

**UNIVERZA V LJUBLJANI
FAKULTETA ZA DRUŽBENE VEDE**

Sabina Korošec

Mentor: izr. prof. dr. Andrej Anžič

VARNOSTNO PREVERJANJE V REPUBLIKI SLOVENIJI

Diplomsko delo

Ljubljana, 2006

KAZALO

SEZNAM KRATIC.....	3
1 UVOD	4
2 TEORETIČNA, METODOLOŠKA IN HIPOTETIČNA IZHODIŠČA	7
2. 1 OPREDELITEV CILJEV PREUČEVANJA	7
2. 2 METODE DELA.....	7
2. 3 HIPOTEZE.....	8
3 TEMELJNI POJMI	10
3. 1 VARNOST	10
3. 2 VARNOSTNO PREVERJANJE.....	12
3. 3 ČLOVEKOVE PRAVICE	15
4 STANDARDI VARNOSTNEGA PREVERJANJA OSEB V NEKATERIH TUJIH DRŽAVAH	20
4.1 VARNOSTNO PREVERJANJE OSEB V ZDA	20
4.2 VARNOSTNO PREVERJANJE OSEB V ZVEZNI REPUBLIKI NEMČIJI	22
4.3 VARNOSTNO PREVERJANJE OSEB V SLOVAŠKI REPUBLIKI.....	24
5 VARNOSTNO PREVERJANJA OSEB V ATLANTSKIH IN EVROPSKIH VARNOSTNIH POVEZAVAH	27
5.1 VARNOSTNO PREVERJANJE V NATU.....	27
5.2 VARNOSTNO PREVERJANJE V EU	29
6 VAROVANJE TAJNIH PODATKOV REPUBLIKI SLOVENIJI	32
6.1 SPLOŠNO O TAJNIH PODATKIH.....	32
6.2 NORMATIVNA UREDITEV VAROVANJA TAJNIH PODATKOV	34
7 VARNOSTNO PREVERJANJE OSEB V REPUBLIKI SLOVENIJI.....	39
7.1 POGOJI ZA ZAPOSLOSTEV V DRŽAVNIH ORGANIH	39
7.2 VARNOSTNO PREVERJANJE ZA PRIDOBITEV DOVOLJENJA ZA DOSTOP DO TAJNIH PODATKOV	43
7.2.1 VARNOSTNO PREVERJANJE V POLICIJI.....	51
7.2.2 VARNOSTNO PREVERJANJE V SLOVENSKE OBVEŠČEVALNO VARNOSTNI AGENCIJI.....	52
7.2.3 VARNOSTNO PREVERJANJE NA OBRAMBEM PODROČJU	52
8 ZAKLJUČEK.....	54
9 VIRI.....	58

9.1 KNJIGE, ČLANKI, MAGISTRSKE NALOGE.....	58
9.2 PRAVNI VIRI.....	61
9.3 INTERNETNI VIRI IN ELEKTRONSKI MEDIJI.....	62

SEZNAM KRATIC

DDR	Deutsche Demokratische Republik - Nemška demokratična republika
GŠSV	Generalštab Slovenske vojske
EU	European Union – Evropska unija
NATO	North Atlantic Treaty Organisation – Organizacija severnoatlantske pogodbe
RS	Republika Slovenija
SFRJ	Socialistična federativna republika Jugoslavija
ZDA	Združene države Amerike
ZEU	Zahodnoevropska unija
ZObr	Zakon o obrambi
ZRN	Zvezna republika Nemčija
ZTP	Zakon o tajnih podatkih

1 UVOD

Preverjanje v najširšem pomenu besede je najbrž staro prav toliko kot človeštvo. V svojem vsakdanjem življenju namreč kar naprej nekaj preverjamo. Ali ceno nekega izdelka v trgovini ali pa se zanimamo za našega novega soseda. Vendar je to preverjanje del našega zasebnega življenja in se ga pogosto niti ne zavedamo.

Že v zgodovini so obstajale organizacije, ki so se poklicno ukvarjale s preverjanjem podatkov. Danes imajo takšne organizacije oziroma državni organi podlago za svoje delovanje v zakonih.

Morda se na prvi pogled zdi, da diplomska naloga o varnostnem preverjanju in tajnih podatkih ne obravnava ravno aktualne teme. Vendar temu še zdaleč ni tako. Tematika v zadnjem času res ni tako medijsko razvpita, v strokovnih krogih pa je še kako prisotna in aktualna. Slovenija je šele dve leti članica Nata in EU in še vedno ne zagotavlja vseh minimalnih standardov, ki jih obe mednarodni organizaciji predpisujeta na tem področju. Ravno v tem času (13. 3. 2006) je bil sprejet tudi nov zakon - Zakon o spremembah in dopolnitvah zakona o tajnih podatkih (Uradni list RS, št. 28/2006). S sprejetimi spremembami in dopolnitvami ZTP se ureja vprašanje aktivne pravne legitimacije za vložitev predloga za izdajo dovoljenja, natančneje se določajo pristojnosti predlagatelja v posameznih fazah postopka, jasneje so razmejene obveznosti in pristojnosti predlagatelja in preverjane osebe v postopku. Razširjena je vsebina ugotavljanja varnostnih zadržkov, povezanih z boleznimi in duševnimi motnjami, natančneje pa so določeni tudi podatki, ki jih mora oseba posredovati v zvezi z ugotavljanjem njenega finančnega stanja(http://www.uvtp.gov.si/fileadmin/uvtp.gov.si/pageuploads/UVTP_usmeritve_ZTP.pdf).

In kaj pravzaprav je varnostno preverjanje? Zakon o tajnih podatkih ga opredeljuje kot poizvedbo, »ki jo pred izdajo dovoljenja za dostop do tajnih podatkov opravi pristojni organ in katere namen je zbrati podatke o morebitnih varnostnih zadržkih« (8. točka prvega odstavka 2. člena Zakona o tajnih podatkih). In ravno glede poizvedbe so se mnenja v slovenskem prostoru tako kresala, da se je Zakon o tajnih podatkih znašel celo pred Ustavnim sodiščem RS. Nasprotniki zakona so namreč trdili, da le-ta posega v človekove pravice. Sodišče je problem rešilo tako, da je prej enotno preverjanje za vse stopnje tajnih podatkov

spremenilo v tri stopnje preverjanja. Bistvo, ki se skriva v tej rešitvi, pa je načelo sorazmernosti, ki je ključnega pomena pri kakršnem koli preverjanju. Vzpostaviti se mora pravo ravnovesje med interesi in intimo države ter zasebnostjo posameznika.

Ne glede na to, kako je varnostno preverjanje urejeno, ostaja dejstvo, da varnostno preverjanje predstavlja poseg v človekove pravice, pravice, ki jih je država dolžna varovati in jih je tudi zapisala v ustavo. Vendar je država dolžna zagotavljati tako varnost svojih državljanov kot tudi svoj obstoj. In del te varnosti lahko zagotavlja s selekcioniranim dostopom do nekaterih podatkov, ki jih je označila za tako pomembne, da jih je odtegnila splošnemu vpogledu. Rešitev paradoksa, ki ob tem nastane, bi lahko strnila v naslednjih besedah: včasih je potrebno za višji cilj tudi kaj žrtvovati.

V državah, kjer je varnostna kultura na visokem nivoju, se državljani tega tudi zavedajo. Varnostna kultura je namreč izredno pomemben del kadrovske varnosti in varnostnega preverjanja. Uspešno opravljeno varnostno preverjanje nam še ne zagotavlja pravilnega ravnanja s tajnimi podatki, ljudi je potrebno tudi izobraziti. Izobraževanje se mora izvajati neprestano in se mora razlikovati glede na stopnjo tajnosti. Usposabljanje pa ni potrebno le novincev, temveč je nujno potrebno dodatno izobraževati tudi že zaposlene. Zavedati se namreč moramo, da še tako dober sistem varovanja tajnih podatkov ne pomeni nič, če nimamo dobro usposobljenih ljudi, ki se z njimi ukvarjajo. Vzpostavljen mora biti torej celosten sistem ravnanja s tajnimi podatki, ki poleg izobraževanja vključuje še tehnične, fizične in organizacijske ukrepe.

V nalogi se seveda ne bom ukvarjala le z varnostnim preverjanjem v Republiki Sloveniji. Navezala se bom na dokumente in direktive Nata in EU ter preverila, kako imajo to področje urejeno v Združenih državah Amerike, Zvezni republiki Nemčiji in Slovaški republiki. Izkušnje držav, ki pripadajo kontinentalnemu pravnemu redu, so nam seveda veliko bližje kot pa denimo izkušnje Velike Britanije ali Združenih držav Amerike, ki imata nam neprimerljivo pravno ureditev. Kljub temu bom predstavila tudi varnostno preverjanje v ZDA, saj je njihova politika varnostnega preverjanja izredno široka in njihove izkušnje še zdaleč niso zanemarljive.

Varnostno preverjanje oseb je najpomembnejši element varovanja tajnih podatkov. Človek namreč še vedno ostaja ključni rizični faktor, zato je temu postopku potrebno nameniti največ

pozornosti. Predhodno opravljeno varnostno preverjanje je namreč pogoj za pridobitev dovoljenja za dostop do tajnih podatkov, ni pa to edini pogoj. Poznamo še dva, ponekod tri. V večini držav se poleg varnostnega preverjanja uporablja tudi že omenjeno dovoljenje za dostop do tajnih podatkov in potrebo po védenju, v nekaterih državah pa še seznam oseb, ki imajo dostop do tajnih podatkov.

Pa vendar, kljub vsem tem varovalnim mehanizmom, tajni podatki še vedno prihajajo na dan. Čeprav skušajo vse države takšne anomalije čimbolj minimalizirati, do njih vseeno prihaja. Opozoriti velja, da je do njih prihajalo tudi v nedemokratskih sistemih, kjer so to skušali zajeziti z represijo. Tako lahko zaključimo, da bo do določenega uhajanja tajnih podatkov prihajalo zmeraj, ne glede na to, na kakšen način in v kakšni meri država, v prizadevanjih za zaščito lastne zasebnosti, posega v človekove pravice svojih državljanov.

Tu pa se po mojem mnenju pokaže, kako pomembno je izobraževanje in posledično dvig varnostne kulture na tem področju. Potrebno je zagotavljati in vzdrževati določeno stopnjo varnostne kulture ter lojalnosti in pripadnosti sistemu in državi. Le s tem se namreč lahko bistveno zmanjša zlorabo tajnih podatkov.

2 TEORETIČNA, METODOLOŠKA IN HIPOTETIČNA IZHODIŠČA

2.1 OPREDELITEV CILJEV PREUČEVANJA

Varnostno preverjanje je eden izmed ukrepov za zagotavljanje tajnosti določenih podatkov in s tem varovanja državnih interesov. Država ima sicer popolnoma legitimno pravico, da varuje svoje interese, vendar s tem kaj kmalu trči v človekove pravice. Postavi se vprašanje, do kam sega zasebnost države in kje se prične zasebnost posameznika, državljana. Država nedvomno posega v človekovo intimo, a mora pri tem upoštevati določene omejitve.

Varnostno preverjanje je prisotno v vseh državah, s katerimi sodeluje Republika Slovenija, prisotno pa je tudi v obeh organizacijah, Natu in EU, v kateri je Slovenija vključena. Zato dobro urejeno področje varnostnega preverjanja ni ključnega pomena le zaradi naših lastnih tajnih podatkov, ampak tudi zaradi tajnih podatkov, ki jih pridobivamo od drugih držav, bodisi preko bilateralnih odnosov bodisi preko obeh mednarodnih organizacij.

Cilj naloge je tako opredeliti vlogo in pomen izvajanja varnostnega preverjanja kot enega izmed najpomembnejših ukrepov za varovanje tajnih podatkov. Cilj naloge je tudi analiza metod varnostnega preverjanja v Republiki Sloveniji in nekaterih drugih sodobnih državah ter mednarodnih organizacijah. Primerjava med starimi članicami Nata, kot so Združene države Amerike in Zvezna republika Nemčija, ter novimi, kot je Slovaška republika, bo pokazala, kje se trenutno nahaja Republika Slovenija in koliko mora na tem področju še postoriti, da bo postala zaupanja vreden partner ter da bo izpolnila vse smernice in minimalne standarde, ki jih postavljata Nato in EU.

2.2 METODE DELA

Metode, uporabljene v tem diplomskem delu, se navezujejo na samo vsebino naloge. Uporabila sem teoretične metode raziskovanja. Z *metodo zbiranja virov* sem dobila splošen vpogled v problematiko varnostnega preverjanja. Že na samem začetku sem ugotovila, da je bibliografija s tega področja na slovenskem področju precej obsežna. Na temo tajnih podatkov in varnostnega preverjanja je bilo veliko člankov napisanih zlasti v obdobju

sprejemanja prvega Zakona o tajnih podatkih. Problematično pa je bilo iskanje gradiva po medmrežju, saj je iskanje s ključnimi besedami dalo ogromno rezultatov, ki pa so bili za moje delo večinoma neuporabni. Naletela sem tudi na nekatere druge omejitve, povezane predvsem z dostopom do literature. Denimo temeljni dokument, ki v Natu ureja raziskovano področje, Varnost v okviru organizacije Severnoatlantskega sporazuma, C-M(2002)49, je zame nedostopen, zato sem si morala žal pomagati le s sekundarnimi viri. Težavo pa sem imela tudi pri zbiranju tuje literature, saj je dostopna le na medmrežju. Tista v angleškem jeziku se večinoma nanaša na ameriški sistem, pri iskanju informacij za druge države, npr. Nemčijo, pa sem naletela na jezikovno oviro.

Nadalje sem se osredotočila na *analizo in interpretacijo primarnih virov*. S primarnimi viri mislim na različne zakone, podzakonske akte, pravilnike, ustavo in druge dokumente, ki urejajo področje varnostnega preverjanja. Osredotočila sem se na jezikovno metodo interpretacije ter na primerjalno metodo, saj sem med seboj primerjala zakonodajo Združenih držav Amerike, Zvezne republike Nemčije, Slovaške republike in Republike Slovenije. Uporabila sem še *analizo in interpretacijo sekundarnih virov*, s katerimi mislim na številne članke, ki se nanašajo na obravnavano temo, s pomočjo katerih sem še dodatno osvetlila problematiko varnostnega preverjanja.

Nenazadnje nisem mogla niti brez *primerjalne analize*, saj je le-ta moje delo lahko zaključila v smiselno celoto. Med seboj sem primerjala ureditve varnostnega preverjanja v Republiki Sloveniji, Združenih državah Amerike, Zvezni republiki Nemčiji, Slovaški republiki, Evropski uniji ter Natu. S pomočjo te metode sem iskala podobnosti in razlike med ureditvami varnostnega preverjanja v različnih državah in mednarodnih organizacijah. Primerjava je omogočila boljše razumevanje ureditve področja v Republiki Sloveniji, obenem pa je pokazala tudi na pomanjkljivosti, ki se v slovenski ureditvi še vedno pojavljajo.

Metoda *študije primerov* mi je služila kot osnova za prej navedeno primerjalno raziskovanje.

2. 3 HIPOTEZE

V skladu z zastavljenim ciljem bom preizkušala naslednjo hipotezo:

Z varnostnim preverjanjem zagotovimo, da so osebe, ki bodo delale s tajnimi podatki, lojalne, zanesljive in vredne zaupanja. Varnostno preverjanje kot tako se izvaja v vseh sodobnih državah in mednarodnih organizacijah in mora biti zlasti med članicami istih organizacij med seboj primerljivo.

Izvedeni hipotezi sta:

1. Za pravilno ravnanje s tajnimi podatki ni dovolj zgolj uspešno opravljeno varnostno preverjanje. Pomembno je tudi izobraziti ljudi, saj si s tem država zagotavlja odgovornejše ravnanje s tako občutljivimi podatki, kot so tajni.
2. Republika Slovenija bo morala še nadgraditi svoj sistem varovanja tajnih podatkov in varnostnega preverjanja, da bo zadostila minimalnim standardom Nata in EU.

3 TEMELJNI POJMI

Zaradi lažjega razumevanja predstavljene tematike je potrebno opredeliti nekaj temeljnih pojmov, ki so bodisi posredno bodisi neposredno povezani s tematiko varnostnega preverjanja oseb.

3.1 VARNOST

Grizold (1999: 23) opredeli varnost »kot stanje, v katerem je zagotovljen uravnotežen fizični, duhovni in duševni ter gmotni obstoj posameznika in družbene skupnosti v razmerju do drugih posameznikov, družbene skupnosti in narave.«

»Razvojno gledano je varnost vgrajena kot biološki mehanizem, kot težnja organizma po obstoju, kot prilagajanje organizma na ogrožajoče vplive okolja. Biološko je torej varnost pogoj za delovanje osnovnih življenjskih funkcij /.../ in je tako vzgib za razvoj, zavestno dejanje, da bi se stanje varnosti (kot pozitivno dejanje) zmeraj znova vzpostavilo« (Grizold, 2001: 126).

Anžič (2002: 455) pa varnost opredeljuje kot »imanentno prvino družbe, ki zajema stanje oziroma lastnost stanja in dejavnost oziroma sistem«. Pojem varnost se nanaša tako na posameznika, na državo oziroma družbo v celoti kot tudi na mednarodno skupnost. Sodobna varnostna paradigma namreč varnost obravnava v treh temeljnih okvirjih, in sicer kot individualno varnost, kot nacionalno varnost ter kot mednarodno varnost. Posameznik vedno najprej občuti potrebo po svoji lastni varnosti in zadovoljitev le-te mu omogoča kakovosten obstoj in razvoj. Varnost »je torej človekovo zavestno prizadevanje za vzpostavitev takšne civilizacijske in kulturne kategorije, ki bo zajemala vse vidike varnosti: politične, gospodarske, pravne, zdravstvene, socialne, kulturne in številne druge« (Anžič, 2002: 455). Razumevanje pojma sodobne varnosti mora nujno vključevati »vse vidike človeškega obstoja in delovanja v družbi /.../ ter vse ravni njegovega povezovanja in oblike družbenega organiziranja (regionalno, nacionalno, mednarodno in svetovno)« (Grizold, 2001: 83). »Varnost ni vezana samo na eno področje človekovega delovanja, ampak je potreba po

varnosti prisotna na vseh področjih človekovega delovanja in delovanja širše skupnosti, v katere se povezuje človek (države, naroda, podjetja itd.)« (Črnčec, 2003:17).

Za temo moje diplomske naloge je potrebno še posebej opredeliti individualno in nacionalno varnost. Obe sta namreč, kot nakazuje že prejšnji odstavek, neločljivo povezani. Nacionalno varnost Grizold (1992: 65) opredeljuje kot varnost državnega ozemlja (kopno, vode, zračni prostor), prebivalstva in njihove lastnine, ohranjanje nacionalne suverenosti ter zagotavljanje ustreznih razmer za uresničevanje temeljnih funkcij družbe. »Pri nacionalni varnosti /.../ gre za prizadevanje države, da zagotovi varnost vsem članom družbe pred ogrožanjem od zunaj (posegi, napadi, okupacija, blokada idr.) in znotraj družbe (ogrožanje reda in miru, kriminal)« (Grizold, 1999: 28). V t. i. notranje grožnje bi nenazadnje lahko vključili tudi nepooblaščen izdajanje tajnih podatkov. Anžič (1997:37) pa poudarja še drug vidik nacionalne varnosti. Pravi namreč, da »nacionalna varnost sicer res na eni strani zagotavlja varnost svojim državljanom ter odpravlja vire njihovega ogrožanja. Toda hkrati lahko preko svojih varnostnih organov tudi sama postane vir ogrožanja individualne varnosti.«

Hermann (1982, v Anžič, 1997: 36) pa nacionalno varnost opredeljuje kot varnost, ki »se vedno nanaša na samostojno in suvereno državo, ki prevzema odgovornost za lastno varnost, pa tudi odgovornost za globalno varnost. Gre torej za varnost naroda, ki zajema: varnost nacionalnega ozemlja, zaščito življenja ljudi, zaščito osebnega in drugega premoženja, varovanje človekovih pravic in svoboščin, ohranitev in vzdrževanje nacionalne suverenosti, uresničevanje temeljnih funkcij družbe, varstvo okolja.«

Nacionalno varnost je seveda v Resoluciji o izhodiščih zasnove nacionalne varnosti opredelila tudi Republika Slovenija. Nacionalna varnost je torej »stanje, v katerem je zagotovljeno uresničevanje človekovih pravic in temeljnih svoboščin, uravnotežen gospodarski, socialni in kulturni razvoj ter uresničevanje drugih življenjskih interesov, delovanje demokratične, pravne in suverene ter ozemeljsko enotne in nedeljive Republike Slovenije« (Resoluciji o izhodiščih zasnove nacionalne varnosti Republike Slovenije, Uradni list RS, št. 71/93).

Ker danes živimo v svetu globalizacije, si je nemogoče predstavljati, da slovenski varnostni sistem ne bi bil vpet v mednarodnega. Še bolj je to dejstvo postalo očitno in pomembno ob vključitvi Republike Slovenije v dve mednarodni organizaciji, Nato in EU. Slovenija bo ob svojem delovanju v okviru teh dveh organizacij namreč razpolagala s številnimi tajnimi

podatki drugih držav članic zveze. In varnostni sistem oziroma sistem varovanja tajnih podatkov v organizacijah kot sta Nato in EU je trden le toliko, kolikor je trden najšibkejši sistem države članice. Zato je še posebej pomembno, da RS dobro in temeljito uredi to področje. V nasprotju z individualno varnostjo pa se mednarodna varnost nanaša na celotno mednarodno skupnost in je »notranji varnostni problem sistema držav in sveta kot celote; je kolektivna dobrina mednarodne globalne družbe in ne le dobrina posamezne države ali zveze držav« (Črnčec, 2003:17).

Kot je bilo že omenjeno, velja, da je varnost povezana z možnostjo svobodnega uresničevanja posameznika, zato lahko rečemo, da se svoboda in varnost medsebojno določata in dopolnjujeta. Šele varnost omogoča svobodo posameznika ali družbe in je zato njen predpogoj (Bunič, 2005: 20).

»Slovenija dandanes še vedno išče optimalno ravnotežje med zagotavljanjem varnosti in pravicami posameznika. Sedaj je tehtnica precej nagnjena na stran posameznika, kar vsekakor ni dobro za državo. Praksa iz tujine kaže, da mora biti vzpostavljeno ravnotežje, če ne že rahla nagnjenost tehtnice v prid države. Kajti če država ne more zagotavljati nacionalne varnosti, ne more zagotavljati individualne varnosti in posledično postane problem v okviru mednarodne varnosti« (Črnčec, 2003:7).

3. 2 VARNOSTNO PREVERJANJE

Varnostno preverjanje oseb je za vsak sistem, v katerem osebe prihajajo v stik s tajnimi podatki, izredno pomembno. Ustrezen sistem varnostnega preverjanja pomeni zmanjšanje možnosti dostopa do tajnih podatkov varnostno spornim osebam, s tem pa se zmanjša tudi verjetnost njihovega nepooblaščenega razkritja (Čaleta, 2003: 14). Varnostno preverjanje je torej »ukrep, s katerim naj bi se preverjala zanesljivost in primernost oseb za varovanje s tajnimi podatki« (Vodovnik, 2001: 90). Cilj varnostnega preverjanja je namreč zagotoviti, da se bo nevarnost razkritja tajnih podatkov zmanjšala na sprejemljivo mero. Tajnosti bodo namreč še vedno ogrožene s strani tujih obveščevalnih služb, katerih temeljni cilj je pridobivanje tajnih podatkov (Anžič, Trbovšek, 2004: 37).

Zakon o tajnih podatkih iz leta 2001 opredeljuje varnostno preverjanje kot poizvedbo, »ki jo pred izdajo dovoljenja za dostop do tajnih podatkov opravi pristojni organ in katere namen je zbrati podatke o morebitnih varnostnih zadržkih« (8. točka prvega odstavka 2. člen Zakona o tajnih podatkih).

»Varnostno preverjanje temelji na pravici države, da varuje svojo zasebnost in da onemogoči prosto razpolaganje s svojimi tajnostmi. Država pri tem posega v zasebnost posameznika, ki je zajamčena z ustavo in zakoni« (Črnčec, 2003: 57). To razmerje bi lahko imenovali trajno in nikoli razrešljivo. Najpomembnejše načelo, ki naj bi ga država pri varovanju svoje zasebnosti upoštevala, je načelo sorazmernosti. Poseg v zasebnost posameznika naj bi bil namreč sorazmeren s pomembnostjo informacije, ki jo država želi zaščititi.

Poznamo dva tipa varnostnega preverjanja. Prvo je varnostno preverjanje kot del kadrovskega postopka za zaposlitev v državni upravi (npr. v policiji ali vojski), drugo pa je varnostno preverjanje kot preventivni varnostni ukrep, katerega namen je zagotoviti ustrezno stopnjo varnosti in tajnosti podatkov (Črnčec, 2003: 57).

Dovoljenja za dostop do tajnih podatkov pa ne potrebujejo le zaposleni v državni upravi za delo s tajnimi podatki državne uprave, ampak tudi osebe iz zasebnega sektorja, ki opravljajo storitve za državno upravo in imajo pri svojem delu vpogled v tajne podatke. »V praksi to pomeni, da podjetje, ki konkurira za posel, ki je označen s stopnjo tajnosti (npr. dobava orožja in opreme) mora med drugimi pogoji, izpolniti tudi pogoj izdanega veljavnega dovoljenja za dostop do tajnih podatkov za tiste svoje delavce, ki bodo vključeni v posel« (Črnčec, 2003: 58). Zakonska ureditev tega področja je še posebej pomembna zaradi vključitve Republike Slovenije v NATO in EU ter obenem pomeni prilagajanje standardom obeh zvez.

Angleške sopomenke za varnostno preverjanje so »vetting« in »screening«, srečamo pa tudi pojem »personnel security«, ki bi ga lahko prevedli kot kadrovska varnost. Kadrovska varnost je opredeljena kot dejavnost, ki obsega ukrepe, s katerimi za določena mesta izbira le tiste ljudi, ki so vredni zaupanja, s predpostavko, da se več napak zgodi zaradi nezanesljivosti ljudi znotraj sistema kot zaradi tistih zunaj sistema (npr. vlomi, ropi, vohunstvo). Celoten proces varnostnega preverjanja pa sloni na dejstvu, da lahko s preteklega obnašanja sklepamo tudi na prihodnje. Najpogostejša metoda pri izvajanju kadrovske varnosti je tako »background investigation« oziroma poizvedba o preteklosti, ki vključuje pridobivanje vseh relevantnih

podatkov o posameznikovi izobrazbi, zaposlitvi in obnašanju, preko katerih lahko sklepajo o posameznikovi prihodnji zvestobi, zanesljivosti in poštenosti. V okviru kadrovske varnosti se poleg poizvedbe o preteklosti izvajajo še druge metode, in sicer: preiskava s poligrafom (detektorjem laži), izvajanje pisnih psiholoških testov in razgovori z uporabo stresa. Ko pa je človek že v sistemu, se uporabljajo še druge tehnike za zagotovitev posameznikove zanesljivosti. To so denimo programi indoktrinacije posameznika in t. i. test ranljivosti (vulnerability testing) (Encyclopaedia Britannica 2005 Ultimate Reference Suite DVD).

Vendar pa namen varnostnega preverjanja, kljub poizvedbi o preteklosti, ni ugotavljanje odgovornosti osebe za njena pretekla dejanja, temveč preprosto skuša le ugotoviti, če gre za lojalno, zaupanja vredno osebo (Rep, 2001: 216).

Po Zakonu o obrambi se varnostno preverjanje oseb opravlja kot »posebna oblika zbiranja osebnih in drugih podatkov zaradi preprečevanja, odkrivanja in preiskovanja:

1. ogrožanja oseb, delovnih mest in dolžnosti, za katere se v skladu s tem zakonom lahko sklene delovno razmerje brez predhodne javne objave ali na katerih se opravljajo upravne in strokovne zadeve na področju obrambe;
2. ogrožanja oseb, del in dolžnosti v vojaških poveljstvih, enotah in ministrstvu, ki so določena kot posebnega pomena za obrambo;
3. ogrožanja vojaških poveljstev, enot in zavodov ter objektov in okolišev, ki so posebnega pomena za obrambo« (35. člen).

Zakon o tajnih podatkih glede na stopnjo tajnosti podatkov predvideva tri vrste varnostnega preverjanja. Tako govori o osnovnem vprašalniku za pridobitev dovoljenja za tajne podatke stopnje zaupno, osnovnem in posebnem vprašalniku za pridobitev dovoljenja za dostop do tajnih podatkov ter osnovnem, posebnem in prvem delu dodatnega vprašalnika za pridobitev dovoljenja za dostop do tajnih podatkov. V sklopu dodatnega vprašalnika je potrebno navesti osebna imena ter naslove stalnih, začasnih in dejanskih prebivališč treh oseb, ki lahko potrdijo podatke, navedene v vprašalnikih. Posebni vprašalnik pa obsega naslednje podatke: sodelovanje v tujih oboroženih silah ali drugih oboroženih formacijah; prezadolženost zaradi finančnih obveznosti oziroma prevzetih jamstev; davčna številka; lastnosti in okoliščine iz življenja preverjane osebe, ki imajo lahko za posledico izpostavljenost izsiljevanju ali drugim oblikam izvajanja pritiska. Podatke, navedene v vprašalniku, je dovoljeno preveriti pri upravljavcih zbirk osebnih podatkov, določene podatke pa še pri izbranem zdravniku

preverjane osebe, pri Slovenski obveščevalno-varnostni agenciji in Obveščevalno varnostni službi Ministrstva za obrambo, pri prejšnjih delodajalcih preverjane osebe in pri organu, pristojnem za davčne zadeve ter na sodišču (25. člen Zakona o spremembah in dopolnitvah zakona o tajnih podatkih).

»Nedvomno sta lojalnost (državi, organizaciji) in zanesljivost (na delovnem mestu in izven njega) ključna kriterija, na podlagi katerih se ocenjuje, ali je posameznik verodostojen. Dvom v lojalnost in/ali zanesljivost predstavlja glavni kriterij pri ocenjevanju varnostnih zadržkov« (Črnčec, 2003: 61).

V Sloveniji in v večini drugih demokratičnih državah je varnostno preverjanje dovoljeno izključno na podlagi pisnega soglasja za izvajanje le-tega. Tako se poseg v posameznikovo intimo in v njegove pravice vsaj deloma zabriše, saj se izvaja le z njegovo privolitvijo.

Varnostno preverjanje pa se lahko konča z izdajo dovoljenja za dostop do tajnih podatkov ali pa z zavrnitvijo. Zavrnitev pomeni, da obstajajo varnostni zadržki. Le-ti so v 2. členu ZTP opredeljeni kot »ugotovitve varnostnega preverjanja, iz katerih izhaja, da obstajajo dvomi o zanesljivosti in lojalnosti osebe, ki naj bi dobila dovoljenje za dostop do tajnih podatkov«.

3. 3 ČLOVEKOVE PRAVICE

Ob razmišljanju o varnostnem preverjanju nikakor ne moremo mimo človekovih pravic, mimo posegov v z ustavo zagotovljene pravice, kot so npr. varstvo osebnih podatkov ali pa pravica do zasebnosti.

»Človekove pravice in temeljne svoboščine so kompleksna kategorija, ki predstavlja temelj vsake sodobne demokratične države« (Črnčec, 2003: 70) in »že sam termin temeljne človekove pravice (nam) razkriva naravo in vir teh pravic: to so pravice, ki jih ima nekdo zgolj zaradi dejstva, da je človek. Veljajo za vse ljudi ne glede na pravice in dolžnosti, ki jih imajo nekateri kot državljani, družinski člani, delavci ali člani javne oz. zasebne organizacije. Ker se dejstvu, da je nekdo človek, ni mogoče odpovedati, prav tako pa statusa ni mogoče izgubiti oz. ga odpraviti, so človekove pravice neodtujljive« (Franetič, 2004: 5). Vendar pa

teh pravic v praksi ne uživajo vsi ljudje oz. jih ne uživajo v enaki meri, čeprav naj bi bile za vse ljudi enake in neodtujljive.

»Pravica omogoča obstoj, razvoj in uresničevanje potreb posameznika v družbi. Imeti določeno pravico pomeni smeti, imeti dovoljenje za realizacijo določenega dejanja oziroma zadovoljitve neke potrebe, ne da bi te pri tem kdo oviral ali nasprotoval. Lahko rečemo, da pomeni torej upravičenje do nečesa« (Bunič, 2005: 13).

Človekove pravice so v leksikonu (Leksikon CZ, 1998: 171, 1074) opredeljene kot »neodtujljive in nedotakljive pravice ter svoboščine posameznika nasproti posegom državne oblasti«. Posebej so obravnavane še temeljne pravice, in sicer kot »nedotakljive pravice posameznika, ki mu zagotavljajo sfero osebne svobode, v katero državna oblast ne sme posegati. Podrobneje jih opredeljujejo in razčlenjujejo ustave posameznih držav«.

Vendar pri opredeljevanju pravic velja opozoriti na dejstvo, da se pojma pravica in svoboščina med seboj razlikujeta. Pojem svoboščina se običajno uporablja v filozofskem smislu, pojem pravica pa v pravnem. Dejstvo pa je, da je vsaka pravica, kot pravni pojem, pravzaprav izvedena iz svoboščine. Pravica kot taka je torej v bistvu svoboščina, vendar je prilagojena pravni terminologiji (pravnemu jeziku in obliki) (več o tem Cerar, 1997: 55–59). Kaučič (2003: 92 v Črnčec, 2003: 70) pa celo zapiše, da »danes svoboščine in pravice uživajo enako pravno varstvo, zato je v pravnem pomenu svoboščina le sinonim za pravico«. Pomembna razlika izhaja tudi iz odgovornosti nosilca pravice in svoboščine. Pravica kot pravna kategorija je povezana z dolžnostjo. Pravica se nanaša na dolžnost neke druge osebe, da upravičencu nekaj da ali stori zanj. Svoboščine pa opredeljujejo neko sfero, v katero druga oseba ne sme posegati (Cerar, 1997: 55–59).

»Krovni pravni akt, iz katerega izhaja ureditev vsake moderne države, je ustava« (Črnčec, 2003: 70). »Ustava omejuje državo pri posegih v ustavne svoboščine in pravice, zato nekateri poudarjajo, da je ustava katalog veljavnih pravic, splošno sprejetih v civilizirani družbi. Te pravice so tudi opredeljene v mednarodnih paktih o gospodarskih, kulturnih in političnih pravicah ter v Evropski konvenciji o varstvu človekovih pravic in temeljnih svoboščin« (Šinkovec, 1996:7).

»V razmerju do države so pozitivne in negativne človekove pravice. Pozitivne so tiste, na osnovi katerih državljan pričakuje in zahteva, da država izpolni vsako svojo dolžnost s tem, da mu zagotavlja določene usluge in dobrine. Pri negativnih pravicah pa gre za to, da državljan ne pričakuje, da bo država zanj naredila nekaj pozitivnega, temveč lahko le zahteva, da se v odnosu do njega vzdrži določenih dejanj in ravnanj« (Anžič, 1997: 167).

Razvoj človekovih pravic se je pričel že v antiki, najdemo jih lahko v delih Aristotela in Platona. Vendar so se človekove pravice v današnjem pomenu besede pričele oblikovati šele v 17. in 18. stoletju.

V 18. stoletju sta bili sprejeti prvi listini svoboščin in pravic. To sta bili Virginijska deklaracija o svoboščinah (Virginia Bill of Rights – 1766) in Deklaracija o pravicah človeka in državljana (La déclaration des droits de l'homme et du citoyen – 1789). Poglavitni dokument prejšnjega stoletja pa je Splošna deklaracija o človekovih pravicah, ki jo je Generalna skupščina OZN sprejela leta 1948. S področja človekovih pravic pa je potrebno omeniti še dva dokumenta, Mednarodno pogodbo o državljanskih in političnih pravicah ter Mednarodno pogodbo o gospodarskih, socialnih in kulturnih pravicah, ki sta bila sprejeti, da bi določbe Splošne deklaracije o človekovih pravicah postale pravno zavezujoče.

Tako so države, predvsem v prejšnjem stoletju, z namenom uresničevanja, spoštovanja in varovanja načel in določil, ki urejajo področje človekovih pravic in njihovega varstva, na mednarodni in nacionalni ravni sprejele številne dokumente ter vzpostavile institucije, ki naj bi z različnimi mehanizmi zagotavljale varstvo človekovih pravic (Bunič, 2005: 6).

Zgodovinsko in razvojno razvrščamo nastajanje in uveljavitev temeljnih človekovih pravic in svoboščin v tri generacije. Prva generacija so politične in civilne pravice, drugo generacijo predstavljajo ekonomske in socialne pravice, tretjo pa informacijske in komunikacijske pravice (Črnčec, 2003:75).

Varnostno preverjanje oseb predstavlja svojevrsten poseg v človekove pravice. Ta poseg je v večini demokratičnih držav omiljen s tem, da posameznik na preverjanje pristane. Z varnostnim preverjanjem pa je povezano tudi nerešljivo nasprotje med zasebnostjo države in intimo posameznika. Lahko rečemo, da je bil ta konflikt v SFRJ rešen močno v prid državni zasebnosti, danes pa se nekatere rešitve morda celo nekoliko preveč nagibajo v prid

zasebnosti posameznika. Najpomembnejše načelo, ki ga je potrebno upoštevati pri varnostnem preverjanju oseb, je načelo sorazmernosti oziroma načelo prepovedi čezmernega ukrepanja. To je bil tudi eden izmed razlogov za spremembo ZTP leta 2003. »Državni ukrepi ne morejo biti neomejeni in svobodni, morajo biti vedno utemeljeni, njihovo sprejemanje mora imeti namen, opredeljen v zakonu, ukrepi pa morajo biti primerni namenu« (Šinkovec, 1996: 27). Danes v demokratičnih družbah velja, da naj bi bili »posegi v zasebnost in osebnost posameznika /.../ dopustni samo z odločitvijo sodišča in ob upoštevanju uporabe najmilejših ukrepov, ki so potrebni za doseg cilja« (Črnčec, 2003:76).

»Za človekove pravice je temeljnega pomena, da so ustrezno varovane in zaščitene. Le tako namreč njihovo uresničevanje poteka nemoteno, morebitne kršitve pa so kaznovane s sankcijami« (Bunič, 2005: 24).

Posamezniki imajo tudi pravico pravnega varstva, saj so zavarovani preko institucij, ki se ukvarjajo s spoštovanjem človekovih pravic in svoboščin. O tem v svojem 8. členu govori tudi Splošna deklaracija o človekovih pravicah, in sicer »da ima vsakdo pravico do učinkovitega pravnega varstva pri pristojnih državnih sodnih oblasteh proti dejanjem, ki kršijo temeljne pravice, priznane mu po ustavi ali zakonu« (Splošna deklaracija o človekovih pravicah, 1948: čl. 8). Deklaracija sicer omenja le državne oblasti, vendar so te institucije lahko tudi nedržavne oziroma naddržavne. Državne so denimo ustavno sodišče ter ombudsman, nedržavne pa Evropsko sodišče za človekove pravice, Amnesty International in Helsinški monitor.

Ustava Republike Slovenije v poglavju o človekovih pravicah in temeljnih svoboščinah v 35. členu zagotavlja nedotakljivost človekove telesne in duševne celovitosti, zasebnosti ter osebnostnih pravic. Človekovo zasebnost zagotavlja tudi s 37. členom, ki govori o tajnosti pisem in drugih občil. Potem so tu še določbe o nedotakljivosti stanovanja in varstvu osebnih podatkov (Pavčnik, 1997: 162). V 39. členu pa govori o zagotovljeni svobodi tiska ter drugih oblikah javnega obveščanja in o pravici vsakogar, da skladno z zakonom dobi informacije javnega značaja (Čaleta, 2004c: 48). Vendar pa ne moremo mimo 15. člena, ki pravi, da se pravice omejujejo zaradi pravic drugih in tedaj, kadar to določa ustava. Torej država lahko omeji pravice posameznika, kadar gre za javno varnost, obrambo ali obveščevalno in varnostno dejavnost države.

Ko omenjamo kratenje človekovih pravic in svoboščin, je pomembno, da razlikujemo med kršitvijo in ogrožanjem človekovih pravic in svoboščin. Pojem kršitev se namreč nanaša na izvršeno dejstvo, pojem ogrožanja pa pomeni, da gre za dejansko stanje, ki potencialno trajno ogroža človekove pravice in svoboščine. Poznamo tudi posredne in neposredne oblike kratenja človekovih pravic in svoboščin. Neposredne so tiste, ki niso v skladu z zakonom, npr. prekoračenje pooblastil, posredne pa so tiste, ki izvirajo iz pomanjkljive, nedoločene ali celo pravno pomanjkljive zakonodaje (Šturm, 1998: 23).

Ustava Republike Slovenije je človekovim pravicam namenila veliko pozornosti. »Kljub temu dejstvu pa kaže poudariti, da so ustavne rešitve zgolj okvir, ki le nakazuje možnosti nadaljnje implementacije vseh prizadevanj za praktično uveljavljanje človekovih pravic in svoboščin« (Anžič, 1997: 163).

Poznamo pravice, ki uživajo absolutno varstvo, poznamo pa tudi take, ki jih je mogoče omejiti. »Vzrokov za omejitev je precej: javna varnost, državna varnost, zavarovanje zdravja in morale, preprečitev neredov in zločinov, ekonomska blaginja države itd. Ker je teh vzrokov relativno veliko, obstaja tudi nevarnost, da bi jih nacionalne zakonodaje preširoko pojmovale in jih tako zlorabile« (Anžič, 1997: 168).

4 STANDARDI VARNOSTNEGA PREVERJANJA OSEB V NEKATERIH TUJIH DRŽAVAH

4.1 VARNOSTNO PREVERJANJE OSEB V ZDA

Sistem varnostnega preverjanja je bil v Združenih državah Amerike utemeljen po 2. svetovni vojni za podporo sistemu klasifikacije tajnih podatkov in za dopolnitev programov preiskovanja lojalnosti uslužbencev vlade. V tem času so bili sprejeti številni dokumenti, katerih namen je bil prilagoditi sistem varnostnega preverjanja nastalim potrebam (Trbovšek, 2004: 90).

Najpomembnejše uredbe s tega področja so:

- izvršilni odlok 10450 Varnostni pogoji za vladne službe (Security Requirements for Government Employment) predsednika Eisenhowerja leta 1953;
- Izvršilni odlok 12968 Dostop do tajnih podatkov (Access to Classified Information) iz leta 1995, ki je le dodal nova pravila;
- Uredba direktorja osrednje obveščevalne službe (CIA) št. 6/4, Standardi in postopki kadrovske varnosti za dostop do posebno varovanih občutljivih podatkov (Director of Central Intelligence Directive 6/4, "Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information (SCI)," July 2, 1998).
- Odredba o kadrovski varnosti v ministrstvu za obrambo (Personnel Security Program – DoD 5200.2-R-Januar 1987).

Izvršilni odlok 10450 predstavlja bazo, osnovo, vsi naslednji dokumenti pa izhajajo iz njega. Zelo pomembna je tudi Odredba o kadrovski varnosti, ki je obvezna v vseh organih ministrstva za obrambo. Vsebuje različna navodila in postopke za izvajanje predpisov. Posebej se dotika tudi dovoljenj za dostop do tajnih podatkov.

Pogoj za pričetek varnostnega preverjanja je seveda izpolnjen varnostni vprašalnik. ZDA poznajo več vrst varnostnega preverjanja, in sicer glede na stopnjo tajnosti podatkov.

- *Preveritve pri državnih službah* (National Agency Check). V sklopu tega preverjanja se preverijo podatki v arhivih služb zvezne vlade. Preverjanje zajema obdobje 5 let, vendar ne pred 18. letom starosti (<http://www.fas.org/sgp/backchek.htm>).
- *Preiskava osebnega ozadja z enkratnim obsegom* (Single Scope Background Investigation). Opravlja se za vse uslužbence, ki potrebujejo dovoljenje za dostop do tajnih podatkov stopnje STROGO ZAUPNO (TOP SECRET). Poleg preverjanja pri državnih službah zajema še preveritev podatkov o zakoncu ali izvenzakonskem partnerju. Preveri se izobrazbo, prejšnje zaposlitve, nedržavne zaposlitve, finančni položaj osebe in njeno zdravstveno kartoteko. Pridobi se ocene znancev, ki jih je oseba sama navedla v vprašalniku, pridobi pa se tudi ocene še vsaj treh oseb, ki jih preverjani ni predlagal sam. Zajema obdobje zadnjih 10 let, vendar ne pred 18 letom starosti, če je to obdobje krajše, pa najmanj za dve leti (<http://www.dss.mil/search-dir/seclib/govsec/chap4.htm>).
- *Periodična ponovna preiskava* (Periodic Reinvestigation). »Preiskava se opravi, če je od prejšnje preiskave preteklo pet let, posameznik pa še vedno dela na delovnem mestu z dostopom do zaupnih podatkov« (Žiberna, 2004: 41). Izvede se obe zgoraj navedeni preiskavi.

Vsekakor pa ne smemo mimo omembe razsodniškega priročnika (The Adjudicative Desk Reference). To je pripomoček, ki ga je razvil Varnostni raziskovalni center Obrambne Varnostne službe Ministrstva za obrambo ZDA. V njem so podrobno opisani možni varnostni zadržki z vseh 13 področij, na katerih se preverja oseba, ta področja pa so: pripadnost Združenim državam, tuji vplivi, naklonjenost tuji državi, spolno vedenje, osebno vedenje, pomisleki finančne narave, uživanje alkohola, vpletenost v uživanje drog, čustvene, duševne in osebnostne motnje, kaznivo vedenje, kršitev varnosti, aktivnosti izven službe in zlorabe sistemov informacijske tehnologije. Vsakega izmed teh faktorjev pa je potrebno oceniti v kontekstu celovite osebnosti (Trbovšek, Brožič, 2002: 4).

Nihče ne dobi dovoljenja za dostop do tajnih podatkov, če ni uspešno opravil varnostnega preverjanja in če informacije ne potrebuje zaradi opravljanja delovnih nalog ter nima t. i. potrebe po vedenju (»need to know«). Prav tako nihče ne dobi dovoljenja za dostop do tajnih podatkov zgolj zaradi svojega položaja (Executive Order 12968).

Če centralno razsodišče odloči, da oseba ni primerna za dostop oziroma podaljšanje dovoljenja za dostop do tajnih podatkov, le-tej pošlje sklep o zavrnitvi oz. preklicu. V sklepu so navedeni tudi razlogi za odločitev. Oseba ima možnost pritožbe, in sicer na dva načina: s pritožbo z osebnim nastopom pred upravnim sodnikom Urada za zaslišanje in pritožbe¹ (Office of Hearings and Appeals) ali s pisno pritožbo brez osebnega nastopa. O zadevi odloča prizivni odbor, njegov sklep pa je dokončen. Sodno varstvo je možno, vendar redko in se običajno konča v prid države (Trbovšek, 2004: 113).

4.2 VARNOSTNO PREVERJANJE OSEB V ZVEZNI REPUBLIKI NEMČIJI

Zvezna republika Nemčija je področje varnostnega preverjanja uredila z Zakonom o pogojih in postopkih zveznega varnostnega preverjanja iz leta 1994. Za to področje sta pomembna še Zakon o sodelovanju zveze in dežel v zadevah varstva ustavne ureditve in o zveznem uradu za varstvo ustavne ureditve ter Zakon o vojaški varnostni službi (Trbovšek, 2004: 127).

Varnostno se preverja osebe, ki so stare najmanj 16 let, seveda po njihovem predhodnem pisnem soglasju. Za dostop do tajnih podatkov stopnje TAJNO ali STROGO TAJNO pa se, ob njegovi pisni privolitvi, preveri tudi polnoletni zakonec ali izvenzakonski partner te osebe. Brez varnostnega preverjanja dobijo dostop do tajnih podatkov člani zveznih ustavnih organov (predsednik republike, kancler in člani vlade, predsednika in člani obeh domov parlamenta), sodniki in tuji državljani, ki naj bi na območju ZRN, v skladu z mednarodnimi obveznostmi, ki jih je prevzela ZRN, pri opravljanju svojih nalog dostopala do tajnih podatkov.

Glede na predviden dostop do tajnih podatkov zakon opredeljuje tri vrste varnostnega preverjanja.

- *Enostavno varnostno preverjanje* za pridobitev dovoljenja za dostop do tajnih podatkov stopnje ZAUPNO. Pri tej obliki preverjanja organ oceni navedbe v vprašalniku, ki ga je preverjana oseba izpolnila, ter pridobi informacije iz osrednjega zveznega registra, od Zveznega kriminalističnega urada, Službe za zaščito meja in Zvezne obveščevalne službe.

¹ Urad za zaslišanje in pritožbe je na svoji internetni strani objavil podrobna navodila za pritožbo z osebnim nastopom - <http://www.defenselink.mil/dodgc/doha/pap-g.html>.

- *Razširjeno varnostno preverjanje* za pridobitev dovoljenja za dostop do tajnih podatkov stopnje TAJNO ali do velikega števila gradiv z oznako ZAUPNO. Pri tej obliki preverjanja organ zbira informacije še na policijskih postajah, na območju katerih je preverjana oseba živela zadnjih pet let, ter še dodatno preveri identiteto osebe.
- *Razširjeno varnostno preverjanje z varnostnim poizvedovanjem* za pridobitev dovoljenja za dostop do tajnih podatkov stopnje STROGO TAJNO ali do velikega števila gradiv z oznako TAJNO. Pri tej obliki pa organ izpraša tudi referenčne osebe, ki jih je navedla preverjana oseba.

Po potrebi se preverjanje lahko razširi na naslednjo stopnjo (Čaleta, 2004a: 83–84 in Škoporc, 2002: 15–16).

Vsebina izjave za varnostno preverjanje pa je naslednja: »Priimek in ime, datum in kraj rojstva, državljanstvo, zakonski stan, prebivališča in začasna bivanja, daljša od dveh mesecev, in sicer v ZRN zadnjih pet let, v tujini pa od 18. leta dalje, poklic, delodajalec, število otrok, osebe, starejše od 18 let, ki živijo v istem gospodinjstvu, starši, krušni straši, rejniki, izobraževanje, identifikacijski dokumenti, opravljene prisilne izvršbe v zadnjih petih letih, stiki s tujimi obveščevalnimi službami in službami nekdanje DDR, stiki s protiustavnimi organizacijami, tekoči kazenski in disciplinski postopki, stiki s prebivalci »terorističnih« držav oziroma potovanja v te države, identifikacijski podatki dveh oseb, ki bosta potrdili identiteto preverjanca, identifikacijski podatki treh oseb, pri katerih bo pristojna služba opravila varnostno poizvedovanje ter podatki o predhodnih varnostnih preverjanjih« (Črnčec, 2003: 97).

Zadržki, ki se ugotavljajo pri varnostnem preverjanju, so predvsem: dvom o varnostni zanesljivosti osebe, poskusi navezovanja stikov s tujimi obveščevalnimi službami in dvomi o opredelitvi osebe za svobodno demokratično ustavno ureditev (Antončič, 2001: 30).

Kadar bi bila osebi zaradi negativnih ugotovitev zavrnjena izdaja dovoljenja, ima le-ta pravico, da se pred zavrnitvijo osebno opredeli do ugotovitev varnostnega preverjanja. Na razgovor lahko pride tudi z zagovornikom. Vendar pa razgovor ne sme ogroziti virov varnostnega preverjanja. »Zoper odločitve organov so dovoljena vsa redna in izredna pravna sredstva, predvidena v pravnem redu Zvezne republike Nemčije« (Trbovšek, 2004: 132).

4.3 VARNOSTNO PREVERJANJE OSEB V SLOVAŠKI REPUBLIKI

Temeljni akt, ki v Slovaški republiki ureja področje varnostnega preverjanja, je Zakon o varovanju tajnih gradiv in spremembah in dopolnitvah določenih zakonov iz leta 2004.² Zakon je zamenjal in dopolnil istoimenski zakon iz leta 2001.

Zakon je predvidel štiri stopnje tajnosti: STROGO TAJNO (prisne tajne), TAJNO (tajne), ZAUPNO (doverne) in INTERNO (vyhradene) (3. člen). Dovoljenje za dostop pa lahko dobi le nekdo, ki izpolnjuje naslednje pogoje:

- a) je državljan Slovaške republike
- b) je opravično sposoben
- c) je dosegel določeno starost
- d) se je strinjal, da bo seznanjen s tajnimi podatki ter da bo varnostno preverjen
- e) ima trdna moralna načela
- f) bo s svojim obnašanjem zagotavljal varovanje tajnih podatkov
- g) je varnostno zanesljiv
- h) ima veljavno dovoljenje za dostop do tajnih podatkov stopnje STROGO TAJNO, TAJNO ali ZAUPNO, ki ga je izdal Nacionalni varnostni urad
- i) potrebuje dostop
- j) je podpisal izjavo o molčečnosti (10. člen).

Zakon je predpisal tudi določeno starostno omejitev za dostop do tajnih podatkov. Tako je za dostop do podatkov STROGO TAJNO potrebno dopolniti 21 let, za dostop do podatkov stopnje TAJNO, ZAUPNO ali INTERNO pa 18. Omejitev 21 let ne velja za pripadnike oboroženih sil, vojaške obveščevalne službe, vojaške varnostne službe in slovaške obveščevalne službe. Omejitev 18 let pa ne velja za gojence vojaških šol (11. člen).

Zakon v 15. členu predvideva štiri vrste varnostnega preverjanja glede na dostop do določene stopnje tajnih podatkov.

- varnostno preverjanje 1. stopnje za dostop do tajnih podatkov stopnje INTERNO
- varnostno preverjanje 2. stopnje za dostop do tajnih podatkov stopnje ZAUPNO

² Uporabljen je angleški prevod zakona z naslovom Act of 11 March 2004 of the Protection of classified information and on the amendment and supplementing of certain acts. Dostopno na http://www.nbusr.sk/index_en.php (17. 3. 2006).

- varnostno preverjanje 3. stopnje za dostop do tajnih podatkov stopnje TAJNO
- varnostno preverjanje 4. stopnje za dostop do tajnih podatkov stopnje STROGO TAJNO.

Dokumenti, ki sestavljajo podlago za varnostno preverjanje 1. stopnje, so: izpolnjen varnostni vprašalnik, življenjepis, izpis iz kazenske evidence ter pisni pristanek, da bo imel dostop do tajnih podatkov ter da bo varnostno preverjen (dokumente mora predložiti kandidat sam).

Dokumenti, ki sestavljajo podlago za varnostno preverjanje 2. stopnje, so: vsi dokumenti, potrebni za 1. stopnjo, ter izpolnjen celoten varnostni vprašalnik, ki ga prav tako priskrbi kandidat, poleg tega pa še podatki o varnostni zanesljivosti iz evidenc policije, slovaške obveščevalne službe in vojaške obveščevalne službe ter podatki o kandidatu, ki so bili zahtevani od drugih državnih služb. Postopek varnostnega preverjanja mora biti zaključen v treh mesecih.

Dokumenti, ki sestavljajo podlago za varnostno preverjanje 3. stopnje, so: vsi poprejšnji dokumenti ter podatki, ki jih je v kraju bivanja kandidata o njem zbrala policija, slovaška obveščevalna služba ali vojaška obveščevalna služba, ter podatki lokalnega organa, kjer kandidat začasno ali stalno biva. Postopek varnostnega preverjanja mora biti zaključen v štirih mesecih.

Za varnostno preverjanje 4. stopnje pa poleg vseh naštetih dokumentov potrebujejo še podatke o varnostnem okolju, v katerem živi in dela kandidat, ter podatke o možnih varnostnih tveganjih. Postopek varnostnega preverjanja mora biti zaključen v šestih mesecih (16., 20., 21., 22., 23. ter 27. člen).

Varnostno preverjanje 1. stopnje izvajajo predstojniki državnih organov, vseh ostalih stopenj pa Nacionalni varnostni urad (17. člen).

28. člen določa veljavnost dovoljenja za dostop do tajnih podatkov. Dovoljenje za dostop do podatkov STROGO TAJNO velja 5 let, za dostop do podatkov stopnje TAJNO 7 let ter za dostop do podatkov stopnje ZAUPNO 10 let.

Če so v postopku varnostnega preverjanja ugotovljeni varnostni zadržki, se kandidatu zavrne izdaja dovoljenja za dostop do tajnih podatkov. Kandidat se lahko v 15 dneh pritoži na Nacionalni varnostni urad. Nacionalni varnostni urad lahko o pritožbi odloča sam, lahko pa jo preda odboru za pritožbe. Po odločitvi odbora se kandidat lahko pritoži še na vrhovno sodišče. Vrhovno sodišče je pristojno tudi v primeru, da je izdajo dovoljenja zavrnila slovaška obveščevalna služba, vojaška obveščevalna služba ali policija.

Podobno kot je slovenski Zakon o tajnih podatkih določil osebe, ki lahko dostopajo do tajnih podatkov brez varnostnega preverjanja, je to storil tudi slovaški zakon. Te osebe so določene v 34. členu in so:

- predsednik Slovaške
- poslanci slovaškega parlamenta
- člani slovaške vlade
- sodniki ustavnega sodišča
- predsednik in podpredsednik vrhovnega slovaškega računskega sodišča
- vsi sodniki, razen sodniki posebnih sodišč, ki se ukvarjajo predvsem s primeri s področja organiziranega kriminala, terorizma, podkupovanja sodnikov in članov parlamenta ipd.; le-ti potrebujejo dovoljenje za dostop do tajnih podatkov stopnje **STROGO TAJNO**.

5 VARNOSTNO PREVERJANJA OSEB V ATLANTSKIH IN EVROPSKIH VARNOSTNIH POVEZAVAH

5.1 VARNOSTNO PREVERJANJE V NATU

NATO varnostnega preverjanja samostojno ne izvaja. Podlaga za pridobitev dostopa do tajnih podatkov zveze Nato je namreč izdano nacionalno dovoljenje. Zato je izredno pomembno, kako imajo to področje urejeno posamezne članice. Jasno pa je, da morajo upoštevati vsaj minimalne standarde, ki jih je zveza določila v svojih dokumentih.

Temeljni akt, ki v Natu ureja varovanje tajnih podatkov, je dokument z naslovom Varnost v okviru organizacije Severnoatlantskega sporazuma C-M(2002)49, ki je sestavljen iz direktiv za vsa področja varovanja tajnih podatkov in je dopolnil ter zamenjal dokument Varnost v okviru organizacije Severnoatlantskega sporazuma C-M(55)15 (FINAL).

V dokumentu C-M(2002)49 je zajeta in določena politika varovanja podatkov, sredstev, naprav in objektov, pomembnih za delovanje in uresničevanje ciljev Nata, ter minimalni varnostni ukrepi in postopki, ki jih pri obravnavanju podatkov, opravljanju nekaterih dejavnosti ali pri uporabi določene infrastrukture, na primer objektov, predmetov in naprav, morajo upoštevati organi in članice Nata (Čaleta, 2004b: 62). Ta dokument »zavezuje države, stranke dokumenta, ter Natove civilne in vojaške organe, da ščitijo in varujejo tajne podatke, ki izvirajo od Nata, so posredovane Natu od držav članic ali pa jih države članice posredujejo drugi državi članici znotraj Natovega programa/projekta ali pogodbe ali jih Nato pridobi iz nenatovskih izvorov, ali pa tajne podatke, ki so zaupani nedržavnim in nenatovskim organizacijam ter posameznikom«(http://www.mors.si/pdf/2004/ravnanje_s_tajnimi_podatki_gradivo.pdf).

Sam dokument C-M(2002)49 je v svojem osrednjem delu pravzaprav kratek. Vse standarde podrobnejše opredeljujejo naslednje direktive:

- direktiva o kadrovske varnosti (AC/35-D/2000 Directive on Personnel Security),
- direktiva o fizični varnosti (AC/35-D/2001 Directive on Physical Security),
- direktiva o varovanju informacij (AC/35-D/2002 Directive on Security of Information),
- direktiva o industrijski varnosti (AC/35-D/2003 Directive on Industrial Security),

- osnovna direktiva o varnosti informacijskih sistemov (skrajšano INFOSEC) (AC/35-D/2004 Primary Directive on INFOSEC),
- direktiva za vodstveno osebje, ki se v komunikacijsko-informacijskih sistemih ukvarja z INFOSEC-om (AC/35-D/2005 INFOSEC Management Directive for CIS) (http://www.mors.si/pdf/2004/ravnanje_s_tajnimi_podatki_gradivo.pdf).

Naslednji pomemben dokument je Varnostna direktiva zavezniškega poveljstva za Evropo, AD 70-1, ki še podrobneje določa postopke in ukrepe ter minimalne standarde varnosti. Ti minimalni standardi, ki so jih sprejele vse članice NATA, so npr.:

- vse države članice morajo zagotavljati dosledno uresničevanje vseh dogovorjenih in sprejetih minimalnih standardov varovanja tajnih podatkov;
- tajni podatki se lahko posredujejo samo tistim osebam, ki izrazijo potrebo po seznanjanju s temi podatki oziroma so zaradi nalog, ki jih opravljajo, upravičene do seznanitve s temi podatki, pred tem pa so se udeležile varnostnega usposabljanja, na katerem so bile seznanjene z osnovnimi varnostnimi zahtevami za varovanje tajnih podatkov;
- samo posamezniki, za katere je bilo opravljeno ustrezno varnostno preverjanje, bodo imeli dostop do tajnih podatkov stopnje zaupno (confidential) ali višje (Čeleta, 2004: 30–31).

Do tajnih podatkov lahko torej dostopajo le osebe z ustreznim dovoljenjem, obenem pa morajo podatek potrebovati zaradi narave svojega dela, torej zaradi t. i. »need to know«.

Varnostno preverjanje za izdajo dovoljenja za dostop do Natovih tajnih podatkov stopnje ZAUPNO (Confidential) ali TAJNO (Secret) mora obsegati obdobje zadnjih petih let oziroma obdobje od 18. leta dalje in mora zajemati izpolnjevanje vprašalnika za varnostno preverjanje, ki je lahko ali vprašalnik Nata ali nacionalni, ugotavljanje istovetnosti (preveri se državljanstvo in/ali narodnost osebe, datum in kraj rojstva) ter preverjanje v državnih in lokalnih evidencah. Za pridobitev dovoljenja za dostop do tajnih podatkov stopnje STROGO TAJNO (Cosmic Top Secret) pa mora to obdobje obsegati deset let in mora zajemati poleg preverjanja podatkov iz prejšnje stopnje še preverjanje finančnega položaja, izobrazbe, zaposlitve (sedanje in pretekle) ter vojaškega roka. Kjer to dopušča nacionalna zakonodaja, se izvajajo tudi razgovori z osebo samo ter z drugimi osebami, ki lahko podajo neodvisno oceno o posamezniku. Ponovno varnostno preverjanje za obnovitev dovoljenja za dostop do tajnih podatkov se mora za stopnjo STROGO TAJNO izvajati na pet let, za stopnjo ZAUPNO ali TAJNO pa na deset let (Anžič, Trbovšek, 2003: 6–7).

Posameznik, ki bo imel dostop do tajnih podatkov stopnje INTERNO (Restricted), mora biti seznanjen z vsemi varnostnimi zahtevami in postopki varovanja teh podatkov, vendar mu ni potrebno opraviti varnostnega preverjanja.

Poznamo pa še dve izjemi dostopanja do tajnih podatkov. »V primeru, da je posameznik imenovan na pozicijo, ki zahteva višji nivo dovoljenja kot ga poseduje, se lahko tako imenovanje opravi začasno. Začasen dostop velja največ 6 mesecev« (Črnčec, 2004: 56).

Druga izjema pa je odobren enkratni dostop v nujnih primerih, če obstaja potreba po vedenju v okviru konkretne naloge in jo upraviči posameznikov nadrejeni. Posameznik mora imeti dovoljenje, ki je le eno stopnjo nižje, poleg tega pa je potrebna presoja, ali je posameznik resno in večkrat kršil varnostne predpise, ter posvet z ustreznim varnostnim organom (Črnčec, 2004: 56).

Omeniti pa je potrebno tudi Urad zveze Nato za varnost, ki usklajuje, spremlja in uresničuje Natovo varnostno politiko, obenem pa tudi koordinira delo z nacionalnimi Uradi za varovanje podatkov. Pri nas je to Urad vlade Republike Slovenije za varovanje tajnih podatkov, ki je pravzaprav nekakšen vezni člen med Republiko Slovenijo in Natom na področju varnostnih zadev.

5.2 VARNOSTNO PREVERJANJE V EU

Evropska unija področju varnosti ni namenjala tolikšne pozornosti kot Nato. To je razvidno tudi iz obstoječih predpisov, ki so v Natu veliko natančnejši pa tudi več jih je.

V EU zakonsko podlago in obenem ključni akt predstavljajo Varnostna pravila Sveta EU (Security regulations 2001/264/EC, Council Decision 19. MAR 200). Predpisi za varovanje tajnih podatkov veljajo za vse institucije EU, države članice ter druge posameznike, ki pri svojem delu prihajajo v stik s tajnimi podatki EU. Države članice pa morajo sprejeti ustrezne ukrepe znotraj države in s tem zagotoviti upoštevanje vsaj minimalnih varnostnih standardov EU (Črnčec, 2004: 54).

»Pravila urejajo naslednja področja: določena so osnovna načela in minimalni varnostni standardi; organiziranost varnostnega področja v Svetu EU; klasifikacija in označevanje tajnih podatkov; fizično in tehnično varovanje; spoštovanje načela potrebe po vedenju; postopki pridobitve varnostnega certifikata; izdelava, prenos, varovanje in uničenje tajnih podatkov; registri EU; varovanje informacijskih sistemov in posredovanje tajnih podatkov nečlanicam EU in mednarodnim organizacijam« (Črnčec, 2004: 54).

Vse osebe, ki potrebujejo dostop do tajnih podatkov stopnje ZAUPNO ali višje, morajo biti ustrezno varnostno preverjene. Podobna varnostna preverjenost se zahteva tudi za osebe, katerih delovne naloge so povezane s tehničnim delovanjem ali vzdrževanjem komunikacijskih in informacijskih sistemov, ki vsebujejo tajne podatke. Namen varnostnega preverjanja pa je ugotoviti, ali preverjene osebe izražajo popolno lojalnost, imajo take osebnostne kvalitete, ki ne dopuščajo dvomov o njihovi integriteti pri delu s tajnimi podatki, in so popolnoma diskretne, ne podlegajo pritisku zunanjih ali drugih virov, na primer sorodstvenim ali prijateljskim zvezam, okolju, iz katerega izhajajo, in drugim vplivom, ki bi lahko pomenili varnostno tveganje. Še natančneje pa je potrebno preveriti osebe, ki bodo dostopale do podatkov STROGO TAJNO, ki bodo redno dostopale do velikega števila podatkov stopnje TAJNO, in tudi tiste, ki imajo zaradi svojih delovnih nalog poseben dostop do pomembnih komunikacijskih ali informacijskih sistemov in s tem možnost nedovoljenega dostopa do velikih količin tajnih podatkov (Čaleta, 2005: 47).

»Pri zaposlitvi oseb, za katere ne velja načelo potrebe po seznanitvi s podatki zaradi opravljanja funkcije ali delovnih nalog, v katerih bi lahko dobile dostop do tajnih podatkov Evropske unije (na primer sli, varnostni agenti, vzdrževalno in čistilno osebje), je treba te osebe najprej ustrezno varnostno preveriti« (Čaleta, 2005: 47).

Vse osebe, ki potrebujejo dostop do podatkov stopnje STROGO TAJNO (TRES SECRET EU/EU TOP SECRET), morajo najprej opraviti ustrezno varnostno preverjanje za pridobitev dostopa do teh podatkov, izpolniti morajo osebni vprašalnik ter podpisati potrdilo, s katerim potrjujejo, da so bile seznanjene z varnostnimi postopki Sveta in da popolnoma razumejo pomen svoje posebne odgovornosti za varovanje strogo tajnih podatkov ter posledice, ki lahko nastopijo ob neprimernem ravnanju. Osebe, ki potrebujejo dostop do podatkov stopnje TAJNO (SECRET EU) ali ZAUPNO (CONFIDENTIEL EU), morajo prav tako najprej opraviti ustrezno varnostno preverjanje in izpolniti vprašalnik z osebnimi podatki. Seznaniti

pa se morajo tudi z ustreznimi predpisi o varovanju tajnosti in se zavedati posledic, ki jih lahko sprožijo s svojim nepravilnim ravnanjem. Osebam, ki potrebujejo dostop do podatkov stopnje INTERNO (RESTRIENT EU), pa ni potrebno opraviti varnostnega preverjanja, temveč se jih le opozori na pomembnost predpisov o varovanju tajnosti in na posledice malomarnega odnosa do njih (Čaleta, 2005: 48–49).

Možen je tudi začasen dostop do tajnih podatkov brez varnostnega preverjanja, vendar največ za 6 mesecev in največ za dostop do stopnje TAJNO. Predlagatelj mora predhodno obvestiti nacionalni organ, in če v enem mesecu ne prejme odgovora, se tako dovoljenje lahko izda (Črnčec, 2004: 55).

Varnostno preverjanje je potrebno izvesti s sodelovanjem posameznika. Celoten proces varnostnega preverjanja pa se opravi v skladu s pravili in predpisi, ki veljajo v državi članici, katere državljan je preverjana oseba.

6 VAROVANJE TAJNIH PODATKOV REPUBLIKI SLOVENIJI

6.1 SPLOŠNO O TAJNIH PODATKIH

Pojem *tajen* Slovar slovenskega knjižnega jezika (CD-rom) opredeli kot nekaj, kar »javnost, oblast ne ve: imeti tajen sestanek; dogodki so ostali tajni; tajna organizacija; tajna radijska postaja; tajno društvo«. V drugem pomenu pa ga opredeli kot »s katerim se javnost, ljudje ne morejo seznaniti: tajno srečanje državnikov, skleniti tajni sporazum; tajna meddržavna pogodba; tajno sojenje, tajno glasovanje za katerega ve ozek krog ljudi«, obenem pa zopet poudari tudi knjižno sopomenko *skrivnost*. Tajnost pa opiše kot »značilnost tajnega« (jamčiti tajnost glasovanja, zavarovati tajnost dopisovanja, podatki morajo ostati v tajnosti) ali kot nekaj, »kar je tajno« (ti podatki so tajnost, državna, poslovna, službena, vojaška tajnost oziroma skrivnost).

V pogovornem jeziku *tajnost* pogosto uporabljamo kot sopomenko *skrivnosti*, vendar pa besedi, vsaj v strokovnem jeziku, ne bi mogli tako zlahka enačiti. »Skrivnost je (namreč) v njenem pravem pomenu nekaj, kar se ne da razumeti, dojeti ali pojasniti. Tajnost pa ni nekaj neznanega, temveč ravno obratno. Pri njeni vsebini gre za znane stvari, ki jo njen posestnik (ali posameznik ali institucija ali država) ne sme ali noče narediti dostopne širši javnosti« (Anžič, 2000: 852).

ZTP tajne podatke definira kot »dejstvo ali sredstvo z delovnega področja organa, ki se nanaša na javno varnost, obrambo, zunanje zadeve ali obveščevalno in varnostno dejavnost države, ki ga je treba zaradi razlogov, določenih v tem zakonu, zavarovati pred nepoklicanimi osebami in ki je v skladu s tem zakonom določeno in označeno za tajno« (1. točka 2. člena ZTP). V 6. členu pa določa tudi, da podatek, ki mu je bila tajnost določena zato, da bi se prikrilo storjeno kaznivo dejanje, prekršček ali zloraba pooblastil, ali prikrilo kakšno drugo nezakonito dejanje ali ravnanje, ni tajen.

Tajni podatek tuje države pa je podatek, »ki ga je Republiki Sloveniji oziroma njenim organom posredovala tuja država oziroma njen organ ali mednarodna organizacija oziroma njen organ v pričakovanju, da bo ostal tajen, ter podatek, ki je rezultat sodelovanja Republike

Slovenije oziroma njenih organov s tujo državo ali mednarodno organizacijo oziroma njihovimi organi, in za katerega se dogovori, da mora ostati tajen« (2. točka 2. člena ZTP).

Določanje tajnih podatkov »je dejanje ali postopek, s katerim se podatek v skladu s tem zakonom oceni za tajnega in se mu določi stopnja in rok tajnosti« (5. točka 2. člena). Podatek določi za tajnega pooblaščen oseb, ki je določena z zakonom. »Pooblaščen osebe so:

1. predstojnik organa
2. izvoljeni ali imenovani funkcionarji organa, ki so za določanje in posredovanje tajnih podatkov pooblaščen z zakonom oziroma s predpisom, izdanim na podlagi zakona, ali jih je za to pisno pooblastil predstojnik in
3. osebe, zaposlene v organu, ki jih je za to pisno pooblastil predstojnik tega organa« (10. člen ZTP).

Stopnjo STROGO TAJNO pa lahko dokumentom določijo le predsednik republike, predsednik državnega zbora, predsednik vlade, ministri in predstojniki organov v sestavi ministrstev, določeni vojaški poveljniki, predstojniki vladnih služb, ki so neposredno odgovorni predsedniku vlade, oziroma osebe, ki jih nadomeščajo (10. člen ZTP). Tajnost podatka preneha na določen datum, z nastopom določenega dogodka, s potekom določenega časa ali s preklicem tajnosti (18. člen ZTP).

ZTP v 13. členu določi štiri stopnje tajnosti. Oznako STROGO TAJNO se določi za tajne podatke, katerih razkritje nepoklicani osebi bi ogrozilo vitalne interese Republike Slovenije ali jim nepopravljivo škodovalo; oznako TAJNO dobijo tisti tajni podatki, katerih razkritje nepoklicani osebi bi lahko hudo škodovalo varnosti ali interesom Republike Slovenije; oznako ZAUPNO se določi za tajne podatke, katerih razkritje nepoklicani osebi bi lahko škodovalo varnosti ali interesom Republike Slovenije; oznako INTERNO pa tistim tajnim podatkom, katerih razkritje nepoklicani osebi bi lahko škodovalo delovanju ali izvajanju nalog organa.

Vendar je za seznanitev »poleg dovoljenja za dostop do tajnega podatka treba imeti tudi upravičeno potrebo po poznavanju tega podatka« (Čaleta, 2003: 12). Pri slednji pooblaščen posestnik tajnega podatka ugotavlja, če bodoči prejemnik potrebuje informacijo zaradi narave svojega dela ali naloge (Trbovšek, 2004: 22). Tudi 31. člen ZTP govori o tem, da imajo pravico dostopa do tajnih podatkov samo tiste osebe, ki imajo dovoljenje in se morajo s temi

podatki seznaniti zaradi opravljanja funkcije ali delovnih nalog. Dostop imajo samo do tajnih podatkov stopnje tajnosti, določene v dovoljenju. Nihče ne sme dobiti tajnega podatka prej in v večjem obsegu, kot je to potrebno za opravljanje njegovih delovnih nalog ali funkcije.

6.2 NORMATIVNA UREDITEV VAROVANJA TAJNIH PODATKOV

Prvi zakon, ki je urejal področje varnostnega preverjanja, je bil Zakon o tajnih podatkih, ki je bil sprejet leta 2001. Sprejet je bil razmeroma pozno, vendar je bil zelo pomemben, saj je enotno uredil sistem varovanja in dostopa do tajnih podatkov z delovnega področja državnih organov, ki se nanašajo na javno varnost, obrambo, zunanje zadeve ali obveščevalno in varnostno dejavnost države. Izraze, kot so državna ali vojaška skrivnost in strogo zaupno, so zamenjale oznake - strogo tajno, tajno, zaupno in interno, kar je primerljivo z ureditvami drugih držav in tudi mednarodnih organizacij, kot sta NATO in EU. Pred sprejetjem zakona je bilo to področje le deloma urejeno v številnih predpisih, ki so bili med seboj neuskklajeni ter pomanjkljivi.

Sledila mu je pritožba na ustavno sodišče. Rezultat vsega pa je bil Zakon o spremembah in dopolnitvah zakona o tajnih podatkih leta 2003. Njegova bistvena sprememba je bila, da je uvedel tri vrste preverjanja – osnovno, dodatno in varnostno preverjanje s poizvedovanjem – ki se ga izvede glede na stopnjo zaupnosti podatkov, do katerih bo imela oseba dostop (<http://nato.gov.si/slo/novinarsko-sredisce/sporocila-za-javnost/2264/>).

Zakonu so sledili še številni podzakonski akti. Najpomembnejši med njimi je Uredba o načinu in postopku varnostnega preverjanja, ki ga je Vlada Republike Slovenije sprejela leta 2003. Sprejetje tega akta je nalagal že Zakon o tajnih podatkih iz leta 2001 v sedmem odstavku 23. člena.

Posebej je potrebno osvetliti dogodke v zvezi s postopkom pred ustavnim sodiščem, ki je bil sprožen zaradi »preverjanja ustavnosti določil zakona o tajnih podatkih, predvsem njegovih določil varnostnega preverjanja« (Čaleta: 2003: 11). »Zaradi mnenja članov sindikata državnih in družbenih organov, da vsebina zakona in vprašalnika ni skladna z ustavo, so podali Ustavnemu sodišču RS pobudo za oceno ustavnosti in zakonitosti 25. člena Zakona o tajnih podatkih in 5. člena Uredbe o načinu in postopku varnostnega preverjanja ter postopku

preklica dovoljenja za dostop do tajnih podatkov« (Trbovšek, 2004: 83). Ustavno sodišče Republike Slovenije je na seji 8. maja 2003 sklenilo, da sprejme pobudo za začetek postopka ocene ustavnosti ter zadrži nadaljnje izvajanje določb. Pobudnik je v svoji pobudi zapisal, da morajo zaposleni v vprašalniku za pridobitev dovoljenja posredovati tudi podatke, ki nimajo nobene povezave s tajnimi podatki, ter da uredba še bistveno razširja obseg podatkov, ki se preverjajo. Ustavno sodišče je tudi ugotovilo, da bi z nadaljnjim izvrševanjem izpodbijanih predpisov lahko nastale težko popravljive posledice, obenem pa menilo, da zadržanje ne bi moglo povzročiti nobene škode, saj 47. člen Zakona o tajnih podatkih tako ali tako pušča dveletni rok, v času katerega posamezniki lahko dostopajo do tajnih podatkov tudi brez dovoljenja.

Vendar pa je pri tem Ustavno sodišče RS pozabilo na mednarodne pogodbe, ki jih je Republika Slovenija podpisala npr. z Natom, EU in ZDA. V vseh pogodbah se je Slovenija namreč zavezala, da bo varnostno preverila državljane, ki bodo imeli dostop do tajnih podatkov zgoraj navedenih organizacij oziroma članic organizacij. Zaradi zadržanja izvajanja izpodbijanih določb se je odložil predvideni odhod vojakov Slovenske vojske na misijo v Afganistan. Pripadniki, ki se udeležijo misije Nato, morajo namreč imeti dovoljenje za dostop do Natovih tajnih podatkov. Le-to lahko pridobijo na podlagi opravljenega varnostnega preverjanja v domači državi, tega pa takrat v Sloveniji niso mogli dobiti (Trbovšek, 2004: 88).

Sicer je pobudnik navajal kršitev 14., 38., in 49. člena Ustave RS, ni pa navajal kršitve 35. člena Ustave RS (varstvo pravic zasebnosti in osebnostnih pravic).

Ustava Republike Slovenije v II. Poglavju opredeljuje človekove pravice in temeljne svoboščine. V luči te diplomske naloge so pomembne predvsem: enakost pred zakonom (14. člen), pravica do zasebnosti (35. člen) ter varstvo osebnih podatkov (38. člen). »Omejitve in posegi (v človekove pravice in temeljne svoboščine) so pod določenimi pogoji ustavno dopustni. Ustavno nedopustni posegi v človekove pravice (pa) so kršitve človekovih pravic« (Šturm, 2002: 198 v Trbovšek, 2004: 74). Pri posegih je torej najpomembnejša sorazmernost posegov s ciljem, ki ga želimo doseči.

Glede domnevne kršitve pravice varstva osebnih podatkov (38. člen) lahko rečemo, da je bila pravzaprav neutemeljena ter da je zakon ni kršil. V zakonu je namreč natančno opredeljeno,

kateri podatki se smejo zbirati in obdelovati, namen uporabe, nadzor nad zbiranjem, obdelovanjem in uporabo ter varstvo tajnosti osebnih podatkov.

»Zakonodajalec sme ustavno varovane pravice posameznika omejiti le s pravicami drugih subjektov in v tem okviru tudi v javnem interesu. Poseg v temeljno svoboščino mora utemeljiti s stvarnim in razumnim tehtanjem ustavno varovanih dobrin in svoje zakonodajne oblasti ne sme zlorabiti za doseg namenov, ki niso stvarno upravičeni. Cilji zakonodajalca morajo biti opredeljivi, razumni in ustavno legitimni« (Trbovšek, 2004: 75).

Pravica do zasebnosti je ustavno zagotovljena pravica. Vendar država ravno na področju tajnih podatkov in varnostnega preverjanja posega vanjo. Kot že omenjeno, so ti posegi pravno dopustni, če le prestanejo test sorazmernosti. Poseg je dopusten, če je v zakonu natančno opredeljeno, kateri podatki se smejo zbirati in obdelovati, namen uporabe, nadzor nad zbiranjem, obdelovanjem in uporabo ter varstvo tajnosti osebnih podatkov. Nemogoče bi bilo pričakovati, da bi se država v celoti odpovedala poseganju v zasebnost svojih državljanov, država namreč s tem varuje ne le sebe, temveč tudi svoje državljanke. »Velja, da je država pooblaščenca, da zavaruje svoj obstoj in da nobena pravica ne more biti tako široka, da bi lahko njen obstoj ogrozila, kajti konec koncev je država glavni porok in okvir vseh pravic« (Trbovšek, 2004: 81).

Vlada RS je dne 17. 3. 2006 sprejela nov Zakon o spremembah in dopolnitvah zakona o tajnih podatkih (ZTP-B) (Uradni list RS, št. 28/06), ki prinaša kar nekaj novosti. Posebej izpostavljam predvsem tiste, ki zadevajo varnostno preverjanje:

- Dostop do tajnih podatkov v zvezi z opravljanjem svoje funkcije ima tudi vsak državni tožilec in ne le generalni državni tožilec ter informacijski pooblaščenec.
- Med osebe, ki lahko določijo stopnjo tajnosti STROGO TAJNO, so vključeni tudi določeni vodje diplomatsko-konzularnih predstavništev, ki jih določi minister, pristojen za zunanje zadeve. Po prejšnjih določilih bi lahko tako stopnjo tajnosti določil le minister, kar pa naj bi oteževalo delo diplomatsko-konzularnih predstavništev zaradi teritorialne oddaljenosti od sedeža matičnega ministrstva.
- V primeru nujnih nalog je mogoče stopnjo tajnosti določiti tudi ustno in ne le pisno. Oseba, ki določi stopnjo tajnosti, izdelava pisno oceno najkasneje v treh dneh.
- ZTP iz leta 2003 je narekoval da lahko tajnemu podatku stopnjo tajnosti spremeni le pooblaščenca oseba, ki mu je določila stopnjo tajnosti. Po novem zakonu pa to lahko

stori tudi druga pooblaščen oseba organa, v katerem je bila stopnja določena. Tako se bomo izognili morebitnim nejasnostim, če bo oseba, ki je prvotno določila stopnjo tajnosti podatku, premeščena ali morda sploh ne bo več delala v organu.

- Nov zakon nalaga pooblaščenim osebam, da mora tajne podatke stopnje tajnosti STROGO TAJNO pregledati enkrat letno, ostale stopnje tajnosti pa vsaka tri leta, in oceniti, ali še obstaja potreba po njihovi tajnosti.
- Zakon uvaja test javnega interesa oziroma škodni test. Gre za presojanje o upravičenosti prevladujočega javnega interesa za razkritje tajnega podatka.
- Zakon nalaga organom, da pri osnovnem in razširjenem varnostnem preverjanju v primeru obstoja suma varnostnega zadržka vselej dodatno preverijo relevantne podatke in okoliščine, ki se nanašajo na posamezni varnostni zadržek, zakon iz leta 2003 pa je to le dopuščal.
- Določa predlagatelje postopka za izdajo dovoljenja. Pomembno je, da kot predlagatelja določi tudi Ministrstvo za gospodarstvo, in sicer za osebe iz organizacije, ki potrebujejo dostop do tajnih podatkov, ker bo organizacija kandidirala na razpisu za pridobitev naročila, ali zaradi izvedbe naročila tuje države ali mednarodne organizacije.
- Zakon navaja nov pogoj za začetek varnostnega preverjanja osebe, tj. njeno obvezno usposabljanje s področja obravnavanja in varovanja tajnih podatkov, kar je eden bistvenih pogojev za zagotavljanje večje varnosti tajnih podatkov.
- V vsebino varnostnega preverjanja se vključujejo tudi neizbrisane pravnomočne obsodbe za vsa kazniva dejanja, ki se preganjajo po uradni dolžnosti, in ne le naklepno storjena. S tem se organu, pristojnemu za varnostno preverjanje, omogoča, da preveri morebitno kaznovanost preverjane osebe za prekrške, ki bi lahko vzbujali utemeljen dvom v njegovo verodostojnost, zanesljivost ali lojalnost za varno obravnavanje tajnih podatkov (npr.: prekrški, storjeni pod vplivom alkohola, zloraba drog ipd.).
- Preverjana oseba mora v posebnem vprašalniku navesti tako odhodke kot tudi prihodke, kajti le oba podatka lahko prikažeta realno sliko.
- Novi zakon pristojnega predlagatelja zavezuje, da sproži postopek vmesnega varnostnega preverjanja vselej, ko je pri osebi, ki ima dovoljenje za dostop do tajnih podatkov, podan sum obstoja varnostnega zadržka iz 27. člena zakona.
- Po dosedanji zakonski ureditvi se je predlog za ponovno varnostno preverjanje lahko posredoval tudi neposredno pred iztekom veljavnosti dovoljenja. Vendar pa za odgovorno obravnavanje tajnih podatkov to ni dopustno, saj v kratkem roku

varnostnega preverjanja ni mogoče izvesti, oseba pa brez izdanega dovoljenja ne sme dostopati do tajnih podatkov. Predlagatelj je nova zakonska določba zavezuje, da pravočasno sprožijo postopke ponovnega varnostnega preverjanja, tako da lahko organi, ki izvajajo te postopke, delo opravijo pravočasno in kakovostno, kar pa je najmanj tri mesece pred iztekom dovoljenja (http://www.uvtp.gov.si/fileadmin/uvtp.gov.si/pageuploads/Besedilo___lenov_ZTP_10.11.05.doc in http://www.uvtp.gov.si/fileadmin/uvtp.gov.si/pageuploads/Obrazlo___itev.doc).

Normativno podlago varnostnemu preverjanju torej predstavlja Zakon o spremembah in dopolnitvah zakona o tajnih podatkih (ZTP-B) (Uradni list RS, št. 28/06), ki je osnovna podlaga, poleg njega pa je pomembna še Uredba o načinu in postopku varnostnega preverjanja (Uradni list RS, št. 110/2003).

Posredno so pomembni tudi naslednji akti:

- Sklep o ustanovitvi, nalogah in organizaciji Urada Vlade Republike Slovenije za varovanje tajnih podatkov (Uradni list RS, št. 6/02),
- Uredba o načinih in oblikah označevanja tajnih podatkov ter fizičnih, organizacijskih in tehničnih ukrepih ter postopkih za varovanje tajnih podatkov (Uradni list RS, št. 70/02),
- Uredba o notranjem nadzoru nad izvajanjem zakona o tajnih podatkih in predpisov, izdanih na njegovi podlagi (Uradni list RS, št. 106/02),
- Uredba o ugotavljanju izpolnjevanja pogojev za posredovanje tajnih podatkov drugi organizaciji (Uradni list RS, št. 106/02),
- Pravilnik o načinu in postopku določanja tajnih podatkov s področja obrambe v gospodarskih družbah, zavodih in organizacijah (Uradni list RS, št. 108/02).

7 VARNOSTNO PREVERJANJE OSEB V REPUBLIKI SLOVENIJI

Varnostno preverjanje oseb je eden izmed ukrepov za zagotavljanje tajnosti (Anžič, Trbovšek, 2004: 37). Poznamo dva tipa varnostnega preverjanja. Prvo je varnostno preverjanje kot del kadrovskega postopka za zaposlitev v državni upravi (npr. v policiji ali vojski), drugo pa je varnostno preverjanje kot preventivni varnostni ukrep, katerega namen je zagotoviti ustrezno stopnjo varnosti in tajnosti podatkov (Črnčec, 2003: 57). Prvega bom predstavila okvirno, bolj pa se bom posvetila drugi obliki, torej varnostnemu preverjanju oseb kot najpomembnejšemu elementu zaščite tajnih podatkov.

7.1 POGOJI ZA ZAPOSILITEV V DRŽAVNIH ORGANIH

Pogoje za zaposlitev javnih uslužbencev v državnih organih in upravah lokalnih skupnosti določa Zakon o javnih uslužbencih (Uradni list RS, 32/06). Pogoje za uradniško delovno mesto opredeljuje v 86. in 88. členu in so: predpisana izobrazba, strokovni izpit, znanje uradnega jezika, državljanstvo Republike Slovenije, da oseba ni bila pravnomočno obsojena zaradi naklepnega kaznivega dejanja, ki se preganja po uradni dolžnosti, in da ni bila obsojena na nepogojno kazen zopora v trajanju več kot šest mesecev ter da zoper osebo ni vložena pravnomočna obtožnica zaradi naklepnega kaznivega dejanja, ki se preganja po uradni dolžnosti.

Eden izmed pogojev za zaposlitev v državnih organih pa je lahko tudi uspešno opravljeno varnostno preverjanje. Varnostno se preveri kandidate za zaposlitev v policiji, Slovenski obveščevalno varnostni agenciji ter kandidate za delo na obrambnem področju.

Varnostno preverjanje na obrambnem področju ureja Zakon o obrambi, ki v 35. členu (Uradni list RS 47/2002) govori o varnostnem preverjanju oseb kot posebni obliki zbiranja osebnih in drugih podatkov, ki se izvajajo zaradi preprečevanja, odkrivanja in preiskovanja:

1. ogrožanja oseb, delovnih mest in dolžnosti, za katere se v skladu s tem zakonom lahko sklene delovno razmerje brez predhodne javne objave ali na katerih se opravljajo upravne in strokovne zadeve na področju obrambe;

2. ogrožanja oseb, del in dolžnosti v vojaških poveljstvih, enotah in ministrstvu, ki so določena kot posebnega pomena za obrambo;
3. ogrožanja vojaških poveljstev, enot in zavodov ter objektov in okolišev, ki so posebnega pomena za obrambo.

Varnostno preverjanje se opravi tudi zaradi preprečevanja ogrožanja opravljanja vojaške službe na dolžnostih podčastnikov in častnikov ter za opravljanje vojaških dolžnosti v diverzantskih in gardnih enotah ter enotah vojaške policije. Varnostno preverjanje se opravi tudi za vojaške obveznike, ki se bodo usposobili ali razporedili na navedene dolžnosti, ter osebe, ki želijo poklicno opravljati vojaško službo (2. odstavek 35. člena ZObr).

Varnostno preverjanje zaradi preprečevanja, odkrivanja in preiskovanja ogrožanja vojaških poveljstev, enot in zavodov ter objektov in okolišev, ki so posebnega pomena za obrambo, in ogrožanja opravljanja vojaške službe obsega poleg preverbe osebnih podatkov tudi preverbo podatkov o ožjih družinskih članih, prejšnjih delodajalcih in predkaznovanosti, vendar seveda s privolitvijo preverjanega. Varnostno preverjanje zaradi preprečevanja, odkrivanja in preiskovanja ogrožanja oseb, delovnih mest in dolžnosti, za katere se lahko sklene delovno razmerje brez predhodne javne objave, ter ogrožanja oseb, del in dolžnosti v vojaških poveljstvih, enotah in ministrstvu, ki so posebnega pomena za obrambo in varnostno preverjanje za pridobitev dovoljenja za dostop do tajnih podatkov, obsega preverbo podatkov, določenih s predpisi za pridobitev dovoljenja za dostop do tajnih podatkov. Varnostno preverjanje opravljajo delavci Obveščevalno varnostne službe Ministrstva za obrambo, ki imajo policijska pooblastila. Oseba, za katero se z varnostnim preverjanjem ugotovi obstoj varnostnega zadržka, ne more začeti delati oziroma nadaljevati z delom na določenem delovnem mestu oziroma dolžnosti. Za osebo, ki ne privoli v varnostno preverjanje, se šteje, da ne izpolnjuje varnostnih pogojev za opravljanje del ali dolžnosti, ki jih opravlja oziroma želi opravljati. Zakon govori tudi o dolžnosti posredovanja osebnih podatkov upravljavcev zbirk osebnih podatkov. Če pa teh podatkov ni, jih pooblaščen delavci Obveščevalno varnostne službe Ministrstva za obrambo zberejo neposredno (Trbovšek, 2004: 36–37 in 35. člen ZObr).

Varnostno preverjanje v policiji ureja Zakon o policiji (Uradni list RS 3/2006), ki v 67. členu opredeljuje pogoje za delovno razmerje za opravljanje nalog v policiji. Med drugimi je naštet tudi pogoj, da je bila oseba varnostno preverjena in da zanjo ne obstaja varnostni zadržek.

Nadalje zakon določa, da lahko policija zbere o osebi, s katero želi skleniti delovno razmerje za opravljanje nalog v policiji, z njeno pisno privolitvijo, še podatke, na podlagi katerih se ugotavlja varnostne zadržke za opravljanje nalog v policiji. Varnostno preverjanje obsega preveritev podatkov, določenih s predpisi za pridobitev dovoljenja za dostop do tajnih podatkov, za kandidate za policiste tudi po predpisih, ki določajo pogoje za pridobitev orožne listine. Policija preveri tudi ostale podatke, ki jih kandidat za sklenitev delovnega razmerja posreduje policiji v postopku sklenitve delovnega razmerja. Oseba, za katero se z varnostnim preverjanjem ugotovi obstoj varnostnega zadržka, ne more skleniti delovnega razmerja za opravljanje nalog v policiji. Za osebo, ki ne privoli v varnostno preverjanje, se šteje, da ne izpolnjuje varnostnih pogojev za opravljanje del in nalog v policiji.

Slovenska obveščevalno varnostna agencija izvaja varnostno preverjanje pred zaposlitvijo na podlagi Zakona o Slovenski obveščevalno varnostni agenciji (Uradni list RS, št. 23/1999, 20/2004), ki v 27. členu opredeljuje pogoje za sklenitev delovnega razmerja za opravljanje nalog v agenciji. Kandidat mora poleg pogojev, določenih v predpisih, ki urejajo sklenitev delovnega razmerja javnih uslužbencev, izpolnjevati še naslednje pogoje:

1. da je v skladu z določbami akta o sistemizaciji delovnih mest ustrezno psihično in telesno pripravljen;
2. da ni bil pravnomočno obsojen zaradi naklepne kaznivega dejanja, za katero se storilec preganja po uradni dolžnosti, ali ni bil pravnomočno obsojen na nepogojno kazen zapora v trajanju več kot tri mesece;
3. da je izključno državljan Republike Slovenije s stalnim prebivališčem v RS;
4. da je bil varnostno preverjen in njegova zaposlitev ne pomeni varnostnega tveganja za agencijo.

Varnostno tveganje pomeni, da dejansko ugotovljene okoliščine iz varnostnega preverjanja kažejo na: utemeljene dvome o zanesljivosti posameznika za izvajanje nalog v agenciji, posebno ogroženost agencije zaradi poskusov navezovanja stikov in poskusov rekrutiranja tujih obveščevalnih služb, zlasti na podlagi izsiljevanja, utemeljene dvome o opredelitvi posameznika za svobodno in demokratično ustavno ureditev ali o tem, da se je v vsakem času pripravljen zavzemati za njeno ohranitev (27. a člen).

Nadalje zakon pravi, da agencija lahko od kandidata, ki želi skleniti delovno razmerje v agenciji, zahteva tudi podatke, na podlagi katerih ugotavlja varnostne zadržke za delo v agenciji in le-te tudi preveri. Če zoper kandidata teče kazenski postopek zaradi kaznivega

dejanja, se odločitev, ali oseba izpolnjuje pogoje, odloži do pravnomočnosti sodbe v tem postopku. Varnostno preverjanje obsega preveritev podatkov, določenih s predpisi za pridobitev dovoljenja za dostop do tajnih podatkov, ter podatkov, določenih s tem zakonom. Preverja se tudi odvisnost od alkohola in narkotičnih sredstev, in sicer v zdravstveni organizaciji, ki jo določi agencija. Za osebo, ki ne privoli v varnostno preverjanje, se šteje, da ne izpolnjuje varnostnih pogojev za sklenitev delovnega razmerja v agenciji.

27. a člen pa opredeljuje tudi, kaj je varnostno tveganje. Le-to pomeni, da dejansko ugotovljene okoliščine iz varnostnega preverjanja kažejo na:

- utemeljene dvome o zanesljivosti posameznika za izvajanje nalog v agenciji,
- posebno ogroženost agencije zaradi poskusov navezovanja stikov in poskusov rekrutiranja tujih obveščevalnih služb, zlasti na podlagi izsiljevanja,
- utemeljene dvome o opredelitvi posameznika za svobodno in demokratično ustavno ureditev ali o tem, da se je v vsakem času pripravljen zavzemati za njeno ohranitev.

Vsebine, ki se nanašajo na preverjanje poštenosti zaposlenih, so zajete tudi v Kodeksu ravnanja javnih uslužbencev, ki ga je sprejel Svet Evrope kot priporočilo vsem državam članicam Sveta Evrope. Kodeks ravnanja je Vlada Republike Slovenije sprejela januarja 2001 in ga skupaj s svojimi sklepi tudi objavila v Uradnem listu. S 3. sklepom je vlada naložila ministrstvu in vladnim službam, da ga upoštevajo v postopkih zaposlovanja in pri pripravi zakonskih in podzakonskih aktov s področja organizacije in delovnopravne zakonodaje. Kodeks tako določa, da mora javni uslužbenec ustrezno ukrepati, da zavaruje varstvo in zaupnost informacij, za katere je odgovoren ali za katere izve nepooblaščen (22. člen). 24. člen Kodeksa pa določa, da mora javni uslužbenec, ki je pristojen za kadrovanje, napredovanje in razporeditve javnih uslužbencev, zagotoviti, da se opravijo primerna preverjanja poštenosti kandidata ali zaposlenega, če tako določa zakon (Trbovšek, 2004: 12–13 in Kodeks ravnanja javnih uslužbencev, Uradni list RS, št. 8/2001).

7.2 VARNOSTNO PREVERJANJE ZA PRIDOBITEV DOVOLJENJA ZA DOSTOP DO TAJNIH PODATKOV

Varnostno preverjanje je najpomembnejša sestavina varovanja tajnih podatkov. Človek je namreč v tem sistemu še vedno najšibkejši element, zato lahko s kvalitetnim varnostnim preverjanjem preprečimo veliko nepravilnosti ali celo zlorab tajnih podatkov.

Republika Slovenija je leta 2001 to področje prvič celostno uredila z Zakonom o tajnih podatkih. Nasledil ga je zakon iz leta 2003, ki je uvedel številne spremembe. 13. marca 2006 pa je Državni zbor sprejel Zakon o spremembah in dopolnitvah zakona o tajnih podatkih.

Varnostno preverjanje opravljajo z zakonom določeni organi, in sicer:

- Ministrstvo za notranje zadeve opravlja varnostno preverjanje za osebe iz organa (izjema so delavci Policije) ter za osebe, zaposlene v organih in organizacijah Republike Slovenije;
- Policija opravlja varnostno preverjanje za osebe zaposlene v njihovem organu,
- Ministrstvo za obrambo - Obveščevalno varnostna služba opravlja varnostno preverjanje za zaposlene v tem ministrstvu in za osebe, organe in organizacije, s katerimi imajo sklenjene pogodbe o sodelovanju ali izmenjavi podatkov, ki so po Zakonu o tajnih podatkih opredeljeni kot tajni podatki;
- Slovenska obveščevalno - varnostna agencija opravlja varnostno preverjanje za zaposlene v njihovem organu (<http://www.uvtp.gov.si/index.php?id=381>).

Dovoljenje pa glede na področje izvajanja delovnih nalog izda minister za notranje zadeve, minister za obrambo, direktor Slovenske obveščevalno-varnostne agencije ali generalni direktor Policije. Minister za notranje zadeve izda dovoljenje še vsem osebam, ki ga potrebujejo za svoje delo v katerem koli drugem organu ali organizaciji Republike Slovenije, minister za obrambo pa osebam, pri katerih gre za opravljanje obrambnih dolžnosti ali vojaške službe (22. člen).

Organi izdajo dovoljenje kandidatom, pri katerih v postopku varnostnega preverjanja ni bilo ugotovljenih varnostnih zadržkov. Zakon jih opredeljuje v 27. členu in so:

- lažne navedbe podatkov preverjane osebe v varnostnem vprašalniku ali v razgovoru za varnostno preverjanje;
- neizbrisane pravnomočne obsodbe na najmanj tri mesece nepogojne zaporne kazni za kazniva dejanja, ki se preganjajo po uradni dolžnosti;

- dokončen disciplinski ukrep zaradi težje disciplinske kršitve s področja obravnavanja in varovanja tajnih podatkov;
- odvisnost od alkohola, drog oziroma druge zasvojenosti, ki bi lahko vplivale na zavrnitev izdaje dovoljenja;
- članstvo ali sodelovanje v organizacijah ali skupinah, ki ogrožajo vitalne interese Republike Slovenije ali držav članic političnih, obrambnih in varnostnih zvez, katerih članica je Republika Slovenija;
- pravnomočne obtožnice za kazniva dejanja, ki se preganjajo po uradni dolžnosti, razen za kazniva dejanja, kjer je kot glavna kazen predpisana denarna kazen ali zapor do treh let;
- nepravnomočne obsodilne sodbe za kazniva dejanja, ki se preganjajo po uradni dolžnosti in za katera je kot glavna kazen predpisana denarna kazen ali zapor do treh let;
- neizbrisane pravnomočne obsodbe ali več izrečenih glob za prekrške, določene s tem zakonom;
- drugih ugotovitev varnostnega preverjanja, ki vzbujajo utemeljene dvome v posameznikovo verodostojnost, zanesljivost in lojalnost za varno obravnavanje tajnih podatkov;
- drugih varnostnih zadržkov, določenih z zakoni ali mednarodnimi pogodbami.

Zakon v 3. členu določa osebe, ki lahko v zvezi z opravljanjem svoje funkcije do tajnih podatkov dostopajo brez dovoljenja za dostop do tajnih podatkov. To so: predsednik republike, predsednik vlade, poslanec, državni svetnik, župan in občinski svetnik, minister in predstojnik vladne službe, ki je neposredno odgovoren predsedniku vlade, varuh človekovih pravic in njegov namestnik, guverner, namestnik in vice guverner centralne banke, član računskega sodišča, sodnik, državni tožilec, generalni državni pravobranilec in informacijski pooblaščenec.

Poleg zgoraj navedenih pa imajo brez varnostnega preverjanja dostop do tajnih podatkov stopnje INTERNO tudi vse osebe, ki opravljajo funkcijo ali delajo v organu.

Sam postopek varnostnega preverjanja določa zakon, še podrobneje pa Uredba o načinu in postopku varnostnega preverjanja (Uradni list RS, št. 110/2003). Postopek za izdajo dovoljenja se prične na podlagi pisnega predloga predstojnika organa, v katerem oseba opravlja delo. Tako denimo pisni predlog za nekoga, ki dela v Slovenski vojski, poda načelnik GŠSV, za nekoga, ki dela na Policiji, generalni direktor Policije, ter za nekoga, ki dela v Slovenski obveščevalno-varnostni agenciji, direktor agencije. Pisni predlog mora vsebovati

podatke o stopnji tajnosti tajnih podatkov, za dostop do katerih je dan predlog za izdajo dovoljenja. Priložiti pa se mu mora tudi pisno soglasje preverjane osebe za varnostno preverjanje, dokazilo o opravljenem usposabljanju s področja obravnavanja tajnih podatkov, pisno izjavo o seznanitvi s tem zakonom in predpisi, izdanimi na njegovi podlagi, ter zaprto ovojnico z izpolnjenim varnostnim vprašalnikom preverjane osebe (22. f in 22. g člen).

Sicer pa je zakon iz leta 2003 korenito posegel v varnostno preverjanje in vnesel prenekatero spremembo. Tako je predvidel tri vrste varnostnega preverjanje glede na predvideni dostop oseb do podatkov različnih stopenj tajnosti.

1. osnovno varnostno preverjanje za dovoljenje za dostop do tajnih podatkov stopnje ZAUPNO,
2. razširjeno varnostno preverjanje za dostop do tajnih podatkov stopnje TAJNO,
3. razširjeno varnostno preverjanje z varnostnim poizvedovanjem za dovoljenje za dostop do tajnih podatkov stopnje STROGO TAJNO.

Osnovno varnostno preverjanje (22. b člen) se opravi tako, da pristojni organ preveri posameznikove navedbe v vprašalniku za varnostno preverjanje. Pri tem od osebe, na katero se podatki nanašajo, ter iz evidenc in drugih zbirk podatkov upravljavcev zbirk osebnih in drugih podatkov zbirajo in uporabljajo podatke iz varnostnega vprašalnika. Če se z osnovnim varnostnim preverjanjem ugotovi sum varnostnega zadržka, lahko pristojni organ z varnostnim poizvedovanjem dodatno preveri posamezne podatke, ki se nanašajo na posamezen varnostni zadržek. Vendar pa mora preverjana oseba po razgovoru o sumu varnostnega zadržka pisno soglašati z varnostnim poizvedovanjem in izpolniti prvi del dodatnega vprašalnika. Če preverjana oseba ne da soglasja oziroma ne izpolni dodatnega vprašalnika, lahko pristojni organ že na podlagi suma varnostnega zadržka zavrne izdajo dovoljenja za dostop do tajnih podatkov.

Razširjeno varnostno preverjanje (22. c člen) se opravi tako, da pristojni organ poleg osnovnega varnostnega preverjanja od preverjane osebe, drugih organov, pristojnih za varnostno preverjanje, ali iz že obstoječih zbirk podatkov preveri še podatke iz posebnega vprašalnika, pomembne za dostop do tajnih podatkov stopnje TAJNO. Če se iz ugotovitev razširjenega varnostnega preverjanja ugotovi sum varnostnega zadržka, pristojni organ z varnostnim poizvedovanjem dodatno preveri tiste podatke, ki se nanašajo na posamezen varnostni zadržek. Vendar pa mora preverjana oseba po razgovoru o sumu varnostnega

zadržka pisno soglašati z varnostnim poizvedovanjem in izpolniti prvi del dodatnega vprašalnika. Če preverjana oseba ne da soglasja oziroma ne izpolni dodatnega vprašalnika, lahko pristojni organ že na podlagi suma varnostnega zadržka zavrne izdajo dovoljenja za dostop do tajnih podatkov.

Varnostno poizvedovanje (22. d člen) se opravi tako, da pristojni organ opravi razgovor z osebami, ki jih je v prvem delu dodatnega vprašalnika navedla preverjana oseba in ki lahko potrdijo podatke, navedene v vprašalnikih. Če se pri preverjanju podatkov iz prejšnjega odstavka ugotovi sum varnostnega zadržka, pristojni organ podatke o okoliščinah, povezanih z varnostnim zadržkom, preveri tudi pri drugih osebah, organih ali organizacijah, ki o preverjani osebi kaj vedo.

Zakon pa v 25. b in 25. c členu govori tudi o *vmesnem varnostnem preverjanju*, ki se opravi na predlog pristojnega predlagatelja, če je zoper osebo, ki ima dovoljenje za dostop do tajnih podatkov, podan sum obstoja varnostnega zadržka iz 27. člena zakona. Predlog za vmesno varnostno preverjanje osebe lahko poda tudi nacionalni varnostni organ, če ob izvajanje fizičnih, organizacijskih in tehničnih ukrepov za varovanje tajnih podatkov tuje države ali mednarodne organizacije ugotovi sum varnostnega zadržka. Vmesno se varnostno preveri tudi oseba: pred izvajanjem nalog, če je od izdaje dovoljenja do nastopa izvajanja nalog preteklo več kot 12 mesecev; pred ponovnim izvajanjem nalog na delovnih mestih, na katerih se zahteva dostop do tajnih podatkov, če v času veljavnosti dovoljenja več kot 12 mesecev ni izvajala nalog na takšnih delovnih mestih; ki je dovoljenje dobila v okviru izvajanja naročila organizacije in je od zaključka naročila, v okviru katerega je dostopala do tajnih podatkov, preteklo več kot 12 mesecev.

Zakon je tudi predpisal, kateri varnostni vprašalnik mora izpolniti preverjana oseba za dostop do tajnih podatkov posameznih stopenj tajnosti (25. člen).

Osnovni vprašalnik tako obsega naslednje podatke:

1. osebno ime, vključno s prejšnjimi;
2. enotno matično številko občana (EMŠO);
3. datum in kraj rojstva;
4. državljanstvo oziroma državljanstva, vključno s prejšnjimi;
5. naslov prebivališča (stalnega, začasnega in naslov dosegljivosti);

6. bivanja v tujini, če so trajala tri mesece ali več (kraj, obdobje in razlog bivanja);
7. zakonski stan in število otrok;
8. poklic in delo, ki ga opravlja;
9. služenje vojaškega roka;
10. šolanje in obiskovanje seminarjev ali drugih oblik usposabljanja v tujini, če so trajala več kot en mesec (kraj in obdobje);
11. delodajalce in njihove naslove;
12. neizbrisane pravnomočne obsodbe zaradi kaznivih dejanj, ki se preganjajo po uradni dolžnosti, ter podatke o prekrških, ki so jih obravnavali prekrškovni organi ali sodišča;
13. tekoče kazenske postopke;
14. odvisnost od alkohola, drog oziroma druge zasvojenosti;
15. bolezen ali duševne motnje, ki bi lahko ogrozile varno obravnavanje tajnih podatkov;
16. stike s tujimi varnostnimi ali obveščevalnimi službami;
17. članstvo ali sodelovanje v organizacijah ali skupinah, ki ogrožajo vitalne interese Republike Slovenije ali držav članic političnih, obrambnih in varnostnih zvez, katerih članica je Republika Slovenija;
18. izrečene disciplinske ukrepe;
19. prejšnja varnostna preverjanja po tem zakonu.

Posebni vprašalnik obsega naslednje podatke:

1. sodelovanje v tujih oboroženih silah ali drugih oboroženih formacijah;
2. finančne obveznosti oziroma prevzeta jamstva z navedbo vrste (npr.: krediti, hipoteke, preživnine) in višine finančnih obveznosti, razlogov za dolg, navedbo upnikov ter navedbo vseh dohodkov v preteklem letu, vključno s podatki o lastništvu nepremičnin. Preverjana oseba navede tudi podatke o povprečnem osebnem dohodku v zadnjih treh mesecih pred izpolnjevanjem varnostnega vprašalnika;
3. davčno številko;
4. lastnosti in okoliščine iz življenja preverjane osebe, ki imajo lahko za posledico izpostavljenost izsiljevanju ali drugim oblikam izvajanja pritiska.

Dodatni vprašalnik je sestavljen iz dveh delov.

1. Prvi del obsega navedbo osebnih imen ter naslovov stalnih ali začasnih prebivališč oziroma naslove dosegljivosti treh oseb, ki lahko potrdijo podatke, navedene v vprašalnikih.

2. Drugi del pa obsega podatke o zakoncu oziroma zunajzakonskem partnerju in polnoletnih osebah, ki živijo s preverjano osebo v skupnem gospodinjstvu (osebno ime, datum in kraj rojstva ter naslov stalnega, začasnega ali dejanskega prebivališča) in so lahko v skladu s tem zakonom varnostno preverjene.

Zakon je v 23. členu določil tudi veljavnost dovoljenja za dostop do tajnih podatkov. Dovoljenje za dostop do tajnih podatkov stopnje ZAUPNO ima veljavnost deset let, dovoljenje za dostop do tajnih podatkov stopnje TAJNO in STROGO TAJNO pa pet let. Pristojni organ mora o zahtevi za izdajo dovoljenja odločiti najkasneje v treh mesecih od dneva, ko je prejel popolno vlogo.

26. člen zakona ureja ponovno varnostno preverjanje. Kadar bo oseba, ki ima dovoljenje, tudi po preteku njegove veljavnosti potrebovala dostop do tajnih podatkov, mora pristojni predlagatelj najmanj tri mesece pred iztekom njegove veljavnosti pristojnemu organu predlagati uvedbo postopka za izdajo novega dovoljenja. Če se ob ponovnem varnostnem preverjanju ugotovi varnostne zadržke, se dovoljenje prekliče.

Zakon iz leta 2003 je opredelil pomembno novost v 22. e členu, ki pravi, da če ugotovljen sum varnostnega zadržka izhaja iz okoliščin, ki so povezane z njenim zakoncem ali zunajzakonskim partnerjem oziroma katero koli polnoletno osebo, ki živi s preverjano osebo v skupnem gospodinjstvu, se lahko z njimi opravi razgovor o domnevnih varnostnih zadržkih, z njihovim pisnim soglasjem pa se lahko osnovno varnostno preverijo.

Zakon o tajnih podatkih iz leta 2001 te rešitve ni predvideval, kar je bila njegova velika pomanjkljivost. Zakonec ali zunajzakonski partner oziroma katera koli druga oseba, ki s preverjano osebo živi v skupnem gospodinjstvu, lahko pomembno vplivajo na preverjano osebo. Ostaja pa, po mojem mnenju, pomanjkljivost v točki, kjer zakon predvideva razgovor oziroma varnostno preverjanje le polnoletne osebe. S tem zanemarja vpliv, ki ga ima na starše njihov mladoletni otrok, ki je npr. odvisen od drog. Stvar bi gotovo morala biti urejena drugače, kot jo predvideva zakon. Tudi z mladoletno osebo bi se lahko opravil razgovor, vendar s prisotnostjo zakonitega zastopnika.

Nepotrebna in zakonsko sporna je določba o preverjanju osebe od dopolnjenega 18. leta dalje. Delovnopravna zakonodaja namreč omogoča zaposlitev mladoletni osebi, ki je dopolnila 15

let in za takšno osebo do sedaj ni bilo ovir za zaposlitev na delovnem mestu npr. telefonista. Zakaj bi za tako osebo torej bile ovire za zaposlitev v državnem organu, kjer bi se seznanila z določenimi tajnimi podatki? Razumljivi so pomisleki glede psihološke zrelosti mladoletne osebe, vendar bi zakon ta problem lahko rešil drugače. Trbovšek (2004: 51) denimo predlaga, da bi dostop do tajnih podatkov stopnje ZAUPNO lahko dobila oseba, ki je dopolnila najmanj 15 let, dostop do podatkov stopnje TAJNO oseba stara najmanj 18 let in STROGO TAJNO najmanj 21.

Pomembno je tudi določilo v zvezi s preverjanjem suma odvisnosti od alkohola, drog ali drugih zasvojenosti oziroma suma bolezni ali duševnih stanj. Zakon iz leta 2001 je organu določal, da okoliščine preveri pri izbranem zdravniku, ki pa s temi podatki morda sploh ni razpolagal. Po novem pa zakon v 25. a členu določa, da pristojni organ ta sum preveri tako, da napoti preverjano osebo na zdravniški pregled v zdravstveno organizacijo oziroma k zasebnemu zdravniku, ki ju je za opravljanje teh pregledov pooblastil minister za zdravje. Če se preverjana oseba pregleda iz neupravičenih razlogov ne udeleži v roku, ki ji je bil določen, se ji izdaja dovoljenja zavrne.

Novela zakona spreminja tudi določilo o možnosti pritožbe. V 23. a členu določa, da je zoper odločbo, izdano v postopku varnostnega preverjanja oseb, dovoljen upravni spor, ki ga lahko sprožita predlagatelj ali preverjana oseba, ni pa dovoljena pritožba, kot je bilo to predvideno z zakonom iz leta 2003.

Še vedno pa ostaja v veljavi 3. odstavek 25. a člena, ki določa, da Slovenska obveščevalno-varnostna agencija in Obveščevalno varnostna služba Ministrstva za obrambo nista dolžni posredovati podatkov o sodelovanju s tujimi obveščevalnimi ali varnostnimi službami, če bi to ogrozilo vire ugotavljanja oziroma preverjanja posredovanih podatkov.

Ugotovljeni stiki s tujimi obveščevalnimi ali varnostnimi službami pa lahko pomenijo varnostni zadržek, če zbujejo utemeljene dvome v posameznikovo verodostojnost in zanesljivost za varno obravnavanje tajnih podatkov. Seveda vedno obstaja možnost, da posameznik tovrstnih stikov v varnostnem vprašalniku ne bo navedel, saj se vsak trudi, da bi se pokazal čim bolj zanesljivega. Slovenska obveščevalno-varnostna agencija in Obveščevalno varnostna služba Ministrstva za obrambo pa po zakonu teh podatkov nista dolžni posredovati, če bi to ogrozilo vire ugotavljanja oziroma preverjanja posredovanih

podatkov. Kadar torej ne bosta želeli posredovati teh podatkov, se bosta sklicevali na to določbo. Na nek način to pomeni priznanje, da podatke imata, vendar jih ne želita posredovati. Organ bo tako lahko izdajo dovoljenja zavrnil, preverjana oseba pa bo imela možnost pritožbe in bo že tekom postopka izvedela, da je bila predmet interesa obveščevalnih in varnostnih služb Republike Slovenije. V nadaljnjem postopku bo izvedela tudi,³ da so bili opaženi njeni stiki s tujimi službami. Tako bo oseba opozorjena, da je bilo njeno ravnanje opaženo. Lahko pa bi oseba kandidirala za tako delovno mesto celo zgolj pod pretvezo, da bi pridobila take informacije (Trbovšek, 2004: 54–55).

Zakon v Sloveniji ne predvideva uporabe poligrafske metode pri varnostnem preverjanju. »Edino zakonsko predvideno področje uporabe poligrafske metode je v okviru predzakonskega postopka, kot to določa Zakon o policiji (6. odstavek 54. člena). Zakon dovoljuje uporabo poligrafske metode policistom pri zbiranju osebnih in drugih podatkov od osumljenca pri preiskovanju kaznivih dejanj« (Dežman, 2005: 98). Vendar se moramo zavedati, da je poligrafska metoda gotovo med najzanesljivejšimi za ugotavljanje lojalnosti in zanesljivosti. Trbovšek (2004: 57) meni, da bo razširitev omenjene metode na področje varnostnega preverjanja v prihodnosti nujna. Njeno uvedbo bi bilo potrebno znanstveno podpreti, saj bi to prispevalo k lažjemu in hitrejšemu sprejetju le-te med strokovno in laično varnostjo. Preverjanje resničnosti podanih izjav v vprašalniku v bivalnem in delovnem okolju pomeni vdor v socialno okolje preverjane osebe, poligrafsko testiranje pa bi lahko to neprijetnost zmanjšalo.

Nenazadnje pa ne moremo niti mimo omembe Urada vlade Republike Slovenije za varovanje tajnih podatkov, ki je bil na podlagi 43. člena ZTP iz leta 2001 ustanovljen 22. 1. 2002. Njegove naloge so: spremljanje in usklajevanje stanje na področju obravnavanja in varovanja tajnih podatkov; predlaganje ukrepov za izboljšanje varovanja tajnih podatkov; skrb za razvoj in izvajanje fizičnih, organizacijskih in tehničnih standardov varovanja tajnih podatkov v organih in organizacijah; koordiniranje delovanje organov, pristojnih za varnostno preverjanje; pripravljanje predlogov predpisov s področja tajnih podatkov za vlado; dajanje mnenj o skladnosti splošnih aktov organov in organizacij z zakonom na področju obravnavanja in varovanja tajnih podatkov; skrb za izvrševanje sprejetih mednarodnih obveznosti in mednarodnih pogodb o varovanju tajnih podatkov; skrb za zagotavljanje

³ 4. odstavek 146. člena Zakona o splošnem upravnem postopku: Pristojni organ ne sme izdati odločbe, preden ne da stranki možnosti, da se izreče o dejstvih in okoliščinah, ki so pomembne za izdajo odločbe.

varnosti tajnih podatkov v nacionalnih organih in v tujini (v zvezi s tem opravlja naslednje naloge: izdaja potrdila za dostop do tajnih podatkov, potrjuje izpolnjevanje predpisanih pogojev za obravnavanje tajnih podatkov s strani posameznega organa tujim državam in organizacijam, predlaga varnostno preverjanje za izdajo dovoljenja za dostop do tajnih podatkov, katerih predlagatelji niso zajeti v 22. členu ZTP in potrebujejo dovoljenje za dostop do tajnih podatkov tuje države ali mednarodne organizacije, izdaja navodila za ravnanje s tajnimi podatki tuje države oziroma mednarodne organizacije); vodi evidenco izdanih dovoljenj; predlaga ukrepe za izboljšanje varovanja tajnih podatkov ter organizira in izvaja usposabljanja s področja varovanja tajnih podatkov (43.a člen ZTP in <http://www.uvtp.gov.si/index.php?id=384>).

Posebej bi rada opozorila na dolžnost organiziranja in izvajanja usposabljanja s področja varovanja tajnih podatkov. Ta naloga se mi namreč zdi zelo pomembna, vendar jo je Urad dejansko pričel izvajati šele lani. Novela zakona kot enega izmed pogojev za pričetek postopka za izdajo dovoljenja za dostop do tajnih podatkov predvideva tudi dokazilo o opravljenem usposabljanju s področja obravnavanja tajnih podatkov (22. g člen).

Urad vlade Republike Slovenije za varovanje tajnih podatkov pa je še posebej pomemben zato, ker je z njim Urad zveze Nato za varnost dobil konkretnega sogovornika za sodelovanje na področju varnostnih zadev (Brožič, Trbovšek, 2002: 6).

V nadaljevanju bi rada poudarila še nekaj posebnosti, ki se pojavijo pri varnostnem preverjanju za pridobitev dovoljenja za dostop do tajnih podatkov, in sicer glede na to, če je oseba zaposlena v Policiji, Slovenski obveščevalno-varnostni agenciji ali na obrambnem področju. Seveda pa vse organe zavezuje krovni zakon – tj. Zakon o spremembah in dopolnitvah zakona o tajnih podatkih (Uradni list RS, št. 28/2006).

7.2.1 VARNOSTNO PREVERJANJE V POLICIJI

V Zakonu o policiji je v poglavju policijska pooblastila tudi pooblastilo za varnostno preverjanje (36. člen). Policisti lahko zaradi varovanja določenih oseb, organov, objektov, okolišev, delovnih mest in tajnih podatkov ter v drugih primerih, določenih v zakonu, varnostno preverjajo osebe. Varnostno preverjanje oseb je ugotavljanje morebitnih varnostnih

zadržkov za delo osebe pri varovani osebi, v varovanem organu, objektu ali v okolišu, na določenem delovnem mestu, pri obravnavanju tajnih podatkov ali v drugih primerih, določenih z zakonom.

Varnostno preverjanje kandidatov za dostop do tajnih podatkov opravlja Sektor za tajne podatke na Ministrstvu za notranje zadeve, obenem pa pripravlja tudi predloge za izdajo dovoljenja za dostop do tajnih podatkov in druge strokovne naloge v zvezi s določanjem in varovanjem tajnih podatkov (Panikvar, 2005: 13). Minister za notranje zadeve izda dovoljenje tudi vsem drugim, ki ne delajo v nobenem od naštetih organov izdajateljev.

7.2.2 VARNOSTNO PREVERJANJE V SLOVENSKI OBVEŠČEVALNO-VARNOSTNI AGENCIJI

Slovenska obveščevalno-varnostna agencija je z zakonom zavezana, da sodeluje s pristojnimi državnimi organi in službami pri varnostnem preverjanju, predvsem tistimi, katerih osnovna dejavnost je skrb za varnostne zadeve v državi, ter posreduje podatke, pomembne za varnost določenih oseb, delovnih mest, organov, objektov in okolišev (2. odstavek 2. člena Zakona o Slovenski obveščevalno-varnostni agenciji, Uradni list RS, št. 20/2004).

Osebam, ki bodo dostop do tajnih podatkov potrebovale zaradi opravljanja funkcij ali delovnih dolžnosti v Slovenski obveščevalno-varnostni agenciji, dovoljenje izda direktor Slovenske obveščevalno-varnostne agencije in o izdaji dovoljenja obvestijo Urad vlade Republike Slovenije za varovanje tajnih podatkov (22. člen ZTP). Prav tako tudi samo varnostno preverjanje za dostop do tajnih podatkov za svoje (bodoče) zaposlene opravlja Slovenska obveščevalno-varnostna agencija sama.

7.2.3 VARNOSTNO PREVERJANJE NA OBRAMBENEM PODROČJU

Zakon o obrambi je določil izvajalca varnostnega preverjanja na obrambnem področju. Varnostno preverjanje oseb po 35. členu navedenega zakona in predpisih za pridobitev dovoljenja za dostop do tajnih podatkov na obrambnem področju lahko opravljajo samo delavci Obveščevalno varnostne službe Ministrstva za obrambo, ki imajo policijska

pooblastila (Trbovšek, 2004: 36–37). Minister za obrambo pa je zakonsko pooblaščen predstojnik organa, ki izdaja dovoljenja za dostop do tajnih podatkov za osebe, zaposlene na ministrstvu. V to kategorijo spadajo tudi pripadniki Slovenske vojske (Čaleta, 2003: 25) in pa tudi vsi ostali, ki ne delajo v nobenem od naštetih organov izdajateljev, katerih naloge so povezane z opravljanjem obrambnih dolžnosti ali vojaške službe.

Sicer so za izvajanje postopka za pridobitev dovoljenja za dostop do tajnih podatkov v Slovenski vojski zadolženi organi za kadrovske zadeve (Čaleta, 2003: 26). Kadrovski organ v enoti obvesti pripadnika o zakonski zahtevi za pridobitev dovoljenja za dostop do tajnih podatkov. Pripadniku nato posreduje vse predpisane obrazce, ki jih je treba izpolniti. Nadalje organ pošlje vse obrazce pooblaščenim v Slovenski vojski, ki imajo po sklepu ministra pooblastila za podajanje predlogov za pridobitev dovoljenj za dostop do tajnih podatkov. Pooblaščene osebe so v kadrovskem organu najvišjega poveljstva operativne ravni ter v kadrovskem organu najvišjega poveljstva strateške ravni. Obrazci z dopisom se od tod posredujejo Obveščevalno varnostni službi, ki je na podlagi zakona pooblaščen za izvajanje varnostnega preverjanja oseb na Ministrstvu za obrambo.

Osebam, ki potrebujejo dostop do tajnih podatkov zaradi opravljanja funkcij ali delovnih dolžnosti na Ministrstvu za obrambo, dovoljenje izda minister, pristojen za obrambo. O izdaji dovoljenja obvestijo Urad Vlade Republike Slovenije za varovanje tajnih podatkov. Osebam, ki potrebujejo dostop do tajnih podatkov zaradi opravljanja nalog ali funkcije v Slovenski vojski, na predlog predstojnika tega organa (načelnika GŠSV) dovoljenje izda minister, pristojen za obrambo. O izdaji dovoljenja prav tako obvesti urad (Čaleta, 2003: 19). Varnostno preverjanje oseb lahko opravljajo samo delavci obveščevalno varnostne službe ministrstva, ki imajo policijska pooblastila.

Po opravljenem postopku varnostnega preverjanja minister za obrambo izda dovoljenje za dostop do tajnih podatkov na obrazcu, ki je sestavni del Uredbe o načinu in postopku varnostnega preverjanja. Ob ugotovljenih varnostnih zadržkih izda predstojnik organa odločbo, s katero zavrne izdajo dovoljenja za dostop do tajnih podatkov (Čaleta, 2003: 24).

8 ZAKLJUČEK

V osrednjem delu diplomske naloge sem predstavila varnostno preverjanje v dveh mednarodnih organizacijah, v kateri je vključena Republika Slovenija. Poleg tega sem prikazala tudi varnostno preverjanje v treh sodobnih demokratičnih državah: v Združenih državah Amerike, Zvezni republiki Nemčiji ter Slovaški republiki. Razlogi, da sem izbrala ravno te države, so naslednji: Zvezna republika Nemčija je sodobna demokratična država, ki ima v mnogočem pravni sistem podoben slovenskemu. Slovaška republika je mlada parlamentarna demokracija v obdobju tranzicije in prav tako kot Slovenija nova članica Nata in EU, zato so njene izkušnje pri vzpostavljanju sistema lahko zelo koristne za Slovenijo. ZDA pa sem vključila predvsem zaradi njenih bogatih izkušenj na področju varnostnega preverjanja, kljub temu, da nima nam primerljivega pravnega sistema.

Najprej bi se rada ustavila pri primerjavi med Republiko Slovenijo, Združenimi državami Amerike, Zvezno republiko Nemčijo ter Slovaško republiko. V ZDA imajo zelo dolgo zgodovino varnostnega preverjanja, saj so to področje pričeli urejati že po 2. svetovni vojni. Področje je bilo še zlasti pomembno med hladno vojno. Nemčija je normativno uredila tajnost in varnostno preverjanje v devetdesetih letih, Slovaška in Slovenija pa sta prve zakone s tega področja sprejeli šele leta 2001, v okviru približevanja Natu in EU. Vsem ureditvam je skupno, da je varnostno preverjanje povsod urejeno s predpisi ter da imajo glede na različne stopnje ogroženosti določene različne stopnje tajnosti, glede na to pa tudi več vrst varnostnega preverjanja. V vseh državah, ki sem jih obravnavala je varnostno preverjanje mogoče začeti le na podlagi pisnega soglasja preverjane osebe, ki omili poseg v človekove pravice in svoboščine posameznika ob varnostnem preverjanju. V vseh štirih državah in tudi v obeh organizacijah obstaja med seboj primerljiva določitev stopenj tajnosti, kar pomeni večjo preglednost in lažje sodelovanje. Vsebina in obseg varnostnega preverjanja sta v primerjanih državah različna, vendar v bistvenih značilnostih podobna. Vse države preverjajo identifikacijske podatke, podatke, ki govorijo o posameznikovi lojalnosti in zanesljivosti, ter podatke v zvezi z različnimi odvisnostmi in duševnimi boleznimi.

Posebnost slovenskega zakona o tajnih podatkih je, da zelo široko opredeljuje krog ljudi, ki lahko zgolj na podlagi svoje funkcije pridobijo dovoljenje za dostop do tajnih podatkov. Med naštetimi so denimo župan in občinski svetniki. Te kategorije nisem našla v nobeni od ureditev treh primerjanih držav, obenem pa je tudi v neskladju z zahtevami Nata in EU, saj

obe organizaciji zahtevata, da je varnostno preverjen vsakdo, ki dostopa do tajnih podatkov. Tako ureditev poznajo tudi Združene države Amerike. Seznam oseb, kot ga opredeljuje slovenski ZTP, se mi zdi preširok in tudi novi zakon ga ni skrajšal. Seznamu v podporo govori le dejstvo, da zakon tem osebam zagotavlja zgolj dostop do tajnih podatkov, ne odvezuje pa jih dolžnosti varovanja tajnosti, ter da te osebe do določene informacije lahko dostopajo le zaradi narave njihovega dela, torej samo, če zadostijo pogojem t. i. »need to know«.

Na podlagi prebranega lahko potrdim svojo hipotezo, da z varnostnim preverjanjem skušamo zagotoviti, da so osebe, ki bodo delale s tajnimi podatki, lojalne, zanesljive in vredne zaupanja. Varnostno preverjanje kot tako se izvaja v vseh sodobnih državah in mednarodnih organizacijah in je zlasti med članicami istih organizacij med seboj primerljivo. Namen varnostnega preverjanja je ugotavljanje, če za določeno osebo obstajajo varnostni zadržki. Le tako lahko namreč ustrezno zavarujemo informacije, posredno pa tudi državo in njene državljane, saj dobro opravljeno varnostno preverjanje pomeni, da na občutljivih delovnih mestih ne bodo delali neustrezni ljudje.

Država ima pravico in dolžnost zavarovati samo sebe. Eden izmed načinov so tudi tajni podatki in omejen dostop do njih. Nepooblaščen razkritje tajnih podatkov lahko povzroči nepopravljivo škodo ali celo izgubo življenj. Pomembno pa je, da država za vse državljane omogoči enake pogoje za dostop do tajnih podatkov. Strog režim izvajanja varnostnega preverjanja in varovanje človekovih pravic se ne izključujeta. Močna država z demokratično ureditvijo je namreč porok za varovanje temeljnih človekovih pravic in svoboščin.

Varnostni standardi EU in Nata poleg podpisane izjave o seznanjenosti z določili Zakona o tajnih podatkih predvidevajo tudi izobraževanja in usposabljanja s tega področja. Urad vlade Republike Slovenije za varovanje tajnih podatkov je sicer tovrstna izobraževanja pričel izvajati šele konec leta 2005, vendar pa to pomeni, da je Slovenija na pravi poti, kajti izobraževanje je ključnega pomena pri zaščiti tajnih podatkov, saj nam le to zagotavlja pravilno in odgovorno ravnanje s tajnimi podatki. Obenem pa zaradi izobraževanja Slovenija postaja kredibilnejši partner.

Izobraževanje na individualni ravni je nujno potrebno tudi zato, ker posameznik podpiše izjavo, da je seznanjen z normativnimi dokumenti, ki urejajo področje varovanja tajnih

podatkov, Kazenski zakonik RS pa za izdajo tajnih podatkov predvideva celo zaporno kazen. Pridobljeno znanje bi bilo potrebno tudi obnavljati in dopolnjevati. Čas ob ponovnem preverjanju za izdajo dovoljenja za dostop do tajnih podatkov se mi zdi več kot primeren. Vendar pa izobraževanja ne bi bilo potrebno izvajati le na najnižji, individualni ravni. Varnostno kulturo bi bilo treba vzpodbuditi na ravni organov, ki pri svojem delu prihajajo v stik s tajnimi podatki, v ta namen pa bi se morali izobraževati tudi nadrejeni. V skladu s tem lahko potrdim tudi svojo drugo hipotezo. Za pravilno ravnanje s tajnimi podatki še zdaleč ni dovolj le uspešno opravljeno varnostno preverjanje. Pomembno je izobraziti ljudi, saj si s tem država na dolgi rok zagotavlja odgovornejše ravnanje s tako občutljivimi podatki, kot so tajni.

Vnos varnostne kulture v različne organe je še posebej pomemben zaradi dediščine, ki jo Slovenci s seboj nosimo še iz prejšnjega sistema. Takrat so bili namreč številni podatki tajni in nedostopni javnosti. Veliko med njimi je bilo tudi takih, ki so si neupravičeno prislužili oznako tajnosti. Po letu 1991 se je zato pojavilo načelno zavračanje tajnega kot nečesa, kar je povezano z nekdanjim sistemom. Ob tem pa smo, zaradi spremenjenega dojemanja individualne in državne zasebnosti, opustili številna osnovna pravila v zvezi z ravnanjem, hranjenjem in dostopanjem do tajnih podatkov.

Razumeti je potrebno, da je le uspešna in učinkovita država lahko porok za varnost vseh njenih državljanov. Na račun tega pa država poseže tudi v pravice posameznika, vendar seveda le v smiselnem obsegu. Dejstvo namreč je, da se lahko v mednarodni sistem izmenjavanja tajnih podatkov vključi le država z urejenim sistemom varovanja tajnih podatkov.

Republika Slovenija po mojem mnenju ni v celoti zadostila minimalnim standardom Nata in EU. Že omenjeni seznam oseb, ki le na podlagi funkcije lahko dostopajo do tajnih podatkov, ostaja predolg, čeprav novela zakona določa, da se dostop do tajnih podatkov tuje države ali mednarodne organizacije ureja v skladu z mednarodno pogodbo, ki jo je s tujo državo ali mednarodno organizacijo sklenila Slovenija. Podobno je problem urejen tudi v slovaški zakonodaji. Seveda pa se pojavlja še mnogo vprašanj, ki bi jih lahko uredili bolje in drugače. Tako nov Zakon o spremembah in dopolnitvah Zakona o tajnih podatkih, ki ga je vlada sprejela 13. 3. 2006, navaja nov pogoj za začetek varnostnega preverjanja osebe, tj. njeno obvezno usposabljanje s področja obravnavanja in varovanja tajnih podatkov, kar je, kot sem že omenila, eden bistvenih pogojev za zagotavljanje večje varnosti tajnih podatkov.

Pomembna novost, ki jo je prinesel novi zakon o tajnih podatkih, pa se nanaša tudi na rok oddaje predloga za ponovno varnostno preverjanje, ki po novem zakonu ne bi smel biti krajši od treh mesecev. Le tak časovni rok namreč lahko zagotovi pravočasno in kakovostno varnostno preverjanje. Novi zakon je dopolnil oziroma nadgradil nacionalni sistem obravnavanja in varovanja tajnih podatkov. Spremembe bodo pripomogle k večji učinkovitosti sistema in posledično večji varnosti nacionalnih in tujih tajnih podatkov.

Zgoraj omenjene spremembe se mi zdijo pozitivne, saj je le država, ki ustrezno varuje svoje tajne podatke, v mednarodni skupnosti sprejeta kot kredibilen partner. Nacionalna varnost je v današnjem času neločljivo povezana z mednarodno varnostjo, seveda pa tudi z varnostjo posameznika. Pri vzpostavljanju tovrstnih sistemov se nam vedno znova postavlja vprašanje razmejitve med zasebnostjo države in intime posameznika. Do katere meje država še lahko posega v pravice posameznika in kdaj natopi tisti trenutek, ko država ne varuje več svojih državljanov, ampak sama postane vir njihovega ogrožanja? To se mi zdi eno izmed ključnih vprašanj na tem področju, odgovor nanj in pravo razmerje, ki ga je zelo težko doseči, pa pravzaprav neke vrste umetnost.

9 VIRI

9.1 KNJIGE, ČLANKI, MAGISTRSKE NALOGE

Antončič, Marjan (2001): Zakonska ureditev varstva tajnih podatkov v nekaterih državah, članicah Severnoatlantskega sporazuma. *Varstvoslovje*, let. 3, št. ½. 19–32.

Anžič, Andrej (1997): *Varnostni sistem Republike Slovenije*. Ljubljana: Uradni list Republike Slovenije.

Anžič, Andrej (2000): Tajnost: vrednota in zlo. *Teorija in praksa*, let. 37, št. 5. 849–863.

Anžič, Andrej (2002): Mednarodni terorizem - varnostni izziv in dileme. *Teorija in praksa*, let. 39, št. 3. 454–466. Dostopno na <http://dk.fdv.uni-lj.si/tip/tip20023Anzic.PDF> (2. 3. 2006).

Anžič, Andrej, Trbovšek, Franc (2003): Varnostno preverjanje v NATO po novih standardih. *Dnevi varstvoslovja - 4. slovenski dnevi varstvoslovja, Bled, 5. do 7. junij 2003*. Zbornik prispevkov (elektronski vir). Ljubljana: Visoka policijsko-varnostna šola.

Anžič, Andrej, Trbovšek, Franc (2004): Varnostno preverjanje oseb v sistemu nacionalne varnosti. *Zbornik prispevkov - 5. slovenski dnevi varstvoslovja, Bled, junij 2004*. Zbornik prispevkov (elektronski vir). Ljubljana: Fakulteta za policijsko-varnostne vede.

Brožič, Liliana, Trbovšek, Franc (2002): Tajni podatki in NATO. *Dnevi varstvoslovja -3. slovenski dnevi varstvoslovja, Bled, 6. do 8. junij 2002*. Zbornik prispevkov (elektronski vir). Ljubljana: Visoka policijsko-varnostna šola.

Bunič, Nataša (2005): *Vpliv protiterorističnih ukrepov na človekove pravice*. Diplomsko delo. Ljubljana: FDV. <http://dk.fdv.uni-lj.si/dela/Bunic-Natasa.PDF> (2. 3. 2006).

Cerar, Miro (1997): O naravi človekovih pravic in dolžnosti. V: Pavčnik, Marijan, Polajnar-Pavčnik, Ada, Wedam-Lukić, Dragica (ur.) *Temeljne pravice*. 52–83.

Čaleta, Denis (2003): Varnostno preverjanje v Slovenski vojski. *Bilten Slovenske vojske*, let. 5, št. 1. 9–37.

Čaleta, Denis (2004a): *Sistem varovanja tajnih podatkov*. Magistrsko delo. Ljubljana.

Čaleta, Denis (2004b): Varovanje tajnih podatkov v zvezi NATO. *Bilten Slovenske vojske*, let. 6, št. 1. 59–81.

Čaleta, Denis (2004c): Konceptualne spremembe na področju varovanja tajnih podatkov v Republiki Sloveniji. *Zbornik prispevkov (Elektronski vir)- 5. slovenski dnevi varstvoslovja, Bled, junij 2004*. Ljubljana : Fakulteta za policijsko-varnostne vede.

Čaleta, Denis (2005): Varovanje tajnih podatkov v Evropski uniji. *Bilten Slovenske vojske*, let. 7, št. 1. 43–59.

Črnčec, Damir (2003): *Tajnost podatkov (varnostno preverjanje in obveščevalno-varnostne službe)*. Magistrsko delo. Ljubljana: FDV.

Črnčec, Damir (2004): Dostop do tajnih podatkov in varnostno preverjanje oseb. *Varstvoslovje*, let. 6, št. 1. 47–58.

Dežman, Marjan (2005): *Varnostno preverjanje kot pogoj učinkovitega varovanja*. Specialistično delo. Ljubljana: Fakulteta za upravo.

Dolinar, Ksenija, Knop, Seta, ur. (1998): *Leksikon Cankarjeve založbe*, dopolnjena 3. izd. 171, 1074. Ljubljana: Cankarjeva založba.

Franetič, Nataša (2004): *Varstvo človekovih pravic v razmerju do državne uprave: primerjava ombudsmana in Amnesty International*. Diplomsko delo. Ljubljana: FDV. <http://dk.fdv.uni-lj.si/dela/Franetic-Natasa.PDF> (2. 3. 2006).

Grizold, Anton (1992): Oblikovanje slovenske nacionalne varnosti. V: Anton Grizold (ur.) *Razpotja nacionalne varnosti: obramboslovne raziskave v Sloveniji*. 59–93. Ljubljana: FDV.

Grizold, Anton (1999): *Obrambni sistem Republike Slovenije*. Ljubljana: Ministrstvo za notranje zadeve, Visoka policijsko-varnostna šola.

Grizold, Anton (2001): Varnostna paradigma v mednarodnih odnosih. V: Evan Luard (ur.) *Človek, država in vojna*. 83–161. Ljubljana: FDV.

Kranjc, Andrej (2004): *Varstvo osebnih podatkov v obdobju tranzicije in vstopanju Slovenije v Evropsko unijo*. Diplomsko delo. Ljubljana: FDV. <http://dk.fdv.uni-lj.si/dela/Kranjc-Andrej.PDF> (2. 3. 2006).

Panikvar, Milko (2005): *Varstvo in dostop do tajnih podatkov*. Diplomsko delo. Ljubljana.

Polajnar – Pavčnik, Ada (1997): Temeljne pravice kot osebnostne pravice. V: Pavčnik, Marijan, Polajnar-Pavčnik, Ada, Wedam- Lukić, Dragica (ur.) *Temeljne pravice*. 150–172.

Rep, Roman (2001): Varnostno preverjanje oseb. V: Belič, Igor (ur.) *Javna predstavitev mnenj o predlogu Zakona o tajnih podatkih*. 215–219.

Šinkovec, Janez (1996): *Pravna, demokratična in socialna država*. Ljubljana: ČZP Enotnost.

Škoporc, Stanislav (2002): *Varnostno preverjanje oseb kot preventivna dejavnost*. Diplomsko delo. Ljubljana.

Šturm, Lovro (1998): Pomen ustavnosodnega varstva človekovih pravic in temeljnih svoboščin. V: Zver, Milan (ur.) *Človekove pravice in svoboščine v tranziciji: primer Slovenije: zbornik referatov in razprav s strokovnega posveta s priloženim besedilom Splošne deklaracije človekovih pravic*. 23–45.

Trbovšek, Franc, Brožič, Liliana (2002): Varnostno preverjanje oseb – vloga obveščevalno varnostnih služb pri izvajanju zakona o tajnih podatkih. *Dnevi varstvoslovja - 3. slovenski dnevi varstvoslovja, Bled, 6. do 8. junij 2002*. Zbornik prispevkov (elektronski vir). Ljubljana: Visoka policijsko-varnostna šola.

Trbovšek, Franc (2004): *Varnostni in pravni vidiki varnostnega preverjanja oseb*. Magistrsko delo. Brdo pri Kranju: Fakulteta za podiplomske državne in evropske študije.

Vodovnik, Zvone (2001): Delovnopравни položaj upravljalcev z državnimi tajnimi podatki (analiza zasnov Zakona o tajnih podatkih). V: Belič, Igor (ur.) *Javna predstavitev mnenj o predlogu Zakona o tajnih podatkih*. 87–95.

Zrim, Klavdija (2005): *Kršenje človekovih pravic v imenu izbrisanih*. Diplomsko delo. Ljubljana: FDV. <http://dk.fdv.uni-lj.si/dela/Zrim-Klavdija.PDF> (2. 3. 2006).

Žiberna, Andrej (2004): *Varnostna preverka kot varnostni standard v NATO*. Diplomsko delo. Ljubljana.

9.2 PRAVNI VIRI

Act of 11 March 2004 of the Protection of classified information and on the amendment and supplementing of certain acts. http://www.nbusr.sk/index_en.php (17. 3. 2006).

Executive Order 12968 Access to Classified Information, August 2 1995. <http://www.presidency.ucsb.edu/ws/index.php?pid=51699&st=12968&st1=> (22. 4. 2006).

Kodeks ravnanja javnih uslužbencev. *Uradni list RS*, št. 8/2001.

Resoluciji o izhodiščih zasnove nacionalne varnosti Republike Slovenije. *Uradni list RS*, št. 71/1993.

Splošna deklaracija o človekovih pravicah (1948). Generalna skupščina Združenih narodov. <http://www.ip-rs.si/index.php?id=221> (2. 3. 2006).

Sklep o začasnem zadržanju drugega odstavka 25. člena zakona o tajnih podatkih in II. dela vprašalnika za dostop do tajnih podatkov kot sestavnega dela uredbe o načinu in postopku varnostnega preverjanja ter postopku izdaje in preklica dovoljenja za dostop do tajnih podatkov, št. U-I-79/03-7. *Uradni list RS*, št. 48/2003.

Uredba o načini in postopku varnostnega preverjanja. *Uradni list RS*, št. 110/2003.

Zakon o javnih uslužbencih. *Uradni list RS*, št. 32/2006.

Zakon o obrambi. *Uradni list RS*, št. 82/1994, 87/1997, 13/1998 (odl. US), 47/2002, 67/2002.

Zakon o policiji. *Uradni list RS*, št. 49/1998, 110/2003, 102/2004, 70/2005, 3/2006.

Zakon o Slovenski obveščevalno varnostni agenciji. *Uradni list RS*, št. 23/1999, 20/2004.

Zakon o splošnem upravnem postopku. *Uradni list RS*, št. 22/2005.

Zakon o spremembah in dopolnitvah zakona o tajnih podatkih. *Uradni list RS*, št. 101/2003.

Zakon o spremembah in dopolnitvah zakona o tajnih podatkih. *Uradni list RS*, št. 28/2006.

Zakon o tajnih podatkih. *Uradni list RS*, št. 87/2001, 135/2003.

9.3 INTERNETNI VIRI IN ELEKTRONSKI MEDIJI

Background Investigations. <http://www.fas.org/sgp/backchek.htm> (22. 4. 2006).

Encyclopaedia Britannica 2005: Ultimate Reference Suite. DVD.

Naloge in cilji, <http://www.uvtp.gov.si/index.php?id=384> (22. 3. 2006).

Obrazložitev členov,

<http://www.uvtp.gov.si/fileadmin/uvtp.gov.si/pageuploads/Obrazlozitev.doc> (6. 3. 2006).

Personal Appearance Guidance. <http://www.defenselink.mil/dodgc/doha/pap-g.html> (22. 4. 2006).

Personnel Security: Protection Through Detection. <http://www.dss.mil/search-dir/seclib/govsec/chap4.htm> (22. 4. 2006).

Ponovno uzakonjeno varnostno preverjanje oseb z dostopom do tajnih podatkov.
<http://nato.gov.si/slo/novinarsko-sredisce/sporocila-za-javnost/2264/> (6. 3. 2006).

Predlog Zakona o spremembah in dopolnitvah Zakona o tajnih podatkih.
http://www.uvtp.gov.si/fileadmin/uvtp.gov.si/pageuploads/Besedilo___lenov_ZTP_10.11.05.doc (6. 3. 2006).

Ravnanje s tajnimi podatki.
http://www.mors.si/pdf/2004/ravnanje_s_tajnimi_podatki_gradivo.pdf (13. 3. 2006).

Slovar slovenskega knjižnega jezika (CD-rom).

Varnostno preverjanje oseb. <http://www.uvtp.gov.si/index.php?id=381> (6. 3. 2006).

Zakon o spremembah in dopolnitvah zakona o tajnih podatkih (Ur. l. RS, št. 28/2006) – temeljni razlogi za spremembo in dopolnitve ZTP.
http://www.uvtp.gov.si/fileadmin/uvtp.gov.si/pageuploads/UVTP_usmeritve_ZTP.pdf (22. 4. 2006).