Postopki o dostopu in postopki v zvezi z nepremičninami so na straneh na e-uprave. Ostali napotki glede osebnih podatkov pa so na strani Informacijskega pooblaščenca.

Kakšen je postopek izbrisa? Obstaja neodvisna revizija ali nadzor izvajanja oz. potrditve brisanja?

Za register nepremičnin se lahko uveljavlja spremembo lastništva na podlagi novega lastnika iz zemljiške knjige oz. z verodostojnim dokumentom.

Ostala vprašanja

Obstajajo zunanji oz. pogodbeni obdelovalci podatkov?

- Ministrstvo za javno upravo: podatkovni center (posebne pogodbe o gostovanju ni);
- Zunanji izvajalci: razvoj informacijskega sistema. Imajo dostop do razvojnega in testnega okolja. Do produkcije imajo ponekod dostop, vendar se poskusi to omejiti oz. se ga odpre samo takrat, ko rabijo dostop. V pogodbi je opredeljeno, da so to pogodbeni obdelovalci osebnih podatkov.

Podatki gredo tudi na Statistični urad skupaj z osebnimi podatki na podlagi zakona o statistiki, za anonimizacijo teh podatkov pa je zadolžen Statistični urad.

Kot rečeno, se podatki izmenjujejo tudi z Vrhovnim sodiščem, ki vodi zemljiško knjigo (vendar niso definirani kot pogodbeni obdelovalci).

Se izvajajo zunanje revizije skladnosti z varovanjem osebnih podatkov?

Če je kakšna zahtevana s strani Informacijskega pooblaščenca, sicer ne.

Je določena odgovorna oseba za varstvo podatkov in pravice podatkovnih subjektov?

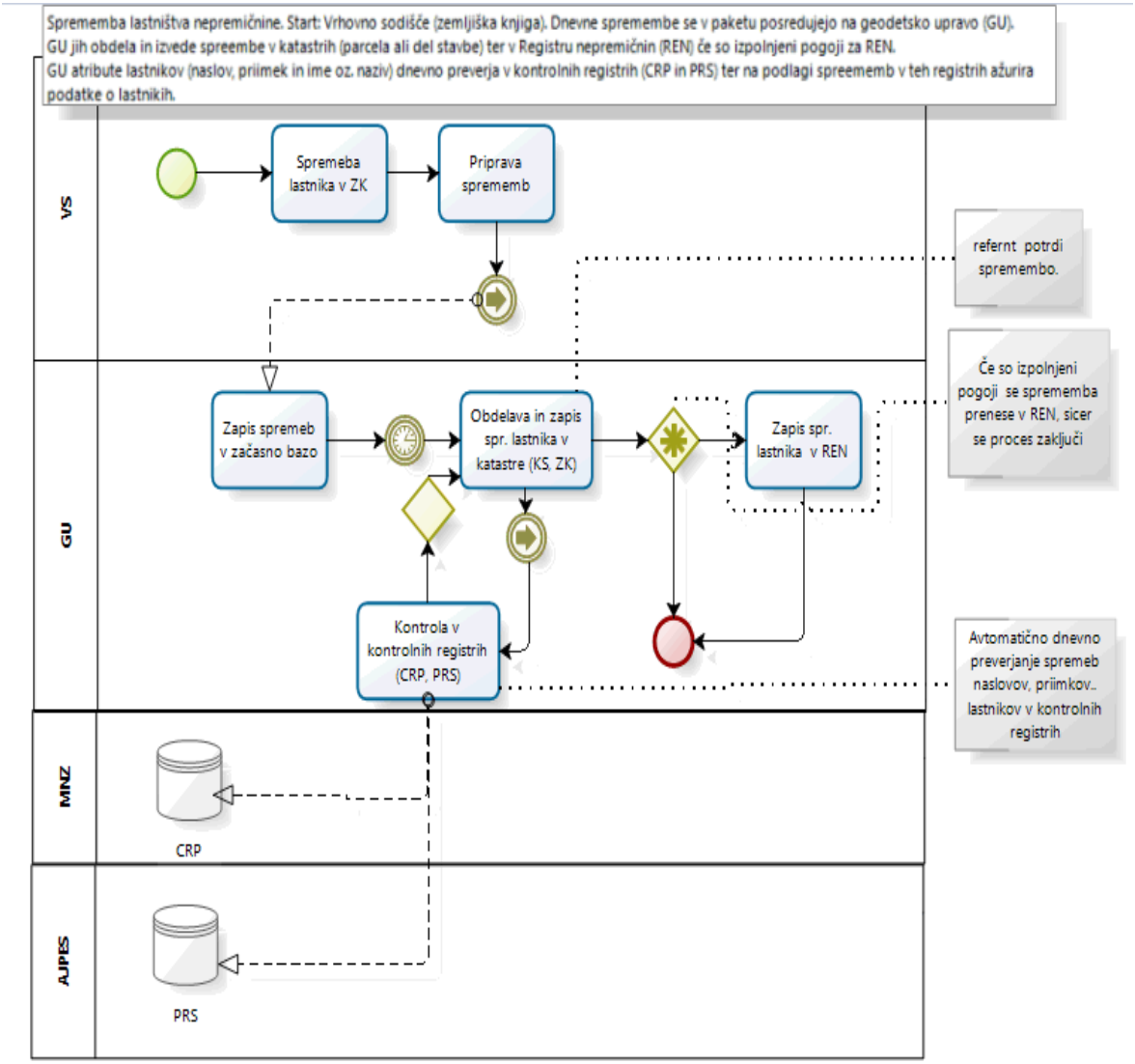
Za vsako evidenco je s sklepom imenovan odgovorni skrbnik za osebne podatke.

Obstajajo še kakšna odprta tveganja glede varstva podatkov oz. zasebnosti?

Ko bo sistem šel v prenovo, naj bi se tudi del varovanja podatkov izboljšal. Tri evidence naj bi se združile v novem sistemu. Vendar pa je predpogoj za kakršnekoli spremembe ustrezna sprememba zakonodaje.

Priloga 3: Poenostavljen diagram procesa spremembe lastništva

Slika: Poenostavljen diagram procesa spremembe lastništva



Vir: U. Mladenovič, osebna komunikacija, 7. marec 2016.